INSS 연구보고서 2020-17

2020 INSS Research Report

국제사회의 해킹 변화 추세 및 대응방안

채재병

INSS INSTITUTE FOR NATIONAL SECURITY STRATEGY 국가안보전략연구원
06295 서울시 강남구 언주로120 인스토피아 빌딩
Tel. 02-6191-1000 Fax.02-6191-1111 www.inss.re.kr

비매품/무료
94340
9 791189 781422
ISBN 979-11-89781-42-2
ISBN 979-11-89781-03-3(세트)

INSS 연구보고서 2020-17 국제사회의 해킹 변화 추세 및 대응방안 | 채재병

INSS 국가안보전략연구원

2020 INSS Research Report

INSS 연구보고서 2020-17

국제사회의 해킹 변화 추세 및 대응방안

채재병 chaejb@inss.re.kr

INSS INSTITUTE FOR NATIONAL SECURITY STRATEGY 국가안보전략연구원

2020 INSS Research Report

INSS 연구보고서 2020-17

국제사회의 해킹 변화 추세 및 대응방안

채재병

INSS INSTITUTE FOR NATIONAL SECURITY STRATEGY 국가안보전략연구원

INSS 연구보고서 2020-17

국제사회의 해킹 변화 추세 및 대응방안

채재병

채재병 (蔡載秉)

| 국가안보전략연구원 책임연구위원

성균관대학교에서 정치학 박사학위를 받았으며, 주요 관심분야는 (사이버)안보, 한반도 통일, 동북아 질서 등이다. 주요 저서 및 논문으로 『한반도 평화의 국제정치학』(공저), 『국제 사이버공격 전개 양상 및 주요국 대응전략』, 『주변국의 사이버 환경과 한반도 평화체제 구축』(공저), "안보환경의 변화와 사이버안보", "동북아 지역질서 변화와 한국의 전략"(공저), "동아시아의 주권인식과 지역협력" 등이 있다.

목차

국문초록 6

I. 서론 8

1. 문제제기 및 연구목적 9
2. 선행연구 검토 12

II. 사이버공간과 주권 16

1. 사이버공간에 대한 인식 17
2. 사이버공간에서의 주권 20

III. 국제사회 해킹 변화 추세 34

1. 개념 35
2. 해킹 유형의 변화 38
3. 해킹 방법의 변화 43

IV. 해킹 주체, 기법, 대상별 분석 48

1. 주체 49
2. 기법 54
3. 대상 77

V. 결론: 한국의 대응방안 86

Abstract 92

참고문헌 96

국문초록

본 연구의 목적은 사이버공간에서 나타나고 있는 주권인식을 토대로 하여 국제사회에서 나타나고 있는 해킹의 변화 추세를 살펴보고, 해킹의 주체, 기법, 대상별로 분석함으로써 해킹에 대한 한국의 대응방안을 제시하는 것이다.

해킹은 지속적으로 증가하면서 더욱 고도화될 것으로 예상되므로 이에 대한 효율적인 대비와 관리 및 대응체계가 필요하다. 특히 4차 산업혁명과 사물인터넷 시대를 맞이하여 사이버공간에서의 주권에 대한 논의가 활발하게 진행되면서 한국도 국가간 사이버 분쟁에 대비해 해킹에 대한 대응책을 적극 강구해야 할 시점이다. 해킹에 대한 한국의 대응방안으로 소위 '한반도 사이버 평화체제' 구축방안을 제시해 보고자 한다.

한반도 사이버 평화체제를 구축하기 위해서는 국제사회와 다양한 협력을 통해 주도적으로 사이버 국제협력 네트워크를 형성해야 한다. 그리고 이를 위해 국제 사이버 파트너십을 강화하고, 사이버억지를 위해 미국, 일본, 중국, 러시아 등 한반도 주변국들과 다자 및 양자 간 사이버 국제협력을 강화해야한다. 나아가 사이버 선도국으로서 사이버 후발국들에 대한 지원과 함께 사이버 국제규범 수립과 관련하여 중립적이고 보편타당한 입장을 견지해야 한다.

한반도 사이버 평화체제 구축을 추진하기 위해서는 우선 국제차원에서 사이버 국제협력 강화를 위해 UN GGE 등 사이버 분야 국제 거버넌스에 주도적으로 참여한다. 다음으로 지역 차원에서 한반도 주변지역, 넓게는 동북아지역에서는 사이버 국제협력을 양자협력보다는 다자협력을 통해 추진한다. 마지막으로 개별국가 차원에서 한반도 주변 사이버 관련 주요국들인 미국, 일본, 중국, 러시아 등과 양자 또는 다자간 사이버 협력을 적극 추진한다.

한편 북한과 관련해서는 북한의 해킹 등을 국제문제로 이슈화하고 국제공조를 통한 제재조치도 유도한다. 동시에 북한을 국제 사이버 규범 논의의 장으로 이끌어 사이버억지 효과를 노린다.

한국이 한반도 사이버 평화체제 구축에 주도적인 역할을 하기 위해서는 한국의 입장을 명확히 반영하는 사이버 원칙을 마련하여 국제사회를 설득할 필요가 있다. 따라서 이러한 한국의 사이버 원칙을 확립하기 위해서는 기본법적 성격을 갖는 가칭 '국가사이버안보기본법'을 제정해야 한다. 이를 통해 사이버 관련 주무기관을 설치하고 사이버 전반에 걸친 원칙을 표명할 수 있을 것이다.

핵심어

해킹, 해킹기법, 사이버공간, 주권, 안보

I

서론

1. 문제제기 및 연구목적
2. 선행연구 검토

1. 문제제기 및 연구목적

오늘날 국제사회는 해킹(hacking)으로 인한 피해가 심각해지면서 해킹에 대한 관심이 매우 높아진 상황이다. 2003년 1·25 인터넷 대란, 2007년 에스토니아 정부 사이트에 대한 해킹, 2008년 러시아의 미군 군사비밀 네트워크에 대한 해킹, 러시아와 조지아 간의 사이버전, 2010년 이란 핵시설에 대해 스턱스넷(Stuxnet)에 의한 해킹, 2014년 북한의 소니 픽처스 해킹, 2015년 중국의 미국 인사관리처 해킹, 2017년 워너크라이 랜섬웨어(WannaCry ransomware) 등이 대표적 사례들이다. 한국의 경우도 2009년 7·7 디도스(DDoS) 공격, 2011년 농협 전산망 해킹, 2014년 북한의 한수원 해킹, 2015년 서울지하철, 청와대, 국회, 통일부 등 해킹, 2016년 청와대 사칭 악성코드 유포, 2017년 롯데 인터넷면세점 대상 디도스 공격 등이 발생했다.

해킹은 심각한 위협으로 대두되었고 공공기관 및 사회기반시설까지 대상이 확대되면서 경제적·사회적 피해가 막대한 상황이다. 특히 국제사회에서 해킹 양상이 다양해지면서 교통·항공·전력 시설에 대한 공격은 국가 재난사태 발생까지 우려되는 상황이다. 개인에 의한 해킹 역시 고도로 조직화되면서 국제해커집단은 조직적 테러리즘의 수준에 도달했다. 국제적인 해커집단인 어나니머스(Anonymous)는 국제기구나 국가기관의 웹사이트와 기업을 해킹했고, 룰즈섹(LulzSec) 역시 미국 중앙정보국(CIA)과 연방수사국(FBI) 등의 데이터베이스를 해킹한 바 있다.

한편 최근 미중 간 갈등의 핵심에 자리 잡고 있는 기술패권경쟁의 대표적 갈등 사례인 화웨이(Huawei) 사태도 국가 간 해킹 문제이다. 미국은 화웨이 장비가 사이버 보안에 취약하여 기술 절도에 이용되고 있다

고 보며, 이는 미중 간 기술패권경쟁을 상징하는 사례이다. 사이버 기술 절도는 가장 전형적인 불법적 기술이전 방식으로 미중 양국이 경제, 군사·안보, 정보, 디지털 거버넌스 등 현재 갈등을 빚고 있는 다양한 영역에서 우위를 점하는 첩경이기도 하다. 미국은 중국으로의 기술이전이 불법적·합법적인 경로를 통해 광범위하게 진행되고 있으며 화웨이 장비는 이를 더욱 심화시킬 것으로 보고 있다. 이에 따라 미국은 동맹국을 대상으로 화웨이 장비 사용금지를 요청하는 동시에 화웨이 장비를 사용하는 국가와는 기밀을 공유하지 않겠다는 입장이다

특히 최근에는 코로나19 팬데믹(pandemic)의 영향으로 새로운 취약점을 공략하는 해킹이 급증하고 있다. 우선 코로나19 상황을 악용해 사람들의 취약점을 공략하는 사회공학(Social Engineering)적 해킹이 많이 발생하였다. 과거에도 메르스와 에볼라 바이러스 발생 시 메르스 또는 에볼라 바이러스 관련 내용이 포함된 이메일과 문자메시지 등을 통해서 악성코드 유포가 증가했었다. 그리고 이러한 감염병 관련 정보제공 사이트로 위장한 해킹도 증가했었다. 다음으로 코로나19로 인해 디지털 전환과 정보통신기술 융·복합이 가속화되고 이로 인한 디지털 공격 범위가 확대되면서 네트워크에 대한 해킹이 많이 발생하였다. 또한 코로나19로 인해 사회적으로 감염병 예방을 위한 거리두기를 실천하고 있는 가운데 온라인을 통한 활동이 대폭 확대되면서 원격접속에 대한 해킹이 많이 발생하였다. 과학기술정보통신부 집계에 따르면, 이와 같은 해킹은 작년에 비해 20% 가량 증가했는데 이는 코로나19가 직·간접적으로 해킹 증가에 영향을 미치고 있는 것으로 볼 수 있다.[1]

1 채재병 외, "코로나19 관련 사이버공격 양상 및 시사점," 국가안보전략연구원 『이슈브리프』 통권 217호 (2020), p. 1.

미국의 의료 서비스업체인 UHS가 랜섬웨어에 의한 공격을 받았고, 독일 뒤셀도르프대학 병원에서는 랜섬웨어 공격으로 응급환자가 사망하는 초유의 사건이 발생하였다. 코로나19 백신 개발에 활용되는 소프트웨어 개발업체인 ERT와 바이오 제약회사 아스트라제네카의 코로나19 백신 임상시험 협력기관인 IQVIA도 랜섬웨어 공격을 받아 코로나19 백신 개발이 지연되는 등 피해를 입었다. 이와 같이 최근의 랜섬웨어 공격은 의료와 제약 부문을 주요 대상으로 하여 이루어지고 있다.

한국은 지난 8월 신한은행·카카오뱅크·케이뱅크 등 금융기관을 대상으로 하는 해킹이 발생하였고, 고려대·중앙대 등 교육기관에 대한 해킹도 발생하였다. 최근 증가된 해킹은 주로 코로나19 관련 메일로 위장된 피싱 사이트 접속 유도와 악성코드 유포 등의 방식으로 이루어지고 있다. 과기부에 따르면, 2017년 이후 한 건도 없던 한국에 대한 북한의 해킹도 올해 코로나19가 급속히 확산되는 상황과 맞물려 7건이나 발생하는 등 갑자기 증가했다. 공격 대상기관은 한국연구재단, 한국방송통신전파진흥원, 한국인터넷진흥원, 한국정보화진흥원 등 사이버 관련 기관들이다. 한편 유엔 대북제재위원회 보고서에 의하면, 북한은 합작회사, 위장회사, 해외계정, 가상자산 등을 이용해 국제금융체계에 지속적으로 접근하고 있고, 특히 최근에는 가상화폐 거래소에 대한 해킹을 이어가고 있다.[2]

이와 같은 해킹은 지속적으로 증가하면서 더욱 고도화될 것으로 예상되므로 이에 대한 효율적인 대비와 관리 및 대응체계가 필요하다. 특히

2 Ibid., p. 2.

4차 산업혁명과 사물인터넷(IoT: Internet of Things) 시대를 맞이하여 사이버공간에서의 주권에 대한 논의가 활발하게 진행되면서 한국도 국가 간 사이버 분쟁에 대비해 해킹에 대한 대응책을 적극 강구해야 할 시점이다. 본 연구의 목적은 이와 같이 사이버공간에서 나타나고 있는 주권인식을 토대로 하여 국제사회에서 나타나고 있는 해킹의 변화 추세를 살펴보고, 해킹의 주체, 기법, 대상별로 분석함으로써 해킹에 대한 한국의 대응방안을 제시하는 것이다.

2. 선행연구 검토

사이버주권 관련 연구는 국제규범과 관련하여 국가주권이 사이버공간에서 어떻게 인정되고 적용되고 있는가에 주목하고 있다. 사이버공간에 대한 기존 국제법 적용에 있어서 주권만큼 적용의 어려움이 나타나는 규범은 없다. 사이버공간에 적용되는 주권의 국제법상 규범적 지위는 사이버공간을 이용하여 이루어지는 활동의 국제법적 합법성을 결정하기 위한 기준이다. 주권의 규범성이 인정되지 않는다면 불간섭 원칙 및 무력 사용의 수준에 이르지 않는 사이버공간의 이용 대부분은 국제법적으로 합법적이 되기 때문이다. 사이버공간은 기본적으로 국가주권이 인정되고 있다. 사이버공간에서의 위해행위는 타국의 주권과 정치적 독립을 침해하는 것으로 간주된다. 따라서 자국의 사이버공간에 관한 정책은 개별 국가의 독자성과 국가통제가 보장된다. 이렇게 사이버공간이 주권의 영역으로 인정받는다면 국제법이 적용될 수 있는 근거는 마련된 셈이다. 사이버공간에서의 주권 인정으로 외부의 공격을 사전에 예방하거나 방지하고 외부의 간섭을 배제하는 정당성이 부여된다. (박주희, 사이버공간에 적용되는 주권의 규범적 성격과 사이버안보, 2020; 배영자, 사이버안보 국제규범에 관한 연구, 2017; 장노순, 사이버안보와 국제규범의 발전: 정부전문가그룹(GGE)의 활동을 중심으로, 2016; 조화순, 정보화시대 국가주권과 사이버공간의 세계정치, 2005.)

한편 해킹에 관한 기존 연구들은 크게 국가안보 차원에서 국제정치학적으로 접근하거나 과학기술 차원에서 기술공학적으로 접근하고 있다. 국제정치학적으로는 급속한 과학기술의 발전과 정보화혁명에 따라 국제안보환경이 변화하고 있다는 점에 연구의 초점을 맞추어 주로 국가안보 차원의 정책 대안적 연구 성과를 도출했다. (김상배 외, 『사이버 안보의 국가전략: 국제정치학의 시각』, 2017; 박종재·이상호, “사이버 공격에 대한 한국의 안보전략적 대응체계와 과제,” 2017; 민병원, “사이버공격과 사이버억지: 국제정치적 의미와 대안적 패러다임 모색,” 2015; 장노순, “사이버안보와 선도국 우위의 전략적 선택,” 2017) 따라서 대부분 사이버안보 이론연구, 사이버안보 법제 또는 정책 연구, 사이버 안보 능력을 높이기 위한 전략연구, 사이버안보 국제규범 등 국제협력을 다루는 연구들로 구성되었다. (박노형·정명현, “국제사이버법의 발전: 제5차 UNGGE 활동을 중심으로,” 2018; 함승현·박대우, “국가 사이버안보를 위한 정책 연구,” 2017; 장노순, “사이버안보와 국제규범의 발전: 정부전문가그룹(GGE)의 활동을 중심으로,” 2016; 배영자, “사이버안보 국제규범에 관한 연구,” 2017)

반면 기술공학적으로는 해킹기법과 전개양상의 변화에 주목하면서 기술적인 분석과 그에 대한 대응방안을 제시하는 연구들이 대부분이다. (박상민·임종인, “사이버공격 의도분석을 통한 공격유형 분류에 관한 연

구," 2019; 김정욱, "사이버 공격 전략 분석을 통한 침해사고분석 방법론," 2019; 최재원, "DNS 스푸핑을 이용한 포털 해킹과 파밍의 위험성," 2019; 조이든·박수진·강남희, "사물인터넷의 경량 IP 카메라 취약점을 이용한 해킹공격 및 대응 방안," 2019; 황진석·장인순·정기수, "웨어러블 기술동향 및 사이버공격 대응방안," 2019) 국제정치학적으로 접근하는 연구들은 기술적인 토대가 거의 반영되지 못함으로써 해킹기법과 전개양상의 변화에 따른 정책적 시사점을 도출하는데 한계를 표출했고, 기술공학적으로 접근하는 연구들은 기술적인 분석에 치중하여 안보적 관점에서 정책적 시사점을 도출하는데 한계가 있다.

최근 사이버공간이 새로운 국가안보 전략영역으로 등장했고, 그에 따른 정책적 대응이 필요한 바 해킹기법과 전개양상의 변화를 적시에 반영하는 전략연구가 요구되는 상황이다. 사이버공간에서의 안보위협인 해킹에 관한 연구는 기존 연구와 달리 그 특성상 기술·정치·법·제도·사회 등 제 학문분야를 포괄하는 학제적 성격을 갖고 있고, 정보화시대와 초연결사회가 도래함에 따라 그 연계성은 더욱 높아지고 있는 상황이나 이에 대한 학제적 연구가 거의 이루어지지 않고 있는 상황이다. 따라서 이와 같은 한계를 극복하는 기술공학적 접근과 국제정치학적 접근을 접목하는 연구 성과를 도출할 필요가 있다. 미흡하나마 본 연구에서는 이러한 접목을 통한 학제적 연구의 첫 걸음을 시도하고자 한다.

II

사이버공간과 주권

1. 사이버공간에 대한 인식
2. 사이버공간에서의 주권

1. 사이버공간에 대한 인식

현재 사이버공간을 어떻게 인식해야 하는지에 대한 논의는 진행형이다. 사이버공간은 수많은 형태와 개념으로 이해되고 있으나 대체로 다음과 같이 이해되고 있다. 우선 사이버공간은 물질적인 동시에 비물질적이라는 것이다. 우리가 사이버공간에 물질적으로 접촉하고 접촉한 이후에 나타나는 대부분의 현상은 비물질적이라는 것이다. 따라서 사이버공간은 하나의 공간만을 형성하고 있지 않고 현실세계와 연결되고 상호 영향을 미친다. 사이버공간에서는 현실세계에서처럼 개인이나 집단, 국가 등이 행위자로서 활동하고 현실사회와 유사한 질서도 갖고 있지만 물리적인 실체를 갖고 있지는 않다. 그리고 사이버공간은 과거에 없었던 새로운 것이며 따라서 그것이 어디로 발전해 나갈지 알기 어렵다는 것이다. 따라서 사이버공간을 이해하기 위해서는 기술에 대한 이해뿐만 아니라 현실세계의 정치, 경제, 사회, 문화적인 이해도 동시에 요구된다. 사이버공간은 현실세계와 동일하게 인간의 삶에 영향을 미치는 하나의 권력공간인 것이다.[3]

사이버공간은 현실세계에서 안보 공간이 영토, 영공, 영해, 우주로 확장되었던 것과 같이 새로운 안보 공간으로 등장했다. 그러나 사이버공간이 갖는 추상적 성격은 새로운 안보 공간의 개념을 명확히 갖기 어렵게 한다. 사이버공간에 대해 국제전기통신연합(ITU)은 “인터넷·컴퓨터 네트워크·전기통신에 직·간접적으로 연결된 시스템 및 서비스”로 정의했

3 채재병 외, 『주변국의 사이버 환경과 한반도 평화체제 구축』, KINU 연구총서 19-29 (2019), p. 27.

고,[4] 탈린 매뉴얼(Tallinn Manual)에서는 "물리적, 비물리적 요소를 통해 만들어진 컴퓨터 네트워크를 통하여 컴퓨터와 전자적 스펙트럼을 이용한 정보의 저장·변경·교류로 특징지어지는 환경"으로 정의했다.[5] 사이버공간은 네트워크상에 구축된 가상의 공간으로 현실세계 전반에 연결된 정보 인프라와 실제 사용되는 모든 정보를 의미하는 것이다.

이렇듯 사이버공간은 현실세계와 모호하게 연결되어 있기 때문에 가상공간에 국한시킬지 아니면 물질적인 부분 즉 현실공간도 포함할지에 대한 문제가 발생한다. 이는 사이버안보의 대상을 결정짓는 중요한 사안으로 사이버공간을 가상공간에 국한시킨다면 물질적인 피해는 사이버안보의 대상에서 벗어나고 네트워크와 시스템에 대한 전자적 피해만이 대상이 될 것이다. 반면에 물질적인 부분을 사이버공간에 포함시킬 경우에는 정보통신기반시설을 포함한 물리적 피해와 정보를 통해 형성된 사회 전반에 걸친 피해가 모두 사이버안보의 대상이 될 것이다. 실제로 사이버공간을 가상공간에 국한시키고 있는 국가들도 정보통신기반시설에 대한 피해를 사이버안보 대상으로 간주하고 있는 상황인 점으로 볼 때 사이버공간은 가상공간과 현실공간과의 통합체로 볼 수 있다.[6]

사이버공간은 단말기를 비롯한 물질적인 시설들을 통해 연결되므로 현실공간과 별개로 볼 수는 없다. 사이버공간은 주로 인터넷으로 연결되고 그 출발은 컴퓨터라고 할 수 있다. 사이버공간이 가상의 정보처리 공간이라고 해도 결국 컴퓨터와 정보통신망을 통한 모든 네트워크와 시스템이다. 사이버공간은 현실공간과 분리시킬 수도 없고 오히려 현실공간과 더 밀접해지고 있는 현실세계와의 유기체적 결합체인 것이다.

사이버공간에서 발생하는 해킹 등에 의한 피해는 직접적 피해와 간접적 피해로 구분되는데 해킹처럼 전자적 수단에 의한 피해뿐만 아니라 여타 물리적인 수단에 의한 피해도 포함된다. 직접적 피해는 주로 해킹에 의해 이루어지며 물리적으로 정보통신 설비에 대해 가해지는 피해도 포함된다. 간접적 피해는 사이버공간을 원활하게 작동시키고 있는 여러 기반시설에 대한 피해를 말하는데 여기에는 주요 정보통신기반시설과 이와 관련된 일반적인 사회기반시설에 가해지는 피해도 포함된다. 케이블이나 라우터(router) 같은 전산시설은 주요 정보통신기반시설에 당연히 포함되지만 이들을 작동시키는 전력을 공급하는 전력시설 등은 포함여부가 불확실하다. 왜냐하면 이러한 전력시설이 사이버공간을 직접 구성하고 있지는 않기 때문이다. 하지만 이러한 전력시설 등이 피해를 입게 되면 사실상 사이버공간이 작동되지 않는 커다란 문제가 발생하게 된다. 따라서 비록 이러한 전력시설 등이 사이버공간의 구성요소는 아니지만 주요 정보통신기반시설에 포함되어야만 사이버공간에 대한 안전을 확보할 수 있게 된다.[7]

이와 같이 사이버공간을 어떻게 인식하느냐 하는 문제는 여전히 논쟁거리로 남아 있으며 국제적인 합의도 도출되지 못하고 있는 상황이다. 그러나 사이버공간이라는 가상세계와 현실세계 간의 경계가 허물어지고 있다는 것은 분명하고, 양 세계 간의 연결과 서로에 대한 상호의존성도

4 ITU, *National Cybersecurity Strategy Guide* (2011), p. 5.

5 Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Defence Centre of Excellence* (Cambridge University Press, 2013), p. 258.

6 채재병, "안보환경의 변화와 사이버안보,"『정치·정보연구』제16권 제2호 (2013), p. 182.

7 Ibid., p. 183.

크게 높아지고 있는 것이 사실이다. 사이버공간에서의 위험이 가상세계뿐만 아니라 현실세계에도 커다란 영향을 미치고 있고 국제사회에 대한 사이버위협은 간과할 수 없게 되었고 이에 대한 대응인 사이버안보 또한 매우 중요해졌다. 국제사회에서 벌어지고 있는 영역 갈등이나 전쟁 그리고 평화와 같은 주요 이슈들이 이제는 가상의 사이버공간에도 나타나고 있는 것이다. 국제사회의 갈등이 사이버 상의 갈등으로 나타나고 이에 대한 사이버공간에서의 제도화 노력도 진행되고 있다. 그리고 이미 4세대 전쟁 시기에 접어들면서 국제사회에서는 육상, 해상, 공중, 우주라는 영역 이외에도 사이버영역에서의 안보체제 구축을 서두르고 있다. 일본의 육·해·공·우주 그리고 사이버 영역에서의 방어체제 구축, 중국의 육·해·공·천·전 5개 영역에서의 방어체제 구축 등이 이러한 맥락에서 추진되고 있는 것이다.

2. 사이버공간에서의 주권

가. 전통적인 주권 개념

주권(sovereignty)은 규범적, 실천적 요인을 함께 가지고 있는 역사적인 산물로,[8] 권력, 권위, 합법성, 질서 등과 같은 정치적인 개념들로 구성되어 있다. 주권은 정치적 결사체인 국가의 등장과 동시에 발전하였으

8 Joseph A. Camilleri, & Jim Falk, *The End of Sovereignty?* (Aldershot: Edward Elgar, 1992).

며,[9] 국제사회를 구성하는 자격의 부여로 이해될 수 있다. 이에 따라 주권 개념이 국가들에게 내재화되고 현실적으로 체험되는 과정은 곧 국가가 국제사회로 편입되는 과정과 그 역사라고 할 수 있다. 대표적으로 주권에 대한 웨스트팔리아(Westphalia)적 전통인 대내적 대중성과 대외적 합법성은 시공간적 흐름 속에서 여러 역사적 사건들을 경험하면서 주권의 개념을 발전시켜왔다.[10] 현재 국제사회에서 나타나고 있는 세계화 현상들은 주권의 개념변화를 이끌어오고 있으며 이 과정에서 역사적인 변화과정을 겪고 있는 주권 개념과 이에 대한 동양과 서양의 인식 및 적용에서 나타나는 차이점들, 그리고 국제사회에 투영되는 주권의 유형별 특징들은 매우 중요한 의미를 갖는다. 궁극적으로 국제사회의 안정을 위한 제도화가 진행되고 국가들 간에 나타나는 다양한 쟁점들을 해결하기 위한 논의의 장으로서 초국가적인 제도의 등장으로 귀결되었다.[11]

주권 개념의 발전과 이에 따르는 주권 개념화 논의의 역사적 발전과정은 국가를 강화시키고 국제사회를 확산시키면서 구체적으로 나타나게 되었다. 이러한 주권 개념의 구체화 과정은 대내적, 대외적 주권의 확보과정이라고 할 수 있다.[12] 여기서 대내적 주권은 경험과 대중을 기반으로 해서 획득되는 지위로 볼 수 있고, 대외적 주권은 국제사회에서 합법성과 독립성을 통해 획득하는 지위로 볼 수 있다. 따라서 대내적 주권은 경험적 주권이고, 대외적 주권은 합법적 주권이라고 할 수 있다. 현실

9 Jorge, A Bartelson, *Genealogy of Sovereignty* (Cambridge: Cambridge University Press, 1995).

10 Stephen D, Krasner, *Sovereignty: Organized Hypocrisy* (Princeton: Princeton University Press, 1999).

11 채재병 외, 『주변국의 사이버 환경과 한반도 평화체제 구축』, pp. 36-37.

12 Walter C. Opello, & Stephen J. Rosow, *The Nation-State and Global Order: A Historical Introduction to Contemporary Politics* (Boulder, CO: Rienner, 1999).

에서 주권 개념이 안착되는 것은 국가와 자본주의 세계질서의 확대로 표현된다. 국가들 간 관계의 국제법적 질서를 제공해 준 웨스트팔리아조약(Treaties of Westphalia) 이후 유럽 국가들은 세력균형정책으로 인한 주권침해의 경험도 하고 이로 인해 주권이 아닌 새로운 개념을 고안해보기도 했지만 결국 국가 주권에 대해 상호 인정하게 되었다. 이러한 인정은 주권이 국제사회를 구성하는 주요 요인이 되는 것과 동시에 국제사회에서 나타나는 여러 이슈 및 현상들을 이해할 수 있는 핵심 담론을 형성하게 해주었다.[13]

웨스트팔리아적 주권은 영토, 인구, 권위, 인정으로 구성되며, 대외적 배타성, 대내적 권위의 인정, 사법적 독립권, 상호의존적 규제 등을 근거로 주권을 실현시켰다.[14] 전통적인 관점에서 볼 때 이와 같은 주권의 정체성이 무너지는 것이 바로 전쟁과 같은 국제사회의 안보부재라고 할 수 있다.[15] 이러한 전통에 변화를 가져온 것이 탈냉전적 국제관계로 탈냉전적 국제질서가 등장함으로써 주권과 전쟁 간에 이어져온 인과관계는 더 이상 유지될 수 없게 되었고 새로운 이해가 필요하게 되었다. 새롭게 등장하는 안보위협들, 즉 테러, 종교, 빈곤, 인권, 인종, 대량살상무기 등은 새로운 전쟁 요인들을 제공해주고 있고, 이제 웨스트팔리아적 주권 개념의 변화를 요구하게 되었다. 지금까지 웨스트팔리아적 주권 개념을 통

13 Samuel J. Barkin, & Bruce Cronin, “The State and the Nation: Changing Norms and the Rules of Sovereignty,” *International Organization*, Vol. 48, No. 1 (1994); Thomas J. Biersteker, & Cynthia Weber, eds., *State Sovereignty as Social Construct* (Cambridge: Cambridge University Press, 1996).

14 Stephen D, Krasner, *Sovereignty: Organized Hypocrisy*.

15 J. G., Ruggie, “Territoriality and Beyond: Problematizing Modernity in International Relations,” *International Organization*, Vol. 47, No. 2 (1993).

해 설명되었던 전쟁의 원인들이 갖고 있는 안보부재(Insecurity)가 탈냉전적 국제질서에서 주요전쟁의 성격을 규정하거나 설명할 수 없기 때문에 새로운 주권 개념에 대한 인식론적 분석이 요구되었다. 더 이상 탈냉전적 전쟁의 유형과 원인이 과거 전통적으로 받아들여진 절대적 주권(Absolute Sovereignty)으로는 주권국가의 정체성과 국제안보가 확보될 수 없다는 것이다. 웨스트팔리아 체제는 국내와 국제영역을 분리함으로써 독자적 차별성을 부여하고 동시에 국제관계를 주권을 중심으로 이해함으로써 국제관계에 근대성을 확립시킨 상징적인 의미를 갖는다. 주권국가가 형성되는 과정은 수많은 전쟁을 통해서 대중적인 합의를 확보해 가는 과정이었으며 이러한 서구의 주권국가체제의 무정부상태를 역사적 경험으로 하여 주권에 대한 이론화를 시도하였던 것이다.[16] 따라서 전쟁이란 근대 국제질서 하에서의 웨스트팔리아적 주권 개념의 실천이라고 할 수 있으며 이러한 웨스트팔리아적 주권 개념은 탈냉전적 국제질서 하에서 현실과 이론적 측면에서 동시에 도전받고 있다.[17]

국제관계에서 핵심적인 개념적 지표들인 주권과 안보를 살펴보면, 주권은 웨스트팔리아적 개념에 따르면 영토와 인정의 정당화, 권위체의 존재를 의미하는 권위, 특정 영토에 대해 사회통합을 이룰 수 있는 정치적 통제, 그리고 인구의 완비이다. 이러한 전통을 통해 근대국제체제가 완성되었고 이후 발전을 이끄는 기준이 되었다. 다시 말해 국제관계의 근대성은 영토에 대한 정치적 지배로 규정될 수 있다. 국제사회의 자본주의적 성장을 가져온 국가라는 지배형태는 영토라는 일정한 공간적 영역

16 Charles, Tilly, Coercion, *Capital and European Sates AD 990-1900* (Oxford: Basil Blackwell, 1990).

17 채재병 외, 『주변국의 사이버 환경과 한반도 평화체제 구축』, p. 39.

에 대한 정치적 통제를 기반으로 하였고 그 공간의 부족에서 발생하는 권위를 보충하기 위해서 국제사회의 확산을 도모한 것이다.[18] 모든 전쟁에서 나타나듯이 근대국제체제 형성 이후에는 주권에 대한 국가의 대내적 합의가 있었고 동시에 국제적 차원에서의 대외적 인정이 있었다. 이것이 웨스트팔리아적 주권 개념인데 현재 웨스트팔리아 주권은 현실과 이론으로서 동시에 도전을 받고 있다. 왜냐하면 현재 나타나고 있는 경제단위로서의 국가, 안보를 제공하는 주체로서 국가, 개인의 정체성을 독점하는 국가, 전 지구적 문제에 있어서 윤리적 책임을 지는 국가, 한정된 영토 내의 민주주의 존속 등 기존에 있었던 국내와 국제 및 정치와 경제 간의 구분, 전통적인 안보와 국제법 개념으로는 설명할 수 없는 변화들이 나타나고 있기 때문이다.[19]

웨스트팔리아적 주권은 국민을 전제로 일정한 정치체 내에서 효율적으로 통제할 수 있는 공적 권위체로서의 능력을 가지며 국내의 공식적인 정치적 권위조직이며 국제관계에서 대외적 배타성의 원리가 상호 인정된다는 점에서 중요한 의미를 갖는다. 따라서 웨스트팔리아적 주권 개념은 절대적 주권에 대한 상호 보장을 의미하며 세계화적 국제질서의 관점에서 보면 이러한 주권 개념은 소위 웨스트팔리아적 족쇄라고 할 수 있다. 왜냐하면 국제자본주의의 안정성 확보, 국제 금융의 관리, 유럽에서의 주권통합을 위한 실험, 생태적 환경 보존의 문제 등으로 나타나는 현

18 Jorge, A Bartelson, *Genealogy of Sovereignty*.

19 Clark, Ian. “Beyond the Great Divide: Globalization and the Theory of International Relations,” *Review of International Studies* Vol. 24, No. 3 (1998); Cutler, Claire. “Critical Reflections on the Westphalian Assumptions of International Law and Organization: A Crisis of Legitimacy,” *Review of International Studies*, Vol. 27, No. 1 (2001).

국제사회의 주요 현안들은 서구 근대국제체제의 역사적 정체성을 확립해 주었던 웨스트팔리아 주권 개념의 변화이기 때문이다.[20]

안보는 위협의 부재라고 할 수 있는데,[21] 이러한 위협의 부재는 근대국제체제 이후 냉전적 국제질서에서 웨스트팔리아적 주권 개념을 기반으로 하였다. 전쟁과 관련한 대내적 합의는 전통적인 주권 개념이 무너지면서 그 정당성을 획득하였고, 개별 국가의 주권에 대한 대외적 독립성과 대내적 질서를 인정함으로써 국제사회에 반영되었다. 국제사회는 국제안보 확보를 위해 주권에 대한 존중을 합의한 것이다. 그러나 탈냉전적 국제안보는 이러한 국제사회의 합의를 근본적으로 변화시켰다. 다시 말해 국제안보 차원에서 주권이 구체화되는 실천양식이 변하고 전쟁 요인과 전쟁 수행의 정당성 근거도 변한다는 점은 웨스트팔리아적 주권 개념에 근본적인 변화가 일어나고 있다는 것이다. 인종, 종교, 권위의 부재, 빈곤 등 다양한 차원에서 국제안보를 위협하고 있는 안보부재는 국제질서의 세계화적 변화의 원인인 동시에 결과라고 할 수 있다. 탈냉전적 국제사회에서 발생하는 전쟁의 원인들은 웨스트팔리아적 관점에서 주권의 대외적 독립성에 대한 부정이며, 웨스트팔리아적 주권 개념은 국제안보에 대한 합의의 주요한 토대가 되었다. 주권 개념의 발달을 통해 국가들 간의 서로 다른 이해관계를 조정하고 안정적인 국제관계를 유지할 수 있다. 유럽연합의 등장은 주권 개념의 확장과 국내외적 문제들에 대한 탈주권적 해석이 이루어짐으로써 가능했다. 탈냉전적 국제상황은

20 채재병 외, 『주변국의 사이버 환경과 한반도 평화체제 구축』, pp. 40-41.

21 Barry Buzan, *People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era* (Colorado: Lynne Rienner Publisher, 1991) p. 363.

국가들로 하여금 주권의 개념적 구성을 고민하게 했으며 국제관계의 다양한 변화요인들로 인해 국가들 간의 안정적인 국제질서를 모색할 시기이다.[22]

나. 사이버주권과 안보

이상의 전통적인 주권 개념이 과연 사이버공간에서도 통용될 수 있는지 그리고 사이버공간에서의 주권 개념이 국가안보 차원에서의 주권 개념과 어떠한 차이점 또는 공통점이 있는지 살펴볼 필요가 있다. 이를 위해 우선 안보 개념의 확장이라는 측면에서 국가안보와 사이버안보를 살펴본다. 일반적으로 사이버안보란 사이버공간을 해킹을 비롯한 다양한 형태의 공격으로부터 보호하는 것이라고 할 수 있다. 따라서 사이버공간에 대한 공격으로부터 국가와 국민을 보호하기 위한 모든 수단들의 집합이라고 할 수 있다. 그런데 사이버라는 용어가 추상적인 개념이라 현실에 적용하기 쉽지 않기 때문에 실제 사이버안보 개념을 논의하는 것은 어렵다. 사이버라는 용어는 컴퓨터와 인터넷 등을 기반으로 하는 정보통신망과 이를 통해 실현되는 가상공간 등 정보통신기술과 관련된 거의 모든 것을 의미한다. 이러한 사이버라는 용어의 추상적인 성격은 현실세계와 가상세계의 경계를 모호하게 만들었고 사이버공간에 대한 규정도 어렵게 하고 있다. 현재 사이버공간이 무엇인지에 대한 명확한 정의도 존재하지 않는 상황에서 이와 관련된 사이버안보 개념을 논의한다는 것은 매우 어려운 일이다. 실제로 사이버안보를 규정하는 국제적 합의는 아직

22 채재병 외, 『주변국의 사이버 환경과 한반도 평화체제 구축』, pp. 41-42.

도출되지 않고 있으며, 다수의 국가들과 국제기구들이 사이버안보에 관한 다양한 개념들을 언급하고 있다. 또한 대부분의 국가들은 안보전략상의 이유로 사이버안보 및 관련 개념들에 대해 규정하지 않고 있기도 하다.[23] 다만 각국에서 발표한 사이버안보 전략의 범위와 내용들을 살펴보면, 사이버공간의 개념을 보다 광범위하게 받아들여 기존의 정보통신망, 정보, 정보통신기술 보호 등 특정 영역에 대한 보호에서 벗어나 사이버안보의 개념을 확장하고 있다는 것을 알 수 있다. 즉 국가 차원에서 사이버안보 개념을 인식하여 국가 사이버공간에 대한 다양한 위협으로부터 안전을 확보하는 조치로 보고 있는 것이다. 과거에는 사이버공간의 안전을 정보통신망. 정보, 정보시스템 보호로 인식하고 있었다.[24]

최근에는 포괄적인 사이버안보 개념이 나타나면서 정보통신망, 정보보호 등보다 좀 더 폭넓은 범위로 발전하고 있다. 사이버공간의 안전을 위해서는 정보보호가 필수적이지만 좀 더 포괄적으로 정보뿐만 아니라 정보통신망 등의 안전도 사이버안보의 핵심요소가 되었다. 따라서 포괄적인 사이버안보 개념은 보호대상에 있어서 기존과 같이 정보의 안전성 보장에 중점을 두기 보다는 현실세계에서와 마찬가지로 전반적인 사이버공간에서 안전을 보장하는데 중점을 두었다. 사이버공간을 독립된 영역으로 보지 않고 현실공간과 연결되어 있는 유기적 공간으로 보고 있기 때문에 사이버공간에서의 안보는 기존의 보호개념보다는 더 확장될 수 밖에 없는 것이다. 여기에는 기존의 정보보호에 더하여 정보통신망에 대

23 ENISA, *National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace* (2012. 5), p. 5.

24 채재병, "안보환경의 변화와 사이버안보," pp. 180-185.

한 보호도 필요하며 결국 사이버안보의 보호대상은 사이버공간에서 저장되고 이용되고 전송되는 정보만이 아니라 사이버공간 그자체가 안전을 확보해야 하는 것이다.[25]

국가안보의 관점에서 주권은 당연히 웨스트팔리아적 주권 개념에서 비롯된다. 그런데 국가안보가 단순히 국가관리 차원을 넘어 주권을 더 확장하기 위해 포괄적인 전략을 구사한다는 점, 다시 말해 육상, 해상, 공중, 우주를 포함하는 전 영역에서의 안전보장과 지역안보 및 전 세계적 차원의 안보를 추구하고 정치, 경제, 사회, 문화 등 전 분야에서의 안보를 추구한다는 점에서 국가안보는 포괄안보 차원에서 추진되고 있는 것이다. 이는 국가안보에서의 주권 개념이 웨스트팔리아적 주권 개념의 변화를 통해 안보 개념의 확장으로 나아가고 있음을 보여준다.[26]

사이버공간의 특수성으로 인해 국가안보 개념이 현실공간과 마찬가지로 사이버공간에 그대로 적용될 수는 없을 것이다. 그렇지만 국가안보가 주권과 주권의 충돌이라는 점에서 이를 논리적으로 확장해보면 사이버공간에서도 주권이 충돌하는 지점이 존재하므로 사이버공간에서의 주권 개념도 국가안보에서의 주권 개념과 연결될 수 있다고 볼 수 있다. 특히 사이버안보가 포괄적인 차원에서 국가안보와 마찬가지로 전개되고 있다는 점에서 더욱 그러하다. 그리고 사이버공간에서의 주권 개념과 국가안보에서의 주권 개념은 주권의 정체성이라는 측면에서 볼 때 사실상 별다른 차이가 없다. 물론 사이버공간에서의 주권 개념을 현실공간인 국가안보에서의 주권 개념과 동일시할 수 없는 부분도 있다. 이는 사이버공간의 특수성 때문이며 우선 사이버국가의 존재가 가능하냐의 문제이다. 사이버공간에서 이러한 물리적 구분은 상당히 어려운 일이며 우선 사이버공간에서 나타나는 현상들은 가시적이지 않다는 점이다. 그렇다고 눈에 보이지 않으므로 발생하지 않는 것은 아니며 더욱이 발생하는 현상들이 감지되지 않는 것도 아니다. 사이버공간에서의 현상들은 대개의 경우 현실세계로 이어지며 사이버공간에서의 분쟁이 보이지는 않지만 주권과 주권의 충돌이 일어났으며 실제로 존재하는 것이다. 이런 이유로 주권의 정체성이라는 측면에서 볼 때 사이버공간의 주권 개념과 국가안보에서의 주권 개념은 사실상 동일하게 보아도 무방할 것이다.[27]

국가라는 현실공간은 현실보다도 더 현실과 밀접한 가상현실의 공간과 결합되어 있고 새로운 공간 네트워크를 만들어 내고 있다. 이와 같은 불가분의 관계에 있는 현실공간과 가상공간은 서로 확장된 공간만큼이나 다양한 위협들에 노출되어 있다. 사이버안보와 관련된 논의는 사이버공간이라는 새로운 국가안보영역이 현실공간에서의 국가와 밀접하게 연결되어 있으며 국가안보와의 상관성을 갖고 있다는 것을 보여준다. 이와 같은 국가안보 개념의 확장은 안보 개념 변화 과정을 통해서도 이해될 수 있다. 안보 개념 변화는 냉전이 종식된 이후 안보에 대한 인식이 변화되면서 시작되었다. 안보 의식의 변화는 우선 안보의 대상 즉 위협하는 주체가 무엇인지에 대한 인식의 변화이다. 그리고 안보의 내용 즉 무엇을 어디까지 보호해야 하느냐에 대한 인식의 변화이다. 마지막으로 안보의 추구방법, 즉 위협 방지를 위한 수단이 무엇이냐에 대한 인식의 변화이다. 구체적으로 안보의 대상은 적국으로부터 주권, 영토, 국민의 생명

25 Ibid., p. 186.

26 채재병 외, 『주변국의 사이버 환경과 한반도 평화체제 구축』, pp. 44-45.

27 Ibid., pp. 45-46.

과 재산 등에 대한 보호라는 국가 중심적 시각에서 테러, 기근, 질병, 환경오염 등 초국가적 위협으로부터의 보호로 변화했다. 안보의 내용은 이러한 초국가적 위협으로 인해 군사적 안보 이외에도 경제안보, 환경안보, 사회안보, 인간안보 등을 포함하는 포괄안보로 변화했다. 안보의 추구방법은 위협에 대처하기 위해 동맹체제를 통한 힘에 의존한 안보에서 초국가적 위협에 대응하는 관계국들 간 협력안보로 변화했다. 국가 중심적이고 군사력에 의존하는 전통안보로부터 초국가적, 비군사적인 비전통안보로 변화했다. 이는 냉전 이후 종교, 인종, 문화, 자원 등을 둘러싼 분쟁이 분출되면서 테러, 국제범죄, 난민, 환경문제 등과 같은 초국가적 위협들이 크게 나타났기 때문이다. 그리고 새로운 사회 문제들이 국가안보를 위협하는 국제안보환경의 변화 상황에서 포괄안보 개념이 크게 부상하였다.[28] 따라서 냉전 이후 국제사회에는 군사문제 외에 테러, 국제범죄, 환경, 자원 등을 대상으로 하는 포괄안보가 핵심 안보 개념으로 확립되었다.[29] 즉 냉전기의 안보 개념이 군사적인 차원에서의 외부 위협에 대한 대응이었다면 탈냉전기에는 환경, 자원, 경제, 사회 문제 등 비군사적인 요소들을 포함하는 개념으로 변화한 것이다.[30] 포괄안보 개념은 군사안보와 비군사안보 요소를 포괄하여 안보정책을 추진한다는 점에서 비전통안보 개념으로 볼 수 있다. 포괄안보는 군사안보와 비군사안보 간의

28 Richard N. Haas, "Paradigm Lost," *Foreign Affairs*, Vol. 74, No. 1 (Jan./Feb. 1995), pp. 43-58.

29 Carolyn M. Stephenson, "New Approaches to International Peacemaking in the Post-Cold War World," in Michael T. Klare (eds.), *Peace & World Security Studies: A Curriculum Guide* (Boulder: Lynne Rienner Publisher, 6th ed, 1994), p. 18.

30 Kanti Bajpai, "The Idea of Human Security", *International Studies*, Vol. 40(3), p. 223.

조화에 의해 안보정책목표를 달성하고자 한다.[31] 포괄안보 개념을 통해 안보의 범위가 크게 확대되었고 이제 안보는 정치와 군사뿐만 아니라 환경, 경제, 사회 등 각 분야를 포괄하지 않고서는 이해할 수 없는 개념이 되었다.[32] 반면 이와 같은 안보 개념의 변화는 위협의 주체가 다양해지고 위협요인이 다양해짐에 따라 어떤 대상에 대해 어떻게 대응해야 할지 훨씬 더 복잡해졌고 안보의 개념과 목표를 불투명하게 만들었다.[33]

사이버안보도 이러한 안보 개념의 변화에 토대를 두고 있는 국가안보 개념의 확장과 같은 범주에서 출발하고 있다. 사이버위협은 냉전 종식 이후 비약적인 정보통신기술의 발전에 기인하여 안보 개념의 변화 속에서 나타난 새로운 안보위협이라고 할 수 있다. 실제로 사이버안보에 대한 논의는 지금까지 앞에서 언급한 안보 개념 논의 과정에 따라 국가안보와 유사한 경로를 통해 전개되어왔다. 안보의 대상, 내용, 추구방법의 변화는 사이버안보의 변화양상과 거의 일치하고 있다. 또한 해킹 등의 사이버위협은 테러와 거의 동일한 속성을 갖고 있는데 테러와 마찬가지로 사이버위협은 공격과 방어를 하는데 있어 비대칭성을 갖고 있다는 점에서 특히 그러하다. 이와 같은 이유로 해킹 등의 사이버위협이 현실화되었을 때 이것이 사이버테러라는 이름으로 이슈화되었고 현재도 테러의 영역에서 다루어지고 있는 것이다. 또한 해킹의 주체가 개인이나 집단, 그리고 국가 차원에서도 이루어지고 있다는 점이 테러와 유사하며 그 피해에 있어서도 막대하다는 것이 유사하다. 이러한 유사성 때문에

31 채재병, "국제테러리즘과 군사적 대응,"『국제정치논총』제44집 제2호 (2004), p. 60.

32 Barry Buzan, *People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, p. 363.

33 채재병, "국제테러리즘과 군사적 대응," pp. 59-61.

해킹 등의 사이버위협이 사이버테러라는 이름으로 아직까지도 테러리즘의 영역에서 논의되고 있지만 향후에는 새로운 방향에서 사이버안보에 관한 논의로 전개될 것이다. 왜냐하면 사이버안보는 사이버공간이라는 가상공간 영역을 갖고 있어서 기존에 논의되는 안보영역과는 별개의 완전히 새로운 영역이기 때문이다. 또한 사이버안보는 국가안보 차원에서 다루어져야 하고, 군사적, 비군사적 수단이 함께 사용되어야 하는 대처방법이나 수단을 효과적으로 구사하기 위해서는 반드시 국제협력이 필요하다는 점에서 안보 개념의 확장이라는 측면에서 접근해야 한다.[34] 이러한 사이버안보의 특성은 국가안보 개념의 확장과 연결되고 현실공간과 가상공간을 연계해주는 동시에 사이버공간에서 국가안보 개념을 정립할 수 있는 근거를 제공해준다. 사이버공간에서의 국가안보 개념의 적용이 동일할 수는 없겠지만 안보 개념의 재정립이라는 관점에서 사이버공간과 국가안보의 상관성 도출은 가능할 것이다.

34 Joseph S. Nye Jr., “Power and National Security in Cyberspace,” in Kristin M. Lord and Travis Sharp (eds.), *America’s Cyber Future: Security and Prosperity in the Information Age*, Vol. II (Center for a New American Security, June 2011), p. 9.

III

국제사회 해킹 변화 추세

1. 개념
2. 해킹 유형의 변화
3. 해킹 방법의 변화

1. 개념

해킹은 컴퓨터 시스템이나 네트워크의 약점을 파악해 그 약점을 악용해 접근성을 확보하는 것이다 해킹은 컴퓨터, 스마트폰, 태블릿, 심지어 전체 네트워크와 같은 디지털 기기에 불법적으로 침입하여 그 안의 자원에 접근하는 활동을 말한다. 그리고 해킹이 항상 악의적인 목적을 위한 것은 아닐 수 있지만, 오늘날 대부분의 해킹과 해커에 대한 언급은 그것을 사이버 범죄자들에 의한 불법 활동으로, 즉 금전적 이득, 항의, 정보 수집, 그리고 단지 도전의 재미를 위해서라고 규정한다.[35] 한편 크래킹(cracking)은 컴퓨터에 침입해 고의적으로 이익을 취하거나 시스템을 마비시키고 데이터를 파괴하는 행위이다. 현재 해킹은 이를 모두 포함하는 포괄적인 의미로 사용되며, 해킹을 통해 침해사고를 유발하는 행위를 해킹공격이라고 한다.[36] 사실 해킹은 공공, 기업, 정부 컴퓨터에 대한 악성 코드와 악의적인 사이버공격의 전부는 아닐지라도 대부분의 배후에서 행해지는 활동이다. 일반적인 해킹 기법에는 봇넷(botnet), 브라우저 가로채기, 서비스 거부(DoS: Denial of Service) 공격, 랜섬웨어, 루트킷(rootkit), 트로이목마, 바이러스, 웜스, 사회공학적 공격 등이 포함된다.

해킹을 하는 사람을 해커라고 하는데 화이트 해커와 블랙 해커로 분류된다. 화이트 해커는 해킹 기법을 사용하는 전문적인 보안전문가이며,

35 "Hacker," Malwarebytes, https://www.malwarebytes.com/hacker/ (accessed: October 30, 2020).

36 Jeff Petters, "A brute force attack," https://www.varonis.com/blog/brute-force-attack/#:~:text=A%20brute%20force%20attack%20(also,attacks%20are%20simple%20and%20reliable (accessed: October 30, 2020).

블랙 해커는 자기만족 등의 이유로 허가받은 범위를 벗어나서 컴퓨터와 네트워크에 대한 침해사고를 일으키는 행위의 주체이다.[37] 많은 사람들은 해커가 컴퓨터 하드웨어나 소프트웨어를 개조하는 데 숙련된 독학한 어린이나 불량 프로그래머로 원래 프로그램 개발자들의 의도 외의 방법으로 사용될 수 있도록 조작한다고 생각한다. 그러나 해킹은 일반적으로 사용자의 상호작용이 필요 없는 드라이브 바이 공격에 악성코드를 축적하는 변태성 생성과 같은 기술적 특성이다. 해커들은 또한 심리를 이용하여 사용자가 악의적인 첨부파일을 클릭하거나 개인 데이터를 제공하도록 속이는데 이러한 전술을 사회공학이라고 한다.[38]

해커가 하는 해킹의 등급은 레이머(Lamer), 스크립트 키디(Script Kiddie), 디벨롭 키디(Developed Kiddie), 크래커 등이다. 레이머는 네트워크와 운영시스템에 대한 지식이 많지 않아 와레즈 사이트에서 트로이목마나 DoS 공격 툴 등의 해킹 툴을 내려 받아 사용한다. 스크립트 키디는 네트워크와 운영시스템에 대한 약간의 기술적인 지식을 갖고 있고, 공격 기법도 기존에 잘 알려진 툴을 사용한다. 디벨롭 키디는 대부분의 해킹 기법을 숙지하고 있으며 해킹 코드가 적용될 수 있는 취약점을 발견할 때까지 수차례 시도해 시스템 침투에 성공하고 만다. 크래커는 구루(guru) 익스페리언스드 테크니션 또는 세미 엘리트와 위저드 엑스퍼트 또는 엘리트로 구분된다. 세미 엘리트는 컴퓨터에 대한 포괄적인 지식과 네트워크와 운영시스템에 대한 지식도 갖고 있어 운영시스템

37 “What is the Difference Between Black, White and Grey Hat Hackers?,” Norton, https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html (accessed: October 30, 2020).

38 “Hacker.”

의 특정 취약점을 공격할 수 있는 해킹 수행 코드를 만들 수 있다. 또한 기존의 해킹 프로그램도 사용하지만 프로그램을 수정할 수도 있다. 다만 해킹 흔적을 지우지 못해 추적당할 수 있는 수준이다. 엘리트는 컴퓨터, 네트워크, 운영시스템, 프로그래밍 등에 대한 포괄적인 지식을 갖고 있어 시스템의 새로운 취약점을 찾아내 해킹할 수 있다. 이외에도 위저드 네메시스라는 세계 최고 등급이 있고, 또 위저드 킹은 컴퓨터, 네트워크, 운영시스템, 보안 등 모든 분야에 완벽한 이해를 가지고 있는 즉 해커가 궁극적으로 지향하는 단계이다.[39]

크래커들은 턴키 해킹 도구를 개발해 판매하는 범죄 인프라를 구축해 기술력이 떨어지는 스크립트 키디에게 판매한다. 예로 윈도우 사용자들은 다크웹 해킹 스토어를 통해 단돈 10달러에 IT 시스템에 원격으로 접속할 수 있는 광범위한 사이버범죄의 표적이 되고 있다. 이러한 도구들은 해커들이 정보를 훔치고, 시스템을 교란하고, 랜섬웨어를 배치하게 한다. 여기서 판매용으로 광고된 시스템들은 윈도우 XP에서 윈도우 10까지 다양하고 심지어 불법 로그인을 사용하는 사람들이 어떻게 적발되지 않을 수 있는지에 대한 팁도 제공하고 있다.[40]

대략적으로 말하면, 해커들이 다음 네 가지 이유 중 어떤 이유로든 컴퓨터와 네트워크에 침입하려고 한다고 할 수 있다. 범죄적인 금전적 이득이 있는데, 이는 신용카드 번호를 도용하거나 은행 시스템을 사취하는 것을 의미한다. 다음으로, 해커 하위문화 내에서 길거리의 신뢰를 얻고 악명을 얻는 것은 해커들이 그들이 해킹을 성공시켰다는 증거로 파괴하

39 박대우, “국가사이버보안정책에서 해킹에 대한 소고,"『정보보호학회지』, 21(6), (2011), pp. 23-40.

40 Jeff Petters, “A brute force attack.”

는 웹사이트에 그들의 흔적을 남기기 때문에 일부 해커들에게 동기를 부여한다. 그리고 한 회사의 해커들이 시장 우위를 점하기 위해 경쟁사의 제품과 서비스에 대한 정보를 훔치려는 기업의 스파이 활동이 있다. 마지막으로, 모든 국가는 기업이나 국가 정보를 훔치거나, 상대의 인프라를 불안정하게 하거나, 심지어 대상 국가에 불화와 혼란을 야기하기 위해 국가 주도로 해킹을 한다. 한편 사이버 범죄자들의 또 다른 범주가 있다. 어떤 목적을 위해 정치적 또는 사회적 동기를 부여받은 해커로 그러한 해커 활동가들 또는 핵티비스트(hacktivist)들은 보통 민감한 정보를 공개함으로써, 목표물에 끊임없는 주의를 기울임으로써, 어떤 문제에 대중의 관심을 집중시키기 위해 노력한다.[41]

2. 해킹 유형의 변화

해킹 유형의 변화 추세를 살펴보면 컴퓨터와 네트워크 등 정보통신기술의 발달이 진행되면서 해킹 유형은 매우 다양하게 그리고 불규칙하게 변화를 거듭하였다. 해킹이 시도되는 과정을 통해 살펴보면, 우선 해킹 대상에 대한 정보를 수집하여 대상을 공격하기 위한 방법 등을 구상하면서 전략을 구축한다. 그리고 의도적으로 대상 컴퓨터나 운영시스템, 네트워크에 접속을 시도한다. 정보 수집은 살라미(salami)식으로 조금씩 소량의 정보를 모으는 것부터 시작하는데 이는 정보 수집과정에 해킹 시도의 조짐이나 이상신호를 해킹 대상이 알아차리지 못하게 하기 위해서

41 "Hacker."

이다. 그리고 다음으로 쓰레기 모으기를 시도하는데 주로 휴지통 뒤지기 등을 통해서 정보 수집을 진행한다. 이 역시 해킹 대상이 눈치채지 못하는 방식으로 접근하여 해킹에 이용할만한 정보를 얻는 것이 목적이다. 충분한 정보 수집이 이루어지면 이를 바탕으로 하여 의도적인 접속을 시도한다. 의도적인 접속 단계에서는 주로 스니핑(sniffing) 방식을 사용하는데 스니핑은 패킷 스니퍼를 이용해 컴퓨터 네트워크를 통과하는 모든 데이터 패킷을 모니터링하고 캡처하는 과정으로 다른 사람의 계정이나 패스워드를 탈취하기 위해 쓰이는 방법이다. 패킷 스니퍼는 네트워크 관리자가 네트워크를 통과하는 데이터 트래픽을 추적하기 위해 사용한다. 이러한 패킷 스니핑 도구를 사용하여 네트워크에서 데이터 패킷을 캡처한다. 네트워크에서 캡처한 데이터 패킷은 암호, 사용자 이름, 신용카드 정보 등 민감한 정보를 추출해 빼내는 데 사용된다.[42]

다음으로 접속이 이루어진 후 본격적으로 해킹을 시도하게 되는데 이때 스푸핑(spoofing)은 알려지지 않은 출처로부터의 통신을 알려진 신뢰할 수 있는 출처로부터 온 것으로 위장하는 행위로 이메일, 전화 통화 및 웹사이트에 적용되거나 컴퓨터가 IP(Internet Protocol) 주소, 주소 확인 프로토콜(ARP; Address Resolution Protocol) 또는 DNS(Domain Name System) 서버 스푸핑과 같은 보다 기술적인 것들을 사용한다. 스푸핑은 대상의 개인 정보에 대한 접근권한 획득, 감염된 링크나 첨부파일을 통한 악성코드 확산, 네트워크 접속 제어 우회, 트래픽 재분산 등을 통해 DoS 공격을 실시하는 데 이용된다. 해커는 컴퓨터

42 "WHAT ARE SNIFFING ATTACKS AND THEIR TYPES?" EC-Council, https://blog.eccouncil.org/what-are-sniffing-attacks-and-their-types/#:~:text=Sniffing%20is%20the%20process%20of,are%20called%20network%20protocol%20analyzers (accessed: October 30, 2020).

IP 주소를 위장하기 위해 IP 스푸핑을 사용할 수 있어 송신자의 신원을 숨기거나 다른 컴퓨터 시스템을 사칭할 수 있다. IP 주소 스푸핑의 한 가지 목적은 IP 주소를 기반으로 사용자를 인증하는 네트워크에 접속하는 것이다. 그러나 해커는 DoS 공격에서 대상의 IP 주소를 스푸핑하여 트래픽으로 피해자를 압도하는 경우가 더 많다. 해커는 패킷을 여러 네트워크 수신자에게 전송하며, 패킷 수신자가 응답을 전송하면 대상의 스푸핑된 IP 주소로 라우팅된다.[43]

버퍼 오버플로우(buffer overflow)는 프로그램에서 메모리 버퍼를 넘치게 해서 이상 동작하게 만드는 기법으로 모든 유형의 소프트웨어에 영향을 미칠 수 있다. 일반적으로 잘못된 입력 또는 버퍼에 충분한 공간을 할당하지 못한 경우 발생한다. 트랜잭션이 실행 코드를 덮어쓰면 프로그램이 예기치 않게 작동하고, 잘못된 결과로 메모리 액세스 오류 또는 충돌을 생성 할 수 있다. 해커는 응용 프로그램의 메모리를 덮어써서 버퍼 오버플로우 문제를 악용한다. 이것은 프로그램의 실행 경로를 변경하여 파일을 손상시키거나 개인 정보를 노출하는 응답을 보내게 한다. 예를 들어 해커는 추가 코드를 도입하여 IT 시스템에 대한 액세스 권한을 얻기 위해 응용 프로그램에 새로운 명령을 보낼 수 있다. 해커가 프로그램의 메모리 레이아웃을 알고 있으면 버퍼가 저장할 수 없는 입력을 의도적으로 공급하고 실행 코드가 있는 영역을 덮어쓰고 이를 자신의 코드로 대체 할 수 있다.[44]

43 “SPOOFING ATTACK: IP, DNS & ARP,” VERACODE, https://www.veracode.com/security/spoofing-attack#:~:text=A%20spoofing%20attack%20is%20when,can%20use%20to%20accomplish%20this (accessed: October 30, 2020).

44 “What is a Buffer Overflow Attack,” imperva, https://www.imperva.com/learn/application-security/buffer-overflow/#:~:text=Attackers%20exploit%20buffer%20overflow%20issues,files%20or%20exposes%20private%20information (accessed: October 30, 2020).

해킹공격이 끝나면 역추적 배제 단계로 보통 인증 우회 방식을 활용한다. 인증 우회란 인증이 요구하는 페이지의 인증을 통과하지 않고 접속을 우회할 수 있는 취약점을 공격하는 방법이다. 관리자 페이지에 접근하여 관리자 권한으로 모든 기능을 악용할 수 있게 되는데 이는 로그인하지 않고 관리자만이 이용할 수 있는 웹 페이지를 만들기 때문이다. SQL 인젝션 공격은 통상 정상적이지 않은 특정 SQL문을 넣어 공격하는 방법이다. 특정 SQL문이 삽입되면 그대로 데이터베이스에 전송되어 공격이 일어난다.[45] 크로스 사이트 스크립팅(XSS: Cross Cite Scripting)) 공격은 XSS 취약점을 갖고 있는 웹사이트에 악의적인 스크립트를 업로드하여 개인 컴퓨터를 공격하는 방법이다. 사용자 쿠키를 훔쳐 로그인하거나 브라우저를 제어한다. XSS 공격은 취약점이 있는 웹서버를 직접 공격하는 것이 아니라 제3자를 공격하는 공격 경유지의 성격을 갖고 있다. 해커의 공격은 웹 애플리케이션에 접근하는 사용자에게 XSS 취약점을 이용하여 자바스크립트를 실행할 수 있게 허용하면서부터 시작된다. XSS 공격을 통해 해커는 악성스크립트와 XSS 공격을 병행하여 사용자의 계정 정보를 탈취하고 탈취한 개인 정보를 도용함으로써 웹서버에 로그인하여 접근할 수 있게 된다.[46]

사회공학적 공격은 사람들의 취약점을 이용하여 공격하는 방법으로,

45 “SQL Injection,” Malwarebytes, https://www.malwarebytes.com/sql-injection/ (accessed: October 30, 2020).

46 “Cross Site Scripting (XSS),” OWASP, https://owasp.org/www-community/attacks/xss/ (accessed: October 30, 2020).

피싱(phishing) 공격은 일반적으로 위조, 변조된 웹사이트를 통해 다른 사람을 사칭하여 개인 정보를 공유하도록 속이는 방법이다. 파밍(pharming) 공격은 DNS 데이터를 위조, 변조하여 공격하는 방법으로 예를 들어 온라인 뱅킹 서비스를 이용하기 위해 특정 은행의 웹사이트에 접속하는 경우 해커는 웹사이트의 주소를 위조, 변조하여 금융 피해를 일으키는 것이다. 대부분의 경우 사람들의 취약점을 공략하여 악성코드를 사용자가 알아채지 못하게 전파하여 컴퓨터를 손상시키고, 개인 정보를 탈취, 도용한다.[47] 최근에는 코로나19 팬데믹의 영향으로 새로운 취약점을 공략하는 해킹이 급증하고 있는데 코로나19 상황을 악용해 사람들의 취약점을 공략하는 사회공학적 해킹이 많이 발생하였다. 과거에도 메르스와 에볼라 바이러스 발생 시 메르스 또는 에볼라 바이러스 관련 내용이 포함된 이메일과 문자메시지 등을 통해서 악성코드 유포가 증가했었다. 전 세계적으로 코로나19 팬데믹 상황을 활용하여 다양한 사이버공격이 시도되고 있다. 우선 코로나19 관련 내용을 미끼로 사용한 통신, 의료, 교육, 금융, 기술 분야에서의 랜섬웨어 공격이 크게 증가했다. 마이크로소프트(MS)사의 MS 시큐리트 인텔리전스 보고서에 따르면, 코로나19는 랜섬웨어의 공격 시간을 크게 단축시켰는데 이는 공격대상이 피해를 최소화하기 위해 비용을 신속히 지불했기 때문으로 1시간이 걸리지 않는 경우도 허다했다. 코로나19의 위기상황은 공격대상으로 하여금 협상을 신속히 진행하게 함으로써 랜섬웨어가 공격대상 시스템에 머무는 시간을 단축시켰다. 랜섬웨어 공격 방식은 이메일을 매개로 한 공격이 주를 이루었는데, MS, 아마존, 애플 등을 사칭한 URL을 사용

47 박대우, “국가사이버보안정책에서 해킹에 대한 소고,” pp. 23-40.

하였다. 그리고 신속하게 공격 도메인과 서버를 전환시키면서 자체 서버를 사용하기보다는 퍼블릭 클라우드 서비스(PCS)를 활용하였다. 구체적으로 메일이나 첨부파일 제목에 COVID19, MASK, WHO 등 코로나19 관련 단어를 넣어 피싱 사이트로 연결시켜 마스크를 주문하도록 하거나 첨부파일을 열어 악성코드에 감염시키는 등 다양한 방식을 사용하였다.[48]

3. 해킹 방법의 변화

해킹 방법의 변화를 살펴보면, 일반적으로 자료나 정보를 위조, 변조하는 공격 방법이 있다. 그리고 CPU와 입출력 장치의 속도 차이를 이용하여 공격하는 비동기성 공격 방법이 있다. 이 경쟁 조건 공격(Race Condition)은 특정 순서로 작업을 처리하도록 설계된 컴퓨팅 시스템이 여러 개의 작업을 동시에 진행해야 하는 경우 발생한다. 이 기술은 서비스가 시작되는 순간과 보안 제어가 적용되는 순간 사이의 시간 차이를 활용한다. 다중 스레드 응용 프로그램에 의존하는 이 공격은 신뢰할 수 없는 프로세스로 인한 간섭과 신뢰할 수 있는 프로세스로 인한 간섭 중 하나의 방법으로 전달될 수 있다. 적절한 제어가 없으면 서로 다른 프로세스가 서로 간섭할 수 있다. 웹 애플리케이션, 파일 시스템 및 네트워킹 환경은 모두 경쟁 조건 공격에 취약하다. 경쟁 조건 공격은 자주 발생하지 않지만 이러한 공격이 발생하면 시스템에 무단 권한을 부여하는 등

48 채재병 외, “코로나19 관련 사이버공격 양상 및 시사점,” pp. 1-2.

심각한 영향을 미칠 수 있다. 또한 경쟁 조건 공격은 본질적으로 탐지하기 어렵다.[49]

암호 해독 방법은 소프트웨어를 사용하여 암호 파일을 해독하여 접근하는 것으로 대표적인 트로이목마는 일반 프로그램을 변경시켜 심어놓음으로써 프로그램이 작동하면 사용자 몰래 정보를 탈취하거나 사용자의 모든 입력 정보를 알 수 있다. 트로이목마는 하나의 기능을 수행하는 것처럼 보이지만 실제로는 다른 악의적인 기능을 수행하는 기만적인 프로그램이다. 무료 소프트웨어, 비디오 또는 음악 또는 합법적인 광고로 위장 할 수 있다. 트로이목마 바이러스라는 용어는 기술적으로 정확하지 않다. 대부분의 정의에 따르면 트로이목마는 바이러스가 아니다. 바이러스는 자신을 다른 소프트웨어에 부착하여 확산되는 프로그램이고 트로이목마는 유용한 소프트웨어 또는 콘텐츠로 가장하여 확산된다. 많은 전문가들은 사용자 활동을 추적하고 로그 또는 데이터를 해커에게 다시 보내는 스파이웨어 프로그램을 트로이목마 유형으로 간주한다. 트로이목마는 해커를 위한 독립 실행형 도구로 작동하거나 다른 악의적인 활동을 위한 플랫폼이 될 수 있다. 예를 들어 트로이목마 다운로더는 해커가 피해자의 장치에 향후 페이로드(payload)를 전달하는 데 사용된다. 트로이목마 루트킷은 사용자의 장치 또는 회사 네트워크에 영구적인 존재를 설정하는 데 사용될 수 있다.[50]

위장 채널은 컴퓨터의 특성을 이용하여 네트워크를 이용한 통신채널

49 “RACE CONDITION,” VERACODE, https://www.veracode.com/security/race-condition (accessed: October 30, 2020).

50 “What is a Trojan? Is it a virus or is it malware?” Norton, https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html (accessed: October 30, 2020).

을 불법적으로 생성시켜 정보를 탈취한다. 또한 DoS 공격과 사용자에게 스팸 메일을 전송해 네트워크의 가용성을 마비시키고 업무를 마비시키기도 한다. 급속하게 발전하고 있는 스마트폰에 대한 공격을 살펴보면, 플랫폼 공격은 스마트폰 OS나 플랫폼 상의 취약점을 이용한 파생 공격을 시도하여 악성코드를 심음으로써 키보드나 메모리를 해킹할 수 있게 한다. 앱 공격은 악성코드와 달리 사용자가 인지하고 있는 실행 앱에 의한 공격으로 피싱, 파일 변조, DoS 및 디도스 공격이 있다. 스토리지 공격은 스마트폰 메모리에 탑재된 파일시스템에 접근하여 기밀정보를 추출하는 것이다. 한편 해커는 해킹툴이나 해킹 스크립터 등을 사용하기도 한다.[51]

백도어(back door)는 시스템에 접근하기 위한 정상적인 인증 절차를 무효화하는 악성 코드 유형인데 데이터베이스 및 파일 서버에 대한 원격 액세스가 허용되어 해커가 원격으로 시스템 명령을 실행할 수 있게 해준다. 백도어 설치는 웹 응용 프로그램에서 취약한 구성 요소를 활용하여 수행된다. 일단 설치되면 파일이 매우 난독화되는 경향이 있으므로 탐지가 어렵다. 백도어가 감지되더라도 일반적인 완화 방법으로는 이를 응용 프로그램에서 제거할 가능성이 거의 없다.[52]

백 오리피스(back orifice)는 윈도우 시스템을 손상시키는 데 사용되는 프로그램으로 인터넷을 통해 원격 위치에서 컴퓨터를 제어할 수 있도록 하는 원격 관리 도구에 적용된다. 자체적으로 서버로 설치되어 해커

51 박대우, “국가사이버보안정책에서 해킹에 대한 소고," pp. 23-40.

52 Robert Roohparvar, “WHAT IS A BACKDOOR ATTACK?” https://www.infoguardsecurity.com/what-is-a-backdoor-attack/#:~:text=The%20backdoor%20attack%20is%20a,plug%2Dins%20or%20input%20fields (accessed: October 30, 2020).

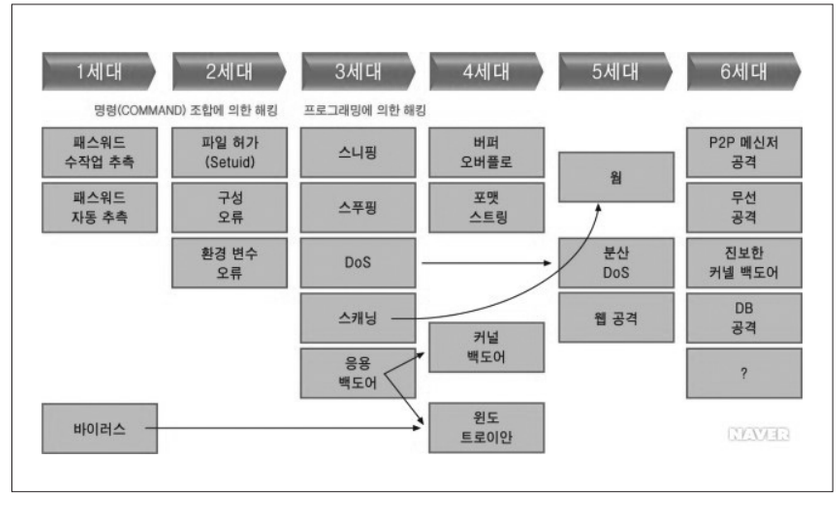
가 키보드에서 사용자보다 더 완벽하게 시스템을 조작할 수 있다. 따라서 시스템에 가할 수 있는 손상은 거의 무제한이다. 컴퓨터 시스템의 원격 관리를 가능하게 하는 프로그램인 백 오리피스의 기원은 합법적이었다. 백 오리피스의 문제점은 트로이목마를 통해 크래커를 실행하여 대상이 잘못된 점을 의심하지 않게 한다는 것이다. 설치 후 트로이목마는 원격 크래커가 대상 컴퓨터에 대한 거의 완전한 제어를 허용한다. 백 오리피스는 바이러스가 아니며 오히려 소프트웨어를 사용하기 전에 호스트에서 기꺼이 수락하고 실행해야한다. 백 오리피스는 종종 사용자가 이메일로 받거나 웹사이트에서 다운로드 할 수 있는 유효한 소프트웨어와 동일한 것임을 내세워 배포된다. 이 원격 관리 소프트웨어에 의해 손상된 정보 시스템은 특히 취약하며 해커는 일반적으로 사용자 또는 소유자만큼 시스템에 대한 액세스 권한을 얻을 수 있다.[53]

시스템 관리자가 구축해 놓은 보안망을 무력화시키는 해킹은 일반적으로 시스템 관리자의 권한을 불법적으로 획득하여 사용자에게 피해를 주게 된다. 해킹 기술은 1세대인 패스워드 수작업 추측이나 패스워드 자동 추측 등으로부터 스니핑, 스푸핑, 버퍼 오버플로, 백도어 등으로 발전되었고 현재는 분산서비스 거부 공격, 웹 공격, 메신저 공격, 무선 공격 등 5세대에서 6세대 이상으로 발전하고 있다.(〈그림 1〉 참조) 해킹 기법도 네트워크 서비스의 가용성에 대한 위협이 증가하고 유해 트래픽이 폭발적으로 증가하는 등 다양하게 발달하고 있다. 또한 기술적으로 시스템과 네트워크에 대한 이해가 높아야 가능했던 해킹이 이제는 자동화 툴

53 “Back Orifice,” F-Secure, https://www.f-secure.com/v-descs/backori.shtml (accessed: October 30, 2020).

이 개발되면서 일반화되고 있는 상황이다. 예전의 해킹 기술과 기법이 여전히 지속되는 속에서 지속적으로 발전된 새로운 형태의 기술과 기법의 등장으로 시스템 및 네트워크 해킹 방법은 셀 수 없는 수준에 이르렀다.

〈그림 1〉 해킹 기술의 발전[54]



54 “해킹 기술 동향,” 네이버, https://terms.naver.com/entry.nhn?docId=3432518&cid=58445&categoryId=58445 (검색일: 2020. 5. 24).

IV

해킹 주체, 기법, 대상별 분석

1. 주체
2. 기법
3. 대상

1. 주체

가. 개인 및 집단

해킹의 공격방식과 양상이 기술적인 발달로 다양해지면서 개인 차원의 해킹도 고도로 조직화되고 있어 중대한 안보위협으로 나타나고 있다. 또한 집단 차원의 국제적 해커집단의 해킹 역시 단순히 개인의 권리 등을 침해하여 피해를 주는 수준이 아닌 조직적인 테러의 수준에 이르고 있다. 해커집단 중 어나니머스의 경우는 IMF, 미국 법무부, 마스터카드와 같이 국제기구, 국가기관, 금융기관, 기업 등을 가리지 않고 해킹하였으며, 또다른 해커집단인 룰즈섹 또한 미국의 CIA, FBI 등을 해킹했다. 이처럼 개인 또는 국제 해커집단이 일으키는 해킹은 그 추세로 보아 지속적인 증가를 보일 것으로 예상된다. 따라서 이를 방지하기 위해서는 국가위기관리 차원에서의 대응이 필요하며 최근 해킹의 규모가 커지고 성격이 국가안보에 대해 위해를 미치는 수준에 이르렀으므로 이에 효과적으로 대응하기 위한 국가안보 차원에서의 대응이 요구된다.[55]

최근 안드로이드 기반 스마트폰의 경우 폭발적인 증가를 보이고 있고 이에 따라 스마트폰을 겨냥한 악성코드가 급증하고 있는 등 모바일 환경에 대한 해킹이 증가하고 있다. 악성코드를 활용하여 스마트폰에서 대화·통화 내용을 도청하거나 폰에 대한 공격 또는 폰을 거점으로 한 디도스 공격도 가능한 상황으로 특히 스마트폰에 이동통신서비스와 무선랜, 블루투스, GPS 등 다수의 통신기능이 가능해짐에 따라 사이버 침해가

55 채재병, “안보환경의 변화와 사이버안보,” p. 189.

발생할 경로가 다변화됨으로써 그에 따른 위협도 크게 증가하였다. 그 내용을 보면 우선 SNS를 통해서 다양한 해킹 피해가 증가했다. 페이스북, 트위터와 같은 SNS를 이용하여 개인 컴퓨터나 스마트폰에 악성코드를 유포하고, 피싱 및 스팸 메일을 발송하는 등 급격히 해킹의 빈도가 늘어났다. 특히 SNS에서 지인을 가장하여 금융 정보 등의 개인 정보를 절취하는 사회공학적 기법의 해킹이 증가하고 있다. 다음으로 폭발적으로 늘어나고 있는 클라우드 서비스에 대해서도 해킹 피해가 증가하고 있다. 클라우드 서비스는 매우 중요한 정보를 보관하고 있는데 이러한 정보에 대한 오남용이나 계정 또는 정보서비스에 대한 하이재킹, 그리고 내부자를 통한 정보유출 등 클라우드 서비스 환경에 대한 위협이 크게 증가했다. 클라우드 서비스와 연결된 PC나 스마트폰 등 어느 하나라도 해킹을 당하면 클라우드 서비스에 연결된 모든 단말 기기들에 대한 해킹이 가능하므로 매우 중대한 위협이라고 할 수 있다. 이외에도 가상화폐 시스템에 대한 위협, 자원공유 서비스에서의 장애발생 위협, 클라우드 서비스 클라이언트가 다양화됨에 따른 정보유출 위협, 정보의 분산 및 위탁에 따른 정보유출 위협, 분산처리에 따른 보안성 침해 위협 등이 있다. 마지막으로 악성코드를 이용하여 의료기기를 오작동시키거나 현금 인출기에서 불법 인출하거나 자동차 엔진의 작동을 정지시키는 등 융합 정보통신 산업에 대한 해킹이 증가했다. 방화벽, 무선 AP, 라우터, 스위치 등 네트워크 시스템에 대해서도 지속적으로 해킹을 시도하고 있다. 스마트폰, 스마트 TV, 태블릿 PC 등이 확산되면서 단말기 중심의 클라우드 컴퓨팅 시대에 접어들어 통신 네트워크에 대한 의존도가 과거에 비해 대폭

증대됨으로써 해킹의 잠재적 위협에도 크게 노출된 것이다.[56]

나. 국가

국가 차원의 해킹이 크게 증가하면서 해킹의 목표도 국가기능을 혼란시키고 상실시키는 것으로 변화했다. 해킹으로 인한 국가의 피해도 갈수록 확대되고 있는 상황이다. 과거 해킹이 금융권에 대한 해킹으로 금전적 이익을 추구했다면 이제는 금융권 해킹을 통해 대규모의 피해자를 발생시켜 인터넷 뱅킹을 전면 중단시키는 등 국가의 금융질서를 무너뜨리고 국가경제의 혼란을 야기하고 있다. 군사 및 외교 분야에서도 전자적으로 관리되는 주요 기밀정보들이 지속적으로 유출되고 있으며, 주요정보통신기반시설에 대한 해킹도 끊이지 않고 있다. 여전히 스턱스넷 악성코드가 매일 50~60건 이상 발견되고 있고 미국에서는 뱅크 오브 아메리카 등 대형은행과 구글이나 지메일 같은 인터넷 업체, 그리고 군수업체인 록히드 마틴 등이 해킹 피해를 입고 있다.

국가 차원의 해킹 사례를 보면, 1991년 걸프전에서 미국이 이라크의 방공망을 다운시킨 해킹이 최초의 사례로, 1999년 코소보 사태 때 나토가 유고를 공격하자 해커들이 나토군 사령부를 해킹하여 군 시스템을 교란시켰다. 1999년 유고 주재 중국 대사관 오폭사건에 대한 보복으로 중국 해커들이 미국 사이트를 해킹하면서 미중 간 사이버 공방이 시작되었다. 2001년 중국 전투기와 미군 정찰기 충돌사고로 중국 해커들이 미국에 대한 해킹을 시도했다. 2003년 이라크 침공 전 미군의 이라크 국

56 채재병,『국제 사이버공격 전개 양상 및 주요국 대응전략』, INSS 연구보고서 2019-18 (2019), pp. 60-62.

가정보시스템에 대한 해킹이 있었다. 2007년 이스라엘이 시리아 레이더 시스템을 해킹하여 시리아의 방공망을 무력화시켰다. 2007년 러시아가 에스토니아 정부 전산망을 디도스 공격하여 국가 주요기능을 마비시켰다. 2008년 조지아를 침공하기 전 러시아가 조지아 정부기관 웹사이트와 전산망 및 방위시설을 해킹하였다. 2010년 미국과 이스라엘이 이란 핵시설 시스템에 악성코드 스턱스넷을 침투시키는 해킹이 있었다. 2012년 이란의 미국과 사우디 및 카타르에 대한 해킹이 있었다. 2014년 크림반도 점령과정에서 러시아의 우크라이나에 대한 해킹으로 정부 전산망이 파괴되었다.[57]

미국이 주도한 이란 핵시설에 대한 해킹 이후에는 국가 차원의 조직화된 해킹이 크게 증가하였다. 그리고 사이버공간의 주도권을 획득하기 위한 대규모의 사이버무기 개발계획들이 진행되고 있어 바야흐로 사이버전이 본격화되고 있는 모습이다. 미군은 플랜-X라는 실전용 사이버무기 개발 프로젝트를 진행하고 있는데, 플랜 X는 사이버공격 능력이 크게 높아지고 있는 상황에서 소극적 방어로는 이를 막을 수 없다는 인식을 바탕으로 하고 있다. 목적은 적의 컴퓨터를 교란하여 전투력을 지원하는 것으로 적군의 레이더망과 통신을 방해함으로써 공격효과를 극대화하는 것이다. 플랜 X는 전 세계의 PC위치를 담은 사이버 전자지도를 작성하여 공격에 대해 즉각 반격할 수 있는 경로를 시각화하여 신속한 결정을 지원할 수 있다. 또한 별도의 조작 없이 필요할 때 정해진 순서에 따라 자동으로 사이버공격을 가할 수 있는 시스템이기도 하다.[58] 중국의 경우도 사이버전에 대비하여 사이버 전력 양성에 중점을 두고 추진하고 있다. 영국도 스턱스넷을 계기로 사이버안보를 국가안보전략의 최우선 순위에 올려놓았고, 사이버무기 프로그램을 개발 중에 있다. 일본 역시 역추적을 통해 공격 근원지를 파괴하는 바이러스를 개발 중이다. 이스라엘도 적국에 대한 공격을 위해 사이버공간을 활용하고 있으며 이란도 대미 사이버전을 강화하고 있고, 인도는 사이버전에 대비하여 사이버 전력을 양성하고 있다.

57 김상배, 『사이버 안보의 세계정치와 한국: 버추얼 창과 그물망 방패』, (서울: 한울아카데미, 2018), pp. 118-120.

58 *Monthly Issue of National Cyber Security*, Vol. 06. (2012), pp. 220-222.

국가안보영역이 사이버공간으로 확대되면서 첨단기술을 보유한 국가에서는 기술유출 범죄가 급격히 증가하고 있다. 중국은 사이버기술을 활용하여 정보 수집에 집중하고 있고, 중국 해커들은 미국의 산업기밀 유출을 시도했다. 사이버전 양상이 방어에서 공격으로 변화하고 있어 이에 대응하기 위해서는 국가 차원의 사이버전을 대비할 필요가 있다. 북한의 경우에도 해커 조직이 피싱 사이트를 통해 금융 정보를 절취하여 공작자금을 마련한 사례가 있었다. 북한은 유투브, 트위터 등 인터넷 매체를 이용하여 대남 사이버 심리전을 전개하고 있으며 북한의 사이버정찰조가 한국군의 전산망을 해킹하기도 했다. 향후 북한의 해킹은 급증할 가능성이 높은데 북한의 사이버전 능력은 이미 상당한 수준이며 정찰총국 산하에 7,000명 이상의 해커를 배치하고 있는 것으로 알려져 있다.[59]

59 채재병, 『국제 사이버공격 전개 양상 및 주요국 대응전략』, pp. 62-64.

2. 기법

해킹 기법은 크게 원격지에서 시도하는 네트워크 해킹과 시스템에 직접 들어간 다음 시도하는 로컬 해킹으로 나누어진다. 네트워크 해킹은 파일을 획득하거나 변경하기 위해 시도되며, 로컬 해킹은 시스템에 접근한 해커가 그 시스템 관리자의 권한을 획득하기 위해 시도된다. 이러한 해킹 시도는 탐지, 스캐닝, 인증 등과 정보에 대한 획득, 변경, 파괴 등으로 이루어진다.[60]

가. 서비스 거부(DoS)

야후나 이베이 등에 대한 해킹으로 유명해진 공격 방법으로, 하나의 시스템에서 다량의 패킷을 집중적으로 보내서 다른 시스템을 마비시키는 것부터 분산된 수많은 시스템에서 하나의 시스템을 공격하는 분산 서비스 거부(DDoS: Distribute Denial of Service)) 공격까지 다양하다. 이 해킹 방법은 시스템을 중단시키거나 방해하는 것이지 정보나 자료의 획득이나 시스템 자원의 획득 등을 노린 고난도의 해킹 방법은 아니다. 디도스 공격은 인터넷 트래픽이 넘쳐 대상 또는 주변 인프라를 압도하게 하여 대상 서버나 서비스 또는 네트워크의 정상 트래픽을 방해하려는 악의적인 시도이다. 디도스 공격은 손상된 여러 컴퓨터 시스템을 공격 트래픽의 소스로 활용하여 효율성을 달성한다. 악용된 컴퓨터에는 컴퓨터는 물론 IoT 장치와 같은 기타 네트워크 리소스가 포함될 수 있다. 높은 수준에서 디도스 공격은 예상치 못한 교통 체증이 고속도로를 막아 일반 트래픽이 목적지에 도달하지 못하게 하는 것과 같다.[61]

디도스 공격은 인터넷에 연결된 컴퓨터 네트워크를 통해 수행되는데 이러한 네트워크는 멀웨어(malware)에 감염된 컴퓨터 및 IoT 장치 등 기타 장치로 구성되어 해커가 원격으로 제어할 수 있다. 이러한 개별 장치를 봇(bot) 또는 좀비(zombie)이라고 하며 봇 그룹을 봇넷(botnet)이라고 한다. 봇넷이 설정되면 해커는 각 봇에 원격 명령을 전송하여 공격을 지시할 수 있다. 피해자의 서버 또는 네트워크가 봇넷의 대상이 되면 각 봇은 대상의 IP 주소로 요청을 전송하여 서버 또는 네트워크가 압도될 수 있으며 결과적으로 정상적인 트래픽에 대한 서비스 거부가 발생한다. 각 봇은 합법적인 인터넷 장치이기 때문에 공격 트래픽을 정상적인 트래픽과 분리하기가 어려울 수 있다.

디도스 공격의 가장 명백한 증상은 사이트 또는 서비스가 갑자기 느려지거나 사용할 수 없게 되는 것이다. 그러나 트래픽의 합법적인 급증과 같은 여러 원인으로 인해 유사한 성능 문제가 발생할 수 있으므로 일반적으로 추가 조사가 필요하다. 트래픽 분석 도구를 사용하면, 단일 IP 주소 또는 IP 범위에서 발생하는 의심스러운 트래픽 양, 기기 유형, 지리적 위치 또는 웹브라우저 버전과 같은 단일 행동 프로필을 공유하는 사용자의 트래픽 홍수, 단일 페이지 또는 엔드 포인트에 대한 설명할 수 없는 요청의 급증, 하루 중 홀수 시간에 급증하거나 10분마다 급증하는 등 부자연스럽게 보이는 패턴과 같은 이상한 트래픽 패턴과 같은 디도스 공격

60 김창범, “해킹기법의 동향,"『정보과학회지』, 18(9), (2000), pp. 45-52.

61 “What is a DDoS Attack?” CLOUDFLRE, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (accessed: October 30, 2020).

의 징후를 발견할 수 있다.[62]

디도스 공격은 단순히 대용량 디도스 공격이라는 형태로 발전하고 있다. 최근에 나타나고 있는 DNS를 대상으로 하는 디도스 공격이 대표적인 사례이다. 그런데 웹서버에 대한 디도스 공격이 실패하게 되는 경우 공격 대상 웹서버의 주소 정보를 갖고 있는 DNS로 목표를 전환하게 되는데 이러한 사례들이 실제로 다수 발생하고 있다. DNS가 저장하고 있는 도메인 정보는 보통 수만 개 이상이기 때문에 전산장애가 발생할 경우 웹서버에 대한 공격으로 인한 피해보다 파급효과가 매우 크다. 그리고 위조가 수월한 UDP 프로토콜을 사용하는 DNS 구조의 특성으로 인해 DNS 대상 디도스 공격은 방어한다는 것이 사실상 거의 불가능하다. 그렇기 때문에 웹서버에 비해 상대적으로 취약한 DNS에 대한 공격을 더욱 강화시키고 있는 실정이다.[63]

국내외에서 스마트폰 사용자가 증가하고 있어 모바일 기기가 해킹에 사용될 가능성도 매우 커지고 있다. 모바일 환경을 이용한 디도스 공격을 현재까지 실제로 감행한 사례는 거의 없다고 할 수 있지만 모바일 기기를 대상으로 하는 악성코드가 급격히 증가하는 점을 고려할 때 모바일 기기를 해킹에 사용할 가능성은 매우 높아지고 있다고 할 수 있다.

최근에 디도스 공격이 정해진 공격기법을 사용하고, 공격기법이 미미한 발전수준을 보이고 있더라도 항상 공격자는 방어자보다 앞선다는 사실이 중요하다. 아무리 디도스 공격에 대한 방어 환경을 구축해 놓았다 하더라도 항상 기존의 대응 방안들을 피해서 진화된 공격기법을 통해 디

62 Ibid.

63 한국인터넷진흥원, 『민간분야 침해사고 동향』, (2013. 3).

도스 공격을 할 것이다. 이를 해결하기 위해서는 공격대상 자원의 종류와 가용성 등을 파악하여 해당 자원을 보호할 수 있는 방어정책을 수립하고, 신기술이나 새로운 공격유형을 연구하여 효과적인 대응방안을 마련해야 할 것이다.[64]

나. 취약성을 이용한 공격

취약성을 이용한 공격은 사람들이 같은 부분에서 실수를 하는 특징을 이용한 것이다. 취약성에 대처하기 위해서 취약성을 해결하기 위한 방안들이 제시되고 있지만 실제로 이러한 방안들을 적용하는 시스템들은 그리 많지 않다. 대부분의 시스템들이 다양한 취약성을 가지고 있다고 할 수 있는데 네트워크를 통한 접근에 취약성이 있다면 이것은 해킹 성공 확률을 아주 높여준다고 할 수 있다. 보안 소프트웨어도 이런 취약성이 있기 때문에 안전하게 보호하는 장치를 하였다고 하여도 지속적으로 해킹 피해가 나오고 있는 것이다.[65]

지능형 지속 위협(APT)은 침입자 또는 침입자 팀이 매우 민감한 데이터를 추출하기 위해 네트워크에 불법적이고 장기적인 존재를 설정하는 공격이다. 매우 신중하게 선택되고 연구되고 있는 이러한 공격의 대상은 일반적으로 대기업이나 정부 네트워크를 포함한다. 그러한 침입의 결과는 영업비밀 또는 특허와 같은 지적재산 도용, 직원 및 사용자 개인 데이터와 같은 중요한 정보 손상, 데이터베이스 삭제와 같은 중요한 조직 인

64 채재병, 『국제 사이버공격 전개 양상 및 주요국 대응전략』, pp. 58-60.

65 김창범, "해킹기법의 동향," pp. 45-52.

프라의 파괴, 총 사이트 인수 등이다. APT 공격을 실행하려면 표준 웹 애플리케이션 공격보다 더 많은 리소스가 필요하다. 해커들은 대개 상당한 재정적 지원을 받고 있는 경험 많은 사이버 범죄자들의 팀이다. 일부 APT 공격은 정부 지원으로 사이버전 무기로 사용되기도 한다.[66]

APT 공격은 기존의 웹 애플리케이션 위협과 달리 훨씬 더 복잡하고 일단 네트워크가 침투되면, 가능한 한 많은 정보를 얻기 위해 해커가 남는다. 특정 표적에 대해 수동으로 실행하고 다수의 목표물에 대해 무차별적으로 공격한다. 그들은 종종 특정 부분과 반대로 전체 네트워크에 침투하는 것을 목표로 한다. 원격 파일포함(RFI), SQL 주입, 크로스 사이트 스크립팅(XSS) 등 보다 일반적인 공격은 해커가 대상 네트워크에서 발판을 마련하기 위해 자주 이용된다. 다음으로 트로이목마와 백도어 공격은 종종 그 거점을 확장하고 목표된 경계선 내에서 지속적인 존재감을 형성하기 위해 사용된다.

성공적인 APT 공격은 네트워크 침투, 해커의 존재 확대, 축적된 데이터의 추출의 세 단계로 구분할 수 있다. 1단계 침투에서 기업은 일반적으로 웹 자산, 네트워크 리소스 또는 공인된 인적 사용자라는 세 가지 공격 영역 중 하나를 침투한다. 이는 RFI, SQL 주입 등 악성 업로드 또는 스피어 피싱 등 사회공학적 공격 그리고 기업이 정기적으로 직면하는 위협을 통해 달성된다. 또한, 해커는 그들의 목표에 대해 디도스 공격을 동시에 실행할 수도 있다. 이는 네트워크 인력의 주의를 분산시키는 연막 역할을 하며 보안 경계를 약화시켜 침입을 용이하게 하는 수단 역할을

66 “Advanced persistent threat (APT),” imperva, https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/#:~:text=An%20advanced%20persistent%20threat%20(APT,to%20mine%20highly%20sensitive%20data (accessed: October 30, 2020).

한다. 초기 액세스가 완료되면 해커는 네트워크 액세스를 허용하고 원격의 스텔스 작동을 허용하는 멀웨어인 백도어 쉘을 신속하게 설치한다. 백도어는 또한 트로이목마가 합법적인 소프트웨어 조각으로 위장된 형태로 올 수도 있다.

2단계 확장은 해커가 거점이 구축된 후 네트워크 내에서 존재감을 넓히기 위해 이동한다. 이것은 조직의 계층을 높여서 직원들이 가장 민감한 데이터에 접근하는 것을 방해하는 것을 포함한다. 이를 통해 제품군 정보, 직원 데이터, 재무 기록 등 중요한 비즈니스 정보를 수집할 수 있다. 궁극적인 공격 목표에 따라, 축적된 데이터는 경쟁 기업에 팔리거나, 기업의 제품 라인을 파괴하도록 변경하거나, 조직 전체를 무너뜨리는 데 사용될 수 있다. 사보타주가 동기일 경우, 이 단계는 복수의 중요 기능에 대한 제어권을 미묘하게 획득하고 특정 순서에 따라 조작하여 최대의 피해를 유발하는 데 사용된다. 예를 들어, 해커는 복구 프로세스를 연장하기 위해 회사 내의 전체 데이터베이스를 삭제한 다음 네트워크 통신을 중단시킬 수 있다.

3단계 추출은 APT 공격이 진행되는 동안, 도난당한 정보는 일반적으로 네트워크 내부의 안전한 위치에 저장되어 피해를 당한다. 일단 충분한 자료가 수집되면, 해커들은 감지되지 않고 그것을 추출해야 한다. 일반적으로 화이트 노이즈 전술은 보안 팀의 주의를 분산시키기 위해 사용되므로 정보가 외부로 이동될 수 있다. 이것은 디도스 공격의 형태를 취할 수 있으며, 네트워크 인력을 다시 묶거나 추출을 용이하게 하기 위해 사이트 방어력을 약화시킬 수 있다.[67]

67 Ibid.

APT 공격 시, 해킹 성공 확률을 크게 제고할 수 있기 때문에 취약점을 이용한 APT 공격은 매우 선호되는 해킹 방법이다. 소프트웨어를 대상으로 한 취약점 공격은 국내 환경에 특화된 주요 소프트웨어의 취약점이 계속 발견되고 있어 이를 이용한 공격도 증가하고 있다. 모바일 환경에 대한 취약점 공격도 스마트폰 등 모바일 기기를 통한 인터넷 접속이 증가하고, PC가 담당하던 업무를 모바일 기기가 대신하게 되면서 PC에서 이루어지던 취약점을 이용한 공격이 모바일 환경에서 발생하고 있다.[68]

다. 스니핑(Sniffing)

스니핑은 패킷 스니퍼를 이용해 컴퓨터 네트워크를 통과하는 모든 데이터 패킷을 모니터링하고 캡처하는 과정이다. 스니핑은 네크워크 상에서 오고가는 패킷들을 몰해 엿보는 것으로 사용자의 계정과 패스워드를 알아내기 위해 쓰이는 방법이다. 이 방법은 주요한 시스템을 해킹한 이후 많은 계정과 패스워드를 알아낼 수 있다. 스니핑은 네트워크 디바이스를 열어서 지나가는 모든 패킷을 읽는다. 대부분의 시스템들이 암호화된 통신을 하지 않기 때문에 스니핑으로 빼낼 수 있는 정보는 많다. 암호화를 하는 통신은 스니핑으로 빼낸 정보를 복호화하지 못하면 내용을 전혀 볼 수 없으므로 안전하다고 할 수 있다. 패킷 스니퍼는 네트워크 관리자가 네트워크를 통과하는 데이터 트래픽을 추적하기 위해 사용한다. 이를 네트워크 프로토콜 분석기라고 한다. 이와 마찬가지로 악의적인 해커는 이러한 패킷 스니핑 도구를 사용하여 네트워크에서 데이터 패킷

68 채재병, 『국제 사이버공격 전개 양상 및 주요국 대응전략』, p. 57.

을 캡처한다. 네트워크에서 캡처한 데이터 패킷은 암호, 사용자 이름, 신용카드 정보 등 민감한 정보를 추출해 빼내는 데 사용된다. 해커는 이러한 스니퍼를 소프트웨어 또는 하드웨어의 형태로 시스템에 설치한다. 사용되는 스니핑 도구는 여러 종류가 있으며 와이어샤크, 에터캡, 베터캡, Tcpdump, WinDump 등이 있다.[69]

스니핑에서 해커는 네트워크의 데이터 트래픽에 귀를 기울이고 패킷 스니퍼를 사용하여 데이터 패킷을 캡처한다. 스푸핑에서 해커는 사용자의 자격 증명을 도용하여 시스템에서 합법적인 사용자로 사용한다. 스푸핑 공격은 해커가 사용자와 시스템 중간에 들어가기 때문에 중간자 공격이라고도 한다. 스니핑 공격에는 능동적인 스니핑과 수동적인 스니핑이 있다. 능동적인 스니핑은 스위치 네트워크에서 수행되는 스니핑이다. 스위치는 두 개의 네트워크 장치를 함께 연결하는 장치다. 스위치는 원하는 대상 포트로 정보를 전달하기 위해 미디어 액세스 제어 주소를 사용한다. 해커는 트래픽을 LAN에 주입하여 스니핑을 활성화함으로써 이를 이용한다. 수동적인 스니핑은 스위치 대신 허브를 사용한다. 허브는 대상 데이터 포트를 읽기 위해 미디어 액세스 제어 주소를 사용하는 스위치와 동일한 방식으로만 작동한다. 해커가 해야 할 일은 단순히 LAN에 접속하기만 하면 그들은 그 네트워크에서 데이터 트래픽을 감지할 수 있다. 해커가 전자 메일 트래픽, FTP 암호, 웹 밀거래, 텔넷 암호, 라우터 구성, 채팅 세션, DNS 트래픽 등 정보에 접근할 수 있기 때문에 스니핑은 사용자나 네트워크 시스템에 해롭다.

스니핑 공격을 방지하기 위해서는 사용자는 신뢰할 수 없는 네트워크,

69 “WHAT ARE SNIFFING ATTACKS AND THEIR TYPES?”

즉 무료 공용 Wi-Fi를 포함하는 보안되지 않은 네트워크에 연결하는 것을 피해야 한다. 이러한 보안되지 않은 네트워크는 해커가 전체 네트워크를 스니핑 할 수 있는 패킷 스니퍼를 배치할 수 있기 때문에 위험하다. 암호화는 해커로부터 메시지를 보호하기 위해 일반 텍스트를 읽지 못하게 변환하는 과정이다. 네트워크를 떠나기 전에, 정보를 암호화하여 네트워크에 접근하는 해커로부터 보호해야 한다. 이는 가상 사설망(VPN)의 사용을 통해 달성된다. 네트워크 관리자는 의심스러운 트래픽을 감지하기 위해 네트워크를 검색하고 모니터링 해야 한다. 이는 대역폭 모니터링 또는 장치 감사를 통해 달성할 수 있다.[70]

라. 스푸핑(Spoofing)

스푸핑은 알려지지 않은 출처로부터의 통신을 알려진 신뢰할 수 있는 출처로부터 온 것으로 위장하는 행위다. 스푸핑은 이메일, 전화 통화 및 웹사이트에 적용되거나 컴퓨터가 IP 주소, 주소 확인 프로토콜(ARP) 또는 DNS 서버 스푸핑과 같은 보다 기술적인 것일 수 있다. 스푸핑은 대상의 개인 정보에 대한 접근권한 획득, 감염된 링크나 첨부파일을 통한 악성코드 확산, 네트워크 접속 제어 우회, 트래픽 재분산 등을 통해 DoS 공격을 실시하는 데 이용될 수 있다. 스푸핑은 종종 진보된 지속적인 위협이나 중간 공격과 같은 더 큰 사이버 공격을 실행하기 위해 접근하는 방법이다. 조직에 대한 공격이 성공하면 감염된 컴퓨터 시스템과 네트워크, 데이터 침해 또는 매출 손실로 이어질 수 있으며, 이는 모두 조직의

70 Ibid.

공적인 평판에 영향을 미치기 쉽다. 또한 인터넷 트래픽의 재라우팅으로 이어지는 스푸핑은 네트워크를 압도하거나 고객을 정보 도용이나 악성코드 배포를 목적으로 하는 악의적인 사이트로 이끌 수 있다. 스푸핑은 다양한 커뮤니케이션 방법에 적용이 가능하며 다양한 수준의 기술 노하우를 활용할 수 있다. 스푸핑은 개인이나 조직으로부터 민감한 정보를 얻기 위해 스캠 인 피싱 공격을 수행할 수 있다.[71]

스푸핑 공격 방법을 살펴보면, 이메일 스푸핑은 해커가 전자 메일 메시지를 사용하여 수신자를 속여 알려진 또는 신뢰할 수 있는 출처로부터 온 것으로 생각하도록 할 때 발생한다. 이러한 전자 메일에는 악성 웹사이트나 악성코드에 감염된 첨부 파일에 대한 링크가 포함될 수 있으며, 수신자가 중요한 정보를 자유롭게 공개하도록 사회공학을 사용할 수도 있다. 발신자 정보는 스푸핑하기 쉽고 다음 두 가지 중 하나의 방법으로 수행될 수 있다. 원본과 약간만 다르게 나타나는 대체 문자나 숫자를 사용하여 신뢰할 수 있는 전자 메일 주소 또는 도메인을 모방하거나 시작 필드를 알려진 소스 또는 신뢰할 수 있는 소스의 정확한 전자 메일 주소로 위장한다. 발신자 ID 스푸핑을 사용하면 해커가 수신자에게 알려지거나 신뢰되는 번호 또는 특정 지리적 위치를 나타내는 번호인 특정 번호에서 걸려오는 전화인 것처럼 보이게 할 수 있다. 해커는 종종 은행이나 고객 지원에서 온 사람으로 가장하는 사회공학을 사용하여 전화로 공격 대상을 설득하여 암호, 계정 정보, 사회 보장 번호 등과 같은 민감한 정보를 빼낼 수 있다. 웹사이트 스푸핑은 웹사이트가 사용자가 알거나 신뢰하는 기존 사이트를 모방하도록 설계된 경우를 말한다. 해커는 이러

71 “SPOOFING ATTACK: IP, DNS & ARP.”

한 사이트를 사용하여 사용자로부터 로그인 및 기타 개인 정보를 얻는다. 해커는 컴퓨터 IP 주소를 위장하기 위해 IP 스푸핑을 사용할 수 있어 송신자의 신원을 숨기거나 다른 컴퓨터 시스템을 사칭할 수 있다. IP 주소 스푸핑의 한 가지 목적은 IP 주소를 기반으로 사용자를 인증하는 네트워크에 접속하는 것이다. 그러나 해커는 DoS 공격에서 대상의 IP 주소를 스푸핑하여 트래픽으로 피해자를 압도하는 경우가 더 많다. 해커는 패킷을 여러 네트워크 수신자에게 전송하며, 패킷 수신자가 응답을 전송하면 대상의 스푸핑된 IP 주소로 라우팅된다.[72]

주소 확인 프로토콜(ARP, Address Resolution Protocol)은 데이터 전송을 위해 IP 주소를 MAC(Media Access Control) 주소로 결정하는 프로토콜이다. ARP 스푸핑은 해커가 해당 IP 주소와 연결된 소유자에 대한 데이터를 수신할 수 있도록 해커의 MAC을 합법적인 네트워크 IP 주소에 연결하는 데 사용된다. ARP 스푸핑은 일반적으로 데이터를 훔치거나 수정하는 데 사용되지만 서비스 거부 및 중간 공격이나 세션 가로채기에도 사용할 수 있다. DNS 서버는 해당 IP 주소로 URL 및 전자 메일 주소를 결정한다. DNS 스푸핑은 해커가 트래픽을 다른 IP 주소로 우회시켜 피해자를 악성코드를 퍼뜨리는 사이트로 유도한다.[73]

마. 버퍼 오버플로우(Buffer Overflow)

버퍼 오버플로우는 프로그램에서 메모리 버퍼를 넘치게 해서 이상 동작하게 만드는 기법이다. 버퍼는 데이터가 한 위치에서 다른 위치로 전송되는 동안 일시적으로 데이터를 보유하는 메모리 저장 영역이다. 버퍼 오버플로우 또는 버퍼 오버런(buffer overrun)은 데이터 볼륨이 메모리 버퍼의 저장 용량을 초과할 때 발생한다. 결과적으로 버퍼에 데이터를 쓰려는 프로그램은 인접한 메모리 위치를 덮어 쓴다. 예를 들어 로그인 자격 증명을 위한 버퍼는 사용자 이름과 암호 입력 8 바이트를 예상하도록 설계될 수 있으므로 트랜잭션에 예상보다 2 바이트 더 많은 10 바이트 입력이 포함되면 프로그램은 초과분을 쓸 수 있다. 버퍼 오버플로우는 모든 유형의 소프트웨어에 영향을 미칠 수 있다. 일반적으로 잘못된 입력 또는 버퍼에 충분한 공간을 할당하지 못한 경우 발생한다. 트랜잭션이 실행 코드를 덮어쓰면 프로그램이 예기치 않게 작동하고, 잘못된 결과로 메모리 액세스 오류 또는 충돌을 생성 할 수 있다. 해커는 응용 프로그램의 메모리를 덮어써서 버퍼 오버플로우 문제를 악용한다. 이것은 프로그램의 실행 경로를 변경하여 파일을 손상시키거나 개인 정보를 노출하는 응답을 보내게 한다. 예를 들어 해커는 추가 코드를 도입하여 IT 시스템에 대한 액세스 권한을 얻기 위해 응용 프로그램에 새로운 명령을 보낼 수 있다. 해커가 프로그램의 메모리 레이아웃을 알고 있으면 버퍼가 저장할 수 없는 입력을 의도적으로 공급하고 실행 코드가 있는 영역을 덮어쓰고 이를 자신의 코드로 대체할 수 있다. 예를 들어, 해커는 프로그램을 제어하기 위해 메모리의 다른 영역을 가리키는 개체인 포인터를 덮어쓰고 공격 페이로드를 가리킬 수 있다.[74]

72 Ibid.

73 Ibid.

74 “What is a Buffer Overflow Attack.”

바. 트로이목마(Trojan Horse)

트로이목마는 하나의 기능을 수행하는 것처럼 보이지만 실제로는 다른 악의적인 기능을 수행하는 기만적인 프로그램이다. 무료 소프트웨어, 비디오 또는 음악 또는 합법적인 광고로 위장할 수 있다. 트로이목마 바이러스라는 용어는 기술적으로 정확하지 않다. 대부분의 정의에 따르면 트로이목마는 바이러스가 아니다. 바이러스는 자신을 다른 소프트웨어에 부착하여 확산되는 프로그램이고 트로이목마는 유용한 소프트웨어 또는 콘텐츠로 가장하여 확산된다. 많은 전문가들은 사용자 활동을 추적하고 로그 또는 데이터를 해커에게 다시 보내는 스파이웨어 프로그램을 트로이목마 유형으로 간주한다. 트로이목마는 해커를 위한 독립 실행형 도구로 작동하거나 다른 악의적인 활동을 위한 플랫폼이 될 수 있다. 예를 들어 트로이목마 다운로더는 해커가 피해자의 장치에 향후 페이로드를 전달하는 데 사용된다. 트로이목마 루트킷은 사용자의 장치 또는 회사 네트워크에 영구적인 존재를 설정하는 데 사용될 수 있다.[75]

트로이목마 유형을 살펴보면, 다운로더 트로이목마는 루트킷, 랜섬웨어 또는 키로거(keylogger)와 같은 기타 악성 코드를 다운로드하고 배포한다. 많은 유형의 랜섬웨어는 사용자의 컴퓨터에 설치하고 다른 멀웨어 구성 요소를 배포하는 다운로더 트로이목마인 드로퍼를 통해 스스로를 배포한다. 드로퍼는 종종 다단계 트로이목마 공격의 첫 번째 단계이며, 해커에게 내부 시스템에 지속적인 발판을 제공하는 또 다른 유형의 트로이목마를 설치한다. 예를 들어 드로퍼를 사용하여 민감한 서버에 백

75 Ibid.

도어 트로이목마를 주입할 수 있다. 백도어 트로이목마는 비밀 통신 터널을 열어 로컬 멀웨어 배포가 해커의 명령 및 제어 센터와 통신할 수 있도록 한다. 해커가 장치를 제어하고 데이터를 모니터링 또는 도용하고 다른 소프트웨어를 배포할 수 있다. 스파이웨어는 사용자 활동을 관찰하여 계정 자격 증명이나 은행 세부 정보와 같은 중요한 데이터를 수집하는 소프트웨어다. 그들은 이 데이터를 해커에게 다시 보낸다. 스파이웨어는 일반적으로 유용한 소프트웨어로 위장하므로 보통 트로이목마의 한 유형으로 간주된다. 루트킷 트로이목마는 시스템에 대한 루트 수준 또는 관리 액세스 권한을 획득하고 운영체제와 함께 또는 운영체제 이전에도 부팅된다. 이로 인해 탐지 및 제거가 매우 어렵다. 디도스 트로이목마는 피해자의 장치를 더 큰 봇넷에 참여하는 좀비로 만든다. 해커의 목표는 가능한 한 많은 시스템을 수집하여 장치 소유자 모르게 악의적인 목적으로 사용하는 것이다. 일반적으로 DoS 또는 디도스 공격의 일환으로 서버에 가짜 트래픽을 범람시키는 것이다.[76]

사. 백도어(Back Door)

백도어는 시스템에 액세스하기 위한 정상적인 인증 절차를 무효화하는 악성 코드 유형이다. 결과적으로 데이터베이스 및 파일 서버와 같은 애플리케이션 내의 리소스에 대한 원격 액세스가 허용되어 해커가 원격으로 시스템 명령을 실행하고 멀웨어를 업데이트 할 수 있는 기능을 제공한다. 백도어 설치는 웹 응용 프로그램에서 취약한 구성 요소를 활용

76 Ibid.

하여 수행된다. 일단 설치되면 파일이 매우 난독화되는 경향이 있으므로 탐지가 어렵다. 웹 서버 백도어는 데이터 도난, 웹사이트 훼손, 서버 하이재킹, 디도스 공격 시작, 웹사이트 방문자 감염(워터 링 홀 공격), APT 공격, 백도어 트로이목마 설치 등과 같은 여러 악의적인 활동에 사용된다.[77]

가장 널리 사용되는 백도어 설치 방법은 외부 스크립트를 동적으로 참조하는 애플리케이션 내의 취약점을 악용하는 공격 벡터인 원격 파일 포함(RFI)을 포함한다. RFI 시나리오에서 참조 기능은 원격 호스트에서 백도어 트로이목마를 다운로드하도록 속인다. 해커는 일반적으로 스캐너를 사용하여 대상을 식별한다. 스캐너는 파일 삽입을 가능하게 하는 패치되지 않았거나 오래된 구성 요소가 있는 웹사이트를 찾는다. 그런 다음 성공적인 스캐너는 취약점을 악용하여 기본 서버에 백도어를 설치한다. 일단 설치되면 주입을 가능하게 하는 취약성이 패치된 이후에도 언제든지 액세스 할 수 있다.

백도어 트로이목마 주입은 종종 특정 크기 이상의 파일 업로드를 방지하는 보안 규칙을 우회하기 위해 2단계 프로세스로 수행된다. 첫 번째 단계는 원격 위치에서 더 큰 파일을 검색하는 유일한 기능을 하는 작은 파일인 드로퍼를 설치하는 것이다. 두 번째 단계로 서버에 백도어 스크립트를 다운로드하고 설치하는 단계를 시작한다. 일단 설치되면 백도어를 제거하기가 매우 어렵다. 일반적으로 탐지에는 소프트웨어 스캐너를 사용하여 서버 파일 시스템에서 알려진 멀웨어 서명을 검색하는 것이 포함된다. 그러나 이 프로세스는 오류가 발생하기 쉽다. 백도어 쉘 파일은

77 Robert Roohparvar, “WHAT IS A BACKDOOR ATTACK?”

거의 항상 별칭 이름과 코드 난독화를 사용하여 마스킹된다. 많은 애플리케이션이 타사 플러그인을 사용하는 외부 프레임 워크에 구축되어 있기 때문에 감지는 더욱 복잡하다. 이들은 때때로 취약점이나 내장된 백도어로 가득 차 있다. 휴리스틱 및 서명 기반 규칙에 의존하는 스캐너는 이러한 프레임 워크에서 숨겨진 코드를 감지하지 못할 수 있다. 백도어가 감지되더라도 일반적인 완화 방법으로는 이를 응용 프로그램에서 제거할 가능성이 거의 없다.[78]

아. 지능화된 악성코드

사이버공간에서 지능화된 악성코드에 의한 타겟 공격이 크게 증가하고 있다. 악성코드는 기업 또는 기관 등 공격대상이 사용하는 소프트웨어의 미공개된 취약점을 활용한다. 그리고 소프트웨어의 업데이트 서버를 해킹하여 변조된 업데이트 파일을 업로드 하는 등 그 수단이 고도로 진화하고 있다. 지속적인 악성코드 공격을 위해 발전된 은폐기술도 사용하고 있다. 백신을 피해 잠복하거나 발견 시 치료를 힘들게 하기 위해 감염형 악성코드와 루트킷이 같이 합쳐진 형태로 공격에 사용되고 있다. 또한 정보유출에 관련되어 사용된 통신채널이 탐지되지 않도록 하기 위해 정상 트래픽과 구별할 수 없는 네트워크 통신도 사용하고 있다. 공격대상도 2010년의 스턱스넷 악성코드와 같이 발전소, 원자력, 수도 등 주요 산업기반 시설뿐만 아니라 기업이나 기관, 개인을 공격하는 타겟 공격도 발생하고 있다. 지능화된 악성코드는 사이버범죄 조직 등에 의해

78 Ibid.

많이 유포되고 있다. 사이버범죄 조직들이 악성코드를 제작하여 유포와 공격 등을 분업화, 기업화하면서 더욱 악성코드가 증가하고 있다.

지금까지 마이크로소프트사의 윈도우 운영체제에서 작동하는 지능화된 악성코드가 최근에는 맥킨토시 사용자를 노리는 형태의 악성코드들로 전환하고 있다. 맥킨토시 사용이 증가하고 있어 맥킨토시 대상 악성코드 유포는 더욱 증가할 것으로 보인다. 다음으로 안드로이드 악성코드가 크게 증가하고 있는데, 전 세계 모바일 악성코드는 2만여 종이 넘고 이중 안드로이드 악성코드는 약 80%이다. 모바일 플랫폼 시장에서 차지하는 비중이 커진 안드로이드 폰이 앱 보안 검증에 취약하다는 점에서 안드로이드 폰을 대상으로 하는 모바일 악성코드가 급증하고 있다. 한국도 스마트폰의 약 90% 이상이 안드로이드 운영체제이기 때문에 매우 위험한 상황이라고 할 수 있다.[79]

최근 지능화된 악성코드는 주로 SNS를 통해 유포되고 있다. 앱 보안성 검증이 취약한 블랙마켓을 통한 모바일 악성코드의 유통이 빈번해지면서 유튜브, 트위터 등과 같은 SNS를 통한 모바일 악성코드의 유통이 늘어나고 그에 따른 감염도 크게 증가하고 있다. SNS 사용자가 많고 전파 속도도 매우 빠르기 때문에 QR 코드, 단축 URL 등을 활용한 피싱 등 사회공학적인 공격 위협도 크게 늘고 있다. 이러한 방식은 사전에 어디로 연결될지 모르는 상태에서 사용자가 클릭하기 때문에 악성코드로 손쉽게 연결시킬 수 있고 결국 모바일 악성코드를 급격히 증가시키게 된다. 블랙마켓에서 더 나아가 앱 마켓의 검증과정을 우회하도록 설계된 악성코드로 나타나고 있다. 구글 마켓에서 공식적으로 등록된 앱 중 악성 앱

79 한국인터넷진흥원, 『민간분야 침해사고 동향』.

으로 드러난 경우도 여러 차례 발견되었다. 공식적으로 허가된 앱으로 위장하여 잘 알려진 앱 마켓에 등록시킴으로써 악성코드의 유포를 유도하고 있는 것이다. 사실상 기술적으로 모든 앱의 악성 앱 여부를 사전에 판독해낸다는 것은 거의 불가능하다. 따라서 서버에 대한 해킹을 시도하는 것보다 앱 마켓에 악성 앱을 등록시켜 해당 앱 마켓의 신뢰성을 악용함으로써 사용자들에게 악성코드를 유포하는 것이 더 손쉬운 방법일 수 있다. 또한 전 세계적으로 안드로이드 기반 스마트기기가 보급되면서 안드로이드 플랫폼을 공격대상으로 삼는 경우도 급격히 증가하고 있다. 이러한 해킹을 통해 개인 정보를 탈취하고 요금체계 등을 혼란시키는 악성코드를 전파하기도 한다. [80]

자. 경쟁 조건 공격(Race Condition)

경쟁 조건 공격은 특정 순서로 작업을 처리하도록 설계된 컴퓨팅 시스템이 두 개 이상 다수의 작업을 동시에 수행해야 하는 경우 발생한다. 이 기술은 서비스가 시작되는 순간과 보안 제어가 적용되는 순간 사이의 시간 차이를 활용한다. 다중 스레드 응용 프로그램에 의존하는 이 공격은 신뢰할 수 없는 프로세스로 인한 간섭과 신뢰할 수 있는 프로세스로 인한 간섭, 두 가지 중 하나의 방법으로 전달될 수 있다. 적절한 제어가 없으면 서로 다른 프로세스가 서로 간섭할 수 있다. 웹 애플리케이션, 파일 시스템 및 네트워킹 환경은 모두 경쟁 조건 공격에 취약하다. 해커는 액세스 제어 목록 (ACL), 급여 또는 인적 자원 데이터베이스, 트랜잭션 시

80 채재병, 『국제 사이버공격 전개 양상 및 주요국 대응전략』, pp. 52-56.

스템, 재무 원장 또는 기타 데이터 저장소를 표적으로 삼을 수 있다. 경쟁 조건 공격은 자주 발생하지 않지만 이러한 공격이 발생하면 시스템에 무단 권한을 부여하는 등 심각한 영향을 미칠 수 있다. 또한 경쟁 조건 공격은 본질적으로 탐지하기 어렵다.[81]

애플리케이션이나 데이터베이스에 대한 정상적인 업데이트가 발생하고 이름, 번호 또는 기타 데이터가 최신 정보 상태를 반영하도록 변경되면 사이버 범죄자가 경쟁 조건 공격을 일으킬 수 있다. 이는 업데이트 프로세스 중에 데이터베이스가 완전히 다시 작성되지 않기 때문에 가능하다. 업데이트가 발생하면 1초 미만 또는 최대 몇 분 동안 지속될 수 있는 간격이 존재하며 그 동안 시스템이 보호되지 않는다. 이를 통해 해커는 무단 액세스를 얻을 수 있다. 이 짧은 기간 동안 해커는 시스템을 손상시키고 경쟁 조건 공격을 유발하는 쿼리를 보낼 수 있다. 침입자가 경쟁 조건 공격을 사용하여 시스템을 침해하면 데이터를 변경, 조작 또는 도용하고, 권한을 변경하고, 악성 코드를 삽입하고, DoS 공격을 일으키고, 보안 제어를 비활성화 할 수 있다.[82]

차. 백 오리피스(Back Orifice)

윈도우 시스템을 손상시키는 데 사용되는 프로그램이다. 시스템 관리자가 일반적으로 인터넷을 통해 원격 위치에서 컴퓨터를 제어할 수 있도록 하는 원격 관리 도구에 적용된다. 자체적으로 서버로 설치되어 클라

81 “RACE CONDITION.”

82 Ibid.

이언트 상대가 있는 해커가 키보드에서 사용자보다 더 완벽하게 시스템을 조작할 수 있다. 이전 버전의 윈도우에는 취약점이 있어 사용자에게 알려지지 않은 멀웨어 서버 코드를 설치하고 원격으로 제어할 수 있다. 시스템에 가할 수 있는 손상은 거의 무제한이다. 이 특정 위협은 이전 버전의 윈도우 기반 운영체제 소프트웨어를 대상으로 한다. 해커에게 부여될 수 있는 제어 수준은 시스템 수준이므로 프로그램을 성공적으로 설치하는 데 특히 해로울 수 있다. 네트워크의 모든 레거시 시스템은 여전히 취약할 수 있다.[83]

컴퓨터 시스템의 원격 관리를 가능하게 하는 프로그램인 백 오리피스의 기원은 합법적이었다. 이전 MS 소프트웨어 제품군인 백 오피스(Back Office)의 플레이로 명명된 백 오리피스(BO)는 윈도우 95 및 98용으로, 백 오리피스 2000(BO2K: Back Orifice 2000)은 윈도우 NT 및 후속 윈도우 운영체제용으로 만들어졌다. BO는 1998년 ‘Cult of the Dead Cow’라는 해커 클럽에 의해 출시되었으며, 1년 후 그룹은 BO2K라는 새로운 버전을 출시했다. 백 오리피스의 문제점은 트로이목마를 통해 크래커를 실행하여 대상이 잘못된 점을 의심하지 않게 한다는 것이다. 설치 후 트로이목마는 원격 크래커가 대상 컴퓨터에 대한 거의 완전한 제어를 허용한다. 백 오리피스는 바이러스가 아니다. 오히려 소프트웨어를 사용하기 전에 호스트에서 기꺼이 수락하고 실행해야 한다. 백 오리피스는 종종 사용자가 이메일로 받거나 웹사이트에서 다운로드 할 수 있는 유효한 소프트웨어와 동일한 것임을 주장하여 배포된다. 이름에 관계없이 이 원격 관리 소프트웨어에 의해 손상된 정보 시스템

83 “Back Orifice.”

은 특히 취약하다. 해커는 일반적으로 사용자 또는 소유자만큼 시스템에 대한 액세스 권한을 얻을 수 있다. 인프라 소유자는 원격 액세스 및 제어 가능성을 잘 알고 있어야 한다. 크랙 공격의 표적이 되는 것을 방지하는 가장 좋은 방법은 신뢰할 수없는 출처의 파일을 받지 않는 것이다.[84]

카. 웹 해킹

웹 해킹은 그래픽 웹 인터페이스를 통해 애플리케이션을 조작하거나 URI(Uniform Resource Identifier)를 조작하거나 URI에 포함되지 않은 HTTP 요소를 조작하여 HTTP를 통해 애플리케이션을 악용하는 것을 말한다. 로컬 파일 업로드 취약성은 애플리케이션이 사용자가 악성 파일을 직접 업로드 한 다음 실행되도록 허용하는 취약성이다. 원격 파일 업로드 취약성은 애플리케이션이 사용자 입력을 사용하여 인터넷 사이트에서 원격 파일을 가져와서 로컬에 저장하는 취약성이다. 웹사이트 해킹은 의심할 여지없이 증가하고 있다. 해커들은 매우 긴밀한 웹 해킹 커뮤니티 내에서 더욱 정교하게 운영되고 있다. 새로 발견된 웹 애플리케이션 침입은 그 독점 그룹의 회원들에게만 알려진 다수의 웹사이트 해킹 포럼과 사이트에 게시된다. 게시물은 매일 업데이트되며 추가 웹 해킹을 전파하고 용이하게 하기 위해 사용된다. 평판이 좋은 사이트의 웹 페이지가 악성코드에 감염되는 해킹공격은 해킹 당한 웹사이트를 방문자들의 컴퓨터에 악성코드를 설치하는 새로운 해킹을 위한 시작 사이트

84 Ibid.

로 바꾼다.[85]

웹사이트 해킹은 e-비즈니스 수행을 위한 웹 기반 기술이 채택된 결과다. 웹 애플리케이션은 조직이 공급업체 및 고객과 원활하게 연결할 수 있도록 하는 반면, 웹 애플리케이션 취약성 또한 해킹공격의 문을 열 수 있는 이전에 알려지지 않았던 수많은 보안 위험을 노출했다. 해커들은 민감한 정보를 훔치는 것에서부터 검색엔진최적화(SEO)의 목적에 이르기까지 여러 가지 이유로 이러한 취약한 웹사이트를 공격한다. 웹 애플리케이션은 웹사이트 방문자가 데이터베이스에 저장된 개인 및 민감한 데이터의 다양한 수준을 포함하여 동적 콘텐츠를 검색하고 제출할 수 있도록 설계되어 있다. 전 세계 어디에서나 밤낮으로 웹사이트에 접속할 수 있어야 하기 때문에, 안전하지 않은 웹 애플리케이션은 백엔드 기업 데이터베이스에 대한 해킹공격을 위한 열린 문을 제공한다. 해커들은 취약한 웹 애플리케이션 내에 코드를 주입해 사용자를 속인 뒤 사용자의 은행 계좌 내역을 검색하는 피싱 사이트로 유도하는 등 악의적으로 웹 페이지 해킹을 수행한다. 주로 은행과 온라인 결제 서비스를 대상으로 하는 이러한 종류의 해킹공격은 웹 서버와 데이터베이스 엔진에 취약성이 없는 경우에도 수행할 수 있는 SQL 주입, 크로스 사이트 스크립팅(XSS) 또는 또 다른 해킹 기법의 결과일 수 있다.[86]

이외에도 파일 업로드 공격은 공격 프로그램을 시스템에 업로드 하여 공격하는 방법이다. 파일 업로드는 공격이 쉬우면서도 파급 효과는 크

85 “How to Hack a Website: Online Example,” Guru99, https://www.guru99.com/how-to-hack-website.html (accessed: October 30, 2020).

86 Ibid.

다. 공격 방식은 내부 명령을 실행할 수 있는 프로그램을 제작하여 공격용 프로그램을 업로드 하는 것이다. 그리고 웹브라우저를 이용해 시스템 내부명령을 실행시킬 수 있게 되면 대상 시스템의 명령창을 자신의 컴퓨터에 띄워 작업할 수도 있으므로 원격지에서 공격 대상 컴퓨터를 완전히 통제하게 되는 것이다.[87] 디렉터리 탐색은 특정 시스템 파일을 웹브라우저에서 다운로드하는 공격 방법이다. 파일을 다운로드할 때 파일 이름을 필터링하지 않아서 생기는 취약점에 대한 공격이다. 디렉터리 리스팅은 웹브라우저에서 디렉터리를 열면 그 안에 있는 모든 파일 목록이 나열되는 것이다. 디렉터리 리스팅 취약점을 이용하여 대상 시스템에 어떤 파일이 있는지 알 수 있으므로 시스템의 취약점도 찾을 수 있다.[88] 인증 우회란 인증이 필요한 페이지의 인증을 거치지 않고 우회하여 접속할 수 있는 취약점을 공격하는 방법이다. 관리자 페이지에 접근하여 관리자 권한으로 모든 기능을 악용할 수 있게 되는데 이는 로그인하지 않고 관리자만이 이용할 수 있는 웹 페이지를 만들기 때문이다. SQL 인젝션 공격은 정상 문자가 아닌 특정 SQL문을 넣어 공격하는 방법이다. 특정 SQL 문이 삽입되면 그대로 데이터베이스에 전송되어 공격이 일어난다. 크로스 사이트 스크립팅(XSS) 공격은 XSS 취약점을 갖고 있는 웹사이트에 악의적인 스크립트를 업로드 하여 대상 컴퓨터를 공격하는 방법이다. 사용자 쿠키를 훔쳐 로그인하거나 브라우저를 제어한다.[89]

87 "Unrestricted File Upload," OWASP, https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload (accessed: October 30, 2020).

88 "Directory Traversal Attacks," acunetix, https://www.acunetix.com/websitesecurity/directory-traversal/ (accessed: October 30, 2020).

89 "Cross Site Scripting (XSS)."

3. 대상

가. 국가 및 사회적 차원

해커집단은 해킹을 통해 전력망을 과부하 시켜 국가기반시설인 전력시설을 마비시키고, 가스 설비를 조작하여 가스관을 폭파시키고, 신호체계에 혼선을 일으켜 교통마비를 일으키고, 국가통신망을 교란시켜 사회적 혼란과 불안을 조성하고, 건물관리시스템에 침입하여 이를 이용해서 건물에 불법침투하기도 하고, 심지어 대중매체를 조작하여 대중을 선동하는 등 국가 및 사회에 악의적인 피해를 주고 있다. 최근의 사물인터넷 시대에는 이러한 해킹을 통한 국가 및 사회에 대한 공격이 더욱 심해지고 있는 상황이다. 이러한 해킹은 국가 차원에서 국가안보를 위협하는 행위이지만 이를 방지하기에는 사실 사물인터넷(IoT)의 특성으로 인해 상당한 어려움이 있다. IoT의 확산에 따른 국가 기반시설과 사회 주요시설 등에 대한 접근성이 더욱 개방적으로 변화함으로써 이를 방어한다는 것은 매우 힘들 것으로 보인다.

실제로 많은 기업들은 국가의 주요 기간망 서비스를 효과적으로 운용하기 위해서 이에 대한 관리시스템을 보다 효율적으로 구축하고자 한다. 이를 위해 IoT를 통한 효율성 제고를 목표로 IoT 확산전략을 채택하여 추진하고 있다. 그런데 이러한 노력이 역으로 중대한 위협으로 작용할 수 있는 것이다. 이와 같은 IoT를 이용한 관리시스템이 해킹 당했을 때는 그 피해는 상상하기 어려울 정도로 심대할 것임에 틀림없다. 브라질의 경우 국제공항의 효율적 운용을 위해 미국 기업인 GE의 IoT 기반 관제시스템을 구축하였지만 만약의 경우 이 시스템이 해킹된다면 공항을

이용하는 항공기 운항을 마비시키는 것은 물론 항공기를 추락시킬 수도 있는 것이다. 이 경우 막대한 인명 피해뿐만 아니라 엄청난 경제적 손실을 입을 것이고 이로 인한 사회적 충격은 금전적으로 계산할 수 없을 것이다. 이러한 GE의 시스템들이 전 세계적으로 확산될 경우 GE의 통합 산업인터넷시스템이 해킹되면 단순히 한 국가의 문제가 아니라 국제적 문제로 비화될 것이다. 특히 단순한 시스템에 대한 피해와 그에 따른 직접적인 피해에 그치지 않고 시스템 자체가 장악되어 통제불능의 상황에 빠진다면 그에 따른 피해는 엄청날 것으로 보인다.[90]

국가 및 사회의 기반시설에 대한 해킹에 주로 사용되는 스턱스넷, Night Dragon, Duqu, Nitro 등의 바이러스는 사물인터넷 시대에 그 위험성이 더욱 높아지고 있다. 국가 기간망에 대한 위협이 IoT로 인해 더욱 커졌으며 만일 스턱스넷 같은 바이러스가 국가 기간망 해킹에 사용된다면 이는 국가 기간망을 순식간에 마비시킬 뿐만 아니라 국가 기간망 자체를 완전히 파괴시킬 수도 있는 것이다. 이 경우 단기간 내에 이러한 시설들이 복구되기 어렵기 때문에 이로 인한 국가적 피해는 막대할 것이다. 이를 방지하기 위해 포괄적인 보안대책들이 요구되지만 현실적으로 완벽한 대비를 하기에는 역부족인 상황이다.

한편 산업정보망에 대한 해킹의 경우도 사물인터넷 시대에 급격히 증가하고 있다. 해킹 기술은 비약적으로 발전하고 있는데 비해 이를 방어하기 위한 기술 개발은 뒤처져 있는 것이 현실이다. 국제적으로나 국내적으로 해킹에 대한 위험성은 널리 알려져 있지만 실제로 이에 대비하는

90 이상호·조윤영, "사물인터넷시대_국가_사이버안보_강화_방안_연구," 『정치정보연구』 제18권 제2호 (2015), pp. 16-18.

노력은 이에 미치지 못하고 있는 실정이다. 국내의 경우 기술과 예산에서 경쟁력이 뒤떨어져 있고 영세적인 경영 상태를 벗어나지 못하고 있는 보안업체들의 상황은 물론이고 실제 피해 대상인 기업들의 인식이나 지원도 한참 미치지 못하고 있다. 기업들은 과거에 비해서는 보다 적극적으로 보안인식을 확산시키고 보안시설들을 구축하려하고 있으나 여전히 재정적 이유와 실제로 피해를 겪을 가능성 등으로 인해 소극적인 자세를 벗어나지 못하고 있다. 보안업체들도 국내시장의 협소함을 이유로 해킹 기술의 발전에 따른 고도의 기술력을 바탕으로 하는 보안설비의 설계 및 제작을 하지 못하고 있는 실정이다. 이로 인해 국내의 보안서비스 시장은 해외에 비해 열악한 상태를 벗어나지 못하고 있고 기술 개발의 후진성을 보이는 악순환을 낳고 있다.

최근에는 북한도 한국에 대한 대남심리전을 IoT를 활용하여 전개할 가능성이 매우 높다. 북한은 해킹을 통해 웨어러블 디바이스 IP 주소 정보를 입수하여 그 위치정보를 확보할 수 있다. 이 경우 북한은 위치 주변에 설치된 IoT를 다시 해킹하여 허위사실을 전파하는 대남심리전을 전개할 수 있는 것이다. 그런데 문제는 이러한 북한의 IoT 해킹을 통한 대남심리전을 막기 어렵다는 것이다. 왜냐하면 이를 방어하기 위해서는 IoT의 네트워크를 차단해야 하는데 기술적으로 지수적 수준으로 발급된 IoT의 IP 주소 전부를 차단하는 것은 불가능하다. 북한의 해킹이 심대한 위험을 초래할 것이라는 것을 알고 있지만 사물인터넷 시대에 물리적으로 인터넷을 차단하는 등의 국가 차원의 조치를 내리는 것은 시간이 갈수록 더욱 어려워질 것이 분명하다. 결국 국가 및 사회적 차원에서 발생하고 있는 IoT를 통한 해킹 위협은 국가 기간망 파괴, 북한의 대남심리전 강화 등으로 표출될 것이며 이에 대응하는 국가 차원의 기술적, 정책

적 대비는 더욱 더 어려워질 전망이다.

나. 개인 차원

사물인터넷 시대에는 특히 개인에 대한 해킹 피해가 두드러지고 그 피해 정도도 매우 클 것으로 보인다. 모든 물체들에 대한 관리가 당사자에 국한되어야만 하지만 실제로 당사자 이외의 타인이 이러한 사물에 대한 통제와 관리를 임의로 조작하게 된다면 그로 인한 피해는 막대할 것이다. 비록 IoT가 사람들에게 주는 편리함이 엄청나다고 할지라도 해킹에 의해 이러한 편리함이 일순간 엄청난 고통과 피해로 바뀐다면 이는 전혀 간과할 일이 아닌 것이다. 이를 방지하기 위한 개인에 대한 보호, 그리고 피해를 방지할 수 있는 보안기술과 정책 등에 대한 신중한 검토가 요구된다. 사물인터넷 시대를 맞이하면서 이에 대한 관심과 논의는 필수적인 것이다.

오늘날 우리는 집안이나 건물 등에 수많은 센서들이 설치되어 있는 상황에서 살고 있다. 대표적으로 CCTV를 비롯해 다양한 센서들이 우리와 함께 생활하고 있으며 앞으로 사물인터넷 시대에는 우리 사회의 거의 모든 곳에 각종의 센서들이 설치되어 있을 것이다. 이러한 센서들은 해커들이 해킹 대상으로 삼기 매우 좋은 것으로 이를 통해 개인의 여러 가지 식습관이나 생활양식 등을 엿볼 수 있고 개인 정보를 탈취할 수 있다. 그리고 개인 정보가 보관되어 있는 클라우드를 해킹한다면 여기에 보관된 개인의 금융 정보를 비롯한 모든 신상이 탈취될 수 있다. 이러한 접근이 IoT 즉 센서에 대한 해킹을 통해 가능하며 이는 사회에 커다란 혼란을 가져올 것이다. 개인 정보에 대한 탈취는 반드시 악의적인 해커에 의해

서만 시도되는 것이 아니다. 예를 들어 정부나 기업도 개인 정보에 접근할 수 있다는 유혹을 뿌리치기 어려울 것이다. 이 경우 정부나 기업은 합법적 또는 불법적으로 획득한 개인 정보를 무분별하게 사용할 가능성이 있다. 이러한 상황은 사물인터넷 시대의 인터넷 사용자들에게 정보유출에 대한 불신감을 증폭시킬 것이고, 사물인터넷 시대는 종말을 고할 수도 있다. 정부와 기업은 빅데이터의 요구로 인해 개인 정보 수집을 비롯해 대량의 우수한 정보에 대한 수집에 집중할 수 있고, 이러한 정부와 기업의 정보 수집 행위는 개인의 권리에 대한 심대한 침해를 낳을 것이다. 그리고 개인은 이러한 정부나 기업의 정보 수집에 대해 기술적으로 대응할 수 없기 때문에 결국 커다란 사회문제로 비화될 가능성이 매우 크다.

한편 개인에 대한 해킹 피해는 한층 개인적인 수준에서도 발생할 수 있는데 그 피해는 극단적일 수 있다. 예를 들어 항상 심박조절 장치를 사용해야 하는 심장병환자의 경우 IoT에 대한 해킹은 이러한 의료기기에 대한 접근도 가능하게 하기 때문에 심박조절 장치의 고의적 오작동에 의한 피해도 가능하다. 사물인터넷 시대에 무선으로 연결된 각종 의료기기는 해커의 공격대상이 될 수 있다. 이 경우에는 만약 의료기기 사용자가 국가안보상 주요인사일 경우 적대국가나 테러집단을 포함하는 세력들에 의해 요인암살과 같은 테러행위로 연결될 수 있다. 사실상 저격 등의 테러행위보다 IoT 해킹에 의한 암살 시도는 훨씬 수월할 수 있고, 해커에 대한 추적도 어렵다. 나아가 이러한 해킹은 의료기기에 국한되는 것이 아니라 집이나 사무실, 또는 원격조정이 가능한 자동차 등으로 확대될 수 있으며 결국 안전하다고 생각하는 곳에서 전혀 무방비 상태에서 위협

에 노출될 수 있는 것이다.[91]

최근에는 코로나19로 인해 늘어난 재택근무자들을 겨냥한 해킹공격이 크게 증가했다. 기관이나 기업 네트워크 외부에서 일하는 재택근무자들의 증가로 디지털 공격 범위가 확장되는 상황을 활용하여 전 세계 모든 이들에게 영향을 미치는 코로나19 팬데믹의 속성과 빠르게 진화한 공격 방법을 통해 해킹공격이 더욱 확대된 것이다. 특히 기관이나 기업 네트워크 공격을 위한 거점을 확보하기 위해 재택근무자들이 네트워크와의 연결을 위해 사용하는 장치인 소비자용 라우터 및 IoT 장치에 대한 취약점 공격(exploit) 시도가 크게 증가하였다. 그리고 코로나19로 인한 재택근무 체제로의 급속한 전환은 다양한 방법을 통해 재택근무자인 개인사용자를 공격대상으로 삼을 수 있는 기회를 더욱 확대시켰다. 가장 취약하고 공격에 노출되기 쉬운 개인사용자들이 가정에서 웹브라우저를 사용할 때 해킹공격이 많이 시도되었고, 재택근무자들을 계속 공격대상으로 삼고 있어 연결 장치뿐만 아니라 웹브라우저도 주요 공격목표가 되었다. 금융기관의 경우 코로나19 확산에 따른 재택근무를 위해 망 분리 완화 조치를 시행함으로써 해킹에 취약해졌고, 재택근무자의 PC를 해킹하여 내부망의 서버와 시스템을 공격할 수 있게 되었다. 기관이나 기업의 내부공간에서는 보안장비 설정 등으로 해킹에 대한 탐지와 차단이 가능하지만, 내부망으로 원격접속을 시도할 경우 재택근무자의 PC는 내부망에 비해 취약할 수밖에 없다. 이에 따라 최근 망 분리가 미비한 의료기관도 이러한 해킹의 주된 대상이 되고 있다.[92]

91 Ibid., pp. 18-19.

92 채재병 외, "코로나19 관련 사이버공격 양상 및 시사점," pp. 3-4.

또한 운영기술(OT) 시스템에 대한 해킹공격도 증가하고 있다. 최근 코로나19 확산으로 디지털 전환이 가속화되면서 한층 개방된 OT 시스템이 해킹공격에 노출되었다. 기술 발전이 아닌 감염병이 가속화시킨 디지털 전환은 IoT와 이를 활용하는 스마트공장(smart factory)의 OT 시스템을 축으로 하고 있다. OT와 정보기술(IT)이 결합돼 운영상의 변화를 감지하거나 구현하는 기술인 IoT가 접목되기 전까지는 OT 시스템은 자동화엔지니어만 알고 있는 특수한 영역이었다. OT 시스템에 대한 지식이 매우 제한적이었기 때문에 해킹공격으로부터 OT 시스템은 비교적 안전한 상태였지만, 최근 IoT를 활용하기 위해 IT 시스템과 호환되는 OT 시스템이 등장하면서 그와 관련된 정보도 널리 알려지기 시작했다. 이에 따라 OT 시스템은 해커들의 공격대상이 되기 시작했고, 소프트웨어 유틸리티와 사용자 인터페이스를 갖춘 일부 최신 장치들은 해커들의 주된 목표가 되었다. 기관이나 기업의 네트워크는 일반적으로 IT 시스템과 OT 시스템이 서로 분리되어 있기 때문에 안전하지만, OT 시스템은 내부에 보호기능이 거의 없다는 약점을 가지고 있다. 왜냐하면 OT 시스템은 고성능으로 유지되어야 하기 때문에 성능유지를 위해 내부 보호기능을 거의 탑재하지 않기 때문이다. OT 시스템에 대한 해킹은 기업에만 국한되지 않는다. 오히려 중요 국가 인프라인 화력 발전소, 원자력 발전소, 수도 시설 등의 OT 시스템이 랜섬웨어에 감염되는 사례가 증가하고 있다. 이 중 상수도 시스템에는 IT와 OT 연결이 필요한 장치들이 많이 있는데, 이러한 장치들은 디도스 공격 같은 해킹에 대해 거의 무방비 상태이다. 특히 디지털 기술의 결집체인 스마트공장은 지능화될수록 해킹에 노출될 가능성이 크다. 이미 2018년 대만의 반도체업체인 TSMC와 2019년 노르웨이의 화학업체인 노르스크 하이드로(Norsk Hydro)에서

이와 같은 피해가 나타났다. 기본적으로 폐쇄망으로 구성된 스마트공장은 안전하지만 최근에는 폐쇄망을 대상으로 하는 해킹도 크게 증가했다. 코로나19로 인해 재택근무와 스마트공장 원격접속 관리가 일상화하게 되면 이러한 해킹은 더욱 증가할 것이다.[93]

이와 같이 코로나19로 인한 해킹 양상에 대응하기 위해서는 우선 재택근무로 인해 가정으로 확장되는 네트워크를 보호할 수 있는 방안을 마련할 필요가 있다. 즉, 재택근무자들이 사용하고 있는 장치들과 홈 네트워크를 보호할 수 있는 장기적인 대책을 마련해야 한다. 구체적으로 기관이나 기업에서는 재택근무 시 통신상황에 대하여 상시 모니터링을 유지해야 한다. 그리고 재택근무자는 신뢰할 수 없는 대상으로부터의 이메일을 열지 않고, 재택근무자의 PC가 악성코드나 랜섬웨어에 감염되지 않도록 최신 버전의 백신을 사전에 설치해야 한다. 다음으로 기관이나 기업들은 그들의 직원과 장치 및 정보를 보호하기 위한 구체적인 조치를 마련할 필요가 있다. 혹시라도 망 분리 완화 조치가 해킹공격에 대한 대응체계를 약화시키지 않도록 그에 대한 안전장치를 마련해야 한다. 마지막으로 네트워크나 퍼블릭 클라우드를 포함한 디지털 공격 범위 전체에 대한 감시와 탐지, 차단과 보호를 제공할 필요가 있다. 코로나19의 영향으로 확장된 공격 범위를 포괄할 수 있도록 기존의 해킹에 대한 대응체계를 개선하고, 새로운 취약점들을 보호할 수 있는 사이버안보 플랫폼을 구축해야 한다.[94]

93 Ibid., pp. 3-5.

94 Ibid., p. 5.

V

결론: 한국의 대응방안

이상에서 사이버공간에서 나타나고 있는 주권인식을 토대로 하여 국제사회에서 나타나고 있는 해킹의 변화 추세를 살펴보고, 해킹의 주체, 기법, 대상별로 분석해 보았다. 결론에 대신하여 해킹에 대한 한국의 대응방안으로 소위 '한반도 사이버 평화체제'[95] 구축방안을 제시해 보고자 한다.

2019년에 공표된 '국가사이버안보전략'을 살펴보면 사이버억지를 활용하여 한반도 사이버 평화체제를 구축하고자 하는 의도를 읽을 수 있다. 한반도 평화체제는 "남북한을 비롯한 관련국 상호간에 공식적으로 전쟁상태를 종식시킴으로써 법적·제도적 및 실질적으로 한반도에 공고한 평화가 보장되어 있는 상태"를 의미한다.[96] 이에 따라 한반도 사이버 평화체제는 한반도 평화체제의 부분을 구성하거나 또는 확장으로 작용할 수 있다. 다시 말해 한반도 평화체제를 구축하기 위한 사이버공간에서의 안보 레짐인 것이다. 따라서 한반도 사이버 평화체제를 구성하는 국내외의 법제도와 거버넌스는 한반도의 평화를 확보하는 사이버안보 레짐을 형성한다.[97] 이를 통해 해킹 등 사이버위협에 대응하여 사이버공간에서의 자유로운 활동과 이익창출, 그리고 자율적 통제를 달성함으로써 구조적 평화체제를 구축할 수 있다.

우선 한반도 주변 사이버공간 실태를 살펴보면, 국제, 지역, 개별국가 차원에서 국제규범과 협력을 통한 거버넌스 구축이 시도되고 있다. 국

95 '한반도 사이버 평화체제'는 아직 확정된 개념은 아니며 본 연구에서는 사이버공간에서의 한반도 평화를 위한 하나의 레짐으로 한반도와 주변국들의 사이버공간에서의 국제규범의 확립과 국제협력의 강화로 이해한다.

96 "한반도 평화체제," 외교부, http://www.mofa.go.kr/www/wpge/m_3982/contents.do (검색일: 2020. 10. 30).

97 채재병 외, 『주변국의 사이버 환경과 한반도 평화체제 구축』, pp. 194-195.

제 차원에서는 국제연합(UN)과 경제협력개발기구(OECD)의 주도로 국제전기통신연합(ITU), UN 정부전문가그룹(GGE)를 중심으로 추진되고 있다. 지역 차원에서는 유럽연합(EU), 동남아국가연합(ASEAN), 북대서양조약기구(NATO), 유럽안보협력기구(OSCE) 등을 중심으로 추진되고 있다. 개별국가 차원에서는 양자 및 다자 간 관계를 중심으로 추진되고 있는데 이러한 개별국가 차원의 거버넌스 추진 이외에도 민간 차원에서의 다자간 국제 협력도 중점적으로 추진되고 있다. 그런데 국제규범과 협력을 위한 사이버 국제공조가 정보통신기술에 관련된 협력이나 사이버범죄 방지에 국한됨으로써 안보 차원에서의 사이버문제를 다루지 못하는 한계가 있다. 안보 차원의 사이버협력은 국제 차원 보다는 지역이나 개별국가 차원에서의 양자 및 다자 간 관계를 중심으로 추진되는 것이 훨씬 더 수월하다. 그러나 한반도 주변지역은 안보 차원의 사이버협력에 대한 공감대와 의지가 유럽에 비해 부족하기 때문에 지역 및 개별국가 차원에서의 국제협력이 미미한 상태이다.

사이버공간에서의 국제규범 및 협력과 관련하여 국제사회는 미국과 유럽 중심의 선도국 진영과 중국과 러시아 중심의 후발국 진영으로 나뉘어 대립하고 있다. 한때 양 진영은 2013년 UN ‘GGE 권고안을 통해 사이버 관련 원칙들에 대해 합의를 이루기도 했지만 여전히 세부적으로 이를 적용하는 문제 등 갈등의 소지를 안고 있다. 예를 들면 인터넷 거버넌스의 주체를 누구로 할 것인지 등에 대한 이견이 존재하며 미국 등이 현 체제의 유지를 지지하는 입장인 반면 중국 등은 새로운 인터넷 거버넌스를 주장하는 입장이다. 사이버 관련 국제규범 및 협력 논의과정에 참여하는 방식에 대해서도 양 진영은 서로 의견을 달리하고 있고, 사이버범죄와 관련하여 기존의 국제법을 적용할지, 아니면 새로운 국제규범을 창출할 지에 대해서도 양 진영의 입장은 대립되고 있다.

한국은 국제 차원, 지역 차원, 개별국가 차원 모두에서 다양한 사이버 관련 국제협력을 추진하고 있다. 그러나 한국이 주도하는 포괄적이며 중장기적인 전략과 방안들을 제시하지는 못하고 있다. 한국으로서는 한반도 주변지역에서의 사이버 주도권 쟁탈전이 벌어지고 있고 북한에 의한 해킹도 지속되고 있는 등 안보적으로 사이버 국제협력이 시급한 상황이다. 한국은 이러한 문제점들을 해결하기 위해 지금과 마찬가지로 지속적으로 국제 차원, 지역 차원, 개별국가 차원에서의 국제협력을 병행 추진할 필요가 있다. 동시에 한국이 주도할 수 있는 포괄적, 중장기적 사이버 전략과 방안을 마련하여 이를 기반으로 적극적으로 국제협력에 참여해야 할 것이다.

한반도 사이버 평화체제를 구축하기 위해서는 국제사회와의 다양한 협력을 통해 주도적으로 사이버 국제협력 네트워크를 형성해야 한다. 그리고 이를 위해 국제 사이버 파트너십을 강화하고, 사이버억지를 위해 미국, 일본, 중국, 러시아 등 한반도 주변국들과의 다자 및 양자 간 사이버 국제협력을 강화해야 한다. 나아가 사이버 선도국으로서 사이버 후발국들에 대한 지원과 함께 사이버 국제규범 수립과 관련하여 중립적이고 보편타당한 입장을 견지해야 한다.[98]

한반도 사이버 평화체제 구축을 추진하기 위해서는 우선 국제 차원에서 사이버 국제협력을 강화하기 위해 UN GGE 등 사이버 분야 국제 거버넌스에 주도적으로 참여한다. 사이버 국제규범 수립과 관련하여 양 진영으로 대립하고 있는 상황에서 성급하게 입장을 정하기보다는 유보적

98 Ibid., pp. 199-201.

입장을 견지하면서 새로운 국제규범 창출에 적극적으로 참여할 필요가 있다. 지금은 제외되어 있는 상태이지만 지속적으로 UN GGE에 참여할 필요가 있고, 사이버 역량 강화 지원에서 한국의 선도적 역할을 확대한다.

다음으로 지역 차원에서 한반도 주변지역, 넓게는 동북아지역에서는 사이버 국제협력을 양자협력보다는 다자협력을 통해 추진한다. 그동안 동북아지역에서는 사이버 국제협력을 외교적으로 접근하거나 기술협력이나 사법공조 차원에서 추진되었는데 이 과정에서 아세안 등의 지역기구는 그다지 효과적이지 못했다. 따라서 유럽의 유럽네트워크보안청, 북대서양조약기구, 유럽안보협력기구의 활동을 참고로 하여 한국이 주도적으로 참여하고 있는 아세안+3나 ARF 등을 중심으로 동북아지역의 사이버 국제협력을 추진할 필요가 있다.

마지막으로 개별국가 차원에서 한반도 주변 사이버 관련 주요국들인 미국, 일본, 중국, 러시아 등과 양자 또는 다자간 사이버 협력을 적극 추진한다. 미국과는 한미동맹에 기반한 공조를 강화하고, 사이버 정보협의체 등을 중점적으로 추진한다. 일본과는 정보협력을 강화하여 사이버정책협의체를 추진한다. 이와 같은 양자관계를 다자관계로 확장하여 한미일 간 사이버 정보공유체제로 확대 발전시킨다. 중국 및 러시아와의 사이버 협력관계에서는 주로 신뢰구축 조치에 중점을 두고 추진한다. 이에 따라 한중 간, 한러 간 사이버 고위급 핫라인 설치를 추진하고 사이버정책협의체도 구성한다.

한편 북한과 관련해서는 북한의 해킹 등을 국제문제로 이슈화하고 국제공조를 통한 제재조치도 유도한다. 동시에 북한을 국제 사이버 규범 논의의 장으로 이끌어 사이버억지 효과를 노린다. 북한의 해킹에 대해

국제적인 사이버 수사공조를 추진하여 북한을 중국으로부터 분리시키는 등 중국에 대한 견제효과도 노린다.

한국이 한반도 사이버 평화체제 구축에 주도적인 역할을 하기 위해서는 한국의 입장을 명확히 반영하는 사이버 원칙을 마련하여 국제사회를 설득할 필요가 있다. 따라서 이러한 한국의 사이버 원칙을 확립하기 위해서는 기본법적 성격을 갖는 가칭 '국가사이버안보기본법'을 제정해야 한다. 이를 통해 사이버 관련 주무기관을 설치하고 사이버 전반에 걸친 원칙을 표명할 수 있을 것이다.

Abstract

The Trend of Changes in Hacking in the International Society and Countermeasures

Chae, Jae-Byung

(Institute for National Security Strategy)

The purpose of this research is to examine the trends of changes in hacking in the international society based on the recognition of sovereignty in cyberspace and to present Korea's countermeasures against hacking by analyzing principal agent, technique, and target of hacking.

Hacking is expected to become more advanced as it continues to increase, so efficient preparation, management, and response systems are needed. In particular, it is time for Korea to actively seek countermeasures against hacking in preparation for cyber disputes as discussions on sovereignty in cyberspace have been active in the wake of the fourth industrial revolution and the Internet of Things era. As a countermeasure against hacking, I'd like to propose a plan to establish a so-called 'Cyber peace regime on the Korean Peninsula'.

In order to establish a cyber peace regime on the Korean Peninsula, Korea should take the initiative in forming a cyber international cooperation network through various cooperation with the international society. And to that end, Korea must strengthen international cyber partnerships and strengthen multilateral and bilateral cyber international cooperation with neighboring countries on the Korean Peninsula, including the United States, Japan, China and Russia, to deter cyber-attacks. Furthermore, as a leading cyber country, it must maintain a neutral and universal position regarding the establishment of cyber international norms, along with support for cyber-latecomer countries.

In order to promote the establishment of a cyber peace regime on the Korean Peninsula, first of all, at the international level, Korea should take the initiative in international governance in cyber fields such as UN GGE to strengthen international cooperation on cyber. Next, at the regional level, cyber international cooperation will be promoted through multilateral cooperation rather than bilateral cooperation in the surrounding areas of the Korean Peninsula and in Northeast Asia. Finally, at the level of individual countries, Korea should actively push ahead

bilateral or multilateral cyber cooperation with major cyber-related countries such as the United States, Japan, China, and Russia.

Meanwhile, regarding North Korea, Korea will issue North Korea's hacking into international issues and encourage sanctions through international cooperation. At the same time, it is aiming for a cyber deterrence effect by leading North Korea to discuss international cyber norms.

In order for Korea to play a leading role in building a cyber peace regime on the Korean Peninsula, it is necessary to establish cyber principles that clearly reflect Korea's position and persuade the international society. Therefore, in order to establish such Korea's cyber principles, the so-called 'Basic Law on National Cyber Security', which has a basic legal nature, should be enacted. Through this, it will be possible to set up cyber-related agencies and express cyber-wide principles.

Keywords

hacking, hacking techniques, cyberspace, sovereignty, security

참고문헌

김상배 외.『사이버 안보의 국가전략: 국제정치학의 시각』. 서울: 사회평론, 2017.

김상배.『사이버 안보의 세계정치와 한국: 버추얼 창과 그물망 방패』. 서울: 한울아카데미 (2018).

김소정·양정윤. “미국과 중국의 사이버안보 전략과 한국의 안보정책에 대한 함의.” 『국가안보와 전략』 제17권 제2호 (2017).

김정욱. “사이버 공격 전략 분석을 통한 침해사고분석 방법론.” 한국통신학회 학술대회 논문집 (2019).

김창범. “해킹기법의 동향.” 『정보과학회지』 18(9), (2000).

민병원. “사이버공격과 사이버억지: 국제정치적 의미와 대안적 패러다임 모색.” 『JPI 정책포럼』 (2015).

박노형·정명현. “국제사이버법의 발전: 제5차 UNGGE 활동을 중심으로.” 『국제법학회논총』 제63권 제1호 (2018).

박대우. “국가사이버보안정책에서 해킹에 대한 소고.” 『정보보호학회지』 21(6), (2011).

박상돈. “사이버안보 거버넌스 개선에 관한 공법적 고찰.” 『공법학연구』 제17권 제4호 (2016).

박상민·임종인. “사이버공격 의도분석을 통한 공격유형 분류에 관한 연구.” 『정보보호학회논문지』 27(1), (2017).

박종재·이상호. “사이버 공격에 대한 한국의 안보전략적 대응체계와 과제.” 『정치·정보연구』 제20권 제3호 (2017).

박주희. “사이버공간에 적용되는 주권의 규범적 성격과 사이버안보.” 『국가안보와 전략』 제20권 제1호 (2020).

배영자. “사이버안보 국제규범에 관한 연구.” 『21세기정치학회보』 제27집 제1호 (2017).

신경수. “북한의 사이버 전력과 블록체인 기반 대응체계 연구: 서큘레이팅 모델을 중심으로.” 『신안보연구』 제2권 제1호 (2017).

신경수·신진. “사이버 위협의 확장과 국가안보적 대응.” 『전략연구』 제25권 제3호 (2018).

이상호·조윤영. “사물인터넷시대 국가 사이버안보 강화 방안 연구.” 『정치·정보연구』 제18권 제2호 (2015).

임종인·권유중·장규현·백승조, “북한의 사이버전력 현황과 한국의 국가적 대응전략.” 『국방정책연구』 제29권 제4호 (2013).

장노순·한인택. “사이버안보의 쟁점과 연구 경향.” 『국제정치논총』 제53권 제3호 (2013).

장노순. “사이버안보와 국제규범의 발전: 정부전문가그룹(GGE)의 활동을 중심으로.” 『정치·정보연구』 제19권 제1호 (2016).

장노순. “사이버안보와 선도국 우위의 전략적 선택.” 『국가안보와 전략』 제17권 제2호 (2017).

조이든·박수진·강남희. “사물인터넷의 경량 IP 카메라 취약점을 이용한 해킹공격 및 대응 방안.” 『한국디지털콘텐츠학회논문지』 20(5), (2019).

조화순. “정보화시대 국가주권과 사이버공간의 세계정치.” 『정보화정책』 제12권 제4호 (2005).

채재병. “국제테러리즘과 군사적 대응.” 『국제정치논총』 44집 2호 (2004).

채재병. “안보환경의 변화와 사이버안보.” 『정치·정보연구』 제16권 제2호 (2013).

채재병.『국제 사이버공격 전개 양상 및 주요국 대응전략』. INSS 연구보고서 2019-18 (2019).

채재병 외.『주변국의 사이버 환경과 한반도 평화체제 구축』. KINU 연구총서 19-29 (2019).

채재병 외. “코로나19 관련 사이버공격 양상 및 시사점.” 국가안보전략연구원 『이

슈브리프』 통권 217호, 2020.

최재원. “DNS 스푸핑을 이용한 포털 해킹과 파밍의 위험성.” 『한국정보통신학회논문지』 23(11), (2019).

한국인터넷진흥원, 『민간분야 침해사고 동향』. (2013. 3).

한희원. “사이버 안보에 대한 국가정보기구의 책무와 방향성에 대한 고찰.” 『한국경호경비학회지』 제39권 (2014).

함승현·박대우. “국가 사이버안보를 위한 정책 연구.” 『한국정보통신학회논문지』 21(9), (2017).

홍동철. “드론 해킹과 악성코드.” 『한국통신학회지(정보와 통신)』 34(10), (2017).

홍준호·유현우. “화이트 해커 양성 및 활성화 방안에 대한 연구.” 『법학연구』 제17권 제4호 (2017).

황진석·장인순·정기수. “웨어러블 기술동향 및 사이버공격 대응방안.” 『한국통신학회논문지』 44(4), (2019).

Bajpai, Kanti. “The Idea of Human Security.” *International Studies*, Vol. 40(3), (2003).

Barkin, Samuel J. & Cronin, Bruce. “The State and the Nation: Changing Norms and the Rules of Sovereignty.” *International Organization*, Vol. 48, No. 1 (1994).

Bartelson, Jorge. *A Genealogy of Sovereignty*, Cambridge: Cambridge University Press, 1995.

Biersteker, Thomas J. & Weber, Cynthia eds. *State Sovereignty as Social Construct*, Cambridge: Cambridge University Press, 1996.

Buzan, Barry. *People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, Colorado: Lynne Rienner Publisher, 1991.

Camilleri, Joseph A. & Falk, Jim. *The End of Sovereignty?*, Aldershot: Edward Elgar, 1992.

Clark, Ian. “Beyond the Great Divide: Globalization and the Theory of International Relations.” *Review of International Studies*, Vol. 24, No. 3 (1998).

Cutler, Claire. “Critical Reflections on the Westphalian Assumptions of International Law and Organization: A Crisis of Legitimacy.” *Review of International Studies*, Vol. 27, No. 1 (2001).

ENISA. *National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace* (2012. 5).

Haas, Richard N. “Paradigm Lost.” *Foreign Affairs*, Vol. 74, No. 1 (Jan./Feb. 1995).

ITU. *Global Cybersecurity Index* (GCI) (2018).

ITU. *National Cybersecurity Strategy Guide* (2011).

Krasner, Stephen D. *Sovereignty: Organized Hypocrisy*. Princeton: Princeton University Press, 1999.

Monthly Issue of National Cyber Security, Vol. 06 (2012).

Nye Jr. Joseph S. “Power and National Security in Cyberspace.” in Lord, Kristin M. & Sharp, Travis (eds.). *America's Cyber Future: Security and Prosperity in the Information Age*, Vol. II (Center for a New American Security, June 2011).

Opello, Walter C. & Rosow, Stephen J. *The Nation-State and Global Order: A Historical Introduction to Contemporary Politics*, Boulder, CO: Rienner, 1999.

Ruggie, J. G. “Territoriality and Beyond: Problematizing Modernity in International Relations.” *International Organization*, Vol. 47, No. 2 (1993).

Schmitt, Michael N. (ed.). *Tallinn Manual on the International Law Applicable to Cyber Warfare: prepared by the International Group of*

Experts at the invitation of the NATO Cooperative Defence Centre of Excellence, Cambridge University Press, 2013.

Stephenson, Carolyn M. "New Approaches to International Peacemaking in the Post-Cold War World." in Michael T. Klare (eds.). *Peace & World Security Studies: A Curriculum Guide*, Boulder: Lynne Rienner Publisher, 6th ed, 1994.

Tilly, Charles. *Coercion, Capital and European Sates AD 990-1900*, Oxford: Basil Blackwell, 1990.

네이버. "해킹 기술 동향." https://terms.naver.com/entry.nhn?docId=3432518&cid=58445&categoryId=58445 (검색일: 2020. 5. 24).

외교부. "한반도 평화체제." http://www.mofa.go.kr/www/wpge/m_3982/contents.do (검색일: 2020. 10. 30).

acunetix. "Directory Traversal Attacks." https://www.acunetix.com/websitesecurity/directory-traversal/ (accessed: October 30, 2020).

CLOUDFLRE. "What is a DDoS Attack?" https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (accessed: October 30, 2020).

EC-Council. "WHAT ARE SNIFFING ATTACKS AND THEIR TYPES?" https://blog.eccouncil.org/what-are-sniffing-attacks-and-their-types/#:~:text=Sniffing%20is%20the%20process%20of,are%20called%20network%20protocol%20analyzers (accessed: October 30, 2020).

F-Secure. "Back Orifice." https://www.f-secure.com/v-descs/backori.shtml (accessed: October 30, 2020).

Guru99. "How to Hack a Website: Online Example." https://www.guru99.com/how-to-hack-website.html (accessed: October 30, 2020).

imperva. "Advanced persistent threat (APT)." https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/#:~:text=An%20advanced%20persistent%20threat%20(APT,to%20mine%20highly%20sensitive%20data (accessed: October 30, 2020).

imperva. "What is a Buffer Overflow Attack." https://www.imperva.com/learn/application-security/buffer-overflow/#:~:text=Attackers%20exploit%20buffer%20overflow%20issues,files%20or%20exposes%20private%20information (accessed: October 30, 2020).

Malwarebytes. "Hacker." https://www.malwarebytes.com/hacker/ (accessed: October 30, 2020).

Malwarebytes. "SQL Injection." https://www.malwarebytes.com/sql-injection/ (accessed: October 30, 2020).

Norton. "What is a Trojan? Is it a virus or is it malware?" https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html (accessed: October 30, 2020).

Norton. "What is the Difference Between Black, White and Grey Hat Hackers?" https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html (accessed: October 30, 2020).

OWASP. "Cross Site Scripting (XSS)." https://owasp.org/www-community/attacks/xss/ (accessed: October 30, 2020).

OWASP. "Unrestricted File Upload." https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload (accessed: October 30, 2020).

Petters, Jeff."A brute force attack." https://www.varonis.com/blog/brute-force-attack/#:~:text=A%20brute%20force%20attack%20(also,attacks%20are%20simple%20and%20reliable (accessed: October 30, 2020).

Roohparvar, Robert. "WHAT IS A BACKDOOR ATTACK?" https://www.in-

foguardsecurity.com/what-is-a-backdoor-attack/#:~:text=The%20backdoor%20attack%20is%20a,plug%2Dins%20or%20input%20fields (accessed: October 30, 2020).

VERACODE. “RACE CONDITION.” https://www.veracode.com/security/race-condition (accessed: October 30, 2020).

VERACODE. “SPOOFING ATTACK: IP, DNS & ARP.” https://www.veracode.com/security/spoofing-attack#:~:text=A%20spoofing%20attack%20is%20when,can%20use%20to%20accomplish%20this (accessed: October 30, 2020).

INSS 연구보고서 2020-17

국제사회의 해킹 변화 추세 및 대응방안

발행처 사단법인 국가안보전략연구원
발행인 김기정
주소 06295 서울시 강남구 언주로 120 인스토피아 빌딩
전화 02-6191-1000 (Fax. 02-6191-1111)
홈페이지 http://www.inss.re.kr
인쇄일 2020년 12월
발행일 2020년 12월
편집 굿플러스커뮤니케이션즈(주)
ISBN 979-11-89781-42-2(94340)
979-11-89781-03-3(전18권)
가격 비매품

※ 본지에 실린 내용은 집필자 개인의 견해이며, 본 연구원의 공식입장이 아닙니다.