INSS
전략보고
May 2020. No. 78

www.inss.re.kr
INSTITUTE FOR NATIONAL SECURITY STRATEGY

국내외 사이버안보 환경의 변화와 한국의 대응

채재병 책임연구위원
chaejb@inss.re.kr

국가안보전략연구원

국문 초록

본 연구는 최근 나타나고 있는 국내외 사이버안보 환경의 변화에 따른 한국의 대응방향을 모색해보고자 한다. 오늘날 국제사회에서 사이버공격의 양상이 다양해지고 이러한 공격이 국가에 미치는 피해규모와 파급영향이 점점 더 심해지고 있다. 이 같은 사이버공격의 특성에 맞게 보다 효율적으로 대응하기 위해서는 국가안보 차원의 대비와 관리 및 대응체계가 필요하다. 이에 따라 한국은 사이버공간에 대한 안전성 확보, 사이버공격에 대한 억지력 확보, 정보보안정책의 성공적 추진을 위한 사이버안보 기반조성, 국제사이버협력 네트워크 확충 등에 중점을 두어야 할 것이다.

핵심어: 사이버안보, 사이버공격, 국제사이버협력, 사이버안보환경, 사이버공간

Ⅰ. 문제 제기

• 오늘날 사이버공격은 국가안보영역에서 비전통 안보위협 중 가장 심각한 위협으로 부상했음[1)]
  – 사이버공격의 대상이 개인 차원의 해킹 수준에서 진화하여 공공기관 및 사회기반시설까지 공격대상으로 삼으면서 사회적, 경제적 피해가 상상할 수 없을 만큼 커진 상황임
  – 만약 교통·항공·전력 등의 기반시설이 사이버공격을 받는다면 단순히 사회혼란에 그치지 않고 커다란 인명피해는 물론 국가 재난사태의 발생까지 초래할 수 있는 위험한 상황에 처해 있으며 이는 전통적인 안보차원에서 보더라도 매우 중대한 위협임
  – 이와 같은 사이버공격이 지속적으로 증가할 것으로 예상되므로 사이버공격의 특성에 부합한 보다 효율적인 대응을 가능하게 하고 종합적 국가위기관리 전략과의 일관성을 유지하기 위해서는 국가안보차원의 대비와 관리 및 대응체계가 필요함

• 한국은 세계의 다른 국가들과는 전혀 상이한 상황에 놓여있는데 이는 한국과 군사안보적으로 대치하고 있는 북한이 매우 강력한 비대칭적인 사이버전력을 갖추고 있기 때문임[2)]
  – 북한의 사이버전력은 매우 높은 수준으로 평가되고 있으며 남북한의 정보화 수준에서의 격차로 인해 북한에 대한 한국의 효과적인 사이버공격은 현실적으로 매우 어려움
  – 북한은 한국을 포함한 다른 국가들과 달리 개인의 인터넷 사용이 허용되지 않고 있을 뿐만 아니라 국가기관에서 사용하고 있는 인터넷 회선조차도 국제전화를 통해 이루어지는 등 북한 내 인터넷 보급수준도 매우 취약함
  – 따라서 북한은 사이버공격에 대한 취약점도 상대적으로 없는 상황임

• 한국은 2011년에 들어 국가차원의 사이버위협 대응체계를 정비하고, 관련부처별 역할을 정립하기 위해 분야별 중점추진과제를 포함시킨 '국가사이버안보마스터플랜'을 수립하였음[3)]
  – 이어 2013년에는 '국가사이버안보종합대책'을 수립하였고, 2019년에는 '국가사이버안보전략'을 공표하기에 이르렀음

1) 채재병, "안보환경의 변화와 사이버안보," 『정치·정보연구』 제16권 2호 (2013), p. 174.
2) 부형욱, "사이버안보의 주요이슈와 정책방향," 『국방연구』 56권 2호 (2013), pp. 11-13.
3) 채재병, 앞의 글.

- 한국은 국내외 사이버공격에 대응하여 다양한 대응방안을 강구하고 있으나 여전히 사이버안보 대응전략을 개선, 추진해야 할 시점임

• 본 연구는 최근 나타나고 있는 국내외 사이버안보 환경의 변화에 따른 한국의 대응방향을 모색해 보고자 함
- 이를 위해 우선 국내외 사이버안보 환경의 변화를 살펴보고, 다음으로 변화의 토대가 되는 사이버공격의 특징들을 유형별, 수단별, 양상별로 검토함
- 이러한 사이버공격의 특징들과 이로 인한 국내외 사이버환경의 변화에 대비하는 한국의 사이버안보 대응방향을 제시함

Ⅱ. 국내외 사이버안보 환경의 변화

1. 국제 사이버안보 환경

• 일반적으로 사이버안보란 사이버공간을 사이버공격으로부터 보호하는 것이라고 할 수 있음[4)]
- 따라서 사이버공간에 대한 다양한 주체와 수단을 통한 공격으로부터 국가와 국민을 보호하기 위한 즉 사이버공간을 안정적으로 유지하고 방어하기 위한 수단들의 총합이라고 할 수 있음
- 그런데 사이버라는 용어가 매우 추상적인 개념이라 현실세계에 적용하기가 쉽지 않음
- 실제로 사이버라는 용어는 컴퓨터나 인터넷 등의 정보통신기술과 이를 기반으로 하는 정보통신망, 그리고 이를 통해 구현되는 가상공간과 관련된 모든 것을 의미함
- 이러한 사이버의 추상적인 성격은 사이버공간과 현실세계의 경계를 매우 모호하게 만들었음

4) 위의 글. pp. 180-181.

• 사실상 사이버공간은 현실공간과 별개로 존재하고 있는 것이 아니라 물질적 기반시설과 단말기 등을 통하여 연결되어 있음[5)]
  - 사이버공간은 인터넷을 중심으로 하는 컴퓨터 및 네트워크를 기반으로 하여 형성된 가상의 정보처리 공간이므로 사이버공간은 물질적 실체 여부에 관계없이 컴퓨터 및 정보통신망을 통하여 정보를 처리할 수 있는 모든 네트워크와 시스템을 포함하고 있음
  - 사이버공간은 현실공간과 명확히 구별되지 않을 뿐만 아니라, 현실의 일상생활 영역과도 점차 일치해가고 있음
  - 즉, 사이버공간은 가상공간인 동시에 현실공간의 일부가 되어 가고 있으므로 현실세계와 유기적으로 연결된 개념인 것임

• 이와 같은 사이버공간의 범위에 대한 국가 간 인식의 차이와 사이버안보의 개념 및 범위에 대한 정책적 접근법의 차이 때문에 사이버안보의 개념에 대하여 전 세계적으로 합의를 이룬 것은 없음[6)]
  - 그러나 사이버안보가 국제협력을 통해서만 지켜질 수 있다는 측면에서 주요 국가 및 국제기구들에서 논의되는 개념과 합치하지 않으면 이는 추진과정에서 커다란 문제를 야기할 수 있음
  - 사이버안보의 특성상 국제적인 협력이 필수적이므로 국제적인 안전보장 체계를 통해 사이버안보를 달성하기 위해서는 관련 개념에 대한 국제적 합의는 반드시 필요함

• 국제사회의 주요 사이버공격 사례들을 살펴보면, 2007년 러시아의 사이버공격으로 에스토니아의 인터넷 전체가 3주 이상 마비된 사건이 있었음
  - 2010년에는 미국과 이스라엘이 악성코드를 이용해 이란의 핵시설을 파괴한 사례가 있었고 이에 대한 반격으로 2012년에는 이란이 미국과 이스라엘을 사이버공격하였음
  - 2014년에는 북한이 소니픽처스 엔터테인먼트 사이트를 공격하여 정보가 유출되었고 러시아가 미 백악관 전산망에 침입해 대통령 일정 정보 등에 접근한 사례가 있었음
  - 2015년에는 중국이 미국 인사관리처를 해킹해 공무원 2,150만 명의 신상정보가 유출되었고 2017년에는 워너크라이 랜섬웨어로 인한 피해 사례가 있었음

5) 위의 글.
6) 이연수·이수연·윤석구·전재성, "주요국의 사이버안전관련 법·조직체계 비교 및 발전방안 연구," 『국가정보연구』 제1권 2호 (2008), p. 42

2. 한국의 사이버안보 환경

- 한국의 경우는 사이버안보를 가리키는 용어에 대해서도 명확한 정의가 합의되지 않은 상태로 사이버안보, 정보통신보안, 전산보안, 정보보안, 정보보호, 컴퓨터보안, 사이버보안, 네트워크보안 등 다양한 용어가 사용되고 있음
  - 사이버안보를 폭넓게 규정하는 국제적 흐름을 고려할 때 사이버안보의 개념을 정보보호, 안보위해공격, 사이버공격 등의 용어로 산발적으로 사용하는 것은 여전히 문제임[7)]

- 한국을 대상으로 한 주요 사이버공격 사례들을 살펴보면, 2004년 중국 해커조직들에 의해 국회, 원자력연구소, 국방연구원 등이 사이버공격을 당한 해킹사건이 있었음
  - 2009년에는 주요 정부기관과 포털사이트, 은행사이트 등을 공격하여 마비시킨 7.7 디도스 공격이 있었음
  - 2011년에는 좀비 PC 10만여 대를 동원하여 국회·행정안전부 등 정부기관 홈페이지와 은행·증권사 등 민간 홈페이지를 마비시킨 3.4 디도스 공격과 악성코드를 통해 원격으로 사이버공격을 한 농협 전산망 해킹이 있었음
  - 2013년에도 신한은행, 농협, MBC, KBS 등 주요 금융사와 방송사들에 대해 동시다발적 사이버테러를 감행한 3.20 사이버공격과 청와대 등 홈페이지와 정당, 언론사 등의 컴퓨터 시스템에 동시다발적으로 사이버테러 공격을 감행한 6.25 사이버공격이 있었음
  - 2014년 서울메트로 서버 해킹과 악성코드 메일을 통해 PC를 감염시킨 한국수력원자력 해킹, 2015년 서울지하철, 청와대, 국회, 통일부 등에 대한 해킹, 2016년 청와대 사칭 악성코드 유포, 2017년 롯데 인터넷면세점 대상 디도스 공격과 워너크라이 랜섬웨어 등이 있었음

- 국제사회에서 급증하고 있는 사이버공격 사례와 마찬가지로 한국도 비약적인 정보화 사회로의 진전에 따라 점차 사이버상의 취약성을 드러내며 사이버공격 사례가 급증하고 있고, 이에 따른 피해의 정도도 높아지고 있음
  - 개인차원의 정보 유출이나 피싱 등에 따른 경제적 피해가 나날이 증가하고 있는 것은 물론이고, 네트워크 보급에 따른 정보 공유 및 교류로 인한 주요 기밀의 유출도 급격히 증가하고 있음

7) 채재병, 앞의 글, p. 184.

• 한국은 사이버공격으로 인한 피해규모가 매년 천문학적인 규모로 확대되고 있음[8)]
  - 이메일은 물론 클라우드, 사물인터넷(IoT) 등을 통한 사이버공격이 급속도로 확대되고 있고, 이메일을 통한 사이버공격이 폭발적으로 늘면서 2019년 상반기 탐지된 악성메일 건수가 17만 1,400건으로 2018년 한 해 동안 탐지된 16만 3,387건을 넘어섰음
  - 특히 이메일과 윈도우 서버를 노린 공격이 크게 증가했으며 상반기에 발생한 해킹사고 중 최초 침입 경로가 이메일이 된 사례가 35%에 달했고 소프트웨어 및 서버의 보안 취약점 등으로 인한 해킹사고는 각각 21%였음

• 사이버공격은 시간이 지남에 따라 그 특성이 변화하여 정치·군사·경제·사회 등 전 분야로 확산되고 있는 추세임
  - 최근의 사이버공격은 국가기능 혼란 및 상실을 목표로 하는 공격이 증가하고 있는데, 3.20 사이버공격의 경우 주요 방송사뿐만 아니라 하루 평균 약 33조원이 거래되는 금융시스템에도 장애를 초래하였음[9)]
  - 사이버공격이 인터넷 뱅킹 전면중단 등 금융질서 및 경제혼란을 발생시키고 있으며, 전자적으로 관리되는 군사·외교·행정 기밀정보도 지속적으로 유출되고 있음
  - 이제 사이버공격은 자기과시형 해킹에서 시작하여 악의적 해킹 단계를 거쳐 최근의 디도스 공격과 같은 해킹의 고도화 단계에 이르렀다고 할 수 있으며, 점차 고도로 발전하고 있는 사이버공격은 향후 기반시설공격이나 사이버전 등 변화하는 사이버환경에 맞게 진화하여 새로운 사이버위협 형태로 발전할 것으로 보임[10)]

• 한국은 북한과 대치하고 있다는 점에서 매우 특수한 사이버안보환경을 갖고 있다고 할 수 있음
  - 즉 한국은 기본적으로 북한으로 인해 전통적 군사안보 측면에서 다른 국가들에 비해 중대하고 상시적인 위협에 직면해 있는 동시에 북한의 사이버위협에도 노출되어 있음[11)]

8) http://www.dt.co.kr/contents.html?article_no=2019071802109931650002&ref=naver(검색일: 2019. 10. 11)
9) http://khnews.kheraldm.com/view.php?ud=20130719000771&md=20130722003209_AT(검색일: 2019. 10. 11)
10) 채재병, 앞의 글, p. 179.
11) 위의 글, p. 180.

- 한국은 국제적으로도 동북아지역의 역학관계 속에 놓여있으며 또한 동시에 사이버위협 및 공격의 주요 근원지로 알려져 있는 중국으로부터의 사이버위협 및 공격에도 상당히 노출되어 있는 상황임
  - 세계 최대의 해커 병력을 보유하고 있는 것으로 알려진 중국의 사이버전 수행 능력과 행태는 국제사회의 큰 우려를 낳고 있는 실정임[12)]
  - 중국 이외에도 국제적인 민간 해커집단의 위협 역시 매우 높은 것으로 나타나고 있으며 앞으로는 한국도 국제 테러조직에 의한 사이버공격을 받게 될 가능성도 매우 높은 것으로 전망됨[13)]

Ⅲ. 사이버공격의 특징

1. 유형

- 사이버공격은 사이버위협 중 "정보의 감청, 변조, 손상, 파괴나 정보시스템의 손상, 파괴 등의 의도적 행위"로 사이버첩보, 사이버테러리즘, 사이버범죄, 사이버무력공격 등이 모두 포함됨[14)]
  - 사이버공간에서 이루어지고 있는 사이버공격의 특성은 시대별로 변화하고 있으며 최근에는 정치, 군사, 사회 등 전 분야로 확산됨과 동시에 피해지역이 범세계적인 특징을 보여주고 있음
  - 국내적으로도 사이버공격은 "정보통신망 또는 정보에 대하여 전자적 수단을 이용하여 불법침입, 교란, 마비, 파괴 또는 위조, 변조, 유출, 훼손 등을 의도하는 일체의 공격"으로 정의됨[15)]

12) Symantec, 2013 Internet Security Threat Report, Vol. 18. Appendix (Apr. 2013), p. 8.
13) 채재병, 앞의 글.
14) Abraham D Soafer, David Clark and Whitfield Doffie, "Cyber Security and International Agreements," in Committee on Deterring Cyber Attacks, *Proceedings of a Workshop on Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* (The National Academies Press, 2010), p. 181.
15) 국가사이버안전관리규정 제2조 (2013); 방송통신사이버안전센터운영규정 제4조 (2013).

- 사이버첩보란 사이버공간에서 이루어지는 첩보행위로 전기통신망을 통해 정보통신기술을 이용한 정보수집 행위를 의미함
  - 사이버첩보는 사이버무력공격의 범위에는 포함시키지 않는데 왜냐하면 정보수집 등의 첩보행위는 자료를 변경하지 않고 네트워크에 손상을 주지 않기 때문임

- 사이버테러리즘은 "특정한 정치·사회적 목적을 가진 개인·테러집단이나 적성국 등이 해킹, 컴퓨터 바이러스의 유포 등 전자적 공격을 통해 주요 정보기반시설을 오동작·파괴하거나 마비시킴으로써 사회혼란 및 국가안보를 위협하는 행위"로 정의됨 [16]

- 사이버범죄는 한국 경찰에서 고도의 기술적인 요소가 포함되어 정보통신망 자체에 대한 공격행위를 통해 이루어지는 사이버테러형 범죄와 사이버공간이 범죄의 수단으로 사용되는 일반 사이버범죄로 분류됨 [17]
  - 사이버범죄는 범죄행위자, 범죄행위자의 의도나 동기 및 침해된 법익 등의 규명을 통해 사이버전쟁이나 사이버테러리즘과 구분될 수 있음
  - 사이버범죄는 노력과 비용에 비해 효과가 크고, 적발 가능성이 적으며, 적합한 범행 대상이 밀집해 있어 계속 증가하고 있음 [18]
  - 사이버범죄의 문제는 사이버공격에 대한 관련성을 부인하려는 국가가 해킹기술을 가진 범죄자를 협력자로 삼고 이들을 통해 사이버공격 행위를 하는 경우, [19] 사이버범죄로 인한 위협이 국가안보에 중대한 위협이 될 수 있다는 점임 [20]

- 이외에도 전자통신기술의 발전에 따라 새로운 무력공격의 양상으로 대두되고 있는 사이버무력공격이 있음
  - 특히 비대칭전력으로서의 사이버무력공격은 기존의 국제안보질서에 대한 위협이 되고 있으며 보다 빈번히 발생하고 있는 추세임

16) 국가사이버안전매뉴얼 (2004).
17) http://www.netan.go.kr/cyber/division.jsp (검색일: 2019. 10. 11)
18) 민수홍 외 역, 『범죄학 이론』 (지산, 2000), pp. 43-47.
19) Dmitri Alperovitch, "Virtual Criminology Report 2009: Virtually Here: The Age of Cyber Warfare," McAfee (2009), p. 11.
20) 이원상·채희정, "사이버범죄의 새로운 유형과 형사정책적 대안연구," 한국형사정책연구원 (2010), p. 17.

2. 수단

- 미국 테크놀리틱스 연구소는 사이버공격의 3대 무기로 컴퓨터 바이러스, 분산서비스 거부(DDoS) 공격, 지향성 에너지 무기를 지목하고 있음[21)]
  - 가장 오래된 사이버공격 무기인 컴퓨터 바이러스는 해킹을 이용하거나 인터넷 웜과 연계되어 강력한 감염력과 파급력을 보유하고 있음
  - 디도스(DDoS) 공격은 대상 시스템 자원을 다운시켜 원래의 용도대로 사용할 수 없게 만드는 것으로 포털, 금융, 온라인 쇼핑 등과 같은 일반대중들이 사용하는 사이트가 주요 공격대상임
  - 지향성 에너지 무기로는 전자장비를 마비시키거나 오작동 시키는 고출력 전자기파, 전투기 등 항공무기를 무력화시키는 전자펄스(EMP), 미사일이나 항공기 또는 지상통신장비 등을 파괴시키는 고출력 마이크로웨이브 등이 있음

- 사이버공간 특히 유선환경에서 타겟 공격을 감행하기 위한 지능화된 악성코드가 유포되고 있고, 정치·경제·사회·종교적인 목적을 가진 핵티비즘(Hacktivism)[22)] 공격 악성코드도 증가하고 있음
  - 사이버범죄 조직 등에 의한 악성코드와 특히 맥킨토시 사용자를 대상으로 하는 악성코드도 증가하고 있음[23)]
  - 무선환경에서는 안드로이드 악성코드의 수가 폭발적으로 증가하고 있고, SNS를 통한 악성코드 유포가 증가하고 있고, 앱 마켓 검증과정을 우회하는 악성코드가 등장했고, 새롭게 등장한 모바일 플랫폼에 대한 위협이 나타났음

- 지능형 지속 위협(APT) 공격 시 공격 대상자가 신뢰하는 한글 등의 워드프로세스나 유틸리티 등에서 발생하는 취약점을 피싱하는데 연계하여 활용할 경우에는 공격자의 입장에서 피싱 성공 확률을 상당히 높일 수 있기 때문에 해커의 입장에서는 취약점을 이용한 지능형 지속 위협 공격을 매우 선호함
  - 소프트웨어를 대상으로 한 취약점 공격이 증가하고 있고, 모바일 환경에 대한 취약점 공격이 지속적으로 증가하고 있음

21) https://www.boannews.com/media/view.asp?idx=44298&kind=3 (검색일: 2019. 10. 11).
22) 정치·사회적인 목적을 위해 자신과 노선을 달리하는 정부나 기업·단체 등의 인터넷 웹 사이트를 해킹하는 행위 (두산백과).
23) 한국인터넷진흥원, "민간분야 침해사고 동향" (2013. 3).

- 디도스 공격은 정형화된 공격수단을 이용하여 단순하게 대용량 디도스 공격의 형태로 발전하고 있음
  - 다른 공격수단들과 달리 방어를 힘들게 하기 위한 공격기법을 개발하기 보다는 점차 공격대상을 다변화하는 형태로 진화하고 있음
  - 이러한 사례를 보여주고 있는 것이 최근의 DNS를 공격대상으로 하는 디도스 공격빈도의 증가임
  - 이에 따라 국내외에서 급격하게 증가하고 있는 스마트폰 사용자로 인해 모바일 기기가 디도스 공격에 사용될 가능성도 매우 높아지고 있음

- 모바일 환경을 이용한 디도스 공격의 경우를 살펴보면, 현재까지 모바일 기기를 사용하여 실질적인 디도스 공격을 감행한 사례는 거의 없음
  - 그렇지만 모바일 기기를 공격 대상으로 하는 각종 형태의 악성코드가 급격히 증가하는 추세를 보이고 있는 것을 감안할 때 공격자가 디도스 공격을 위한 수단으로 모바일 기기를 사용할 가능성은 매우 커지고 있다고 할 수 있음

3. 양상

- 사이버공격을 시기적으로 구분해 보면, 2001년까지의 컴퓨터 바이러스에 의한 자기과시형 해킹 시기, 2002년부터 2006년까지의 1.25 인터넷 대란 등으로 나타난 악의적 해킹 시기, 2007년부터 2011년까지의 7.7 디도스 및 3.4 디도스 공격, 농협 전산망 다운사태, 네이트 해킹 등을 발생시킨 해킹의 고도화 시기, 2012년부터 현재까지의 기반시설공격, 사이버전, 클라우드 보안위협, 스마트폰 보안위협 등의 새로운 사이버공격 시기로 발전해오고 있음
  - 실체적 국가안보 위협은 2010년대부터 나타나기 시작했고 신기술 개발 영역에 대한 공격이 증가하고 있는 것으로 파악됨
  - 또한 사이버안보 강화에 따른 반작용 또는 확산 현상으로 금전 탈취 등이 발생하고 있음
  - 요컨대 전 방위적 사이버공격 양상이 특징으로 나타나고 있음

- 개인차원의 공격으로 최근 스마트폰 및 모바일 환경에 대한 위협이 증가하고 있음
  - 스마트폰을 노린 악성코드가 급증하고 있으며, 안드로이드 OS기반 스마트폰의 경우 폭발적으로 증가하고 있어 스마트폰 악성코드를 이용하여 대화·통화 내용 도청 및 디도스 공격이 가능한 상황임

- 블루투스, 이동통신서비스(3G, 4G), 무선랜(Wi-Fi), GPS 등 복수의 통신기능이 탑재됨에 따른 사이버 침해경로의 다변화로 인한 위협이 증가하고 있음
- 특히 SNS를 통한 사이버공격, 클라우드 서비스에 대한 사이버공격, 융합 정보통신 산업을 목표로 하는 다양한 사이버공격이 증가하고 있음

• 국가차원의 사이버공격을 살펴보면, 1990년 미국이 이라크에 수출하는 프린터에 컴퓨터 바이러스를 침투시켜 1991년 걸프전 당시 이라크의 방공망을 마비시킨 사이버공격이 최초의 사례임
- 2003년 미군의 이라크 침공 전 이라크 정보시스템에 대한 사이버공격이 있었고 이후 전장에서 미군은 전자폭탄을 투하하여 전자장비를 마비시키는 등 다양한 첨단 전자무기를 활용하여 정보체계를 마비시켰음
- 2007년 이스라엘이 시리아 폭격 전 시리아 레이더 시스템에 악성코드를 침투시킨 사이버공격은 시리아의 방공망을 무력화시켰음
- 2007년 러시아의 에스토니아 대한 사이버공격은 정부 전산망에 연결된 수만 대의 컴퓨터에 대한 디도스 공격으로 인해 3주 이상 국가의 주요 기능이 마비되는 피해를 발생시켰음
- 2008년 조지아에 대한 러시아의 사이버공격은 러시아가 조지아를 침공하기 전에 조지아 정부기관 웹 사이트와 전산망, 방위시설에 대한 사이버공격을 감행한 것으로 직후 진행된 물리적인 군사작전과 동시에 진행됐다는 특징을 보여줌
- 2010년 이란에 대한 미국과 이스라엘의 스턱스넷을 이용한 사이버공격은 핵시설 시스템에 악성코드를 침투시켜 이란의 핵무기 개발을 상당기간 지연시키는 결과를 얻었음
- 2014년 러시아의 크림반도 점령과정에서의 우크라이나에 대한 사이버공격으로 우크라이나 정부의 전산망이 파괴되었고 러시아는 오우로보로스라는 사이버 무기를 사용했는데 물리적 파괴가 아닌 정보의 절도와 조작 위주의 사이버첩보활동의 형태로 진행되었음[24)]
- 미국 정부가 주도한 이란 핵시설 공격이 드러난 이후, 국가차원의 조직화된 사이버공격이 증가하면서 사이버 공간의 주도권 장악 및 사이버무기 개발을 위한 대규모 프로젝트들이 가동되고 있어 이제는 사이버전이 본격화되고 있는 양상임

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

- 사이버공간으로의 국가안보영역의 확대로 세계 수준의 기술을 보유한 국가에서 기술유출 범죄가 증가 추세를 보이고 있음
  - 중국 해커들은 사이버 기술을 이용하여 미국의 산업기밀 유출을 시도했고 국가 역량을 사이버 기술을 이용한 첩보 수집에 집중하고 있음
  - 예를 들어 중국 해커들은 대만 정보기관을 사이버공격하기도 하였고 이에 따라 사이버전 대응 양상이 방어에서 공격으로 전환되고 있음
  - 사이버 심리전 차원의 일반 국민 여론과 인식의 조작도 발생하고 있어 이에 대응하기 위해 국가 차원의 사이버전을 준비할 필요가 있음

- 북한의 경우에도 해외에 거점을 둔 북한의 사이버공격 조직이 국내 금융사이트를 사칭한 피싱 사이트를 개설하여 금융정보 절취 및 공작 자금을 마련하는 사례가 있었음
  - 북한은 유투브, 트위터, 페이스북 등 새로운 인터넷 매체를 이용 대남 선전 등 사이버 심리전을 전개하고 있음
  - 북한은 인민무력부 총참모부 산하에서 기술정찰조를 운영하여 정보수집을 하고 있고, 사이버 정찰조를 통해 한국군의 전산망 해킹도 시도했음
  - 북한은 러시아의 기술을 도입하여 강력한 전자파 무기도 개발 중임

- 향후 북한의 사이버공격이 급격히 증가할 가능성이 있으며 북한의 사이버전 능력은 상당한 수준으로 유지되고 있음
  - 1980년대부터 사이버전 대비 인민군 총참모부에 평양자동화대학을 설립하여 정찰총국을 비롯해 약 7,000명에 가까운 사이버전력을 갖춘 것으로 알려짐
  - 7.7 디도스 사태와 같은 공격 능력을 보유함과 동시에 인터넷 연결 최소화를 통해 효과적인 방어능력도 보유하고 있어 상당한 위협이 될 만함
  - 사이버전을 통해 적은 비용으로 한국에 치명적 타격을 가하기 위하여 창설된 사이버전 수행부대는 광역망을 이용한 사이버공격 가상훈련 및 한국을 대상으로 악성코드 유포 및 디도스 실전훈련 등을 수행하고 있음

Ⅳ. 한국의 대응방향

- 오늘날 국제사회에서 사이버공격의 양상이 다양해지고 이러한 공격이 국가에 미치는 피해규모와 파급영향이 점점 더 심해지고 있음
  - 나아가 개인에 의한 사이버공격 역시 국가에 의하여 주도되거나 고도로 조직화됨에 따라 심대한 안보위협으로 부상하고 있음
  - 국제적 해커집단의 행위 역시 단순히 개인의 권리에 대한 침해 수준을 넘어 조직적 테러리즘의 수준에 도달하고 있음
  - 이와 같이 국가를 배후로 하거나 국제적 해커집단에 의한 사이버공격의 추세는 지속적으로 증가할 것으로 예상되므로 국가안보차원에서의 대응방안이 요구됨
  - 특히 사이버공격의 특성에 부합한 보다 효율적인 대응을 가능하게 하고, 종합적 국가위기관리 전략과의 일관성을 유지하기 위해서는 국가안보차원의 대비와 관리 및 대응체계가 필요함[25)]

- 한국의 대응방향으로 첫째 사이버공간에 대한 안전성을 확보하는 것이 필요함
  - 네트워크의 보호와 국가핵심시설의 안정성을 확보하기 위해 사이버공격에 대한 방어선을 구축하여 정부, 공공기관, 민간부문의 네트워크 취약성을 보완하고 예방능력을 증진해야 함
  - 일원화된 사이버안보 추진 체계를 확립하여 국가 사이버안보 업무의 실질적인 총괄 조정 능력을 확보하기 위해 별도의 정보보안 기금을 조성하고 필요한 기술을 전담 개발할 수 있는 전담 연구 기관을 지정해야 함
  - 국가 사이버안보 기술개발의 법적근거를 마련하기 위해 사이버안보기본법을 제정하고 개별법들을 통·폐합하는 등 정보통신기술 변화에 따른 사이버공격에 대한 대응을 보다 효과적으로 수행하기 위해 관련법들을 지속적으로 정비해야 함

25) 채재병, 앞의 글, p. 189.

• 둘째 사이버공격에 대한 억지력을 확보하는 것이 필요함
  – 사이버반격 능력 확보 및 공격 의지 무력화, 국제 공조 강화를 통해 사이버 억지력을 확보하기 위해 사이버 방어능력을 강화하고 선제적 사이버 방어체제를 구축해야 함
  – 사이버공격 대응체계를 사전예방 중심으로 전환하고, 사이버공격 수단이 다양화하는데 따른 방어수단의 개발, 즉 사이버공격 대응기술 개발 등에 중점을 두어야 함
  – 수동적 방어 형태에서 벗어나 선제적·적극적 방어로 전환하여 사이버공격 정보의 적극적 수집과 위해세력 적발 시스템 및 자원 무력화를 포함한 총괄 대응체계를 확립해야 함

• 셋째 정보보안 정책의 성공적 추진을 위한 사이버안보 기반을 조성하는 것이 필요함
  – 국가·공공기관 사이버안보 의식을 강화하고 대국민 홍보를 통해 사회전반에 사이버안보 의식을 고취시키기 위해 전 국민을 대상으로 하는 다양한 교육 및 홍보 프로그램을 개발하고, 사이버안보 의식 확산, 대국민 사이버안보 인식 확대 및 저변 확대를 위해 정부 및 공공기관, 민간기업, 국민 등을 대상으로 사이버안보 의식 제고와 실천 활동을 강화해야 함
  – 민·관·군 협력시스템을 강화하여 사이버안보 개념에 대한 인식 공유와 민·관·군 역할 정립을 통해 공동체 개념의 유기적 협력체제로 발전시키기 위해 사이버공격과 관련된 이슈들과 각 기관별 시스템을 통합할 수 있는 국가차원의 정보공유 시스템을 구축하여 민·관·군 합동대응체계를 정립해야 함
  – 유사시 사이버예비군으로 사용할 수 있는 사이버안보 전문 인력을 양성하기 위해 국가 사이버안보 강화를 위한 정보보안 핵심 인재양성 프로그램을 개발 및 시행함으로써 화이트해커 등 사이버안보 관련 인재육성을 강화해야 함

• 넷째 국제 사이버협력 네트워크를 확충하는 것이 필요함
  – 국제 사이버정보공유체계를 구축하고, 사이버안보 국제규범화 및 국제 거버넌스에 주도적으로 참여할 필요가 있음[26)]
  – 주요 국가들과 양자 및 다자간 사이버협력 확대 및 정보공유체계를 구축하고 정보공유체계를 주변국으로 확대시켜 국제 사이버안보 공조체제를 구축, 강화해야 함
  – 공공·민간분야 공조 강화 및 사이버 분야 중재자로서 국제협력을 확대하고 이를 위해 사이버보안 취약국가들에 대한 지원을 위해 사이버 공적개발원조를 시행해야 함
  – 이러한 지원은 정보통신기술 선·후진국 간의 정보격차를 줄이는데 기여하고 국제사이버공간 주도권 확보에도 도움이 될 것임

26) 위의 글, p. 190.

참고문헌

국가사이버안전관리규정. 제2조. 2013.

국가사이버안전매뉴얼. 2004.

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

민수홍 외 역.『범죄학 이론』. 지산, 2000.

방송통신사이버안전센터운영규정. 제4조. 2013.

부형욱. "사이버안보의 주요이슈와 정책방향."『국방연구』56권 2호 (2013).

이연수·이수연·윤석구·전재성. "주요국의 사이버안전관련 법·조직체계 비교 및 발전방안 연구."『국가정보연구』제1권 2호 (2008).

이원상·채희정. "사이버범죄의 새로운 유형과 형사정책적 대안연구." 한국형사정책연구원, 2010.

채재병. "안보환경의 변화와 사이버안보."『정치·정보연구』제16권 2호 (2013).

한국인터넷진흥원. "민간분야 침해사고 동향." 2013. 3.

Alperovitch, Dmitri. "Virtual Criminology Report 2009: Virtually Here: The Age of Cyber Warfare." McAfee (2009).

Soafer, Abraham D., David Clark and Whitfield Doffie. "Cyber Security and International Agreements." in Committee on Deterring Cyber Attacks. *Proceedings of a Workshop on Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*. The National Academies Press, 2010.

Symantec. 2013 Internet Security Threat Report, Vol. 18. Appendix (Apr. 2013).

http://khnews.kheraldm.com/view.php?ud=20130719000771&md=20130722003209_AT (검색일: 2019. 10. 11).

https://www.boannews.com/media/view.asp?idx=44298&kind=3 (검색일: 2019. 10. 11).

http://www.dt.co.kr/contents.html?article_no=2019071802109931650002&ref=naver (검색일: 2019. 10. 11).

http://www.netan.go.kr/cyber/division.jsp (검색일: 2019. 10. 11).

Abstract

Changes in the Cybersecurity Environment and the Response of Korea

This study aims to explore Korea's response to the recent changes in the cybersecurity environment at home and abroad. Cyber attacks in the global society are becoming more diverse and the extent of the damage and ripple effects of these attacks on the nation are getting serious. In order to respond more efficiently to the characteristics of such cyber attacks, national security-level preparedness, management and response systems are needed. Accordingly, Korea should focus on securing safety in cyberspace, securing deterrence against cyber attacks, creating a cybersecurity base for the successful implementation of its cybersecurity policy, and expanding the network of international cyber cooperation.

Keywords: cybersecurity, cyber attack, international cyber cooperation, cybersecurity environment, cyberspace

INSS 전략보고

May 2020. No. 78

※ 본지에 실린 내용은 집필자 개인의 견해이며, 국가안보전략연구원의 공식입장이 아닙니다.

국가안보전략연구원

06295 서울시 강남구 언주로 120 인스토피아 빌딩
02-6191-1000 02-6191-1111 www.inss.re.kr