4차 산업혁명과 보안 패러다임 변화

송근혜, 이승민*
ETRI School(UST) 박사과정
한국전자통신연구원 책임연구원 *

I. 서론

4차 산업혁명 시대가 도래하면서 사람과 사람, 사람과 사물, 사물과 사물이 긴밀하게 연결되고 있다. 블록체인, 사물인터넷, 인공지능과 같은 4차 산업혁명을 동인하는 기술들은 우리 사회를 풍요롭게 만들고 윤택한 삶을 가져다 줄 것으로 기대된다. 그러나 이러한 기술을 악용하여 기존 공격수법을 더욱 정교하게 만들거나 과거에는 존재하지 않았던 완전히 새로운 방식의 사이버 공격이 발생할 가능성이 높아졌다. 특히, 인터넷에 연결되는 기기의 수가 많아지는 4차 산업혁명 시대에는 사이버 공격대상이 기존에 비해 더욱 광범위해질 수밖에 없다. 이러한 흐름을 반영하여 정보보호 개념을 새롭게 정립하고 합당한 전략을 세울 필요성이 생겼다. 이에 본 고는 새로운 보안 위협을 심층적으로 분석하고, 보안 패러다임의 변화에 맞춘 신규 대응책을 마련하고자 한다.

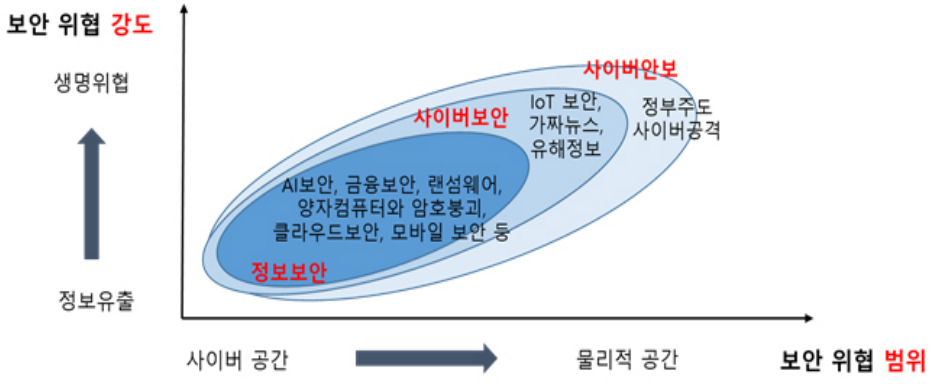
II. 보안 패러다임 변화 방향

본 절에서는 세계 주요 기관(McAfee, Trend Micro, Kaspersky Lab, Symanctec, Gartner, IBM, CISCO, Wired, AhnLab, KISA 등)에서 최근 1년 동안 제시한 보안 트렌드를 분석하여 4차 산업혁명 시대의 보안 패러다임 변화 방향을 제시하고자 한다[24]. 최근의 보안 트렌드를 살펴보면 민간 영역에서 발생하는 위협의 범위가 국가 안보를 위협하는 수준으로 확대될 뿐만 아니라, 정보유출에 국한되던 공격의 강도가 인간의 생명을 위협하는 수준으로 높아지고 있다. 이렇게

* 본 내용은 송근혜 저자(☎ 042-860-6702, ghsong0227@etri.re.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

보안 위협의 범위와 강도가 증가하는 원인은 4차 산업혁명을 주도하는 신기술의 급속한 발전에 따른 것으로 보인다. 예를 들어, 인공지능과 양자컴퓨팅 등의 신기술을 적용한 새로운 공격 수법은 전례 없는 위협을 초래할 수 있다. 물리적 현실 세계와 디지털 가상 세계를 연결하는 사물인터넷으로 발현되는 초연결사회에서는 보안위협의 범위가 더 이상 사이버 공간에 국한되지 않는다. 뿐만 아니라 과거 정보보호기술에서 소극적으로 대응해도 충분했던 사이버위협이 국가 안보를 위협하는 수준으로 강해지고 있다.

본 절에서는 4차 산업혁명 시대에 발생하는 보안 위협 수준을 기준으로 정보보호개념을 정보보안, 사이버보안, 그리고 사이버안보로 구분하였다. 정보보안(Information Security)은 정보의 비밀성, 무결성, 가용성을 유지하기 위해 권한 없는 사용자로부터 정보의 유출, 훼손, 변조를 예방하고 대응하는 전략이다[1]. 사이버보안(Cyber Security)은 ICT 기술을 매개로 개인, 기업, 정부기관의 취약점을 공격하여 인간의 생명과 정신 그리고 물리적 자산을 위협하는 공격으로부터 방어하는 전략을 의미한다[17]. 사이버안보(Cyber Defense)란 국가의 안보를 위협하는 사이버 공격으로부터 국가를 방어하는 전략이다[4]. [그림 1]에서는 이러한 세 가지 보안개념을 위협의 강도와 범위에 따라 구분하여 보안 패러다임의 변화를 표현하였다.



<자료> ETRI 자체 작성

[그림 1] 보안 패러다임 변화

양적・질적으로 변화하는 보안위협에 대한 대응은 기존과는 다른 방식으로 전개되어야 한다. 이를 위해서는 4차 산업혁명 시기에 신기술을 적용한 새로운 방식의 보안위협이 어떠한 양상으로 이루어질 것인지, 피해의 종류에는 무엇이 있는지를 구체적으로 살펴보는 것이 중요하다. 보안 위협의 강도에 따른 피해 유형을 살펴보면 [표 1]과 같다.

[표 1] 보안 위협에 따른 피해 유형

보안 위협	피해 유형(개인, 기업, 국가)
정보유출	[개인] 개인 데이터・생체정보 유출(PC, 모바일, 웹캠, CCTV 등) [기업] 고객정보 유출, 기업 기밀정보 유출 [국가] 국가정보・군사정보 유출, 국가기반시설정보 유출
금전・경제적 피해	[개인] 단말기 오작동, 데이터 삭제, 암호화 등 사용 불가 [기업] 기업 전산망・시스템 오작동・마비 [국가] 국가기반시설 마비, 재난사고 유발
정신적 피해, 사회 건전성 위협	[개인] 인신공격(사이버왕따, 가짜뉴스 등) [기업] 기업 이미지 하락(가짜뉴스) [국가] 사회갈등・대립・혼란조장(가짜뉴스), 건전성 훼손(불법・유해정보 유통)
생명위협	[개인], [기업] 개인 및 고객의 생명위협(자동잠금장치 해킹으로 주거침입, 개인 의료장비 해킹, 자동차 해킹 등) [국가] 국가를 향한 사이버테러 위협

<자료> ETRI, 정보보호동향 및 보안위협 분석, 2017.

Ⅲ. 신규 보안 위협

1. 정보보안

정보보안은 각종 위협으로부터 정보를 보호하는 것을 의미한다. 구체적으로, 정보를 제공하는 공급자와 정보를 소비하는 사용자가 정보를 다루는 과정에서 발생할 수 있는 정보의 유출, 훼손, 변조를 예방하고 제한하는 조치를 뜻한다. 1990년대 말 정보화시대에 접어들면서 정보를 자산으로 여기고 관리하는 활동의 중요성이 커졌다. 이에 따라 많은 기관들이 정보자산을 안전하게 보호하기 위해 네트워크, 시스템, 통신 및 전산시설, 사용자의 정보유출 예방행동 등에 초점을 두고 정보자산을 관리해 왔다. 그런데 최근 사이버 공격 기법을 강화하고 피해 범위를 확대시킬 수 있는 기술들이 새롭게 부상하고 있다. 즉, 과거 정보의 유출, 훼손, 변조에만 국한되었던 사이버 공격이 신기술의 등장과 함께 공격의 강도를 높이고 공격범위를 확장할 수 있게 되었다. 정보보안 측면에서 새롭게 부상하는 위협으로는 양자컴퓨팅, 랜섬웨어의 보편화와 익명화, 블록체인의 취약점을 파고드는 사이버 공격, 그리고 인공지능기술의 악용을 들 수 있다. 위협양상과 위협에 대응하기 위한 각종 기관의 노력을 살펴보겠다.

첫째, 양자컴퓨팅 기술의 발전과 실용화는 기존 암호체계의 붕괴 가능성을 높이고 있다. 미국 국가안보국(NSA)은 2016년부터 양자컴퓨팅 기술이 현재의 암호질서를 파괴할 수 있음을

전망하였고[12], 캐나다 연구기관 Global Risk Institute는 2031년 현재의 암호체계가 양자컴퓨터로 붕괴될 가능성이 50% 이상임을 주장하였다[16].

이러한 위험을 사전에 감지한 전 세계의 주요 국가들은 암호붕괴가 결코 먼 미래의 일이 아님을 인식하고 복제 불가능한 암호통신 기술과 포스트 양자암호 기술 개발에 힘쓰고 있다. 예를 들어, 미국은 NSF, IARPA, DARPA 등의 연구기관의 주도로 양자암호 통신기술을 비공개로 연구하고 있다. EU는 'EU Qurope 프로그램'을 통해 양자정보통신 R&D 로드맵을 제시하고 연간 525억 유로를 투자할 계획을 수립하였다. 중국은 양자암호통신 위성 묵자호를 발사하고, 이를 이용하여 1,203km 떨어진 지역에서 양자 정보의 순간이동을 성공적으로 구현하였다. 일본은 2010년부터 NICT 주도로 양자암호통신기술을 개발하고 있으며, 2017년 통신위성 SOCRATES를 매개로 우주와 지상 간 양자 암호키 분배 실험에 성공하였다. 우리나라도 2017년 SKT가 왕복 112km 구간에서 양자 암호키 전송에 성공하였고, KT와 KIST는 공동으로 양자통신 응용연구센터를 개소하여 양자통신연구에 박차를 가하였다[24].

소인수 분해나 이산대수 문제 기반이 아닌 새로운 수학적 어려움을 이용한 포스트 양자암호(Post-quantum Cryptography) 기술 개발도 진행 중이다. 미국 NIST는 포스트 양자암호 공개키 알고리즘 공모를 2017년 11월에 진행하였고, Google은 Chrome Canary 브라우저에 포스트 양자암호 CECPQ1을 구현하여 서버와 브라우저 간 보안기능이 향상된 알고리즘을 개발하였다. 캐나다 정부 및 금융기관에 보안제품을 공급하는 ISARA는 RSA 2017에서 양자컴퓨터에 대응하는 보안기술을 개발하고 있다고 발표하였다. 국내 보안업체 NSHC도 포스트 양자 암호 모듈 SIDH(Supersingular Isogeny Diffie-Hellman)를 탑재한 모바일 보안제품을 생산하기 위한 노력을 기울이고 있다.

둘째, 신기술로 익명화된 랜섬웨어 공격주체들이 증가함에 따라 랜섬웨어로 인한 피해가 더욱 확산될 것으로 전망된다. 랜섬웨어는 다른 악성코드와 달리 파일을 암호화하고 화면을 잠그는 등 정보의 가용성을 침해하여 금전을 요구하는 특징을 지닌다. 또한, 오픈소스로 코드가 공개된 암호화 알고리즘을 사용하기 때문에 상대적으로 생성이 쉬운 악성코드에 속한다. 그런데 최근 봇넷으로 랜섬웨어 제작을 대행하고 금전적인 대가를 요구하는 RaaS(Ransomware-as-a-Service)가 등장하여 기술적 역량이 없는 사람도 언제든지 랜섬웨어를 대행 제작하여 활용할 수 있게 되었다. 랜섬웨어 제작과 관련하여 수요-공급이 오가는 시장이 생겨나고 있는 것이다. 랜섬웨어 공격자들은 다크 웹(Dark Web)을 이용하거나 암호화폐를 사용하여 계좌 추적을 피하는 등 자신을 익명화하고 있다. 랜섬웨어의 제작 및 활용 가능 주체가 증가하고 이에 대한 추적이 더욱 어려워진다는 사실은 랜섬웨어 공격으로 인한 피해가 많아질 것임을

의미한다.

셋째, 전 세계가 자본주의 체제로 전환하면서 금융기관은 보안의 핵심 대상으로 관리되어 왔다. 그러나 전자금융거래가 보편화되면서 금융기관을 대상으로 한 사이버공격은 갈수록 정교하게 진화하고 있다. 특히, 전 세계 금융기관에서 사용하고 있는 SWIFT(Society for Worldwide Interbank Financial Telecommunication)를 표적으로 삼은 공격이 증가하고 있다. SWIFT는 표준화되고 신뢰할 수 있는 국제 금융 네트워크로 전 세계 200여 개국의 약 11,000개의 금융기관이 SWIFT 네트워크에 연결되어 있다. SWIFT를 대상으로 한 사이버공격으로는 SWIFT 메시지 조작, 은행원들이 보는 화면 상 거래금액의 변조 등이 있다. 블록체인 기술이 SWIFT의 보안문제를 상당부문 해결해 줄 것으로 기대되고 있으나, 최근 EU 산하 정보보호기구 ENISA(European Union Agency for Network and Information Security)는 블록체인이 기존 금융시스템에 적용된다 하더라도, 기존의 금융보안 취약성이 사라지지 않는다고 주장하였다. 예를 들어, 사이버 공격 주체들은 암호키 생성 알고리즘의 취약성을 이용하여 금융자산 및 기밀거래 내역을 누출하거나, 도난 및 분실된 암호키를 악용하여 거래정보를 유출할 수 있다. 또한, 블록체인 상 합의과정을 조작하여 원하는 방향으로 합의를 유도하거나, 거래량을 증가시켜 블록체인 처리속도를 떨어뜨리고 서비스를 제한할 수 있다. 블록체인의 익명성을 이용하여 사기거래, 자금세탁, 이중지불과 같은 비정상거래도 발생할 수 있다[10]. 따라서 블록체인 기술이 도입된다 하더라도 금융기관을 대상으로 하는 사이버공격은 여전히 위협적일 것이며, 블록체인 네트워크에 연결된 모든 컴퓨터가 공격대상이 될 수 있기 때문에 피해의 범위도 더욱 커질 수밖에 없다.

넷째, 인공지능 기술 개발의 문턱이 낮아지면서 사이버공격 수단으로 인공지능 기술을 활용하려는 조짐이 커지고 있다. 최근 Amazon, MS, IBM, Google이 TensorFlow, DMTK 등과 같은 인공지능 기술을 클라우드 서비스로 제공하면서 인공지능 기술 개발의 대중화가 시작되었다. 그러나 한편으로는, 사이버 공격 주체들이 인공지능 기술을 공격 수단 진화용도로 악용할 가능성도 높아졌다. 현재의 인공지능 기술은 보안 전문가가 장시간 코드를 분석하여 발견해야만 하는 보안 취약점을 쉽게 포착할 수 있다. 사이버 공격 주체는 표적기관의 보안 취약점을 찾아내는 방법으로 인공지능 기술을 활용하고자 할 것이다.

4차 산업혁명이 현실화될수록 사이버 전쟁의 주체가 인간에서 인공지능으로 전환될 가능성 또한 높아졌다. 세계 최대 보안행사인 DEFCON에서는 사이버전쟁의 공격과 방어가 모두 인공지능 기술만으로도 가능함을 보여주었다[7]. 인공지능 기술은 피해자의 취약점을 찾아내고 정밀한 공격이 가능하도록 사이버 무기를 스스로 제작하는 잠재성을 갖고 있으므로 이에 대한 대응책을 마련할 필요가 있다.

양자컴퓨터의 실용화, 랜섬웨어의 보편화, 블록체인 보안이슈, 그리고 인공지능 기술을 악용한 사이버 공격은 단순 정보 유출, 훼손, 변조를 넘어 자금을 갈취하고 사회 합의과정을 침해하는 위협으로 진화할 것이며 이에 따른 피해 범위도 더욱 넓어질 것이다.

2. 사이버보안

사이버보안이란 해킹으로부터 컴퓨터 내의 정보뿐만 아니라, 인간의 신체와 심리, 물리적 시설과 같은 비정보 자산을 보호하는 행위를 의미한다. 4차 산업혁명 시대에 사이버보안을 위협하는 요인에는 IoT 공격과 가짜뉴스가 있다.

4차 산업혁명 시대에는 IoT 기기의 보급 확산에 비례하여 사이버 공격으로 인한 피해가 함께 증가할 전망이다. 과거에는 인터넷에 연결되는 기계가 주로 PC에 국한되어 있었고, PC를 '좀비화'하여 DDoS 공격을 시도한 사례가 종종 발생하였다. 그러나 모든 사물이 인터넷에 연결되는 4차 산업혁명 시대에는 '좀비화'의 위험에 놓인 기계가 매우 많아지게 된다. 시장조사기관 Errricson에 의하면, IoT 기기의 보급률은 2015년 약 46억 개에서 2021년 약 160억 개에 이를 것이며, 연평균 23%의 시장 성장률을 보일 것으로 예상된다[6]. 그런데 IoT 기기는 오픈소스를 활용하는 특징 등으로 인해 보안 취약성이 높을 뿐만 아니라 공격에 쉽게 노출되어 있다. 실제로 이러한 약점을 이용하여 IoT 기기를 표적삼은 공격이 발생하였다. 2016년 미국에서 IoT 기기를 감염시켜 아마존, 뉴욕타임즈 등의 주요 사이트를 두 시간 이상 마비시킨 DDoS 공격이 발생하였다[9]. 더욱이 IoT가 사이버공간과 현실공간의 경계선에 위치한다는 특징 때문에 단말기와 사이버세계에 한정되었던 사이버 공격의 대상이 인체, 물리적 자산 등의 현실세계로 확대될 가능성이 높아졌다. 예를 들어, 스마트 의료기기를 공격하여 건강에 악영향을 미치거나, 자율주행차를 해킹하여 차량 사고를 유도할 수 있다. 또한, 웨어러블 디바이스를 통해 수집한 개인의 심리 및 생리적 데이터를 조작하여 생명을 위협하는 범죄가 발생할 가능성도 커졌다.

4차 산업혁명 시대에는 인간의 감정이나 인지적 과정에 개입하여 현실적인 이득을 취하는 새로운 공격수단도 나타날 전망이다. 모바일 보급 확산으로 개인의 일상생활에서 SNS가 차지하는 비중이 커지고 있다. SNS의 발달로 전 세계 어느 곳에서나 생성되는 정보를 손쉽게 받아볼 수 있게 되었고, 정보의 내용에 대해 직접 소통할 수 있게 되었다. 4차 산업혁명 시대에는 정보의 접근성이 더욱 높아지고, 사이버 세계에서의 타인과의 소통도 더욱 빈번해질 것이다. 문제는 비도덕적이거나 진실과는 거리가 먼 정보를 접할 가능성도 함께 증가한다는 점이다.

최근 검열되지 않은 다양한 콘텐츠가 쏟아지고 있는 SNS를 이용하여 개인의 감정과 인지적 과정을 조작하는 가짜뉴스가 SNS를 중심으로 확산되고 있다. 가짜뉴스는 사실 여부와 관계없이 자신의 기호에 맞는 콘텐츠를 즉흥적으로 소비하는데 집중하는 대중의 성향[25]을 이용한다. SNS 사용자가 접한 가짜뉴스는 현실 정보를 왜곡하여 처리하도록 사용자의 지각(perception)을 조작하는 인지적 해킹(cognitive hacking)이다. 가짜뉴스가 사이버보안 문제로 부상하는 이유는 집단의식을 부추겨 정치적 의사결정 과정에 결정적인 영향력을 행사할 수 있기 때문이다. 실제로 지난 미국 대선의 마지막 3개월 간 주요 언론 기사에 대해 페이스북에서 공유되고 댓글이 달린 반응은 약 730만 건이었던 반면, 생성된 가짜뉴스는 870만 건에 이르렀다[15]. 지난 프랑스 대선 기간에 양산된 정치뉴스의 25%가 가짜뉴스임이 드러나기도 하였다[11]. 가짜뉴스를 이용하여 정치적 의사결정에 영향을 미치려는 시도가 세계 곳곳에서 벌어지고 있는 것이다. 뿐만 아니라, 가짜뉴스를 퍼뜨려 경쟁기업의 이미지를 훼손시키거나, 사회적 손실을 유발하는 사례도 보고된다. 예를 들어, 중국의 Xiezuobang이라는 업체는 부동산, 금융, 엔터테인먼트 등 다양한 분야에서 내용의 진위여부와 관계없이 고객이 원하는 정보를 생성하고 전파하는 대가로 금전적 이득을 취한다[18]. 중국 투자자본이 핏빗(Fitbit)을 인수한다는 소식에 핏빗의 주가가 2.11% 상승했으나 가짜뉴스인 것이 밝혀지기도 하였다[8]. 미얀마에서는 무슬림세력이 불교 신자가 많이 거주하는 지역을 공격한다는 가짜뉴스가 유포되어 무슬림신자를 폭행하는 사건이 발생하였다[2].

가짜뉴스의 악영향을 제한하기 위해 페이스북과 같은 글로벌 ICT 기업들은 가짜뉴스를 식별하고 기사 내용의 신뢰성을 담보하는 기술을 적극적으로 개발하고 있다[3],[5]. 그러나 인공지능 기술을 악용한 가짜 뉴스 제작 역량이 이를 간파하는 능력을 압도하기에 디지털 콘텐츠에 대한 불신은 더욱 커질 전망이다[14].

이처럼 4차 산업혁명 시대에는 사이버 공격 주체가 IoT와 가짜뉴스를 매개로 가상세계를 뛰어넘어 현실세계에 금전적, 심리적, 신체적 위협을 초래할 수 있다. 즉, 사이버 공격으로 인한 피해범위가 더욱 넓어지고, 공격수단은 더욱 다채로워질 전망이다.

3. 사이버안보

사이버안보는 국가 안보에 위협을 주는 모든 사이버 공격에 대한 대응 전략을 말한다. 사이버안보에서는 공격의 주체를 개인과 집단, 국가로 설정하는데, 이는 과거 국가의 안보를 위협하는 공격의 주체를 국가 단위로 한정했던 범위를 확장하는 것이다. 이러한 변화는 기존에

국가가 안보전략을 육・해・공 영역에 맞춰 세워온 인식에서 벗어나 가상공간도 국가 안보 영역임을 시사하는 것이다.

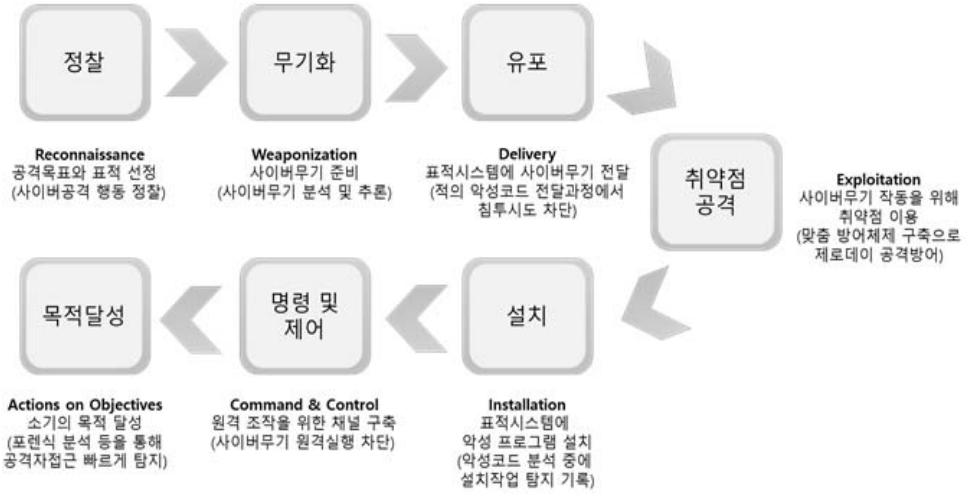
사이버공격이 국가안보에 실질적인 위협이 될 수 있다는 사실은 여러 사례를 통해 밝혀지고 있다. 예를 들어, 2010년 이란의 우라늄 농축 시설에 대한 공격이 Stuxnet이라는 악성코드를 사용한 사이버공격에서 비롯되었으며, 물리적 군사 공격에 버금가는 타격을 입힌 것으로 나타났다. 당시 이란의 핵시설에 대한 사이버 공격의 배후로 미국과 이스라엘이 지목되었다. 미국의 영화제작업체 소니픽처스에 대한 해킹으로 미공개작품과 직원정보 등이 유출된 사건도 발생했는데, 당시 소니픽처스는 북한의 김정은 위원장을 암살하는 내용을 다룬 영화상영을 앞두고 있었다. 소니픽처스 해킹 배후로 FBI는 북한을 지목하였다. 2016년 미국 대선 기간에 민주당 주요 인사들의 이메일이 해킹되어 당시 대통령 후보였던 힐러리 클린턴은 이미지에 큰 타격을 입었다. 힐러리 클린턴 후보 진영의 이메일 해킹의 배후로 FBI와 CIA는 러시아가 의심된다는 입장을 밝혔다. 이러한 사례들은 현실세계의 분쟁이 사이버공격으로 이어질 수 있으며, 실제 군사 공격에 버금가는 피해를 입힐 수 있음을 알려준다[25].

사이버공격에 대응하기 위해 국가 차원에서의 노력이 활발하게 진행되고 있다. 선진국에서는 사이버공간을 육・해・공・우주에 이어 제5의 전장으로 설정하여 사이버안보 체계를 구축하고 있다. 미국은 국가 사이버안보정책을 총괄하는 사이버안보 거버넌스 체계를 오바마정부 시절부터 마련하였다. 오바마정부는 사이버안보 정책으로 미국의 안보와 가치, 국제질서를 아우르는 '2015국가안보전략'과 미국 본토의 이익을 보호하고 군사작전을 지원하기 위한 사이버 전술 제공 내용을 담은 'US DoD 사이버전략'을 발표하였다. 미국의 안보전략 싱크탱크인 국제전략문제연구소(Center for Strategic International Studies)는 트럼프 대통령 당선 직후 '사이버보안 아젠다'를 발간하여 사이버공격 기준과 방어 대상에 대한 우선순위를 마련하고, 백악관에 사이버안보조정관을 새롭게 임명하여 사이버안보 인적역량 강화를 위해 상비군과 예비군을 활용할 것을 제안하였다. 최근 트럼프 정부는 "연방 네트워크와 주요기반 시설의 사이버보안강화 행정명령"을 발표하여 국가 핵심시설의 사이버보안 및 국가 사이버안보역량 강화를 위한 전략을 수립하였다[22]. 중국은 2016년 네트워크보안법을 제정하여 사이버공간의 주권과 사이버보안 체계 전략을 세웠다. 중국이 사이버공간을 국가 주권으로 포함시켰다는 점을 주목할 필요가 있다. 또한, 2016년 '국가사이버공간안전전략', 2017년 '사이버공간 국제협력전략'을 발표하여 군사적 관점에서 대내외 전략을 수립하였다. 특히, 위성, 사이버, 정보, 전자자원을 통합하여 정보자산을 중국의 전군에 제공하는 '정보우산' 역할을 담당하는 전략지원부대를 창설하였다. 시진핑 주석은 빅데이터와 인공지능 기술을 활용하여 사이버전쟁 역량을

갖출 수 있도록 전략지원부대를 중심으로 군사 지휘체계를 마련하였으나, 전략지원부대의 구체적인 구조와 임무는 베일에 가려져있다[23],[27]. 일본은 2014년 내각관방에 사이버보안 전략과 정책을 종합・조정하는 사이버보안센터를 설치하여 사이버위협을 분석하고 사이버보안에 대한 중장기계획을 수립하였다. 또한, 총무성 산하에 '정보보안 자문위원회'를 두어 사이버보안 정책을 검토하고 새로운 정책 방향을 제시하였다. 일본의 사이버안보전략에는 안전한 IoT 시스템 구축을 위해 산・학・관이 협력하여 보안품질을 갖춘 시스템을 개발하거나, 핵심 인프라 분류체계 및 정보공유 환경을 마련하여 보안대책을 지원하고 강화하려는 노력이 들어가 있다[26].

국가의 사이버안보전략이 사이버 세계에서 적용된 사례도 있다. 예를 들어, 오바마 행정부 시절 'Left of Launch'라는 프로그램을 통해 미국이 북한의 미사일 발사가 실패하도록 교란작전을 펼쳤을 가능성이 제기되었다[19]. 또한, 2006년 이래 북미와 유럽의 정부기관에서 발생한 141건의 해킹에 중국 인민해방군 61398부대가 관련되어 있다는 주장이 제기되었다[20].

사이버안보 위협에 대응하여 미국 방위산업체 록히드 마틴이 제안한 '사이버 킬 체인'(Cyber Kill Chain) 개념을 중심으로 사이버안보 대응책을 마련할 필요가 있다. 사이버 킬 체인이란, 사이버공격을 탐색하고 파괴하는 일련의 과정에서 전략적 대응을 제시한 것으로 모두 7단계로 구성된다. 사이버 킬 체인 상 발생하는 공격의 행위를 단계별로 규정 및 분석하여 효과적으로 대처하면, 사이버공격의 전체 프로세스에 영향을 주어 궁극적으로 공격실패를



<자료> Hutchins, Cloppert, & Amin (2011)의 자료를 바탕으로 재구성

[그림 2] 사이버 킬 체인 전략

유도한다는 내용이다. 록히드 마틴이 제안한 사이버 킬 체인을 표현하면 [그림 2]와 같다. 실제로 미국 국방부는 사이버 킬 체인을 응용하여 사이버보안 킬 체인(Cybersecurity Kill Chain) 전략을 수립하였고, 미국 미래유망기술 예측업체인 Gartner는 향후 사이버공격에 대응하기 위한 전략으로 '공격체인모델(Attack Chain Model)'을 제안하였다[21].

사이버공격에 대응하고 사이버안보를 구축하기 위한 국제사회의 합의를 위한 노력도 진행되고 있다. NATO 산하 사이버방어국제협력센터는 2012년 탈린 매뉴얼을 발표하여 사이버테러와 사이버전쟁 대응전략을 수립하였다. UN의 사이버공간 국제 안보문제 전문가그룹인 GGE는 사이버공간에서 발생하는 교전규칙의 국제적인 규범을 마련하고 있다. 유럽사이버범죄협약(European Convention on cybercrime)은 서방국가들이 중심이 되어 사이버범죄 대응을 위한 국제 수사공조를 강화하는 내용을 담고 있다. 중국과 러시아를 중심으로 이루어진 상하이협력기구(Shanghai Cooperation Organization)는 사이버안보를 위한 지역협력을 강조하며 국제평화를 위협하는 용도로 정보기술을 사용하는 행위를 제한할 것을 주장하였다[6].

4차 산업혁명 시대에 새롭게 등장하고 발전하는 기술을 악용하여 국가안보에 위험을 주는 사례는 점차 늘어날 것이다. 이미 주요 국가들은 사이버전쟁에 대비하여 군사전략을 마련하고 있으며, 국제협약도 활발하게 진행 중이다. 가상공간 상 공격대상은 더 이상 개인과 기업에 국한되지 않는다. 국가 핵심시설에 대한 사이버공격이 현실세계에서의 전쟁 못지 않은 피해를 야기할 수 있다는 사실에 유념하고, 사이버 킬 체인 개념을 중심으로 사이버안보 전략을 마련할 필요가 있다.

Ⅳ. 결론 및 시사점

본 고에서는 4차 산업혁명 시대에 새롭게 부상할 보안위협을 도출하고 정보보호 개념을 확장하였다. 4차 산업혁명은 초연결, 가상세계와 물리적 세계의 결합, 인공지능 등의 신기술 등장을 통해 이루어진다. 본 고는 4차 산업혁명의 이러한 특징을 악용하여 더욱 강력한 보안위협이 등장하고, 더욱 광범위한 피해사례가 발생할 것으로 보았다. 구체적으로, 보안위협의 강도가 정보유출에서 생명을 위협하는 수준으로 높아지고, 피해범위가 사이버공간에서 물리적 공간으로 확장하고 있음을 확인하였다. 그리고 이러한 현상을 정보보안, 사이버보안, 사이버안보의 세 가지 관점에서 분석하였다. 구체적으로, 정보보안 관점에서 양자컴퓨팅 실용화에 따른 기존 암호체제의 붕괴, 랜섬웨어의 보편화, 블록체인 보안이슈, 그리고 인공지능 기술을

악용한 사이버공격을 다루었다. 사이버보안 측면에서 가상세계와 현실세계의 경계를 넘나드는 사이버위협이 IoT와 SNS상 가짜뉴스를 매개로, 현실세계에 금전적, 심리적, 신체적 피해를 입힐 수 있음을 살펴보았다. 사이버안보 관점에서 가상공간에서 이루어지는 공격이 국가 안보를 위협할 수 있음을 심층적으로 검토하였다.

4차 산업혁명 시대에 등장하는 새로운 보안위협들로부터 개인, 기업, 국가를 보호하기 위해서는 다음과 같은 전략을 수립할 필요가 있다. 첫째, 4차 산업혁명 시대의 보안기능은 시스템 설계 단계에서부터 보안을 내재화하는 개념을 적용해야 한다. 이를 위해서는 신규 기술적 대응이 필요한 분야를 집중 지원하고 인력을 구축하는 정책적 노력이 우선되어야 한다. 둘째, 기존의 수동적이고 방어적인 보안대응을 넘어 능동적이고 적극적인 보안 전략을 추진해야 한다. 셋째, 기술적 측면에서의 네트워크 경계 보호를 넘어 사람을 중심으로 보안 대응전략을 세워 나가야 한다. 넷째, 민간주도의 정보보호시장에서 벗어나 국가차원에서 사이버전쟁에 대비한 기술적 대응책을 마련할 필요가 있다. 마지막으로, 양자컴퓨터나 인공지능과 같은 신기술을 악용한 사이버공격에 대응하기 위해 신규 보안기술을 준비해야 한다. 이러한 전략을 통해 4차 산업혁명으로 인한 보안상 역기능을 최소화하고, 보다 안전한 사회를 실현할 수 있는 토대가 마련되길 기대한다.

[참고문헌]

[1] Andress, “What is Information Security?,” The Basics of Information Security, 2014. 6. 9.
[2] BBC Trending, “The fake pictures of the Rohingya crisis,” 2015. 6.
[3] Bloomberg, “Facebook has a new plan to curb fake news,” Fortune, 2017. 8.
[4] Bujaki, “Cyber Defense it is not the same with Cyber Security,” 2015. 5. 17.
[5] Calfas, “Google is changing its search algorithm to combat fake news,” Fortune, 2017. 4. 25.
[6] Cerwall et al., “Erricson Mobility Report on the Pulse of the Networked Society,” Erricson, 2017. 6.
[7] Coldewey, “Carnegie Mellon’s Mayhem AI takes home $2 million from DARPA’s Cyber Grand Challenge,” TechCrunch, 2016. 8. 5
[8] Crowe, “Fitbit just got a very fishy takeover offer,” Business Insider, 2016. 11. 10.
[9] ENISA, “Major DDoS Attacks Involving IoT Devices,” 2016. 11. 3.
[10] ENISA, “Distributed ledger technology & cybersecurity: Improving information security in the financial sector,” 2016. 12.
[11] Howard, Bradshaw, Kollanyi, Desigaud, & Bolsover, “Junk News and Bots during the French Presidential Election: What Are French Voters Sharing Over Twitter?,” Oxford, 2017. 4. 22.
[12] Hutchins, Cloppert, & Amin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” Proc. 6th Int’l Conference, Information Warfare and Security(ICIW 11), Academic Conferences, Ltd.pp.113-125.

[13] NSA, “Commercial National Security Algorithm Stuite and Quantum Computing FAQ,” 2016. 1.
[14] Panetta, “Gartner Top Strategic Predictions for 2018 and Beyond,” Gartner, 2017. 10. 3.
[15] Silverman, “This analysis shows how viral fake election news stories outperformed real news on Facebook,” BuzzFeedNews, 2016. 11. 17.
[16] Simonte, “NSA says it must act now against the quantum computing threat,” MIT Technology Review, 2016. 2. 3.
[17] Solms, Niekerk, “From information security to cyber security,” Computers & Security, 2013. 4. 11.
[18] Trend Micro, “The Fake News Machine,” TrendLabs, 2017.
[19] William & Sangler, “U.S. strategy to hobble North Korea was hidden in plain sight,” NYT, 2017. 3. 4.
[20] Johnson, “China has found a brutally simple way to steal corporate secrets,” Business Insider, 2013. 2.
[21] 손태중, 김영봉, “사이버킬체인 개념과 국방 적용방향,” KIDA, 2017. 1.
[22] 송은지, 배병환, “최근 미국 사이버보안 정책 동향,” IITP, 주간기술동향, 2015. 5. 20.
[23] 신경진, “우주・첩보・사이버군 통합, 중국군 살상력 일취월장,” 중앙일보, 2018. 1. 14.
[24] 이승민, 송근혜, “정보보호동향 및 보안위협 분석,” ETRI, 2017. 11. 30.
[25] 이승민, 정지형, 송근혜, “ECOsight 2017: Socio-Tech 10대 전망,” ETRI, 2017. 7. 30.
[26] 정보통신기술진흥센터, “일본 정보보안 정책 현황,” 해외 ICT R&D 정책동향, 2016.
[27] 최윤정, 박근영, 김수연, “4차 산업혁명 시대를 준비하는 중국의 ICT융합 전략과 시사점,” KOTRA, 2016. 12.