사이버 안보화 문제와 사이버 위협의 포괄적 대응 방안

고경민*, 정영애**
*제주대학교 원자력과학기술연구소
**선문대학교 IT교육학부
e-mail: dr.youngae.jung@gmail.com

Cyber Securitization and Comprehensive Response of Cyber Threats

Kyungmin Ko*, Young-Ae Jung**
*Institute for Nuclear Science & Technology, Jeju National University
**Dept of Information Technology Education, Sun Moon University

요 약

한국의 사이버 위협에 대한 대응은 북한이라는 변수 때문에 안보적 접근 강화가 불가피한 측면이 있다. 그러나 과잉 안보화는 개인과 사회 차원의 안보를 약화시킬 수도 있다. 이 글은 안보적 시각에 경도된 사이버안보 담론에 대한 문제를 제기하고 개인과 사회, 국가가 직면하게 되는 다양한 사이버위협에 대한 포괄적 대응의 필요성을 제기하고 있다.

1. 서론

스마트폰과 태블릿 등 스마트 디바이스의 보급으로 일상생활 전반에서 정보통신 기술이 활용되고 있다. 여기에 클라우드 컴퓨팅, 스마트 플랫폼, 빅데이터 등과 같은 새로운 기술이 개발되면서 사이버 공간은 단순한 가상의 공간이 아니라 일상의 공간으로 진화하고 있다. 사이버 공간에 대한 의존성이 커질수록 사이버 위협에 대한 취약성도 커질 수밖에 없다. 정부와 기업, 개인은 다양한 사이버 위협에 상시적으로 노출되어 있다.

사이버 테러와 같은 위협은 개인과 사회를 넘어 국가적 문제이면서 전 지구적 문제로 부상하고 있다. 불법적인 보안망 접근과 정보시스템 위해, 기업과 정부가 보유한 정보의 불법적 탈취, 국가의 주요 정보통신 인프라의 파괴 등은 사이버 공간에서 이루어지는 사이버 위협들이다.

한국에서는 북한의 사이버 위협 때문에 '국가 안보'의 시각에 초점을 맞춘 대응 기술과 조직, 그리고 제도를 구축하는 경향을 보이고 있다. 북한의 소행으로 추정되는 사이버 위협을 수차례 경험하면서 대북 사이버 테러 대응이 사이버 안보의 주요 쟁점으로 부상했고, 그로 인해 사회와 개인 등을 대상으로 한 다양한 사이버 위협 이슈들은 국가안보를 위한 사이버 테러 이슈에 수렴, 통합되는 경향을 보이고 있다. 그로 인해 민간 부문의 사이버 보안에 관한 관심은 상대적으로 약화되거나 차 순위로 밀리고 있는 상황이다.

한국의 사이버 위협에 대한 대응은 북한이라는 변수 때문에 안보적 접근 강화가 불가피한 측면은 충분히 인정된다고 할 수 있다[1]. 그러나 경계 없는(seamless) 사이버 공간의 특성을 고려할 때, 과연 이러한 안보적 시각에 과도하게 초점을 맞춘 사이버 위협 대응체계가 최선인지에 대해서는 깊이 있는 토론이 필요할 것이다.

이 글은 안보적 시각에 경도된 사이버 안보 담론과 전략에 대한 문제를 제기하고, 개인과 사회가 직면하게 되는 다양한 사이버 위협에 대한 포괄적 대응의 필요성을 제기하는 것을 목적으로 한다.

2. 사이버 안보화의 시각

사이버 공간을 구성하는 컴퓨터 시스템과 네트워크의 안전은 영토·영해·영공 못지않게 중요한 영역이다[2]. 사이버 공간에 대한 위협은 국가의 사활이 걸린 중대한 문제인 만큼 안보적 시각으로 이 문제를 접근하는 것이 최근 국내의 경향이다.

다양한 형태의 사이버 위협을 안보적 시각으로만 접근하는 것은 문제이다. 최근 안보적 시각에 경도된 사이버 안보 담론에 대한 문제를 제기하는 국내외의 연구들이 나오고 있다[3-6]. 국제정치학의 구성주의(constructivism) 안보론에 바탕을 둔 코펜하겐 학파에 따르면, '안보화(securitization)'는 안보담론이 사회적으로 형성되는 과정을 설명하는 개념이다. 이 시각에서 안보란 현존하는 위협이 무엇인가에 대한 사회적 합의를 간주관적으로 구성하는 정치적 담론과 그 결과이다[5-6].

이런 관점에서 사이버 안보 담론이 형성, 확산되는 과정에 대한 비판 중의 하나는 실제로 존재하지 않는 위협을 과장하고 있다는 것이다[7]. 같은 맥락에서 사이버 안보의 '과잉 안보화 담론'의 문제점으로 하이퍼 안보화

(hypersecuritization), 일상적 안보 관행(everyday security practice), 기술 담론화(technification)를 지적한다. 사이버 안보담론은 아직 발생하지 않는 잠재적 재난들의 영향력을 과장하고, 대중들의 일상적인 경험과 감정에 호소하여 자발적으로 안보담론에 수긍하고 참여하게 하며, 이 과정에서 기술적 지식을 가진 전문가들의 위상이 높아지고 담론을 주도하고 독점할 수 있다는 것이다[5-6, 8].

이런 맥락에서 사이버 공간의 기술적 속성을 탐구하는 컴퓨터와 정보보호 분야의 연구들은 물리적 환경으로써 인터넷이라는 기술체계 자체에서 발생하는 가능성에 주된 초점을 맞춰 사이버 공격과 테러가 낳을 위험성을 과장하는 경향을 보인다. 이러한 기술담론을 안보적 시각에서 접근할 경우에 사이버 공간은 국가안보를 위협하는 갈등과 분쟁의 공간이 되고, 사이버 위협에 대한 대응에서도 안보를 위협하는 이슈가 우선순위에 놓이게 된다.

사이버 공격으로부터 컴퓨터와 인터넷을 안전하게 보호하는 사이버 안전과 국가의 안보를 위협하는 사이버 공격은 상호 연관되어 있기 때문에 이를 명확하게 구분하기는 쉽지 않다[6]. 사이버 위협을 국가안보의 차원에서 통합적으로 접근하는 것은 개인과 사회적 차원에서 직면하게 되는 사이버 위협을 간과할 뿐만 아니라, 그러한 위협들까지 모두 국가안보의 시각으로 통합시키는 우를 범할 수 있다.

3. 한국의 사이버 테러와 대응: 안보 중심적 시각의 문제

우리 정부는 사이버 위협에 대응하기 위해 특화된 법제와 전문기구 설립을 통해 능동적으로 그러한 위협들에 대응해 왔다. 정부는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「정보통신기반보호법」 등 관련 법령을 제정했고, 2004년에 국가사이버안전센터를 설립하고 「국가위기관리기본지침」(대통령령) 및 '국가사이버위기관리 매뉴얼'을 제정했으며, 2005년에 대통령령으로 「국가사이버안전관리규정」을 제정했다.

끊임없이 실제 위협으로 다가오는 다양한 사이버 위협들에 대응하기 위해 정부는 '사이버 테러'로 불리는 대형 사이버 위협사건이 발생할 때마다 사이버 대응책 마련에 부심해 왔다. 국가적 차원에서 제시된 첫 번째의 종합대책은 2009년에 수립된 「국가 사이버 위기 종합대책」인 것으로 보인다. 그 이후 2011년에는 「국가 사이버 안보 마스터플랜」, 2013년 「국가 사이버 안보 종합대책」, 2015년 「국가 사이버 안보 태세강화 종합대책」 등이 차례로 수립되었다.

이러한 국가적 대책들이 수립되는 과정은 대체로 '사후약방문'의 특징을 보여 왔다는 점에 주목할 만하다. 2009년 11월 수립된 「국가 사이버 위기 종합대책」은 같은 해 7월 '7·7 사이버 테러'가 계기가 되었다. 2011년 8월에 발표된 「국가 사이버 안보 마스터플랜」도 같은 해 3월에 발생한 '3·4 사이버 테러'가 계기가 되었다. 2013년 7월 정부부처 합동으로 수립된 「국가 사이버 안보 종합대책」 역시 같은 해 3월에 발생한 '3·20 사이버 테러'가 계기가 되었다. 2015년 3월에 수립된 「국가 사이버 안보 강화방안」도 2014년 12월에 발생한 한국수력원자력 해킹 사건이 계기가 되었다[9].

이러한 정부 차원의 대책에서 나타나는 또 다른 주요 특징은 대형 사이버 사건을 계기로 수립된 대책들의 대부분이 '사이버 안보'와 관련된 대책이나 방안이라는 점이다. 이것은 아마도 국가적 대책 수립의 계기가 된 사이버 위협 사건들이 '사이버 테러'로 명명되었다는 데서도 적지 않은 영향을 받았을 것이다. 그리고 이와 함께 지적되어야 할 것이 대형 사이버 위협 사건은 국가안보를 위해하는 사건으로 정의하고 국가안보의 차원에서 접근하고 있다는 점이다.

실제 각각의 사이버 위협 사건들을 일별해 보면 국가 차원의 네트워크 인프라와 각종 공공 및 기업과 개인 정보들에 위해를 가할 수 있다는 점에서 안보적 사안으로 접근하는 데 대해 근본적인 의문을 제기하기는 어려울 것이다. 그러나 문제는 모든 사이버 위협 사건들을 사이버 국가안보의 관점으로 수렴하여 문제를 인식하고 대응체계와 전략을 수립하는 것이다. 과연 오늘날 우리에게 가해지는 사이버 위협이 국가안보의 시각으로 적절한 대응이 가능한 것인지는 의문이다. 기업과 개인의 사이버 위협에 대한 인식과 대응까지도 안보적 시각으로 치환하여 대응책을 마련하는 것이 적절한가?

4. 개인과 사회에 대한 점증하는 사이버 위협

실제 사이버 테러로 불리는 사건들은 정보통신망을 마비시키거나 국회, 국방연구원, 원자력발전소나 관련 연구기관 등 주요 국가기관을 대상으로 보안시스템을 무력화시키는 해킹을 통해 국가기밀과 주요 인사의 이메일을 빼내가는 사건들이 적지 않았다.

그러한 사건은 개인의 PC를 좀비PC화하거나 악성코드를 개인 이용자의 PC에 감염시켜, 이를 통해 원하는 목적을 달성하는 해킹 공격이 이루어지는 경향을 보인다. '지능형 지속 위협'이라 불리는 APT 공격도 이처럼 해커의 악성코드가 개인 이메일을 통해 개인 PC에 감염되고, 해커는 자신이 심어 놓은 악성코드를 이용하여 원격 제어 및 내무방 정보를 수집하고, 데이터 유출 및 정보시스템을 파괴한다.

따라서 사이버 테러와 같은 대형 사건에 대한 대책과 전략은 개인과 기업 등 기초적 사회 구성단위로부터 시작되어야 하며, 거시적인 국가안보적 맥락에 중점을 둔 사이버 대응책은 한계가 있을 수밖에 없을 것이다. 해마다 사후약방문식의 대응책에도 불구하고 그러한 사이버 위협 사건에 효과적으로 대응하지 못하는 이유 중의 하나도 바로 이처럼 지나치게 거시적인 안보적 시각으로 사이버 위

협에 대응하는 것도 한 원인일 수 있을지 모른다.

이에 덧붙여 지적되어야 할 문제는 대형 사이버 테러 사건 못지않게 개인의 정보인권이 위협받는 대형사고도 지속되어 오고 있다는 점이다. 2016년 7월의 인터파크 개인정보 1천 30만 건 유출사건이 발생했다. 해킹 세력은 인터파크에게 한화 30억 원에 해당하는 비트코인을 요구하면서 조건이 지켜지지 않을 경우 정보를 공개하겠다고 협박했다.

또 2014년 1월 KB국민카드·롯데카드·NH농협 등 국내 신용카드 3사의 개인정보 유출 사고는 전 세계 개인정보 유출 사고 상위 10위 안에는 드는 대형 사고였다[2]. 이 사고로 1억 400만 건의 신용카드 정보가 유출되었다. 2001년에는 네이트 해킹으로 3,500만 건의 개인정보가 유출되기도 했다.

2011년 9월 「개인정보 보호법」 제정 이후 2015년 6월까지 4년 여 동안 모두 64회의 '확인된' 개인정보 유출사고가 있었다. 그리고 이러한 사고로 유출된 개인정보를 단순 합산하면 총 1억 3,024만 8000여 명으로 추산된다. 연평균 약 3,260만 건의 개인정보가 유출되고 있으며 이는 국민의 60% 이상에 해당하는 상상을 초월하는 규모이다.

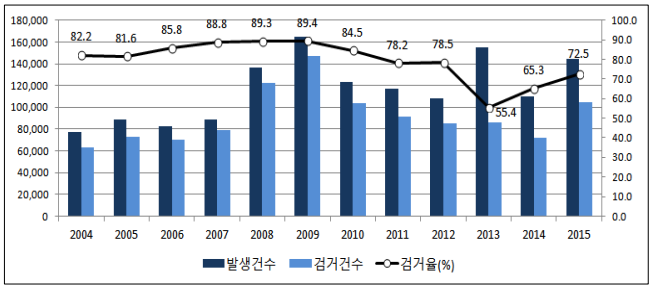
개인적 차원을 넘어 사회적인 측면에서도 사이버 보안 문제는 갈수록 심각한 이슈로 대두될 가능성이 높다. 정보통신기술이 국가의 핵심 인프라로 자리 잡았고 인터넷은 항상 어디서든 연결되어 있다. 최근 '사물인터넷(IoT)'이 현실화되면서 상호 연결된 수많은 기기들이 상호 정보를 교환하고 있다. 시스코(Cisco)는 IoT 기기의 수가 2014년 144억 개에서 2020년이 되면 501억 개로 약 3.5배 증가할 것이라고 전망했다. Machina Research는 M2M 시장이 2014년 45억 개에서 2024년 290억 개로 증가할 것이라고 예상했다.[10] 이제 물리적 세계와 사이버 세계는 마치 통합된 하나의 공간처럼 밀접해지고 있다.

비영리 연구기관인 ATARC(Advanced Technology Academic Research Center)는 최근 발표한 「정부와 사물인터넷」 보고서에서 사물인터넷 확산을 위해 정부가 추진해야 할 5가지 권고 사항을 제시하였는데 극복 과제로 사이버 보안 강화, 프라이버시 보호, 사물인터넷의 위험관리를 제안했다[11]. 이런 지적처럼 다양한 기술이 어우러진 IoT 서비스는 기술 자체 혹은 구현하는 방법의 문제점 등으로 보안상 취약점도 다양할 수 있다. 예컨대 데이터 위·변조, 비인가 서비스 및 이용자 접근, 인증 방해, 신호 및 데이터의 기밀성/무결성 침해, 정보유출, 복제 공격 등의 형태로 발생 가능하며, 개인 프라이버시 침해 문제도 심각하다고 할 수 있다[10].

IoT 시대에서의 보안 위협은 실생활과 관련된 사물로 확대되면서 사람의 생명을 위협하거나 사회 혼란을 야기할 수 있고, 또 피해 속도와 규모도 광범위하기 때문에 사회적 비용 부담은 기하급수적으로 증가할 수밖에 없다. 다양한 의료장치와 자율주행 자동차 같은 경우는 해킹으로 인한 오동작은 바로 사고로 이어지게 되며 사람의 생명과도 직결된 문제라고 볼 수 있다. 따라서 IoT는 새롭고 한층 강화된 사이버 보안대책이 필요하다.[12]

IoT 시대에는 웨어러블, 가전, 자동차, 의료기기 등 다양한 기기들이 IoT에 연결되고, 보안 주체도 과거의 ISP(Internet Service Provider), 보안업체, 이용자뿐만 아니라 제조업체까지 확대되고 있다[10].

한국인터넷진흥원 외(2016)가 「2017 정보보호 10대 이슈 전망」에서 "보안 고려없는 사물인터넷(IoT) - 커져가는 일상의 위험"을 10대 이슈의 하나로 꼽았다. IoT 기기 보급이 늘어나면서 보안취약성으로 인해 일상의 위험이 커지고 있다. IoT를 이용한 사이버 공격 발생으로 대규모 피해 현실화되고 있다. 2016년 10월 미국에서 악성코드 '미라이(Mirai)'에 감염된 50만 개 이상의 IoT기기(DVR)들을 통한 대규모 DDoS 공격으로 아마존, 트위터, 넷플릭스 등 1,200여 개 사이트 2시간 마비된 사례가 보고된 바 있다[13].



출처: 사이버경찰청(2016)

(그림 1) 사이버 범죄의 연도별 추이(2004~2015)

정보통신망에서 일어나는 사이버 범죄는 크게 정보통신망 침해범죄와 정보통신망 이용범죄, 불법컨텐츠범죄로 구분된다. 2015년 사이버 범죄 발생건수는 총 144,679건, 검거건수는 104,888건이다. (그림 1)과 같이 2010년대 이후 발생건수는 크게 줄지 않고 있지만 검거건수는 줄어들어 검거율이 다소 정체되는 경향을 보이고 있다. 특히 2013년에는 검거율이 55.4%에 불과할 정도였다. 이러한 현상은 피싱, 파밍, 스미싱, 랜섬웨어 등 신종 범죄의 출현으로 양상이 점차 다양해지기 때문인 것으로 보인다.

5. 결론적 함의

국내외적으로 해킹과 같은 사이버 범죄, 테러리스트의 사이버 공격으로부터의 방어, 국가 간의 사이버 전쟁, 혹은 국가 감시로부터 개인 프라이버시의 보호에 이르기까지 다양한 이슈들이 중첩되어 사이버 안보/보안 이슈들이 등장한다. 그러나 아직까지 합의된 개념과 정의는 존재하지 않는다. 개념 정의의 주체에 따라 또는 주요 관심사에 따라 다양하게 정의되는 경향을 보인다. 보안 기술자나 보안 기업, 수사기관, 이용자, 정부 등 다양한 이해관계자들이 이 문제와 관련이 있기 때문이다.

종종 보안과 인권은 상반되는 것으로 여겨지는 경향이 있지만, 개인적인 차원에서 보안과 인권은 동전의 양면이다. 예컨대 휴대폰 보안을 지키는 것이 곧 내 인권을 보호하는 것이 될 수 있기 때문이다. 비교적 분명한 것은, 앞서 검토한 바와 같이, 국내에서의 사이버 위협에 대한 대응은 주로 사이버 안보의 관점에서 이루어지고 있다는 점이다. 인권적 관점에서 이런 시각은 개인의 보안을 중심에 놓기보다 시스템과 인프라를 중심으로 하는 접근이다[14]. 사이버 범죄 문제나 개인정보 보호의 문제까지도 안보적 시각에서 접근하는 것은 정보인권과 관련된 불필요한 논란과 함께 모든 사회적 문제를 안보적 시각으로 수렴하고 통합한다는 비판을 불러올 수 있다.

미국은 사이버 위협을 안보적 시각으로 대응하는 대표적인 국가이다. 그러나 미국은 인터넷 자유와 프라이버시의 보호에 초점을 맞춘 개인안보에 대해서도 적지 않은 관심을 보인다. 개방된 공간으로써 인터넷 상에서의 개인의 권리와 표현의 자유, 프라이버시 등의 가치를 표방하고 이에 대한 침해를 경계한다. 특히 국가와 기업에 의한 프라이버시의 침해 가능성과 이러한 과정에서 개인의 권리와 인권의 보호를 중요시했으며 이러한 담론은 실제로 미국 내에서 엄격한 프라이버시를 보호하는 정책적·법적 대응으로 나타난 바 있다.[5]

사이버 공간은 그 특성상 국가 간 경계나 공공과 민간의 경계가 모호한 공간이다. 그리고 주요 정보통신 인프라는 주로 민간에 의해 운용되고 있다. 국가 안보에 영향을 미치는 사이버 위협이 있을 수 있지만, 대다수 사이버 위협은 그 규모나 목적의 측면에서 국가 안보와는 무관한 경우도 적지 않다. 사이버 보안에 대한 위협은 비단 사이버 공격에 의해서만 발생하는 것이 아니기 때문이다. 지진 등 천재지변, 화재 등 인재, 내부자에 의한 중요 정보의 유출 등 다양한 요인에 의해서 발생할 수 있다. 또한 사이버 보안에는 정보통신망의 안정성과 무결성의 유지뿐만 아니라, 개인 기기의 데이터와 개인정보의 보호 역시 포함된다.[15]

국가안보 중심적 접근으로 인해 개인의 정보인권을 위협할 수 있는 가능성도 간과해서는 안 될 중요한 문제이다. 2012년 이탈리아의 해킹도구 제작업체 '해킹팀(Hacking Team)'에서 'RCS(리모트컨트롤시스템: Remote Control System)이라는 핸드폰 해킹도구를 구입했다는 사실이 2015년 7월 9일 '위키리크스(WikiLeaks)'에 공개되면서 국내 민간인 사찰 가능성을 둘러싸고 정치공방이 벌어진 바 있다. 그 목적이 무엇이든 간에 RCS는 악성코드를 이용하여 기기의 보안을 해제하거나 소프트웨어의 취약점을 이용하는 방식으로, 이용자의 정보 인권뿐만 아니라 사이버 보안에 해를 끼치는 도구가 될 수도 있다. 따라서 사이버 위협에 대한 대응은 '국가의 안전과 이익'뿐만 아니라 이용자인 국민의 기기와 정보의 보안을 위해서도 중요하다.

결론적으로 사이버 위협으로 인한 엄청난 사회, 경제적 피해와 손실에 대한 대비를 안보적 시각으로 접근한다는 것은 그만큼 사이버 위협이 가지는 해악의 범위와 규모가 크다는 의미일 것이다. 그러나 사이버 위협에 대한 과도한 안보적 시각의 대응, 즉 지나친 '사이버 안보화'의 경향 또한 경계해야 할 문제이다. 국가안보에 못지않게 개인과 사회의 안보 또한 중요한 문제이기 때문이다.

참고문헌

[1] ASPI(The Australian Strategic Policy Institute Limited). 2016. *Cyber Maturity in the Asia-Pacific Region 2016*. September.

[2] 윤해성. 2012.『사이버 테러의 동향과 대응 방안에 관한 연구』, 연구총서 12-B-03(한국형사정책연구원).

[3] Matusitz, Jonathan A. 2006. "Cyberterrorism: A Postmodern View of Networks of Terror and How Computer Security Experts and Law Enforcement Officials Fight Them." Ph.D. Dissertation, University of Oklahoma.

[4] 김상배. 2015. "사이버 안보의 복합지정학: 비대칭 전쟁의 국가전략과 과잉 안보담론의 경계."『국제·지역연구』, 24권 3호.

[5] 김상배. 2015. "사이버 안보의 미중관계: 안보화 이론의 시각."『한국정치학회보』, 49집 1호.

[6] 조화순·김민제. 2016. "사이버 공간의 안보화와 글로벌 거버넌스의 한계."『정보사회와 미디어』, 제17권 2호.

[7] Kenney, M. (2015). "Cyber-terrorism in a Post-Stuxnet World." *Orbis*, Vol. 59, No. 1.

[8] Hansen, Lene and Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly*, Vol. 53, No. 4.

[9] 오병일. 2016. "국가정보원과 국내 사이버 보안 정책 개혁 방안"(정보인권연구소 보고서). 정보인권연구소·민변 디지털정보위원회 주최 토론회 자료집(12. 16).

[10] 배상태·김진경. 2016. "사물인터넷(IoT) 발전과 보안의 패러다임 변화." KISTEP InI, 14호.

[11] ATARC. 2015. "Government and the Internet of Things: Findings and Recommendations of the Internet of Things Innovation Lab." November.

[12] KISA, "2015 국내 정보보호산업 실태 조사"(12월).

[13] 한국인터넷진흥원·고려대사이버보안정책센터·인텔코리아. 2016. "2017 정보보호 10대 이슈 전망." 한국인터넷진흥원.

[14] Freedom Online Coalition. 2015. "Why Do We Need a New Definition for Cybersecurity?" September.

[15] 참여연대·천주교인권위원회. 2016. "6개 시민단체, 국가정보원의 '사이버 보안' 권한 강화한「국가 사이버 안보 기본법」제정(안) 반대 의견서 제출." 보도자료(10. 10).