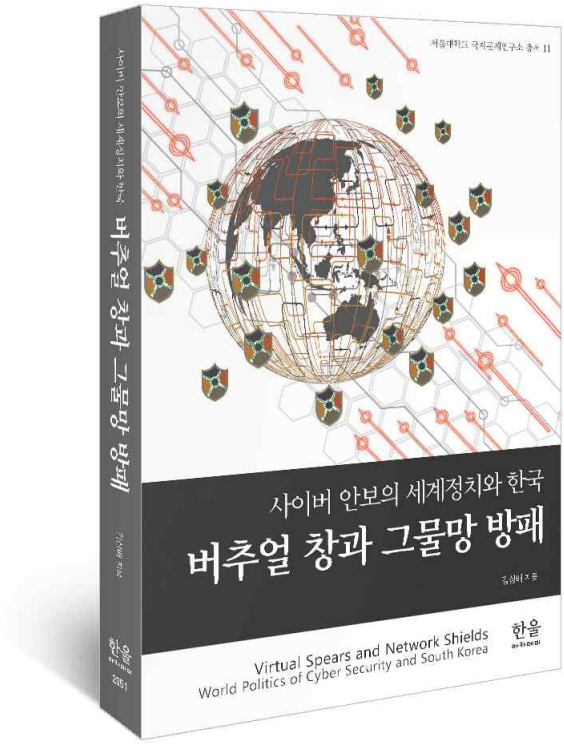
버추얼 창과 그물망 방패

사이버 안보의 세계정치와 한국



김상배 지음 | 한울엠플러스(주) 펴냄
2018년 2월 26일 발행 | 신국판(153×224) | 양장
400쪽 | 값 36,000원 | 정치·국제관계
ISBN 978-89-460-7051-6 93340

사이버 공간의 미래 국가전략을 논하다!

복합지정학과 네트워크 세계정치론의 시각에서
바라본 사이버 안보

'버추얼 창과 그물망 방패'라는 이 책의 제목은 모순(矛盾)이라는 고사성어에서 유추했다. 오늘날 해커들의 공격은 실재(real)하지만 드러나지(actual) 않는 '버추얼 창'을 연상케 한다. 컴퓨팅 환경의 특성상 누가 해킹의 주범인지를 밝히기란 쉽지 않다. '피해자는 있는데 가해자가 없다'는 말을 방불케 한다. 국가 행위자 이외에 다양한 비(非)국가 행위자들이 나서는 경우가 많으며, 컴퓨터 바이러스나 악성코드와 같은 비(非)인간 행위자도 중요한 변수가 된다. 경우에 따라서 컴퓨터와 사용자들의 네트워크 그 자체가 범인이 되기도 한다. 따라서 사이버 안보 분야에서는 실제 범인을 잡는 것보다 누가 범인인지에 대한 담론을 구성하는 것이 더 중요한, 일종의 '범죄의 재구성 게임'이 벌어지기도 한다.

버추얼 창의 공격을 막기 위해서 필요한 것은, 철벽방어를 목표로 '벽돌집'을 짓는 전통안보의 방어 개념이 아니라, 지푸라기나 나뭇가지를 하나하나 모아서 '그물망'을 짜는 복합적인 발상이다. 그물망 방패의 구축은 버추얼 창의 공격을 막기 위한 고육지책이다. 기술적으로 완벽한 방화벽을 치는 것이 힘들기 때문에 다양한 비(非)기술적 메커니즘에도 의존하게 된다. 사이버 공간의 안보를 확보하기 위해서는 기술과 인력, 국방의 역량을 강화하는 것뿐만 아니라 법제도 정비와 국제협력과 외교 등을 포함하는 복합적인 대응이 필요하다. 이 책은 버추얼 창과 그물망 방패의 대결로 비유한 사이버 안보 세계정치의 구조와 동학을 분석하고 이에 대응하는 한국의 미래 국가전략에 대한 고민을 펼쳐놓았다.

편집 배유진(031-955-0632, ujin@hanulbooks.co.kr)
10881 경기도 파주시 광인사길 153 한울시소빌딩 3층
031-955-0655(대표전화) | 031-955-0656(팩스)
www.hanulmplus.kr | blog.naver.com/hanulnew

책 소개

디지털 '모순'의 세계정치와 사이버 안보를 말하다!

"어떤 방패도 꿰뚫을 수 있는 창." 현대의 해커들은 자신들이 뚫을 수 없는 방화벽이란 없다고 뽐낸다. 하루가 멀다 하고 새로운 컴퓨터 바이러스와 악성코드가 출현하고, 해커들의 창은 점점 더 보이지 않는 위력을 발휘한다. 이를 막기 위해서 정보보안 기술자들은 새로운 방화기술과 백신 프로그램의 개발에 열을 올리고 아무리 교묘한 공격이라도 그 진원지를 추적해 색출할 수 있다고 장담한다. "어떤 창으로도 꿰뚫지 못하는 방패"인 셈이다. 그런데 디지털 시대의 '모순' 대결은 전국시대 고사성어에서 등장하는 그것과는 양상이 많이 다르다. 아날로그 시대의 '모순'이 한 개의 창으로 한 개의 방패를 찌르는 이야기였다면, 디지털 시대의 '모순'은 여러 개의 창으로 찌르는 공격을 여러 개의 방패로 막아내는 이야기이기 때문이다. 오늘날 '신흥안보'로 일컬어지는 다양한 안보 영역 중 사이버 안보에 특히 주목하고 있는 이 책은 통상적인 전통안보론의 시각이 아닌 새로운 이론적 시각에서 이 디지털 시대의 모순 이야기를 보자고 제안하고 있다.

21세기 세계정치를 특징짓는 네트워크 권력 게임, '망제정치'를 분석하다!

이제 사이버 안보의 문제는 기술공학 분야를 넘어서 21세기 세계정치 연구의 주요 주제로서 부상했다. 특히 종전에는 조연의 역할에 머물렀던 국가 행위자들이 사이버 공격과 방어의 주요 주체로서 부상하면서 사이버 안보는 명실상부하게 국제정치학의 논제가 되었다. 그렇다면 신흥안보에 속하는 사이버 안보의 국제규범을 현실주의, 자유주의, 구성주의로 대별되는 전통적인 국제정치이론의 틀에서 접근하는 것은 어느 정도의 적실성을 가질까? 이 책은 사이버 안보를 전통적인 국가 행위자들이 벌이는 '국제정치'가 아니라 복합적인 성격의 행위자들이 벌이는 다층적인 '망제정치(網際政治)'의 시각에서 볼 것을 제안하면서, 사이버 안보 분야의 복합성을 설명하기 위한 새로운 이론적 분석틀로서 '복합지정학'과 '네트워크 세계정치론'을 제시하고, 이를 통해 다양한 행위자들의 무수한 '버추얼 창' 공격에 가장 효과적으로 대응할 수 있는 '그물망 방패'의 구축전략을 모색하고 있다.

네트워크 권력과 3차원 표준경쟁이 사이버 안보의 관건!

오늘날 세계정치에서는 기존의 자원권력을 넘어서는 새로운 권력의 부상이 주목을 받고 있다. 바로 네트워크의 속성을 활용하고 나아가 네트워크 전체를 창출하거나 변경시킬 수 있는 네트워크 권력과 다양한 표준경쟁에서 우위를 점하는 능력이다. 이 책은 네트워크 권력의 속성과 그것이 작동하는 과정을 분석하고 사이버 안보가 어떻게 '네트워크 국가'의 메타 거버넌스 기능을 필요로 하는지 상술하면서, 최근 점점 더 다양하고 복잡한 방식으로 펼쳐지고 있는 기술, 제도, 담론의 3차원 표준경쟁을 주목한다. 미국과 중국은 이미 사이버 안보 분야에서 이러한 표준경쟁을 치열하게 벌이고 있는데, 이 책은 이러한 경쟁의 역사적 궤적을 추적하고, 서방 진영과 비서방 진영이 글로벌 인터넷 거버넌스를 둘러싸고 벌이는 담론 경쟁, 즉 '프레임 경쟁'에 대해서도 주목한다.

‘IT강국’ 한국의 디지털 방패는 충분히 견고한가?

2007년 4월, 에스토니아 정부의 전산망에 연결된 수만 대의 컴퓨터들이 디도스 공격을 받아 3주 넘게 국가의 주요 기능이 마비되는 사건이 발생했다. 반러시아계 정당이 집권한 후 구성된 에스토니아 정부가, 2차 대전 참전을 기념해서 수도 탈린에 세워진 옛 소련 군인의 동상을 수도 외곽으로 이전하려던 사건이 빌미를 제공했다. 러시아계 주민들은 동상 이전에 반대하는 시위를 벌였고 끝내 유혈사태가 발생하기까지 했다. 이후 100만 대 이상의 좀비 PC가 동원된 디도스 공격에 인구 130만 명에 불과한 에스토니아는 속수무책으로 당할 수밖에 없었다. ‘이스토니아(E-stonia)’라고 불리며 세계 최초로 온라인 투표를 도입했을 정도로 인터넷이 발달했던 에스토니아가 받은 사이버 공격의 충격은 매우 컸다. 이 사건으로 사이버 공격의 파괴력에 대한 국제사회의 인식이 매우 높아졌으며 이후 나토가 탈린에 CCDCOE(합동사이버방어센터)를 설립하고 탈린매뉴얼을 만드는 계기가 되었다.

이렇게 점점 더 강력해지고 있는 버추얼 창의 위협 앞에서, 이미 ‘한수원 해킹’이나 ‘국방망 해킹’ 등으로 북한의 지속적인 사이버 공격을 받아온 한국은 어떻게 대응해나가야 할까? 이 책은 주요한 국제 사이버 분쟁의 사례들을 살피고, 북한의 사이버전 능력과 조직을 개관하며, 국내의 사이버 안보 분야의 법제도 구축실태와 함께 전반적인 사이버 안보 체계 및 전략을 점검한다. 아울러 미국, 일본, 중국, 러시아, 영국, 독일, 프랑스의 사이버 안보 체계와 전략에 대한 비교분석을 통해 우리의 사이버 안보 전략에 도움이 될 만한 함의와 시사점들을 도출하고 있다.

한반도 주변4망(網)을 포괄하는, 사이버 안보의 중견국 외교가 필요하다!

한국은 전통적으로 주변4강(强)으로 불려온 미국, 중국, 일본, 러시아 등과의 양자 및 다자 간 협력이 중요한 지정학적 변수였다. 사이버 안보 분야도 이러한 지정학적 구조의 영향을 받지만 디지털 기술의 발전과 함께 그보다 더욱 광범위하고 입체적인 네트워크 구조가 형성되고 있다. 그런 점에서 이 책은 주변4강 대신 네 개의 네트워크라는 의미에서 주변4망(網)이라는 용어를 제안하면서 한반도의 사이버 안보 문제를 남북한만의 아니라 미, 중, 일, 러 주변4망과의 복합지정학적인 시각에서 볼 것을 주문한다.

오프라인 국제정치에서와 마찬가지로 사이버 안보 분야에서도 한미동맹과 한중협력을 갈등 없이 효과적으로 조율하는 것은 가장 큰 과제다. 또한 한국은 일본과의 사이버 안보 협력을 추진하고 한중관계나 남북관계의 맥락에서 러시아라는 변수를 활용할 줄 알아야 한다. 이 책의 저자인 김상배 서울대학교 정치외교학부 교수는 한국이 중견국 외교를 추진하는 과정에서 집합지성을 활용하는 연대외교와 지식외교를 지향해야 한다고 지적하며, 관건은 생각을 공유하고 행동을 같이하는 동지국가(同志國家)를 최대한 모으는 데 있다고 말한다. 또한 저자는 중견국 외교를 또 하나의 강대국이 되기 위해 힘의 논리를 따르는 ‘강대국 외교’와는 분명하게 구분하면서, 한국이 지향하는 중견국의 꿈이 언젠가 또 다른 강대국이 되어 정점에 올라서겠다는, 즉 혼자서 거미줄을 치는 ‘거미의 꿈’이 아니라 비슷한 처지에 있는 나라들이 함께 어울려 좋은 세상을 만들겠다는 ‘꿀벌의 꿈’이어야 한다고 역설한다.

신간 출간의의(출판사 서평)

21세기 사이버 안보와 세계정치의 복잡성을 이해하게 해주는 독창적인 전략연구서!

"아기돼지 삼형제"의 우화 속에서 늑대의 공격에 대비하여 힘들지만 꾸준히 벽돌을 하나하나 쌓아올린 막내 아기돼지의 '안보전략'은 지난 백여 년 동안 우리 모두가 본받아야 할 덕목이었다. 하지만 이제는 이렇게 벽돌집을 짓는 것이 더 이상 안보전략의 덕목일 수 없는 시대가 되었다. 오늘날 신흥안보를 비롯한 사이버 안보의 문제는 새로운 위협에 대응하는 새로운 집짓기의 발상을 필요로 한다. 이 책에서 그물망이라는 은유를 사용한 것은 그물망을 아무리 촘촘하게 짜더라도 빈틈은 있다는 의미를 살리기 위해서이다. 사이버 공간의 네트워크 구조는 아무리 애를 써도 빈틈을 완전히 없앨 수가 없기 때문이다. 이 책은 기존의 국제정치이론들이 상대적으로 인식을 결여해왔던 네트워크 게임과 그러한 네트워크 게임을 기반으로 하는 망제정치의 게임에 주목하면서, 단 한 차례의 공격으로 복구가 불가능해질 수도 있는 '벽돌집'이 아니라 몇 차례 피해를 입어 군데군데 구멍이 뚫리더라도 여전히 유효하게 사용할 수 있는 촘촘한 '그물망' 방패를 만들 수 있는 방략을 제안하고 있다.

종합적으로 볼 때 이 책의 논의는 기존의 사이버 안보 연구에 국제정치학적 시각을 가미하기 위한 문제제기이며, 기존 국제정치의 시각을 넘어서기 위한 네트워크 세계정치이론의 사례연구인 동시에, 사이버 공간의 미래 국가전략을 제언하는 실천전략 연구로서의 3중적 의미를 가진다. 기존 국제정치이론의 틀로는 디지털 시대의 국제정치를 제대로 이해할 수 없다는 문제의식을 가져온 연구자들, 시간이 갈수록 사이버 안보 문제를 중요하게 고려할 수밖에 없는 정책입안자들, 그리고 다층적이고 변화무쌍한 현재의 안보환경에 관심을 가져온 일반 독자들에게 이 책은 새로운 통찰과 긴요한 지혜들을 제공해줄 수 있을 것이다.

지은이

김상배(金湘培) 서울대학교 사회과학대학 외교학과를 졸업하고, 동 대학원에서 석사학위를, 미국 인디애나 대학교에서 정치학 박사학위를 받았다. 정보통신정책연구원(KISDI) 책임연구원, 일본 GLOCOM(Center for Global Communications) 객원연구원 등을 역임했고, 현재 서울대학교 사회과학대학 정치외교학부(외교학 전공) 교수로 재직하면서 '정보혁명과 네트워크 세계정치'를 연구 및 강의하고 있다.

저서로는 『아라크네의 국제정치학: 네트워크 세계정치이론의 도전』(2014), 『정보혁명과 권력변환: 네트워크 정치학의 시각』(2010), 『정보화시대의 표준경쟁: 윈텔리즘과 일본의 컴퓨터 산업』(2007)이 있으며, 편저로는 『4차 산업혁명과 한국의 미래전략: 국제정치학의 시각』(2017), 『사이버 안보의 국가전략: 국제정치학의 시각』(2017), 『신흥안보의 미래전략: 비전통 안보론을 넘어서』(2016), 『제3세대 중견국 외교론: 네트워크 이론의 시각』(2015) 외 20여 편이 있다.

차례

책 속으로

위험의 대상과 성격이라는 점에서 신흥안보는 전통 군사안보 이외에도 비군사적 영역, 즉 환경안보, 원자력안보, 보건안보, 인간안보, 사회안보 등을 포괄한다. 이 책의 주제인 사이버 안보는 이러한 신흥안보의 대표적인 사례이다. 이러한 사이버 안보 문제에 적절히 대응하기 위해서는 새로운 전략이 필요하다. 어쩌면 사이버 위협을 '감기'와 같은 일상적인 위험으로 보는 의연한 태도가 필요할 수도 있다. 사이버 공간에서 제기되는 위협을 '비정상적인 위기'로 인식하여 과도하게 군사화하기보다는, 항상 겪을 수밖에 없는 일상적인 상태, 즉 '신일상성'의 개념으로 이해하자는 제안이 나오는 것은 바로 이러한 이유 때문이다. 질병을 완벽하게 퇴치하는 대신 적절한 수준에서 통제하려는 질병안보 전략과 마찬가지로, 웬만한 수준의 사이버 공격과 위협을 어느 정도 용인하면서 심각한 폐해를 방지하는 데 주안점을 두는 전략이 필요할 수도 있다. (64~65쪽: 제1장_ "신흥안보로 보는 사이버 안보" 中)

요컨대, 최근 강대국들이 사이버 안보 분야에서 벌이는 경쟁은 인터넷 기술의 혁신과 이를 뒷받침하는 인터넷 관련 정책 및 제도의 성격, 그리고 미래질서 비전의 제시라는 세 가지 차원에서 파악되는 표준경쟁이다. 이러한 표준경쟁이 작동하는 메커니즘은 네트워크 권력의 논리를 따라서 움직인다. 더 나아가 이러한 네트워크 권력경쟁은 21세기 세계정치의 플랫폼을 장악하기 위한 경쟁이기도 하다. 여기서 플랫폼 경쟁은 판을 만들고, 그 위에 다른 행위자들을 불러서 활동하게 하고, 거기서 발생하는 규모의 변수를 활용하여 이익을 취하는 경쟁을 뜻한다. 사이버 안보 분야에서 나타나는 플랫폼 경쟁도 기술-제도-담론의 3차원 표준경쟁의 모습을 띠고 있다. (102~103쪽: 제3장_ "네트워크로 보는 사이버 안보" 中)

이 외에도 2102년 5월 역사상 가장 정교하게 제작된 악성코드인 플레임(Flame)도 발견되었다. 플레임의 출현은 스턱스넷 공격 이후 이란에 대한 사이버 공격이 시행된 추가적 증거로 간주된다. 컴퓨터 네트워크와 USB 메모리를 통해 전파되는 플레임은 소리, 화면, 키보드 동작, 네트워크 활동 등을 엿보는 첩보 프로그램이다. 하물며 블루투스가 설치되어 있는 컴퓨터의 경우 그 주변에 있는 블루투스 기기의 활동과 데이터까지도 탐지하는 종합적인 기능을 지니고 있다. 예를 들어, 블루투스를 통해서 컴퓨터 주변에 있는 스마트폰의 전화번호부에도 접근할 수 있다. 플레임은 스턱스넷보다 약 20배 정도 큰 대용량 악성코드임에도 불구하고 최소 2년 이상을 보안 소프트웨어 및 보안장비에 탐지되지 않아 보안기능을 우회하는 다양한 기법들이 포함되어 있었을 것으로 추정된다. 게다가 발각되는 것을 피하기 위해 프로그램의 흔적을 스스로 지워버리는 기능도 탑재하고 있었다. (132~133쪽: 제4장_ "버추얼 창 공격의 복합지정학" 中)

북한은 사이버 전사들에게 최고 사양의 각종 컴퓨터와 메인프레임, 주변기기, 인터넷 훈련망 등과 같은 첨단 장비시설들을 구비해주는 데 돈을 아끼지 않았다고 한다. 1990년대 바세나르 협약이나 미국 상무성 규제에 의하면 북한에 반입될 수 있는 컴퓨터는 IBM PC XT급 정도였다. 그러나 이러한 급의 컴퓨터로는 효과적인 해킹을 할 수 없다는 판단하에 북한은 "정보전사들이 사용할 고성능 컴퓨터를 비롯한 첨단장비들을 중국과 해외에서 대량 입하"했다. 특히 "중앙당 9국은 김정일과 일가족, 중앙당 특수부서들에서 필요되는 첨단전자제품들을 수입해오는 업무를 전담하는 부서"인데, 1995년 이후 사이버 부대가 해킹공격 능력 함양에 필요한 일체 설비들을 구입해주었다고 한다. 중앙당 9국이 바세나르 협약에 가입하지 않은 국가에서 활동하는 해외공관과 무역회사들을 활용하여 사이버 전력을 증강하기 위해 필요한 모든 장비와 설비들을 최신으로 구입했다는 것이다. 북한이 사용하는 사이버 무기체계의 최근 현황을 보면, 바이러스, 웜, 해킹, 디도스 공격, 우회 공격 및 역추적 방지기술, 해킹통신 암호화, 흔적삭제, EMP 공격, GPS 교란 등을 수행하는 데 필요한 첨단 소프트웨어를 보유하고 있는 것으로 평가된다. (194쪽: 제6장_ "북한의 버추얼 창, 한국의 그물망 방패" 中)

양국의 정부까지 가세한 6개월여 간의 논란 끝에 결국 2010년 6월 말 구글은 중국 시장에서의 인터넷영업면허(ICP)의 만료를 앞두고 홍콩을 통해서 제공하던 우회서비스를 중단하고 중국 본토로 복귀하는 결정을 내리게 되었다. 이러한 구글의 결정은 중국 내 검색 사업의 발판을 유지하기 위한 것으로서 중국 당국을 의식한 유화 제스처로 해석되었다. 구글이 결정을 번복한 이유는 아마도 커져만 가는 거대한 중국 시장의 매력을 떨쳐버릴 수 없었기 때

문일 것이다. 이에 대해 중국 정부는 7월 20일 구글이 제출한 인터넷영업면허의 갱신을 허용했다고 발표했다. 지메일 해킹 사건으로 촉발된 구글과 중국 정부 사이의 갈등에서 결국 구글이 자존심을 접고 중국 정부에 '준법서약'을 하는 모양새가 되었다. (243쪽: 제7장_ "사이버 안보의 미중 표준경쟁" 中)

미국의 입장에서도 북한의 사이버 공격에 대처하는 데 있어 중국과의 협력은 중요한 변수였다. 미국은 소니 해킹 사건 이후 그 배후로 지목한 북한의 사이버 공격을 차단하기 위해 중국 정부에 협조를 요청한 것으로 알려져 있다. 그러나 미중 두 강대국이 사이버 안보협력을 펼치는 것은 쉽지만은 않아 보인다. 정작 양국 간에 사이버 안보 분야에서 갈등이 진행 중이기 때문이다. 2000년대 후반부터 미국 정부와 언론은 중국의 해커들이 중국 정부와 군의 지원을 받아서 미국 정부와 기업들의 컴퓨터 네트워크를 공격한다는 주장을 펼쳐왔다. 2014년 3월 미 법무부가 미국의 정보인프라에 대한 해킹 혐의로 중국군 장교를 기소한 사건은 양국 간 갈등의 현주소를 극명하게 보여준다. 이에 대해 중국 정부도 미국의 주장이 근거가 없을 뿐만 아니라 미국이 중국 해커의 공격설을 유포하는 이면에는 중국의 성장을 견제하고 사이버 안보를 빌미로 하여 자국 이익의 보호에 나선 미국의 속내가 있다고 받아치고 있다. 이러한 와중에 2013년 6월에 터진 이른바 '스노든 사건'은 중국이 미국의 주장을 맞받아치는 유리한 환경을 제공하기도 했다. (272~273쪽: 제8장_ "사이버 안보의 주변4망과 한국" 中)

이러한 프레임 경쟁의 가장 밑바닥에는 글로벌 질서의 미래상과 관련하여 서방 진영과 비서방 진영이 지닌 근본적으로 상이한 관념이 자리 잡고 있음에도 주목해야 한다. 서방 진영은 사이버 공간에서 표현의 자유, 개방, 신뢰 등의 기본 원칙을 존중하면서 개인, 업계, 시민사회 및 정부기관 등과 같은 다양한 이해당사자들의 의견이 수렴되는 방향으로 글로벌 질서를 모색해야 한다고 주장한다. 이에 대해 러시아와 중국으로 대변되는 비서방 진영은 사이버 공간은 국가주권의 공간이고 필요시 정보통제도 가능하다고 주장하며 이에 동조하는 국가들의 국제연대담론을 내세우고 있다. 다시 말해, 전자의 입장이 민간 영역의 인터넷 전문가들이나 민간 행위자들이 전면에 나서야 한다는 이른바 다중이해당사자주의의 관념으로 요약될 수 있다면, 후자는 인터넷 분야에서도 국가 행위자들이 나서 합의의 틀을 만들어야 한다는 국가 간 프레임의 외연확대 담론으로 요약해볼 수 있다. (325쪽: 제9장_ "사이버 안보 국제규범의 세계정치" 中)

실제로 이와 유사한 사태가 2014년 초 중국의 통신업체인 화웨이로부터 한국의 정보통신기업인 LG 유플러스가 네트워크 장비를 도입하려 했을 때 미국이 나서서 만류하자 나타난 바 있다. 당시 미국은 화웨이의 LTE 장비에 도청을 가능하게 하는 '백도어'(악성코드)가 심어져 있을 가능성을 제기했는데, 이는 한국에 압력으로 작용한 것으로 보인다. 이후 실제로 LG 유플러스는 용산 주한미군 기지 지역에서는 화웨이 기지국 장비를 쓰지 않았고, 화웨이 장비의 수입 물량도 당초 계획했던 4천여억 원에서 1천여억 원으로 75% 정도 줄이겠다고 발표했으며, 미 8군 소속 군인들도 LG 유플러스 이동통신 가입 해지에 들어가기도 했다. 그러나 LG 유플러스의 입장에서는 가격대비 효율성이 큰 화웨이 장비의 유혹이 커서 이후에도 4세대(4G) 활용 협대역 사물인터넷(NB-IoT) 장비 등에서 화웨이와 협력관계를 이어온 것으로 알려져 있다. 그러던 것이 2017년 3월 미국 의회가 화웨이의 5세대(5G) 통신장비에 대한 경계령을 내리면서 한국이 5G 장비로 화웨이를 선택하여 네트워크를 구축하는 것을 미국 국방부가 나서서 막아

야 한다는 주장을 제기했다. 이러한 주장은 한국이 5G와 관련하여 화웨이와 2018년 평창동계올림픽 공식파트너 계약을 맺은 상황에서 미국의 견제로 해석될 수 있는 행보라고 할 수 있다. (343쪽: 제10장_ "사이버 안보의 중견국 외교전략" 中)

대부분의 우화가 그렇듯이 "아기돼지 삼형제"도 교훈을 담고 있다. 피리를 불고 바이올린을 켜며 놀기만 좋아해서 튼튼한 집짓기를 게을리한 첫째와 둘째 아기돼지의 안이한 태도에 경종을 울리고, 나쁜 늑대의 공격에 대비하며 힘들지만 꾸준히 벽돌을 하나하나 쌓아올린 막내 아기돼지의 성실성을 본받아야 한다는 것이다. 지난 백여 년 동안 "아기돼지 삼형제"가 시대의 변화에 따라 각색이 되어도, 이러한 막내 아기돼지의 '안보전략'은 우리 모두가 본받아야 할 덕목이었다. 그런데 이렇게 벽돌집을 짓는 것이 21세기를 맞이한 오늘날에도 여전히 안보전략의 덕목일까? 만약에 시대가 달라져서 아기돼지들을 공격하는 위협이 이제는 더 이상 '늑대'로 비유되는 존재가 아니라면 우리는 어떠한 우화를 써야 할까? 여전히 벽돌집을 짓는 것이 아기돼지들이 안전하게 살 수 있는 상책이라고 말할 수 있을까? '늑대'의 위협으로부터 자신들을 지키려 했던 '아기돼지 삼형제'의 우화를 거꾸로 읽는 상상력이 필요할 것은 아닐까? (366~367: 맺음말_ "사이버 안보의 중견국 외교전략" 中)