사이버 공간과 한반도 통일:

복합지정학으로 보는 사이버 안보의 국가전략

김상배(서울대학교)

Ⅰ. 머 리 말

최근 지정학에 대한 관심이 커지고 있습니다. 1980년대 이후 일군의 학자들이 지정학의 부활을 선언했고 다양한 각도에서 연구를 수행해 왔습니다. 이러한 지정학적 관심은 21세기 국제정치 현실의 변화를 바탕으로 해서 피어나고 있습니다. 대표적으로 러시아의 크림반도 점령, 중국의 공격적 해상활동, 중동 지역의 고질적인 분쟁 등이 배경이 되었습니다. 특히 미국이 주도해온 탈냉전 이후의 세계질서에 대한 지정학적 합의를 뒤집으려는 러시아, 중국, 이란 등의 문제제기가 출현하면서 그야말로 지정학이 부활하는 조건이 마련되고 있는 듯합니다. 미·중·일·러의 전통 4강의 틈바구니에서 생존과 번영의 길을 모색해야 하는 한반도도 이러한 지정학 부활의 연구관심으로부터 자유로울 수 없습니다. 특히 최근 북한이 벌이고 있는 행보는, 아무리 탈냉전과 지구화, 정보화, 민주화의 시대가 되었다 해도 한반도 국제정치는 여전히 지정학적 분석의 굴레에서 벗어날 수 없음을 보여주는 듯합니다.

시대가 아무리 변하더라도 국제정치의 분석에 있어서 지정학적 시각은 사라지지 않고 꾸준히 남아있을 것입니다. 특히 동아시아와 한반도 주변 국제정치에서는 더욱 그러할지도 모릅니다. 그러나 21세기 국제정치를 이해하기 위해서 지정학의 시각을 다시 소환한다고 할지라도, 19세기 후

반과 20세기 전반의 국제정치 현실에서 잉태된 고전지정학의 시각을 그대로 복원하여 적용하려는 시도는 경계해야 합니다. 지구화와 정보화를 배경으로 탈(脫)영토공간적인 활동이 부쩍 늘어나고 있는 오늘날의 사정을 돌아볼 때, '영토 발상'에 기반을 두고 이를 부분적으로만 개작하려는 현재의 시도로도 부족합니다. 오늘날 세계와 한반도의 상황이 변화한 만큼, 이를 보는 지정학의 시각도 변화한 국제정치의 현실에 걸맞게 변용을 거쳐서 달라진 상황에 부합하는 방향으로 새로워질 필요가 있습니다. 이러한 점에서 한반도 통일을 둘러싼 국제정치학적 역학과 통일의 미래를 연구하는 새로운 분석틀로서 '통일의 신(新)지정학'이 지니는 의미는 매우 크다고 아니 할 수 없습니다.

그런데 이렇게 21세기 한반도 통일의 '신지정학'을 논하는 과정에서 간과되어 그 중요성이 제대로 인식되지 못한 대표적인 변수가 바로 탈지정학적 공간으로서 사이버 공간입니다. 사이버 공간은 1990년대 중후반 이후 컴퓨터와 정보인프라, 인터넷과 소셜 미디어 등의 급속한 성장과 함께 국제정치적 삶의 공간으로서 자리매김하고 있습니다. 이제 사이버 공간은 단순한 기술·경제 공간의 의미를 넘어서 사회·문화 공간이자 국제정치 공간이 되었다고 해도 무리가 없습니다. 최근 동아시아 국제정치의 전개를 보면, 사이버 공간은 이미 남북한뿐만 아니라 미국이나 중국과 같은 주변국들이 대결과 협력을 벌이는 새로운 공간으로서 자리를 잡았습니다. 사이버 공간이 전통적인 지정학 공간과 만나 한반도 주변 국제정치의 전면에 부상한 사례는 여러 가지가 있겠지만, 그 중에서도 이 글이 주목하는 사례는 최근 남북한 관계, 미국과 중국, 그리고 북한과 미국 간에 쟁점이 되고 있는 사이버 공간의 안보 문제입니다.

사이버 안보 분야의 갈등은 동아시아 및 글로벌 차원의 세계정치를 이해하는 데 있어서 이제 사이버 공간이 빼놓을 없는 변수가 되었음을 보여줍니다. 예를 들어 북한의 소행으로 추정되는 대남 사이버 공격이 지속적으로 늘어나고 있습니다. 가장 최근에 국내의 관심을 증폭시킨 사례로

는 2014년 12월 한국수력원자력에 대한 해킹 사건이 있었습니다. 미중 사이에서도 미국의 정보 인프라와 지적재산에 대한 중국 해커들의 공격을 놓고 공방이 오고가고 있습니다. 이러한 미중 양국의 사이버 갈등은 마치 21세기 패권경쟁의 한 단면을 보는 듯합니다. 한편 2014년 11월에는 소니 영화사에 대한 북한의 해킹 사건으로 북미 간에 긴장감이 있었습니다. 이러한 과정에서 사이버 안보의 문제는, 단순히 민간 영화사의 정보시스템에 대한 해커들의 침입을 넘어서 미국 영토에 위치한 시설에 대한 공격이라는 의미가 부여되면서, 북미 양국 간의 물리적 분쟁을 야기할 수도 있는 국제정치적 사건으로 간주되었습니다.

사이버 안보가 국가적 관심사가 되면서 이에 대한 대응도 정치군사적 발상을 바탕으로 이루어지고 있습니다. 사이버 공격으로 인해 인명 피해가 발생했을 경우 해당 국가에 대한 군사적 보복이 가능하고, 해커나 테러리스트 등과 같은 비국가 행위자뿐만 아니라 사이버 공격의 배후지를 제공한 국가나 업체에 대해서도 전쟁법을 적용하여 책임을 묻겠다는 구상이 제기되었습니다. 냉전기 핵전략에서 잉태된 핵 억지의 개념을 사이버 안보 분야에 적용한 '사이버 억지'의 개념도 적극적으로 검토되고 있습니다. 이러한 주장들은 사이버 공격에 대해서는 그 진원지를 찾아 미사일을 발사해서라도 강력하게 보복하겠다는 미국 정부의 최근 입장과 맞물리면서 세간의 관심을 끌고 있습니다. 그런데 이러한 주장들은 기본적으로 온라인에서 벌어지는 탈영토공간적 현상에 대해서 오프라인의 경험에서 추출된 지정학적 전략으로 대처하겠다는 오류를 안고 있습니다.

기본적으로 사이버 안보의 게임은 복잡계의 양상을 보이는 네트워크 구조 하에서 다양한 행위자들이 서로 얽히면서 구성해 가는 탈지정학적 게임입니다. 네트워크 구조의 특성상 사이버 공격의 범인을 밝힐 수 있더라도 매우 복잡한 인과관계를 바탕으로 하고 있어 상대에게 보복을 하거나 명확한 법적 책임을 지우기가 쉽지 않습니다. 국가 간의 관계를 규율하는 국제규범(예를 들어 전쟁법)을 적용해서 처벌하기란 더욱 어렵습니다.

사이버 테러와 공격은 힘과 규모의 면에서 비대칭적인 행위자들이 비대칭적인 수단을 동원하여 서로 다른 비대칭적 목적을 수행하기 위해서 이루어지는 '비대칭 전쟁'의 대표적 사례이기 때문입니다. 이 글이 기존 지정학의 단순계적 발상만으로는 사이버 안보의 게임을 제대로 이해할 수 없다고 주장하는 이유는 바로 여기에 있습니다.

이러한 문제의식을 바탕으로 이 글은 사이버 안보의 세계정치를 이해함에 있어 기존의 지정학 시각을 비판적으로 보완하는 작업의 연속선상에서 사이버 공간이라는 변수를 추가한 탈지정학의 이론적 시각을 제안하고자 합니다. 그러나 탈지정학적 공간으로서 사이버 공간을 강조하려는 이 글의 의도가 영토와 장소의 발상을 기반으로 하는 기존 지정학의 시각을 폐기하려는 데 있지는 않습니다. 오히려 아날로그 시대의 오프라인 지정학과 디지털 시대의 온라인 탈지정학을 21세기 국제정치학의 관점에서 복합하려는 데 있습니다. 이러한 맥락에서 이 글이 추구하는 이론적 시각을 굳이 명명하자면, 기존 지정학의 시각에 사이버 공간으로 대변되는 탈지정학의 시각을 가미한다는 의미에서 복합지정학(complex geopolitics)이라고 부를 수 있을 것입니다.

이러한 이론적 인식을 바탕으로 이 글은 비대칭 전쟁으로서 사이버 공격과 방어에 임하는 국가전략의 대응방향도 모색하고자 합니다. 사이버 안보가 국제정치의 문제가 된 것만큼 지정학적 대응전략도 필요하지만 사이버 안보의 고유한 성격에 부합하는 탈지정학의 전략도 복합적으로 모색되어야 한다고 주장할 것입니다. 그러나 이 글의 관심은 정책연구의 관점에서 사이버 안보의 국가전략을 뒷받침하는 실천방안의 제시뿐만 아니라, 비판이론의 시각에서 각 전략방안들이 지니고 있는 문제점들을 경계하는 성찰적 시각의 제시에도 있습니다. 다시 말해 단순 지정학의 시각에서 추진되는 사이버 안보의 국가전략은 일종의 '과잉 안보담론'으로 치우칠 위험성이 있다는 것이 이 글의 인식입니다. 이러한 맥락에서 현재 거론되고 있는 국가전략의 사안들이 지나친 기술전문가 담론이나 군사안보 우선담

론으로 경도되거나, 국가안보 담론을 과장하거나 정파적 이해관계를 투영하려 함으로써 지나치게 정치화될 가능성이 있음을 지적할 것입니다.

이 글은 크게 세 부분으로 구성되었습니다. 제2장은 사이버 안보의 세계정치가 지니고 있는 복합지정학적 성격을 사이버 공간의 구조적 속성, 최근 부각되고 있는 국가 행위자들의 역할, 법제도 정비 과정에 담긴 안보담론의 성격, 사이버 안보 분야의 국제규범과 글로벌 거버넌스의 모색 등을 통해서 살펴보았습니다. 제3장은 사이버 안보의 국가전략이 지니고 있는 복합지정학적 성격을 사이버 방어를 위한 기술개발과 인력양성, 사이버 억지 개념의 적용 가능성, 추진체계 정비와 관련법의 제정, 주변국들과의 국제협력과 외교전략 등을 통해서 살펴보았습니다. 제4장은 사이버 안보의 국가전략을 추구하는 과정에서 경계해야 할 안보담론의 내용을 과잉 안보화, 과잉 군사화, 과잉 정치화, 과잉 현실주의 담론 등의 네 가지 측면에서 비판적으로 검토하였습니다. 끝으로 맺음말에서는 사이버 안보의 복합지정학을 제안한 이 글의 주장을 종합·요약하였습니다.

Ⅱ. 사이버 안보의 세계정치

1. 사이버 공간의 기술구조적 성격

사이버 테러와 공격은 사이버 공간이라는 초국적이고 탈지정학적인 환경에서 발생합니다. 사이버 공간의 기반이 되는, 네트워크로 연결된 컴퓨터들은 전지구적 차원을 염두에 두고 설계되고 발전해왔으며, 그러한 과정에서 전통적인 국민국가의 경계를 넘나들며 작동하고 있습니다. 이러한 네트워크 시스템의 복잡계적 특징은 단순히 영토의 경계만 넘는 것이 아니라 영토귀속성으로부터 어느 정도 자유롭기까지 합니다. 사이버 테러와 공격이 발생하더라도 사이버 공간의 이러한 구조와 작동방식의 성격상 누가 주범인지를 밝히기 어렵습니다. '피해자는 있는데 가해자가 없다'는 말을 방불케 하는 현상이 벌어지기도 합니다. 방어하는 측의 입장에서 보

더라도 사이버 공격이 어디서 감행될 지 알아내는 것은 전통안보의 경우처럼 쉽지 않고, 이를 막기 위해서 완벽한 방화벽을 치는 일도 거의 불가능합니다.

사실 사이버 테러나 공격과 관련된 문제의 많은 부분들이 인터넷이라는 독특한 시스템을 배경으로 해서 발생합니다. 아무리 잘 설계된 정보시스템이라도 기술적으로 복잡하다보면 그 부산물로서 버그를 완전히 없앨 수는 없습니다. 그런데 이러한 빈틈은 해커들이 외부에서 침투하여 시스템의 변경이나 훼손을 시도하는 목표가 됩니다. 컴퓨터 바이러스나 각종 악성코드들은 이러한 빈틈으로 침투하여 시스템의 정상적인 기능을 착취하는 대표적 사례들입니다. 이러한 컴퓨터 바이러스, 악성코드 등은 단순한 도구가 아니라 사이버 공격의 성격을 여타 공격과 구분 짓는 변수입니다. 전쟁에서 사용되는 무기가 재래식 무기냐 핵무기냐에 따라서 전략전술이 달라지듯이, 사이버 공격에서도 컴퓨터 바이러스와 악성코드의 존재는 사이버 안보의 게임 자체에 큰 영향을 미치는 독립변수입니다.

물론 사이버 테러와 공격의 문제를 단순히 컴퓨터나 인터넷의 물리적 속성과 관련된 기술적인 문제로만 보기는 어렵습니다. 사이버 테러와 공격은 다양한 행위자들이 복합 네트워크 환경을 배경으로 하여 참여하는 비대칭 전쟁의 대표적 사례입니다. 비대칭 전쟁이란 힘과 규모의 면에서 비대칭적인 행위자들이 비대칭적인 수단을 동원하여 서로 다른 비대칭적 목적을 수행하기 위해서 이루어지는 전쟁을 의미합니다. 기본적으로 사이버 테러와 공격은 국가 행위자들이 아니라 위계조직의 모습을 따르지 않고 체계적으로 조직되지 않은 네트워크 형태의 다양한 비국가 행위자들이 벌이는 게임입니다. 최근 인터넷의 확산으로 인해서 네트워킹에 드는 비용이 급속히 하락함에 따라 이러한 비국가 행위자들이 역사의 전면에 그 모습을 드러내면서 예전에는 상상할 수도 없었던 독특한 종류의 '힘'을 발휘하고 있습니다.

사이버 테러와 공격에서는 행위자들이 수행하는 역할의 스펙트럼이

매우 넓습니다. 일반 사용자가 공격자가 될 수도 있고 악의적인 공격의 대상이 되기도 하며 디도스 공격에 이용되는 것처럼 자신도 알지 못하는 사이에 봇넷에 동원되는 공범이 되기도 합니다. 이러한 탈지정학적 행위자들이 지정학적 목적과 연계되기도 합니다. 애국주의 해커집단은 국민국가와 암암리에 연대하여 다른 국가의 주요 정보인프라를 공격하기도 합니다. 심지어 조직적인 범죄집단도 단독으로 산업스파이, 해적 행위, 금융자산의 절도 등을 행하지만 국가의 사주 하에 다른 국가의 공공 및 민간 시스템을 해킹하기도 합니다. 게다가 이들은 국가기관에 의해 아무리 적발되어도 끊임없이 새로운 형태로 진화를 거듭해 나갑니다. 분산 네트워크로서의 특성 때문에 특정 대상을 선정하여 미리 억지하기도 또 대비해서 방어하기에도 매우 까다로운 안보 문제를 제기하고 있습니다.

2. 사이버 공격의 지정학적 성격

2000년대 말엽 이후로 종전에는 비국가 행위자들의 배후에서 조연 배우의 역할을 담당하던 국가 행위자들이 사건의 전면에 나서고 있습니다. 2007년의 에스토니아에 대한 사이버 공격이나 2008년 그루지야에 대한 디도스 공격의 사례처럼, 실제로 물리적 전쟁의 개시를 전후하여 이와 병행하는 방법으로 국가 간의 사이버 공격이 감행될 가능성은 매우 큽니다. 2010년 미국과 이스라엘의 대(對)이란 사이버 공격은, 국가가 직접 나서서 사이버 공격을 주도한 것이 언론을 통해서 알려진 첫 사례입니다. 미국-이스라엘과 이란 사이에서 오고간 사이버 공격은 사이버 안보를 국가안보라는 지정학적 지평에 올려놓았습니다. 게다가 종전에는 방어자의 입장을 대변하던 미국이 나서서 국가 주도의 사이버 공격을 벌임으로써 다른 나라에서도 주저하지 않고 국가가 나서서 사이버 공격에 개입하게 되는 물꼬를 텄다는 우려와 비판도 제기되었습니다.

사이버 안보를 둘러싼 국가 간 분쟁은 21세기 세계패권을 놓고 벌이는 미중관계의 현안으로도 등장했습니다. 특히 미국의 시각에는 중국 해

커들이 중국 정부의 지원을 받아서 미국 정부와 기업들의 컴퓨터 네트워크를 공격하는 것으로 비칩니다. 이러한 중국의 해킹은 미국의 기업뿐만 아니라 심지어는 미국 고위 관리의 계정까지도 목표로 하고 있어 미국의 근간을 뒤흔드는 위협이라고 인식되고 있습니다. 예를 들어 미국 정부가 이른바 '오로라 공격'이라고 명명한 2009년의 해킹 사건은 구글뿐만 아니라 아도비나 시스코 등과 같은 미국의 IT기업들을 목표로 하여 중국 해커들이 벌인 일이라는 것입니다. 2010년 구글 사건 당시에도 중국의 해커들이 적극적인 역할을 한 것으로 알려져 있습니다.

군사적 수단으로서 사이버 공격의 부각은 약소국들에게도 새로운 변화를 가져올 가능성이 큽니다. 다시 말해 재래식 무기로는 강대국과 경쟁할 수 없는 약소국들이 비대칭 전쟁의 관점에서 사이버 전쟁을 국방전략으로 채택할 가능성이 있기 때문입니다. 이러한 사이버 안보의 지정학적 양상은 북한의 대남 사이버 공격에서 두드러지게 나타납니다. 북한의 사이버 공격은 한국의 공공기관이나 금융사 및 언론방송사 등의 전산망의 빈틈을 노리고 수십만 대의 좀비 PC를 동원하여 디도스 공격을 벌이거나 좀 더 교묘하게 이루어지는 APT 공격을 가하는 방식으로 이루어진 것으로 알려졌습니다. 아직은 사이버 공격의 대상이 공공기관이나 언론·방송사 또는 금융기관 등에 국한돼 있지만, 일단 유사시에는 재래식 공격이나 핵 공격과 연계될 가능성이 매우 크다는 점에서 큰 우려를 낳고 있습니다. 실제로 최근 북한의 사이버 공격들이 재래식 무력도발이나 핵실험 등과 같은 지정학 이슈들과 복합되어 발생하고 있습니다.

북미관계에서도 2014년 11월 미국의 소니 영화사에 대한 북한의 해킹 공격은 지정학적 이슈를 제기했습니다. 당시 미국 오바마 대통령은 북한의 사이버 공격을 미국 국가안보에 대한 중요한 도전으로 간주한다고 말했습니다. 그 후 2015년 들어 북한에 대한 오바마 행정부의 강한 복합 억지가 추진된 것으로 알려졌습니다. 북한 사이버 공간에 대한 제재(예를 들어 북한의 웹사이트에 대한 역 해킹)도 한국, 일본, 호주와 같은 동맹국들

과 중국을 비롯한 유관당사국과의 협력아래 추진된 것으로도 알려졌습니다. 미국은 북한의 행동 변화를 위해 2015년 초에 금융제재의 행정명령을 새로이 추가하기도 했습니다. 그야말로 사이버 공간의 문제가 자칫하면 북미 간의 지정학적 갈등으로 번질 수도 있는 상황이 창출되었습니다.

3. 사이버 안보의 안보화 경쟁

국가 행위자는 사이버 공격의 주체가 될 수도 있겠지만 방어의 주체이기도 합니다. 이러한 역할을 수행하는 대표적인 나라는 미국입니다. 미국은 사이버 공격을 감행할 수 있는 자원과 기술을 보유하고 있는 나라이지만, 만약에 사이버 공격을 받을 경우 가장 많은 피해를 볼 수밖에 없는 나라입니다. 미국은 세계 어느 나라보다도 발달된 정보 인프라를 구비하고 있고, 사이버 공간이 개방적이기 때문에 사이버 공격에 대한 취약성이 지극히 높습니다. 따라서 전통적 군사력에서 열세인 국가들이 미국을 상대로 하여 사이버 공간에서 비대칭적 공격을 감행할 유인과 여건을 높을 수도 있습니다. 이러한 취약성을 인식하고 미국에서의 사이버 안보에 대한 논의는 1990년대에서부터 시작되었고 9.11 테러 이후 본격화되었으며, 오바마 행정부에 이르러서는 시급한 정책현안이 되었습니다.

미국이 이러한 인식을 발전시킨 계기는 중국 해커들의 공격에 대한 위협인식입니다. 이러한 위협인식은 미국으로 하여금 중국에 대해서 사이버 안보 문제를 양국 간의 현안으로 제기하게 만들었습니다. 2013년 6월 미국과 중국의 두 정상이 만나 양국이 당면한 현안 중의 하나로 거론했으며, 그 후 양국 간 전략경제대화의 의제 중의 하나로서 다루어지고 있습니다. 그러나 이러한 협력의 몸짓에도 불구하고 물 밑에서는 미·중 사이버 갈등은 계속 진행되었습니다. 이러한 갈등은 2014년 5월 미 법무부가 미국 내 기관들에 대해서 해킹을 감행한 것으로 지목한 중국군 61398부대 장교 5인을 기소하면서 정점에 달한 듯이 보였습니다. 미국도 중국을 상대로 비밀스러운 정보작전을 벌이기는 마찬가지였습니다. 2013년 6월 미

국 중앙정보국(CIA) 전 직원인 에드워드 스노든이 폭로한 내용에 따르면, 미국 정부는 '프리즘'이라는 프로그램을 통해서 장기간에 걸쳐 개인 이메일을 비롯한 각종 데이터를 감청해 온 것으로 드러났습니다.

미중경쟁에서 보는 바와 같이, 각국은 사이버 공격의 위협이 되는 잠재적인 적국을 상정하고 이들을 봉쇄해야 한다는 안보담론을 자국민들에게 심어주려는 행보를 보입니다. 이러한 과정에서 사이버 안보 게임에 효율적으로 대응하기 위해서 필요한 예산, 인력, 조직 등과 같은 국내자원을 동원하는 것이 관건입니다. 현재 이러한 안보담론의 생산과 전파 경쟁을 벌이는 대표적인 국가들은 미국과 중국입니다. 미중경쟁의 논점은 기본적으로 사이버 안보의 대상이 무엇이며 그 문제를 해결하는 주체가 누구인가를 규정하는 담론의 차이에서 비롯됩니다. 이는 단순히 관념의 차이가 아니라 이를 통해서 구성될 미래의 방향을 놓고 벌이는 이익규정의 차이에 기반을 두고 있습니다.

현재 미국과 중국 사이에는 상이한 안보담론을 가지고 현실을 재구성하려는 안보화(securitization)의 게임이 벌어지고 있습니다. 미국의 담론이 주로 물리적 정보 인프라로서 컴퓨터 시스템과 네트워크 인프라, 지식정보 자산, 지적재산권의 안보를 유지하는 데 관심이 있다면, 중국의 담론은 인터넷 상에서 유통되는 콘텐츠, 즉 정치적 담론이나 이념의 내용에 주안점을 둡니다. 미국의 담론이 민간의 프라이버시 보호, 보편적 인권과 표현의 자유에 관심이 있다면, 중국의 담론은 정권안보의 차원에서 인터넷에 대한 검열과 규제를 강조합니다. 미국의 담론이 글로벌 패권의 자유주의적 담론을 강조하는 입장이라면, 중국의 담론은 반(反)패권주의적이고 민족주의적인 국가주권의 안보담론입니다.

4. 사이버 안보의 국제규범

초국적으로 발생하는 사이버 공격에 대해서 일국 차원에서만 대응하는 데는 한계가 있을 수밖에 없습니다. 위협과 공격 자체가 초국적이고 글

로벌한 차원에서 발생하는 만큼 그 해법도 국가의 경계를 넘어서는 다양한 행위자들의 협력을 통해서 마련되어야 할 것입니다. 그러나 아쉽게도 아직까지 사이버 안보 분야에 어떠한 규정이나 법규범을 적용할지에 대한 국제적 합의기반은 마련되지 않고 있습니다. 그럼에도 각국의 영토적 경계를 넘어서 다자적 차원에서 또는 글로벌 차원에서 새로운 질서와 규범을 만들려는 모색이 진행되고 있는데, 현재 크게 세 가지의 프레임이 경합 중입니다.

우선 주목할 필요가 있는 것은 전통적인 국제법(특히 전쟁법)의 틀을 원용하여 사이버 공간에서 발생하는 해킹과 공격을 이해하려는 움직임입니다. 2013년 3월 NATO의 CCDCOE(Cooperative Cyber Defence Centre of Excellence)가 발표한 사이버 전쟁의 교전수칙인, 탈린 매뉴얼이 일례입니다. 전통적인 국제기구인 유엔 차원에서 사이버 안보 문제를 다루려는 시도도 최근 빠르게 진행되고 있습니다. 그 대표적인 사례가 2013년 6월 유엔 군축 및 국제안보 위원회 산하 정보보안 관련 정부전문가그룹(Group of Governmental Experts, GGE)에서 합의해서 도출한 최종 권고안입니다. 이 권고안에서는 사이버 공간에서도 기존의 국제법이 적용될 수 있다는 점에 합의되었습니다.

두 번째는 사이버 안보의 국제규범을 마련하려는 서방 선진국들의 국제협력 움직임입니다. 사이버공간총회가 대표적인 사례인데, 2011년 런던에서 첫 총회가 열린 이후, 부다페스트(2012년), 서울(2013년)을 거쳐 2015년 헤이그에서 제4차 총회가 열렸습니다. 사이버 범죄에 대응해서 국가들이 나서서 상호 간의 법제도를 조율하는 정부 간 네트워크를 구성한 초기 사례로 2001년 조인된, 유럽사이버범죄협약(일명 부다페스트 협약)에도 주목할 필요가 있습니다. 유럽사이버범죄협약은 여러 나라의 사이버 범죄 조목을 일관되게 함으로써 사이버 범죄와 관련하여 공격당한 국가가 범죄자가 있는 국가에 이를 고발하면 해당 국가가 처벌할 수 있도록 한 협약입니다.

마지막 세 번째는 인터넷 거버넌스의 일환으로 보는 사이버 안보의 글로벌 거버넌스 모색 움직임입니다. 현재 우리가 사용하는 인터넷의 기본골격은 미국에 활동기반을 두는 민간전문가들이 자율적으로 구축한 이른바 '다중이해당사자주의' 메커니즘을 통해 형성되었습니다. 이러한 면모를 잘 보여주는 사례가, 초창기부터 인터넷을 관리해온 미국 캘리포니아 소재 민간기관인 ICANN(Internet Corporation for Assigned Names and Numbers)입니다. 이러한 미국과 ICANN 주도의 인터넷 거버넌스 모델에 대해서 최근 구사회주의권 국가들과 개도국들이 반론을 제기하고 있습니다. 이들 국가들은 미국의 인터넷 패권을 견제하기 위해서는 '정부간주의'에 기반을 두고, 모든 국가들이 참여하는 전통적인 국제기구의 틀을 활용해야 한다고 주장합니다.

이상의 세 가지 프레임을 가로질러서 미국과 유럽 국가들이 주도하는 서방 진영을 한편으로 하고, 러시아와 중국을 중심으로 한 개도국 진영을 다른 한편으로 하는, 두 개의 진영이 대립하는 지정학적 구도가 겹쳐집니다. 서방 진영은 사이버 공간에서 표현의 자유, 개방, 신뢰 등의 기본 원칙을 존중하면서 개인, 업계, 시민사회 및 정부기관 등과 같은 다양한 이해당사자들의 의견이 수렴되는 방향으로 세계질서를 모색해야 한다고 주장합니다. 이에 대해 러시아와 중국으로 대변되는 진영은 사이버 공간은 국가주권의 공간이며 필요시 정보통제도 가능한 공간이므로 기존의 인터넷 거버넌스를 주도해 온 서방 진영의 주장처럼 민간 중심의 이해당사자주의에 의해서 사이버 공간을 관리할 수는 없다고 주장합니다.

Ⅲ. 사이버 안보의 국가전략

1. 사이버 방어기술의 개발과 인력양성

사이버 안보의 기술구조적 특성을 고려할 때, 사이버 공격에 대한 대응전략의 첫 단계는 기술적인 측면에서 방어의 역량을 강화하는 데 있을

수밖에 없습니다. 한국이 사이버 공격을 감행하여 방어의 효과를 올리기에는, 북한에는 공격할 정보 인프라도 없을 뿐만 아니라 자칫 잘못 공격하다가는 물리적 전쟁으로 비화할 가능성이 있습니다. 게다가 막상 공방이 벌어지면 한국의 발달된 정보 인프라로 인해 손해 볼 것이 너무 많습니다. 따라서 한국이 취할 수 있는 일차적 방안은 기술적인 차원에서 방패를 가능한 한 촘촘히 짜서 사이버 공격을 막아내려는 노력에 집중될 수밖에 없습니다. 이러한 인식을 바탕으로 최근 국내에서도 연구개발을 위한 예산 지원을 늘리고, 정보보호 산업의 육성을 위한 민간 및 정부 지원사업의 확대 등과 같은 대책들이 강구되고 있습니다. 이러한 대책들은 크게 예방력과 탐지력 및 복원력의 증대를 목표로 하고 있습니다.

첫째, 공격을 미리 예측하고 사고 발생을 최소화하는 예방력을 키우는 것입니다. 이와 관련해서 '사이버 보안 인텔리전스 네트워크 기반의 국가 통신망 모니터링 체계'의 구축이 거론됩니다. 이밖에도 전력·금융·의료 등 기반시스템 운영기관 및 기업들의 중요 정보 암호화 등 보호조치 강화, 주요 핵심시설에 백업센터 및 재해복구 시스템 확대 구축, 정부 소프트웨어 개발 단계에서의 보안취약점 사전 진단 제도 의무화 등도 거론됩니다. 사이버위협 정보 종합 수집·분석·공유 시스템 구축도 중요하게 거론되는데, 이는 해커들의 동향이나 악성코드에 대한 빅데이터 공유 환경을 구축하여 사이버 공격을 막을 수 있다는 인식을 바탕으로 합니다.

둘째, 해킹 공격 루트에 대해 수사하고 공격자를 확인하는 탐지력을 키우는 것입니다. 이는 근원지를 역추적하고 공격자의 신원을 식별하며, 사이버 공격 증거들을 확보하고 공격 원점을 타격하거나 동일한 수준의 목표물에 대해 부수적 피해 없이 동일한 수준의 대응공격을 할 수 있는 능력입니다. 특히 '포렌식 준비도'가 주목을 받고 있습니다. 포렌식 준비도가 도입되면 효과적인 사후 대응을 위해 보안 전문인력을 보유하고, 하드웨어와 소프트웨어가 로그를 많이 남기도록 정책을 설정함으로써 침해사고가 발생했을 때 신속한 대응으로 피해를 최소화 할 수 있습니다.

끝으로, 공격이 발생했을 때 최단시간 내에 차단하여 피해를 최소화하고 빠르고 원활하게 복구하는 복원력을 키우는 것입니다. 그동안 보안 분야의 주된 관심과 투자가 사이버 공격을 막거나 예방하는 데 있었다면, 앞으로는 공격을 당하더라도 피해를 최소화하자는 것입니다. 방패가 뚫리더라도 중상을 입지 않고 타박상에 그치도록 하자는 것입니다. 이러한 맥락에서 기업경영이나 국정운영, 에너지·자원 등 사이버 공격이 예상되는 분야를 중심으로 '해킹 리스크'를 상수로 설정하자는 의견도 제기됩니다. 이밖에 유사시에 대비한 위기대응매뉴얼이나 사이버 위기 상황을 가정한 모의훈련, 민간 차원의 사이버 민방위 훈련, 사이버 심리전에 대한 대응 등도 이러한 맥락에서 이해할 수 있습니다.

이러한 방어기술의 역량을 강화하는 데 있어 인력양성은 중요한 이슈가 아닐 수 없습니다. 효과적인 사전 예방과 사후 대응을 위해서는 전문가가 필요합니다. 공공 영역에서는 사이버 방어에 종사하는 이른바 '사이버 전사' 인력의 양성이 필요합니다. 이들을 양성하고 활용하며 적절히 대우하기 위한 체계적인 계획을 마련해야 합니다. 또한 민간 영역에서도 주요 기반시설의 보안관리와 정보보호 산업에 종사할 전문인력 육성의 필요성도 강력하게 제기되고 있습니다. 그러나 현재 국내의 상황은 정보보호 전문기업 대부분이 중소업체 위주로 되어 있고, 대학의 전문인력 배출도 미흡한 것이 문제점으로 지적됩니다.

2. 사이버전 전략과 사이버 억지의 가능성

적극적으로 맞받아치는 공격은 아니더라도 상대방이 공격하려고 해도 반격이 두려워 공격하지 못하게 하는 억지력도 대응전략의 하나로 거론됩니다. 최근 냉전기의 핵억지 개념에서 유추한 '사이버 억지' 개념이 원용되고 있습니다. 2012년 5월 미 국무부는 이러한 억지 개념에 입각하여 사이버 공격의 배후지를 제공한 국가의 주요시설에 대해서 사이버 보복을 가하거나 또는 그 가능성이 있는 국가에 대해서 사이버 선제공격을 가하겠

다고 엄포를 놓은 바 있습니다. 또한 2014년 12월 북한의 소니 해킹 이후 미국은 북한의 통신망을 마비시키거나 금융제재 조치를 단행한 것으로도 알려졌는데, 이는 복합적인 대응을 통해서 미국에 대한 사이버 공격이 어떠한 보복을 야기할 수 있는지를 보여주려 한 것으로 해석됩니다.

최근 한국에서도 이러한 사이버 억지의 개념을 원용하는 방안이 거론되고 있습니다. 상대가 공격할 것인지 미리 살피고 공격 행위 이전에 '방어'하는 차원에서 공격하는 선제공격의 구상도 제기되고 있습니다. 이른바 '사이버 킬 체인'의 구상의 그 사례인데, 이는 공격자가 시스템에 침투하기에 앞서 사전 작업을 할 때 이를 면밀히 감시하여 선제 대응을 하자는 것입니다. 그러나 이러한 발상들에 대한 우려의 목소리도 큽니다. 사이버 공격의 특성상 이러한 선제공격이 쉽지 않기 때문입니다. 또한 보복을 하는 경우에도 '누구에게 보복할 것인가'의 문제가 중요한데, 사이버 공격의 경우 보복의 대상을 확인하는 과정은 재래식 전쟁이나 핵전쟁에 비해서 훨씬 복잡합니다.

그렇다면 냉전기의 지정학적 핵억지 개념에서 유추한 사이버 억지의 개념을 원용하는 것은 어느 정도까지 가능할까요? 현재 국내외 학계의 논의는 억지의 개념들 중에서 '보복에 의한 억지'의 실효성은 의심하는 것이 중론입니다. '보복에 의한 억지'는 선제공격과 보복공격의 가능성이 상존하기 때문에 섣불리 먼저 공격을 감행하지 못하게 한다는 전략발상입니다. 그런데 앞서 살펴본 바와 같이, 비대칭 전쟁의 환경에서 사이버 공격을 사전 탐지하거나 사후 확인한다는 것이 쉬운 일은 아닙니다. 게다가 북한의 경우처럼 정보 인프라가 제대로 구축되지 않은 상대에게는 보복공격의 효과가 매우 낮기 때문에 억지력을 기대하기도 쉽지 않습니다.

이에 비해 '거부에 의한 억지' 개념은 사이버 안보 분야에 원용할 여지가 조금 더 많은 것으로 평가됩니다. '거부에 의한 억지'는 예상되는 공격에 대한 '방어'를 강화함으로써 적의 공격 자체가 성공하지 못할 것이라는 확신을 주는 데 주안점이 있습니다. '공격해 봤자 헛수고'라는 인상을

심어주어 상대방의 공격의지를 무력화시키는 방패의 구축이 관건입니다. 아무리 예리한 창으로 공격해도 뚫을 수 없는 방패라는 일종의 '철옹성 이미지'를 심어 주어 공격 자체를 아예 단념시키는 것입니다. 그러나 공격이 방어에 비해 압도적으로 유리한 사이버 안보의 특성상 여전히 '거부에 의한 억지' 개념을 원용하는 데 있어서도 제약요인이 없지 않습니다. 이러한 맥락에서 사이버 억지의 개념에, 기술과 전략의 변수뿐만 아니라, 정치외교적인 변수까지도 포함시킨 '수정된 사이버 억지'의 개념이 필요하다는 문제제기들이 출현하였습니다.

3. 사이버 안보의 추진체계 정비와 법 제정

사이버 공격에 효과적으로 대응하기 위해서 국내 거버넌스와 관련법을 정비하는 것은 필수적입니다. 2014년 말 한수원 해킹 사건을 계기로 사이버 안보의 중요성이 크게 강조되면서 사이버 안보 추진체계의 정비가 급물살을 타고 있습니다. 특히 2015년 3월말 청와대 국가안보실 산하에 사이버안보비서관이 신설되면서 청와대가 실질적인 사이버 안보 컨트롤타워 역할을 수행하게 되었고 이를 기반으로 공공기관들의 협력체계가 실질적으로 가동될 것으로 기대되고 있습니다. 이러한 추진체계에서는 최상위에 위치한 컨트롤타워(청와대 국가안보실)를 주축으로 국가정보원(이하 국정원), 미래창조과학부(이하 미래부), 국방부, 경찰청, 검찰청 등이 기타 정부기관들과 협력하는 이른바 '국가사이버안전체계'가 근간을 이루고 있습니다.

여기서 더 나아가 국무조정실이 관장하는 주요기반시설 보호체계도 청와대 국가안보실 주도의 국가사이버안전체계와 일원화할 필요성도 지적되고 있습니다. 또한 중앙행정기관, 지자체와 주요 기반시설 관리기관의 보안능력 확충을 위해 사이버 보안 전담조직을 신설·확대하자는 안도 거론됩니다. 또한 효율적인 민·관·군 사이버위협 정보공유 및 공동대응체계를 확립해야 한다는 주장도 제기됩니다. 이러한 위협정보 공유체계를 구

축하기 위해서는 공공 부문의 대책 마련과 더불어 정부와 민간 부문의 긴밀한 협력이 필요합니다. 사이버 안보의 중장기 국가전략을 수립하여 공표할 필요성도 지속적으로 거론되고 있습니다. 그동안 정부는 북한의 사이버 공격이 있을 때마다 종합대책, 마스터플랜, 강화방안 등의 형태로 대책을 마련해 왔지만 단기적인 수습방안에 주안점을 두었습니다.

한편 사이버 위기 발생 시 체계적이고 효율적인 대응을 위한 법적 근거를 마련해야 한다는 지적도 거셉니다. 현재 한국의 사이버 안보 관련 법제는 대통령 훈령으로 만든 국가사이버안전관리규정이 전부인데, 그나마 사이버 위기가 발생했을 때 상황 전파 등에 관한 내용만을 다루고 있다는 평가가 있어 왔습니다. 또한 전자정부법, 정보통신기반보호법, 정보통신망법 등에 사이버 안전 관련 규정이 산재해 있지만, 이는 일상적인 정보보호에 중점을 둔 것이어서 사이버 공격에 대응하기에는 역부족이라는 우려도 제기되어 왔습니다. 이러한 법제정의 필요성에 동조하여 현재 국회에는 '국가사이버테러 방지에 관한 법률안'(서상기 의원 발의), '국가 사이버안전관리에 관한 법률안'(하태경 의원 발의), '사이버위협정보 공유에 관한 법률안'(이철우 의원 발의) 등이 계류 중이지만 국정원의 권력남용이나 프라이버시 침해에 대한 우려 등을 이유로 그 처리가 지연되고 있습니다.

이러한 사이버 안보 관련 법률 제정 과정에서 관건이 되는 것은 국정원의 위상과 역할입니다. 찬성하는 측의 주장은, i) 국가차원의 사이버 위기관리 등을 위한 법제가 시급히 요구된다는 점, ii) 현재 사이버안보마스터플랜과 훈령에 따라 국정원이 실제 컨트롤타워 역할을 수행하고 있는 부분을 법률에 규정함으로써 그 기능을 강화할 수 있다는 점, iii) 국정원은 국내에서 사이버 공격 등에 대한 분석 및 대응에 있어 최고의 기술력과 노하우가 있다는 점 등을 강조하고 있습니다. 이에 비해 반대하는 측의 주장은 i) 국정원의 사이버 공간에 대한 통제력이 과도하게 될 위험이 있다는 점, ii) 국정원의 활동이 민간의 영역에까지 개입하게 되는 빌미를 제공할 수 있다는 점, iii) 민간과 공공 간의 정보공유 과정에서 개인정보가

유출되어 프라이버시가 침해될 수 있다는 점 등을 들고 있습니다.

4. 사이버 안보의 국제협력과 외교전략

사이버 공격으로 피해를 본 국가나 기관들끼리 서로 정보를 공유하고 정책적으로 공조하는 것도 중요한 국가전략의 사안입니다. 특히 사이버 선진국이자 한국의 우방국인 미국과의 정보공유 및 협력관계를 구축하는 문제가 핵심입니다. 예를 들어 2014년 11월 북한의 소니 해킹 사건이 발생했을 때 미국은 자국의 사이버 수사력을 총 동원하여 공격의 배후를 북한이라고 규정했는데, 당시 북한의 소행을 밝혀내는 과정에서 한국의 기술협조가 있었던 것으로 알려져 있습니다. 이러한 맥락에서 최근 국내에서는 사이버 안보 분야의 한미공조를 강화하고 사이버 안보의 문제를 한미 상호방위조약의 틀 내에 포함시킴으로써 미국의 '사이버 우산'을 빌어 북한을 억지하는 방안이 거론되고 있습니다.

그러나 한미 사이버 안보협력을 풀어나가는 데 있어서 중국이 변수입니다. 최근 미국이 사이버전 능력을 강화하면서 한국과 일본, 호주 등 전통적 동맹국에 사이버 협력을 요청했을 때 한국 정부는 머뭇거리면서 적극적인 참여를 유보했던 것으로 알려져 있는데, 미국과 사이버 동맹을 맺으면 중국이 반발할 것이란 우려 탓에 제대로 판단하지 못했다고 합니다. 외교 차원에서도 중국은 중요한 변수입니다. 현재 한국이 스스로 북한의 사이버 공격을 탐지하고 수사할 기술력이 모자란 상황에서 중국의 협조를 얻어낼 수 있는 외교력은 중요한 변수가 아닐 수 없습니다. 실제로 2014년 말 한수원 사태 때 정부 합동수사단은 해커의 공격 IP가 중국 선양지역이라는 것을 찾아냈지만 중국 정부의 협조를 얻지 못해 더 이상 수사를 하지 못하고 중단했다고 합니다.

초국적으로 발생하는 사이버 공격에 대한 국제적 대책은 양자협력을 통해서 이루어지기도 하지만 국제사회에의 호소, 국제기구와의 긴밀한 협력, 그리고 새로운 국제규범 형성에의 참여 등을 통해서도 우회적인 효과

를 볼 수 있습니다. 그러나 현재로서는 사이버 테러와 공격이 발생하고 그 공격주체를 색출하더라도 국제적으로 호소하거나 공격행위에 대한 처벌이나 제재에 대해 논의할 수 있는 외교의 공간도 마땅히 없습니다. 이러한 맥락에서 현재 다양한 방식으로 모색되고 있는 사이버 안보의 질서형성 과정에 적극적으로 참여하는 것 자체가 중요한 대응전략이 될 수 있습니다. 앞서 언급한 사이버 안보 분야의 세 가지 프레임의 특성을 이해하고 각 층위에서 나타나는 국가 간 이해갈등이나 입장 차이를 읽어내는 것이 중요합니다.

한국은 아직도 사이버 안보의 질서형성에 대한 명확한 입장을 설정하지 못하고 있습니다. 이러한 혼란은 2012년 12월 두바이에서 열린 WCIT (World Conference on International Telecommunication)에서 시도된 ITR (International Telecommunications Regulation)의 개정 과정에 참여할 당시에 드러났습니다. ITR의 규제조항이 급변하는 기술환경에 부합하지 않으므로 폐기해야 한다는 선진국들의 입장과 ITR의 개정과 강화를 통해 개별국가 차원의 규제정책의 기조를 유지하려는 개도국들의 입장이 대립했습니다. 그 사이에서 한국은 후자의 편에 섰는데, 이러한 선택은 이후 국내 언론의 신랄한 비판의 대상이 되었습니다. 인터넷 비즈니스의 많은 부분을 서방 선진국과 도모하고 있는 한국이 국제규범 형성과정에서는 사이버 공간의 활동에 대한 국가개입에 찬성하는 모순적 행태가 아니냐는 지적이었습니다.

Ⅳ. 사이버 안보의 과잉담론

1. 기술전문가 담론과 과잉 안보화의 경계

앞서 살펴본 기술적 특성상 사이버 안보 분야에서는 안보담론이 안보현실을 재구성하는 '안보화'의 문제가 관건이 됩니다. 사실 버추얼 위협으로서 사이버 위협에 대처하는 데 있어 어느 정도의 안보화 메커니즘을 배

제할 수는 없습니다. 사이버 안보의 문제는 실제로 큰 재앙의 형태로 발생한 실재하는 위협이거나 또는 검증 가능한 형태의 사건이라기보다는 아직까지는 전문가들이나 정치가들이 구성한 현실 속에서 존재하는 가상 위협입니다. 따라서 사이버 위협의 '실체'를 논하는 것보다는 사이버 위협의 성격, 안보의 대상과 주체, 그리고 이러한 과정에서 파생되는 결과에 대해서 '말하는 것' 즉 '담론'이 더 중요할 수 있습니다. 다시 말해, 사이버 공격의 위협을 상정하고 이에 대처해야 한다는 안보담론을 생성하고 이를 바탕으로 예산, 인력, 조직 등과 같은 국내자원을 동원하는 문제가 중요할 수밖에 없습니다.

이러한 안보화의 시각에서 보면 사이버 안보담론의 형성과정은 단순히 중립적 시도가 아니라 각 입장에 따라서 다르게 구성될 수밖에 없는 정치적인 과정이며, 그렇기 때문에 힘 있는 자가 주도하는 권력정치일 가능성이 큽니다. 사실 이러한 안보화 담론의 부상에는 정보화 선진국으로서 미국이 큰 역할을 담당했습니다. 가장 발달된 정보 인프라를 가지고 있는데다가 개방사회로서 미국은 외부로부터의 사이버 위협에 취약할 수밖에 없습니다. 설상가상으로 9.11 테러 이후로 높아진 안보의식이 이러한 안보화 담론이 성장하는 토양이 되었습니다. 세계 패권국이 생성하는 안보화 담론은 실제로 미국의 정책에도 반영되고 더 나아가 주위 국가들과의 관계에도 영향을 미칩니다. 현재 진행 중인 미중 사이버 갈등 양상을 보면, 이러한 안보화 담론을 기반으로 하여 양국의 국내체제를 재구성하고 더 나아가 국제정치에서의 경쟁의 양상을 만들어가는 경향이 두드러지게 나타납니다.

그런데 이러한 사이버 안보담론은 과장되게 느껴질 정도로 아직 발생하지 않은 재난과 그 재난이 야기할 파장을 부각시키는 이른바 '과잉 안보화'의 위험성을 안고 있습니다. 그리고 이러한 과잉 안보화의 저변에는 일반 대중에게 잘 알려지지 않은 비밀정보와 고도의 전문지식을 독점한 전문가들이 형성하는 기술전문가 담론이 있곤 합니다. 다시 말해, '망치를

잡으면 모든 게 못으로 보인다'는 말이 있는 것처럼 기술적 가능성과 효율성을 과대평가하는 기술결정론적 경향이 나타날 우려가 있습니다. 실제로 최근 국내에서 거론되고 있는 '공세적인 방어'나 '예방적 선제공격,' '사이버 킬 체인' 등과 같은 구상에는 일정한 정도의 과잉 안보화의 경향성이 담겨 있음을 부인할 수 없습니다. 이러한 안보화 담론은 사이버 공간의 군사화를 부추겨 자기실현적으로 사이버 공간을 위험하게 만들 가능성마저도 있습니다.

2. 군사안보 우선담론과 과잉 군사화의 위험

사실 오늘날 사이버 안보는 명실상부한 21세기 국가안보의 문제로 부각했습니다. 최근 사이버 안보는 전쟁과 평화의 문제, 즉 군사안보 문제로 자림 매김을 하고 있습니다. 영토, 영해, 영공, 우주 등의 공간에 이어 사이버 공간이 '제5의 전쟁터'가 되었다는 말까지 나옵니다. 특히 최근 글로벌 패권국인 미국이 보여주는 행보는 사이버 안보의 문제를 군사안보의 관점에서 접근하는 경향을 선도하고 강화하고 있는 것으로 파악됩니다. 사이버 공간에서의 갈등과 분쟁이 늘어나는 상황에서 어느 정도의 군사적 접근은 불가피하다는 사실을 인정하더라도 과도한 냉전의 논리에 의거하여 사이버 공간의 안보 문제가 지나치게 군사화되는 이른바 과잉 군사화의 위험성에 대해서는 경계하지 않을 수 없습니다.

최근 미국 고위관료들의 발언은 사이버 공간을 과잉 군사화할 우려를 낳고 있습니다. 앞서 지적한 바와 같이, 2012년 5월 미 국무부는 사이버 공격의 배후지를 제공한 국가의 주요시설에 대해서 사이버 보복이나 사이버 선제공격의 가능성을 언급한 바 있습니다. 미국과 이란이 사이버 공방과 관련하여 리언 패네타 미 국방장관은 2012년 10월 11일 미국이 '사이버 진주만' 공격을 받을 위험에 처했다고 지적했습니다. 북한의 소니 해킹에 대해서 2015년 2월 26일 미국 국가정보국 제임스 클래퍼(James Clapper) 국장의 상원 증언은, 미국이 북한의 소니 해킹을 미국 영토를 목

표로 사이버 공격이 감행되어 민간 기업에게 피해를 입힌 국가안보 이슈로 인식하고 있다는 사실을 보여주었습니다.

이러한 미국의 태도에 대해서 중국도 정치군사의 논리로 맞받아치면서 자국 내의 정보시스템과 정치체제에 대한 주권적 권리를 주장합니다. 이러한 와중에 21세기 패권을 겨루는 두 강대국 간의 사이버 공방 게임은 계속 상승하고 있습니다. 또한 북한과의 관계에서 군사전략의 시각으로 현실을 이해하는 접근도 조심스럽게 살펴보아야 합니다. 이러한 군사전략 담론에 의거하여 한미 간의 사이버 안보협력을 이해하고 중국이나 북한과의 관계를 설정하는 것은 자칫 큰 부담으로 다가올 우려가 있습니다. 예를 들어, 중국이나 북한의 소행으로 추정되는 사이버 공격에 대해서 한미 간의 집단자위권을 근거로 물리적 반격을 가해야만 하는 상황이 창출될 경우 자칫 한반도가 사이버 전쟁터, 더 나아가 물리적 전쟁터가 될 우려도 있습니다.

기본적으로 사이버 안보의 문제는 국가 중심의 군사안보의 개념으로만 접근할 전통안보의 문제가 아닙니다. 오히려 원자력·에너지 안보, 환경안보·기후변화, 보건안보 등과 같이 복합적인 이슈영역과 국가, 경제, 사회, 개인 등의 다양한 행위자들이 관여하는 초국적인 신흥안보의 이슈입니다. 이러한 사이버 안보 문제에 적절히 대응하기 위해서는 사이버 위협을 '감기'와 같은 일상적인 위험으로 보는 의연한 태도가 필요할 수도 있습니다. 사이버 공간에서 제기되는 위협을 '비정상적인 위기'로 인식하여 과고하게 군사화하기보다는, 항상 겪을 수밖에 없는 일상적인 상태의 개념으로 이해하자는 제안이 나오는 것은 바로 이러한 이유 때문입니다. 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 있습니다.

3. 국가의 빅브라더화와 과잉 정치화의 딜레마

사이버 안보의 추진체계 정비와 법제정 문제에 있어서 지속적으로 논란거리가 되는 것은 국가권력의 비대화, 이른바 국가의 '빅브라더화' 가능성입니다. 이러한 논란은 사이버 안보 관련 추진체계와 법제 안에 담기는 '국가'가 어떤 '국가'이냐에 대한 인식의 차이를 바탕으로 합니다. 추진체계 정비와 법제정 필요성을 주장하는 측이 상정하고 있는 '국가'는, 다소 중립적인 의미로 사이버 공간의 안전과 정보시스템의 보호를 담당하는 '정부'이거나 더 나아가 외부로부터의 사이버 공격으로부터 '국가안보'를 수호하는 대외적 차원의 국가, 즉 '네이션(nation)'에 대한 인식을 바탕으로 합니다. 이에 비해 반대하는 측에서 상정하고 있는 '국가' 인식은, 사회와 대립되는 의미에서 파악된 '국가' 또는 조금 좁은 의미에서 '정권'이며, 이러한 연속선상에서 생각하는 안보는 오히려 보안이나 공안이라는 의미로 이해되는 정치권력의 정당화라는 인식을 바탕으로 합니다.

이러한 구도에서 볼 때, 정보보안 전문가들 사이에서는 사이버 공격을 막을 컨트롤타워나 사이버테러방지법 제정의 필요성은 인정하면서도 그 컨트롤타워의 주체(또는 실무총괄)로서 국정원의 빅브라더화에 대한 의구심이 없지 않습니다. 2015년 7월 발생한 국정원의 해킹 프로그램 구입에 대한 야당의 문제제기와 국민들의 걱정도 이러한 국정원의 빅브라더화에 대한 우려와 밀접한 관련이 있습니다. 이러한 맥락에서 국정원을 견제하는 차원에서 컨트롤타워로서 청와대 국가안보실의 위상을 설정해야 한다는 지적도 있습니다. 사정이 이러하다 보니, 일각에서는 국정원 산하 국가사이버안전센터로의 권한 집중이 문제가 된다면, '사이버보안청'과 같은 별도 조직을 신설하는 것도 대안이 될 수 있다는 얘기가 나오고 있습니다.

이러한 국가의 빅브라더화에 대한 경계의 이면에는 사이버 안보를 지나치게 '정치화'하는 문제도 없지 않습니다. 사실 사이버 안보 관련 법제정 논란은 고도로 '정치화된' 이슈로서, 어찌 보면 정치적 차원에서 이루어지

는 왜곡된 인식의 결과라고 할 수 있습니다. 게다가 사이버 안보 추진체계와 법제정 논리의 이면에는 정책의 주도권을 둘러싼 관료정치의 문제, 즉 국정원과 국방부, 미래부 간의 이해관계도 충돌하고 있습니다. 21세기 국가안보 문제인 사이버 안보가 여야 간의 지나친 정치적 논리, 또는 좌우 논리에 휩쓸려서 과잉 정치화될 가능성도 상존합니다. 실제로 국가안보 차원에서 다루어야 할 사이버 안보의 문제를 모두 국내정치와 민간사찰 문제로 환원하는 오류도 없지 않습니다.

궁극적으로 사이버 안보와 관련하여 관찰되는 국가의 빅브라더화와 과잉 정치화의 딜레마는 현재 한국 정치와 사회가 풀어야 할 난제가 아닐 수 없습니다. 사이버 안보의 국가전략을 모색하는 글로벌 추세를 염두에 둘 때 대승적 차원에서 사이버 안보의 중요성을 인식할 필요가 있습니다. 그 과정에서 기존의 전문성이 있는 기관이 실무를 책임지고 담당하는 것이 효율적이고 또한 더 나은 효과를 거둘 가능성이 클 것입니다. 그러나 이러한 정치사회적 결정을 내리기 위해서는 '국민' 모두가 납득할 수 있는, 그리고 21세기 변화하는 세계정치 환경에 부합하는 '국가'의 역할에 대한 인식이 필요합니다. 이러한 '국가' 개념의 재정립 필요성은, 전통안보와는 그 구조적 성격을 달리하는 사이버 안보 분야의 특성상 더욱 더 강하게 제기될 수밖에 없습니다.

4. 과잉 현실주의 담론을 넘어서

사이버 안보의 국제협력을 모색하는 과정에서도 경계해야 할 과잉담론이 없지 않습니다. 이는 현실주의 국제정치이론에서 상정하고 있는 국제정치의 이미지를 과도하게 강조하는 담론이라는 의미에서 '과잉 현실주의' 담론이라고 부를 수 있겠습니다. 근대 국제정치이론의 주류를 이루는 현실주의 담론은 주요 행위자로서 국민국가를 설정하고 이들이 벌이는 권력정치의 과정에서 생성되는 제로섬 게임의 양상에 주목합니다. 지구화, 정보화, 민주화로 대변되는 변화를 겪고 있는 오늘날에도 이렇게 현실주

의 담론이 그리고 있는 현실은 엄연히 존재합니다. 그러나 오늘날 세계정치의 변화는 단지 그러한 제로섬 게임의 양상으로만 파악할 수 없는 복합적인 모습으로 전개되고 있는 것도 엄연한 사실입니다. 따라서 현실주의 국제정치이론의 담론에 지나치게 집착해서 세상을 볼 경우, 자칫 담론이 현실을 왜곡하는 과잉담론 현상이 출현할 가능성이 있습니다.

최근 사이버 공간에서 벌어지는 경쟁과 갈등, 그리고 그러한 연속선상에서 출현하는 주요 국가들의 사이버 안보 전략의 양상을 보면, 이러한 과잉 현실주의 담론에 의해서 현실이 재구성되고 있는 것 같은 느낌을 지울 수 없습니다. 특히 미국이나 중국, 러시아 등과 같은 강대국들이 벌이는 안보화 게임이나 사이버 공간의 군사화 게임은 단순히 관련 행위자들의 이해관계가 조정되고 갈등하는 차원을 넘어서 강대국들이 나서서 벌이는 21세기 패권경쟁의 한 단면을 보는 듯합니다. 게다가 아직 사이버 안보 문제를 다룰 국제규범이 마련되지 않은 상황에서 사이버 안보 분야는, 현실주의 국제정치이론이 상정하는 것과 유사한, 전형적인 무정부상태로 개념화되고, 그러한 환경 아래에서 전통적인 국제정치 행위자로서 국가 행위자들이 전면에 나서 제로섬 게임의 경쟁을 벌이는 세상으로 그려집니다.

강대국들이 벌이는 패권경쟁 담론이 사이버 공간에까지 침투하는 구도는 한국의 입장에서 볼 때 결코 좋을 것이 없습니다. 게다가 남북한이 대치하고 있고 한반도를 두고 미국과 중국이 주도권 경쟁을 하는 상황에서 한국이 양국 사이에 벌어질 사이버 전쟁이나 무역 분쟁에서 어느 한 편을 들기는 어려운 실정입니다. 미국에 대한 안보 의존도나 중국에 대한 무역 의존도가 매우 높은 상황에서 자칫 큰 문제가 불거질 우려가 있기 때문입니다. 예를 들어, 미국은 2012년 국방수권법을 제정해 외국 장비가 국가시설에 도입되는 것을 사실상 원천 봉쇄했습니다. 마찬가지로 중국도 외산(특히 미국산) 장비를 국가시설에 들이려면 소스코드를 공개하라는 원칙을 주장하고 있습니다. 이러한 미중 갈등의 와중에 최근 한국의 통신업체가 중국산의 저가 통신장비를 수입하려다가 미국의 반대에 봉착한 적이 있었

습니다. 미중관계가 국가 간 경쟁의 구도로 전개될 경우 한국이 처할 어려움을 엿보게 하는 대목이었습니다.

이러한 연속선상에서 보면, 전통적인 국제법과 국제기구의 틀을 활용하여 사이버 안보의 국제규범을 만들려는 시도 자체도 성찰적으로 보아야 할지 모릅니다. 최근 미국과 NATO, 유엔 등을 중심으로 사이버 공격에 대해 전쟁법을 적용하려는 시도를 벌이고 있는데, 이러한 접근이 한국에 주는 의미가 무엇일지에 대해서 냉철하게 생각해 볼 필요가 있습니다. 사이버 안보의 국제규범을 국민국가들의 관계, 즉 국제(國際, inter－national)의 틀에서 접근하는 것이 맞는가에 대한 성찰이 필요합니다. 다시 말해 탈지정학적이고 초국적으로 작동하는 사이버 안보의 문제를 국민국가들 간의 관계라는 틀로 보는 근대 국제정치 담론 그 자체에 대해서 성찰적인 입장이 필요합니다. 사이버 안보의 이슈는 탈린 매뉴얼이나 유엔 GGE 같이 전통적인 국제법과 국제기구의 형식에만 의존해서는 해결될 문제가 아니라는 것을 알아야 할 것입니다.

Ⅴ. 맺 음 말

사이버 안보는 전통적인 국가안보의 지정학 시각을 넘어서 이해해야 하는 문제입니다. 사이버 안보 분야는 영토성을 기반으로 하여 국가가 독점해온 안보유지 능력의 토대가 잠식되는 현상을 보여주는 사례입니다. 특히 탈지정학적 공간으로서 사이버 공간의 부상은 테러 네트워크나 범죄자 집단들에 의해 도발될 비대칭 전쟁의 효과성을 크게 높여 놓았습니다. 결과적으로 사이버 공간에서 등장한 새로운 위협은 국가에 의해 독점되어 온 군사력의 개념뿐만 아니라 군사전략과 안보의 개념 자체도 그 기저에서부터 뒤흔들어 놓고 있습니다. 이러한 변화에 직면하여 기존의 지정학과 국가안보 중심의 국제정치학 시각은 시원한 해답을 제시하지 못하고 있습니다. 이러한 맥락에서 이 글은 복합지정학의 시각에서 사이버 안보의 세계

정치를 이해하고 이에 대응하는 국가전략의 방향을 제시하였습니다.

첫째, 사이버 안보의 세계정치와 국가전략은 고전지정학과 탈지정학을 섞는 복합지정학의 시각에서 이해해야 합니다. 최근 강대국들이 관여하면서 지정학적 양상을 보이고 있는 사이버 안보 게임의 이면에는 인터넷과 컴퓨터 바이러스, 악성코드 등과 같은 기술 변수와 해커나 테러리스트 등과 같은 비국가 행위자들이 벌이는 탈지정학적 게임이 자리 잡고 있습니다. 이러한 탈지정학적 공간에서 다양한 해킹 수법을 동원하여 공격하는 비국가 행위자들과 이를 막으려는 국가 행위자들이 경합하는 양상을 보이고 있습니다. 여기에 최근 국가 행위자들이 사이버 공격에 좀 더 본격적으로 개입하는 지정학적 게임의 양상이 더해지면서 그 복잡성을 더해가고 있습니다.

이러한 맥락에서 한국의 국가전략은 기술역량이라는 지정학적 변수의 증대를 통해서 탈지정학적 사이버 공격을 막아야 하는 복합적인 과제를 안고 있습니다. 이러한 기술역량을 키우는 데 있어 인력양성은 중요한 변수가 아닐 수 없습니다. 한편 적극적으로 맞받아치는 공격은 아니더라도 상대방이 공격하려고 해도 반격이 두려워 공격하지 못하게 하는 억지력의 증대에도 관심을 기울여야 합니다. 현재 국내외 학계의 논의는 '거부에 의한 억지'의 가능성에 주목하고 있는데, 이는 예상되는 공격에 대한 방어를 강화함으로써 적의 공격 자체가 성공하지 못할 것이라는 이미지를 심어주는 데 주력합니다. 그런데 이러한 사이버 억지는 기술역량으로만 달성되는 것이 아니라 외교역량의 발휘와 병행해야 한다는 점도 명심해야 합니다.

둘째, 사이버 안보의 세계정치와 국가전략은 고전지정학과 비판지정학을 섞는 복합지정학의 시각에서 이해해야 합니다. 최근 사이버 안보 분야에서는 미국과 서방 국가들을 한편으로 하고, 러시아와 중국을 다른 한편으로 하는 국가 행위자들 간의 지정학적 대결이 벌어지고 있습니다. 이들 사이에서 실제로 오고가는 공격과 방어의 실체를 파악하기는 어렵지만, 적어도 이들이 벌이는 안보화 담론경쟁은 그야말로 전쟁을 방불케 합

니다. 특히 미국과 중국의 안보담론 경쟁은 21세기 패권경쟁의 예고편을 보는 듯합니다. 현재 양국 간에는 사이버 위협의 성격이 무엇이고, 안보의 대상과 주체가 무엇인지, 그리고 사이버 안보와 관련된 양국의 국내체제와 세계질서의 미래에 대한 안보담론의 경쟁이 진행되고 있습니다.

이러한 맥락에서 볼 때 한국의 국가전략에서도 사이버 위협이 되는 잠재적인 대상을 상정하고 이들을 대응하기 위해서 예산, 인력, 조직 등과 같은 자원을 배분하는 안보화의 정치가 벌어지고 있습니다. 특히 이러한 자원배분의 과정은 사이버 안보 분야의 국내 추진체계를 정비하는 문제나, 단순히 사이버 안보 추진체계를 정비하는 차원을 넘어서 사이버 안보 관련 법제정 문제에서 나타나는 중요한 관건입니다. 현재 이러한 추진체제의 정비와 법제정의 필요성에 동조하여 현재 국회에는 관련 법안들이 다수 제출되어 계류 중인데, 실무기관들의 정책집행의 효율성뿐만 아니라 국민적 동의를 얻을 수 있는 방향으로 처리되어야 합니다.

끝으로, 사이버 안보의 세계정치와 국가전략은 고전지정학과 비지정학을 섞는 복합지정학의 시각에서 이해해야 합니다. 사실 탈지정학적 메커니즘을 빌어서 발생하는 사이버 테러와 공격은 단순히 일국 차원의 대응책 마련과 법제도의 정비 등으로 해결될 문제가 아닙니다. 기본적으로 국민국가의 국경을 초월하여 발생하는 문제이니만큼 이해 당사국들의 긴밀한 국제협력을 통해서 그 해법을 모색하는 것이 필요합니다. 그런데 이러한 국제협력의 메커니즘을 마련하는 과정에 미국과 서방 국가들을 한편으로 하고 구사회주의권 국가들과 개도국들을 다른 한편으로 하는 지정학적 대립구도가 투영되고 있다는 사실도 잊지 말아야 합니다.

이러한 맥락에서 한국의 국가전략도 주변국들과의 국제협력을 강화하고 국제규범 형성 과정에도 적극적으로 참여하는 데 힘써야 합니다. 한반도가 처한 지정학적 특성상 전통적 우방국인 미국이나 새로이 부상하는 중국 등과의 기술협력과 정책공조를 펼치는 것은 매우 중요한 외교적 사안입니다. 또한 사이버 안보의 대응방안을 모색하는 데 있어서 양자 간의

국제협력이라는 지정학 구도를 넘어서 좀 더 넓은 의미의 다자 구도에서 접근하는 시도도 필요합니다. 이러한 과정에서 국가 간 관계를 조율하는 기존의 국제규범을 정비하는 움직임과 동시에 새로운 글로벌 거버넌스의 메커니즘을 모색하는 움직임이 경합하고 있음을 주목할 필요가 있습니다.

한편 이러한 사이버 안보의 국가전략을 모색하는 과정에서 나타날 수 있는 과잉 안보담론의 출현을 경계해야 합니다. 이 글은 복합지정학의 시각에서 크게 네 가지 과잉 안보담론의 위험성을 지적하였습니다. 첫째, 기술합리성과 효율성의 논리에 지나치게 매몰되는 과잉 안보화, 둘째, 사이버 공간의 활동을 지나친 냉전논리와 군사논리로 이해하는 과잉 군사화, 셋째, 사이버 안보 문제를 지나친 정치적 논리, 특히 국가권력의 논리나 좌우이념의 논리로 몰고 가는 과잉 정치화, 끝으로 국가 행위자들이 벌이는 제로섬 게임의 양상을 과장하는 과잉 현실주의 담론 등이 그것입니다. 이러한 과잉담론들은 모두 사이버 안보 문제의 복합적인 성격을 간과하고 단순 지정학의 발상에 입각해서 추진되는 정책들의 소산이라고 할 수 있습니다.

요컨대, 사이버 안보의 세계정치는 전통적인 의미의 국민국가들이 벌이는 지정학의 게임이라는 관점만으로는 이해할 수 없습니다. 국가 및 비국가 행위자 그리고 경우에 따라서는 네트워크 환경과 기술시스템이라는 변수들까지도 적극적으로 관여하는 복합지정학의 게임으로서 이해해야 할 것입니다. 이러한 과정에서 국가 행위자는 사이버 공격이라는 위협 요인을 제공하는 주체인 동시에 초국적으로, 또는 국가 간에 발생하는 사이버 위협을 방지하는 방어의 메커니즘을 만드는 주체로서 그 입지를 강화해 가고 있습니다. 최근 국내에서 모색되고 있는 사이버 안보의 국가전략은 이러한 사이버 안보 분야의 특성에 대한 이해를 바탕으로 추진되어야 할 것입니다.