서울대학교 통일평화연구원
The Institute for Peace and Unification Studies
Seoul National University

통일평화연구원 지식과 비평 | 제14호 (2023년 1월 11일)
IPUS HORIZON | No. 14 (11 Jan 2023)

사이버 안보의 진화: 복합지정학의 시각

김 상 배 (서울대 정치외교학부 교수)

최근 사이버 공격이 양적으로 굉장히 많이 증가하고 있을 뿐만 아니라, 질적인 내용도 변천하고 있습니다. 과거에 사이버 공격은 시스템 교란을 위한 해킹 공격만을 의미했다면, 현재는 이를 넘어서 국제정치·경제·군사 이슈와 연결되어 미래 사이버 전쟁까지 확장되었습니다. 사이버 안보의 가장 큰 특징은 기존의 전통적인 안보 이슈가 갖는 고유한 성격과 다르다는 것입니다. 그 특징을 한마디로 요약하자면, 수년 전 출간한 책 제목이기도 한 "버추얼(Virtual) 창과 그물망 방패"입니다. 창과 방패를 동시에 파는 어느 상인이 창을 자랑할 때는 이 창으로 뚫을 수 없는 방패는 없다고 하는데, 방패를 자랑할 때는 이 방패가 막지 못하는 창은 없다고 말했다고 합니다. 모순이라는 뜻으로 널리 알려진 이 오래된 고사성어가 디지털 시대에 특히 사이버 안보 이슈와 관련되어 있습니다. 사이버 안보는 버추얼한(보이지 않는) 창이 굉장히 많은 수로 공격을 가하고 있는 상황이며 이를 막아야 되는 방패는 단단한 판으로 만들어진 방패가 아닌 구멍이 숭숭 뚫려 있는 그물망으로 되어있다고 볼 수 있습니다. 막아야 되는 보이지 않는 창과 굉장히 허술한 방패의 상호 대결인 것입니다.

사이버 안보는 새로운 이슈이다 보니 고전적인 의미에서 지정학적인 시각을 통해서 이 문제를 분석해야 할 필요성이 있습니다. 그럼에도 불구하고 이 성격이 갖는 복잡성으로 인해서 지정학을 넘어서 복합적인 시각들을 원용해야 한다는 의미로 '복합지정학 시각에서 사이버 안보'를 연구하고 있습니다. 사이버 안보의 진화 과정을 살펴보면, 초기에는 비국가 행위자들 해커 또는 테러리스트들이 벌이는 해킹 행위들의 양이 늘어나고 그 패턴이 다변화되는 과정이 있었습니다. 그러나 이러한 초기 사이버 안보 이슈가 국가 간 전쟁을 논할 정도로 이슈가 창발해갔습니다. 창발(emergence)이라는 용어는 복잡계 이론에서 사용하는 용어로, 미시적 차원에서 다양한 요소들이 복잡한 상호작용을 거치거나 다양한 이슈 연기의 과정을 거쳐서 새로운 질서와 패턴을 만들어가는 과정을 칭하는 용어입니다. 최근에 사이버 안보 분야에서 벌어지고 있는 변화는 창발이라는 복잡계 이론의 개념을 원용해서 봐야 될 정도로 굉장히 복잡한 양상으로 진행되고 있어, 전통적인 지정학 또는 안보 문제뿐만 아니라 수면 밑에 있는 문제들도 복합적으로 살펴보아야 할 필요성이 제기되고 있습니다.

사이버 공격에 대한 논의를 함에 있어서 우선, 사이버 스페이스라고 하는 독특한 공간을 바탕으로 하는 공격이 갖는 고유한 특성을 이해할 필요가 있습니다. 사이버 공간이라고 하는 복잡하고 복합적인 네트워크 구조를 띤 환경에서 벌어지는 안보 이슈이자 공격과 방어 이슈를 이해해야 합니다. 인터넷 자체가 굉장히 여러 빈틈이 있는 취약한 환경이기 때문에 그 틈새를 겨냥해 공격이 이루어지는데, 방어를 하더라도 버추얼 창과 그물망 방패처럼 제대로 방어가 될 수 없어 전반적으로 공격이 방어보다 유리한 상황입니다. 경우에 따라서는 피해 대상을 구분하기도 쉽지 않으며, 공격한 쪽이 공격으로 끝나는 게 아니라 자기가 한 공격이 또 자신에게 부메랑처럼 되돌아오기도 하는 복합적인 네트워크 환경에서 벌어지는 공격과 방어의 게임입니다.

다음으로, 사이버 스페이스라고 하는 것이 컴퓨터 네트워크를 만들어내고 있는 과학기술의 산물이라는 점에서 사이버 안보가 이루어지는 공간은 과학기술 변수에 영향을 많이 받고 있습니다. 사이버 공격의 대상이 되는 것들도 컴퓨터 바이러스나 악성 코드 등 대부분이 어떤 면에서는 소프트웨어 프로그램으로 볼 수 있습니다. 과학기술을 통해 만들어진 공격의 수단이자, 공격이 이루어지는 패턴도 디도스 공격이나 또는 APT(Advanced Persistent Threat)라 알려져 있는 지능형 지속 공격, 최근에 논의가 되었던 스턱스넷(Stuxnet)이나 랜섬웨어 같은 것들이 인간이 아닌 비인간의 행위자들이 수단으로 활용되어지고 있습니다. 이러한 비인간 행위자들이 나름대로의 에이전시 행위 능력을 갖는 적극적인 행위자로서 의미를 가지면서 발생하는 게임이라 할 수 있습니다. 이외에는 안보 게임이라는 건 전통적으로 국가 행위자들간의 위협과 방어의 게임으로 알고 있었지만 사이버 안보 분야는 기본적으로 국

가가 아닌 민간 행위자들이 많이 참여하고 있습니다. 최근에는 국가 행위자들이 그 배후에서 민간 행위자들을 조종하거나 또는 배후에서 전면으로 나와 직접적으로 공격 행위를 하는 것들이 증가하고 있는 것도 큰 특징이라고 할 수 있습니다.

마지막으로 사이버 공격이 오늘의 위협일 수도 있지만 내일의 큰 위협될 수 있습니다. 잘 보이지 않는 위협인 것이죠. 그렇기 때문에 객관적으로 존재하는 안보 위협도 엄연히 존재하지만 주관적인 판단으로 더 큰 위협이 될 수 있다는 것을 가정하는 안보화 (securitization) 담론의 특징을 갖습니다. 하지만 사이버 안보 분야에서는 공격이 발생한 이후 책임 소재를 귀속해 나가는 과정 자체도 엄밀하게 원인과 결과를 밝힐 수 없는 복합적인 네트워크 환경에서 이루어지고 있기 때문에 현실에서 벌어지고 있는 사이버 안보 게임에 누가 어떤 식으로 공격했다라는 스토리텔링이 중요해집니다.

학계에서는 사이버 공격 패턴을 다양한 형태로 개념적인 구분을 하고 있습니다. 공격의 목적이나 대상이라는 차원에서 물리적 파괴, 시스템 교란, 자원 획득을 한 축에 놓고, 공격의 주체를 국가와 집단, 개인 다른 한 축으로 넣고 볼 때, 국가간의 물리적인 공격과 연동되어 있는 사이버 전쟁에서부터 사이버 테러와 사이버 교란 또는 사이버 간첩 행위라든지 사이버 범죄까지 여러 가지로 나누어서 볼 수 있습니다. 그러나 최근의 특징은 이러한 구분이 무색하게 서로 엉켜져 있는 상황들이 벌어지고 있다는 것입니다. 사이버 공격이 그저 민간 행위자들의 개인 범죄인 것 같은데 어떤 면에서 국가적인 차원에서 갈등의 소지가 되거나 데이터나 시스템을 교란하고 하는 행위 자체가 물리적인 공간에서의 전쟁과 연계되고 있습니다. 사이버 공격의 패턴 역시 역사적인 차원에서 변천을 겪고 있는 것 같습니다. 지난 10~15년 정도를 돌이켜 보았을 때, 초반기에 국제정치학에서 문제가 된 것은 국가의 기반 시설에 대한 공격들 공공기관이나 국가적으로 굉장히 중요한 의미를 갖는 금융기관, 언론기관, 핵심 인프라에 대한 사이버 공격이었습니다. 그러나 현재는 지적재산권이라든지 기밀 데이터나 핵심 기술에 대한 공격이 문제가 되어지는 양상입니다. 데이터나 기술 중에서도 경제적으로 이익이 되는 부분들을 타겟팅해서 공격이 이루어지고 있습니다. 랜섬웨어를 심어 금전을 요구하거나 암호화폐와 관련된 부분들에 대한 해킹들이 이루어지고 있을 뿐만 아니라, 정보심리전이라 불리는 심리적 차원에서의 결함을 바탕으로 새로운 것들을 얻어내기 위한 공격의 수단으로 진화하고 있습니다. 이런 과정에서 또 하나의 획을 긋는 사건은 코로나19의 발생으로, 코로나로 인해 조성된 비대면 환경을 위협하는 사이버 공격이 늘어나고 있다는 점입니다. 현재 우리는 굉장히 많은 프로그램들을 비대면 환경에서 쓰고 있습니다. 이러한 프로그램을 매개로 벌어지는 개인간 또는 기업과 국가간 활동 사이에 침투해 교란 행위나 절취 행위가 이루어지고 있습니다. 또한, 코로나19 관련하여, 코로나 치료제와 백신의 첨단핵심기술을 절취하는 것도 문제가 되고 있습니다. 코로나 바이러스를 피해 들어간 비대면 환경을 매개로 컴퓨터 바이러스가 급습하여, 코로나 바이러스가 지나간 자리에 컴퓨터 바이러스가 찾아오는 양상입니다.

최근에 AI를 활용한 사이버 공격과 방어가 대두되고 있습니다. 사이버 공격이 지능화되고 자동화를 넘어서 자율화되고 있는 것입니다. 프로그램으로 자동화된 메커니즘, 알고리즘을 따라서 자율적으로 공격하고 있으며, 이를 방어하는 측에서도 위협 정보를 분석하고 이상 징후를 감지하는 예측 프로그램에 AI를 활용하고 있습니다. 어느 순간부터는 인간은 빠진 상태에서 기계 스스로 방어하는 자율적인 사이버 공격 무기와 이들로부터 자율적으로 방어하는 AI 기반의 방어망이 서로 공방을 주고받는 그런 세상이 올지도 모르겠습니다. 또 다른 최근 경향으로 국제정치 전반에 지정학적 부활의 현상과 맥이 연결되는 부분으로, 과거에 민간 행위자들이 주도적으로 나오고 국가가 뒤에 숨어 조종하는 공격이었다면, 최근에는 사이버 공격에 전면으로 국가 행위자들이 나서고 있다는 점입니다. 이러한 조짐은 2000년대 후반부터 러시아가 동유럽의 국가들에 대해 가했던 사이버 공격이 드러나면서 알려지게 되었습니다. 한편, 2010년대 초반에 미국과 이스라엘이 이란과 벌였던 사이버 공방에서도 국가 행위자들이 명시적으로 드러나고 있습니다. 이후 2010년대 중후반을 거치면서 미국과 중국이 벌이고 있는 패권 경쟁의 맥락 속에서 사이버 공격 사이버 안보 이슈가 핵심적인 현안이 되고 있습니다. 또한, 한반도에서도 북한의 공격으로 추정되는 공격이 몇 차례 있었습니다. 국가가 배후가 되어 이루어지는 사이버 공격은 점점 더 명시적으로 시스템을 교란하고 다운시키고 있습니다. 하지만 누가 공격을 했는지 표가 나는 공격이라기보다는 핵심 데이터를 잠깐 들여다 본다든지 빼내 오는 방법으로 표가 나지 않는 공격이 특징적입니다. 2010년대 중후반에 중국의 해커들이 미국의 국가기관 시스템에 가했던 공격들이 미국의 정보당국에서 주장하고 있는 바입니다. 최근에 북한이 한국과

다른 나라 주요 시설들에 대해 가하고 있는 다양한 종류의 해킹들도 데이터의 설치 정보기술 절취 더 나아가서는 금전적인 목적을 노리는 절취와 연결되어, 전체적으로 사이버 공격이 진화해가고 있다고 할 수 있습니다. 복합적인 국가 전략의 대응 체계 차원에서 주목해야 하는 중요한 부분입니다.

2021년 초, 미국에서 사이버 위협 증대에 대한 논의가 떠들썩했습니다. 새롭게 출범한 바이든 행정부에서 러시아나 중국의 해커들이 부쩍 미국의 시스템을 공격하고 있음을 강조하며 강경한 어떤 대응 태세를 갖추게 됩니다. 2021년 7월, 바이든 대통령이 국가정보국(DNI)를 방문했을 당시 러시아를 상대로 미국에 대한 사이버공격을 지속한다면 실제 전쟁을 초래할 수 있음을 경고하며 강경한 태도를 보였습니다. 비슷한 시기에 미국은 아프가니스탄에서 철수하면서 미국 외교 정책의 기조에 두 가지를 중심으로 재편하겠다고 하였는데, 그중 하나가 중국이었으며, 다른 하나가 사이버전이었습니다. 이에 따라, 미국 정부는 사이버 안보 분야에 공세적인 성향의 전문가들을 기용하고 있으며 다양한 형태의 행정명령을 통해 경계태세를 강화하는 조치를 취하는 등 국내적인 차원을 넘어서, 국제적인 차원에서도 유럽 NATO나 EU 회의에서 이러한 문제점들을 지적함으로써, NATO로 하여금 중국의 사이버 활동을 비난하는 성명을 발표하게 합니다. 바이든 행정부가 강경한 태도를 취하는 이면에는 실제로 러시아를 배후로 추적할 수 있는 사이버 공격들이 굉장히 많이 진행된 것으로 알려져 있습니다. 2000년대 후반, 미 대선에 대한 방해 시도에서부터 2020년 미국의 최대 보안솔루션업체인 솔라윈즈 공격, 2021년 5월 미국 최대 송유관 업체인 콜로니얼 파이프라인에 대한 랜섬웨어 공격이 이루어졌습니다. 이외에도 다양한 종류의 생필품 관련 공급망에 대한 공격이 많이 있었습니다. 러시아뿐만 아니라 중국을 배후로 한 사이버 공격도 논란이 되었습니다. 미국 정부는 코로나 국면에서 코로나19 백신을 개발 중인 미국 연구소들을 노리는 해커들을 중국 정부가 지원하고 있다고 주장하며 미국에 있는 영사관 중 한 곳을 폐쇄하는 명령을 내렸습니다. 이외에도 마이크로소프트의 익스체인지 서버가 해킹 당하는 사건도 있었습니다.

북한도 한국뿐만 아니라 미국, 글로벌 시스템들을 향해서 공격을 가하고 있는 것으로 알려져 있습니다. 2009년부터 시작해 2010년대 초반까지 다양한 종류의 디도스 공격과 APT 공격이 있었습니다. 한국에 대한 가장 큰 공격으로 알려진 것은 2013년 3월에 있었던 방송사와 금융기관 사이버 공격입니다. 피해 규모도 컸지만 언론사를 공격했다는 점에서 언론에 많은 관심을 받았습니다. 한편, 2014년 소니 영화사에 대한 해킹 사건은 북한이 미국을 상대로 해서 해킹 공격을 함으로써 미국이 비례적 대응 즉, 강경한 대응을 유발한 사건으로 알려져 있습니다. 북한 김정은 위원장을 암살하는 내용을 다룬 '인터뷰' 영화를 제작한 소니 영화사를 해킹하여 상영을 방해하고자 했던 것입니다. 미국은 이에 대해 사이버 반달리즘(Cyber Vandalism)이라 규정하고 비례적인 대응 조치를 취할 것을 천명하였습니다. 알려져 있는 바로는 북한에 대해서도 통신망 교란, 금융 제재를 포함한 경제 제재 조치가 고려되었으며 일부 실현되었습니다. 민간 영화사에 대한 해킹 공격이 국제정치적인 사건으로 연계된 사례로 볼 수 있습니다. 이밖에 2016년 방글라데시 스프트스 중앙은행 시스템을 해킹 사건 등 일부 금융 시스템에 대한 공격들의 배후로 북한이 지목되고 있습니다. 2020년대를 넘어서는 시점에서도 북한은 여전히 전세계 금융기관들에 해킹을 하는 것으로 알려져 있습니다. 코로나 백신에 대한 해킹은 물론이며, 특히 2021년에 들어와서 한국의 국방시설과 국방연구시설들에 대한 해킹을 시도한 것으로 알려져 있습니다. 한국원자력연구원, 대우조선해양, 한국항공우주연구원 등의 연구기관에서 정보를 빼내기 위한 공격들이 진행되면서 국내 차원에서도 경각심을 불러일으킨 바 있습니다.

여기서 염두에 두어야 하는 것은 해킹 공격이 이루어지는 대상이 주로 공급망과 관련된 분야라는 것입니다. 미국과 중국이 벌이고 있는 경쟁의 과정에서도 공급망의 보완 이슈는 굉장히 중요하게 간주되어지고 있습니다. 특히 2010년대 후반으로 오면서 중국의 5G 이동통신 장비를 만드는 화웨이의 장비에 대한 사이버 안보 문제들이 제기되어지면서 수출입 규제가 이루어지는 등 미국과 중국의 갈등의 핵심적인 논제로 등장한 바 있습니다. 앞서 말씀드린 솔라빈스 보안 솔루션 업체에 대한 공격 등 소프트웨어 업체들에 대한 공격들 대부분이 전체 공급망 중에서도 그 공급망을 관장하는 소프트웨어 시스템에 대한 공격이었습니다. 최근에 주목 받는 경제 안보 즉, 공급망 안보의 문제와도 연결되는 대목입니다. 생필품 원자재부터 중간재, 완제품에 이르기까지 공급망을 이루는 시스템 자체를 사이버 공격의 대상으로 삼음으로써, 그것들이 야기하는 군사적인 피해뿐만 아니라 생활 속에서의 경제 피해를 야

기할 수도 있습니다. 특히 미국과 중국이 벌이고 있는 공급망 이슈와 사이버 암호에 대한 이슈들은 국제 정치의 전통적인 테마라고 할 수 있는 사이버 동맹과도 연결됩니다. 화웨이 사태가 벌어졌을 때 화웨이 장비에 대한 논란이 일자, 미국은 화웨이 수입을 통제하는 조치를 취했고 캐나다, 호주, 뉴질랜드, 영국 국가 등 전통적인 미국 우방국들에게 화웨이 제품 금지 압박을 가하는 상황들로 창출되었습니다. 최근에는 5G+ 전선이 확장되어지는 모습을 보이고 있습니다. 물론 그 안에서 대형 전선에 균열도 있었지만, 사이버 동맹이 전반적으로 유지되는 상태에서 중국과 대결하는 모습을 보입니다.

사이버 동맹은 트럼프 행정부에서부터 바이든 행정부로 이어져 내려오고 있는 미국의 인도 태평양 전략과 연동되면서 진영의 새로운 결속을 다지려고 하는 모습을 보이고 있습니다. 이에 대응하려는 중국은 소위 '일대일로'로 프레임 속에서 사이버 안보 또는 데이터 안보를 강조하며 맞붙고 있습니다. 이러한 갈등의 정점에서 트럼프 행정부의 말기인 2020년대에 미국이 '클린 네트워크'를 내세우고 이에 대응하여 중국이 '글로벌 데이터 이니셔티브'를 내세웠습니다. 이는 다시 넓은 의미에서 양자 외교 또는 다자 외교의 장에서 다양한 협상과 협의 또는 국제적인 차원에서 부당한 행위들을 제약하기 위한 규범 형성의 과정과 연결됩니다. 2015년 당시 오바마 대통령과 시진핑 중국 주석 간 일정 이상의 공격을 하지 않도록 하는 합의를 하며 새로운 돌파구를 마련하고자 했으나, 사이버 안보 특성상 두 정상이 나서서 더이상 공격하지 말자라고 약속한다고 공격이 없어지지 않습니다. 아직까지도 미국과 중국 간에는 서로의 공격과 방어의 문제가 쟁점으로 되고 있습니다. 그럼에도 불구하고 다양한 종류의 양자적인 외교 협의가 진행이 되고 있으며, 한국도 20여 개 국과 사이버 정책 협의들을 진행하는 과정을 통해서 이 문제를 풀어나가려고 하는 노력하고 있습니다. UN은 OEWG(Open Ended Working Group)를 통해 국제규범을 만들고자 시도했고, 지난 10여 년간 어느 정도의 성과가 있었지만 그 자체가 많은 과제가 되기도 했습니다. 국제기구에서 190개 정도 국가의 대표들이 나서서 합의해서 해결되는 종류의 문제가 아니라는 것이 이 분야에서 국제규범 형성을 어렵게 만듭니다. 더 중요한 것은 이러한 논의에 미국과 중국, 러시아 또는 서방 진영과 비서방 진영 또는 선진국과 개도국 간에 이해관계를 달리하는 대립의 요소들이 많이 있다는 것입니다. 기존의 국제법 또는 전쟁법을 사이버 안보 분야에서의 전쟁 행위에도 적용할 것인가에 대한 논의부터 인도주의적인 차원에서의 국제법을 적용할 수 있는 영역이냐에 대한 논의까지 다양한 시각 차이를 보이고 있습니다.

최근에 우크라이나 전쟁 때문에 더 많이 부각되고 있는 현상은 사이버 공간이라고 하는 것이 물리적인 공격을 가하는 행위이거나 또는 그 안에 있는 정보나 데이터 자산을 탈취하려는 행위에 그칠 수도 있지만 더 나아가서는 이에 관여되어 있는 행위자들의 심리적인 공간 또는 그 상대방에게 어떤 그릇되고 조작된 정보를 제공하거나 다른 어떤 인지적인 교환을 야기할 수도 있는 효과를 만들어내므로 인해서 자신들이 얻고자 하는 바를 얻으려고 하는 일종의 정보심리전 양상들이 사이버 공간을 중심으로 해서 벌어지고 있고 있으며, 우리가 알고 있는 사이버전의 영역들을 더욱 확장시키고 있습니다. 2016년 미국 대선 시기에 사이버 공간의 정보심리전이 쟁점화되었습니다. 힐러리 클린턴과 도널드 트럼프 대통령의 대선 과정에 러시아의 개입 여부가 쟁점이 되었습니다. 근거 없는 억측이라는 이야기도 있지만, 러시아의 개입이 대선 결과를 바꿨다는 공방도 있었습니다. 소셜 미디어를 활용해서 만들어지는 다양한 정보의 유포, 일종의 가짜 뉴스의 유포가 만연해지면서, 단순히 사회·정치적인 갈등 문제를 넘어서 전쟁 행위에 준하는 형태로 제기되고 있습니다. 어떻게 보면서 초국적인 차원에서 온라인 공론장은 참여 민주주의와 직접 민주주의의 이상을 실현할 수도 있는 공간으로서의 역할을 기대하였는데, 사실상 그 공간이 그릇된 정보를 유포하고 이를 무기화시키는 전쟁의 공간이 되어가는 현상이 전개되고 있습니다.

정보 우위를 달성하여 상대방을 제압하는 정보전이 이제 심리와 연결되어 활용되고 있습니다. 4차 산업혁명 시대에 다양한 기술과 데이터 환경을 배경으로, 상대방의 인식 체계에 영향을 미치는 커뮤니케이션 전쟁 성격을 갖기 시작했습니다. 이와 같은 정보심리전의 개념 변환은 세 가지 차원에서 주목해 볼 필요가 있습니다. 첫 번째, 전쟁을 수행하는 수단 차원에서 SNS와 같은 디지털 미디어가 굉장히 중요한 의미를 갖게 되었다는 것입니다. 인터넷 세상이 우리가 편의에 의해서 만들어 놓은 공간인데 나를 공격하는 환경의 도구가 되고 말았습니다. 두 번째, 전쟁 수행의 주체 차원에서 전통적인 정보심리전은 국가적인 차원에서 이루어지는 군사전쟁의 양상이었다면 최근에는 컴퓨터 환경을 제어하고 있는 민간 빅테크 기업 또는 소극적 차원에서의 해커들, 일반 시민들이 중

요한 역할을 하고 있다는 점입니다. 과거에는 민간 행위자들은 전쟁의 대상이자 객체였는데 새로 등장하고 있는 정보심리전에서는 전쟁의 주체로서 부상하고 있는 것입니다. 세 번째, 전쟁 수행의 목표 차원에서, 정보심리전에서는 전쟁 자체가 목표일 수도 있다는 것입니다. 물리적인 공간에서 전쟁은 상대의 하드웨어를 제압하여 목숨을 탈취하는 행위가 전쟁의 목표였다면, 최근에는 상대방에게 설득력 있고 감동적인 네러티브를 전파하여 상대방의 마음과 동의를 얻거나 잘못된 상황을 전달함으로써 원하는 바를 이루는 고도의 행위가 또 하나의 전쟁의 목표로서 등장하고 있습니다. 전쟁이 이루어지는 공간은 사이버뿐만 아니라 우주까지 확장되었는데, 정보심리전의 중요성을 강조하시는 분들은 전쟁의 공간을 우리의 인지 공간 즉, 뇌 공간까지 포함합니다. 우리의 인지 공간이 중요한 전쟁 공간이 됨으로써, 정보를 생산하고 취합해서 단순히 전달해서 효과를 보기보다는 상대의 인지 체계를 교란하고 조작하는 구체적인 목적을 갖습니다. 즉, 전달하는 메시지가 중요한 게 아니라 그 메시지를 소비하는 메신저의 인지 체계를 타격하는 것입니다. 따라서, 메신저들이 가지고 있는 급소 핵심을 알아내어 새로운 시스템 환경을 만들어내는 것이 전쟁에 중요한 승리 요소가 될 수 있습니다. 핵심은 스토리를 만들어내고 문제를 보는 프레임을 조작하고 짜는 능력이 중요한 네러티브 전쟁 혹은 프레임 전쟁이 대두되고 있다는 것입니다. 새로운 전쟁의 양상으로 부상하고 있는 만큼 우리도 조금 더 적극적인 대응이 필요하리라 생각합니다.

국가적인 차원에서 이루어지는 정보 활동 분야에서도 디지털 시스템을 활용한 활동들 또는 그런 과정에서 사이버 안보가 갖는 의미가 재조명되어지고 있습니다. 과거 아날로그 시대에 첩보 활동의 핵심은 소위 Small Data 세상에 숨겨져 있는 정보를 취득해서 분석하는 것이었다면, 디지털 세상에서는 개방적으로 널려 있는 정보 일종의 빅데이터를 가져와 분석하는 것입니다. 이러한 변화들은 최근 우크라이나 전쟁을 통해서 우리에게 하나씩 모습을 선보이고 있습니다. 우크라이나 전쟁은 전통적인 전쟁 양상을 보이기도 하지만 여태까지는 없었던 새로운 전쟁의 양상들을 보이고 있어, 전쟁인 것 같지만 또 전쟁이 아닌 것 같은 요소들이 얽혀 있습니다. 전쟁이 이루어지는 수단이나 그 목적, 수행의 주체라는 차원에서 복합성을 보여주는 사례로서 우크라이나 전쟁을 거론해 볼 수 있을 것 같습니다. 최근 전쟁과 관련된 또다른 쟁점은 사이버전쟁이 별도의 독자적인 전쟁으로 수행되어질 것인지 아니면 Multi Domain Operation이 되어 여러 공간에서 발생하는 복합적인 양상이 될 것이냐는 것입니다. 점차적으로 후자 쪽으로 의견이 기울고 있는 것 같은데, 전쟁 전후, 전쟁 중에 연동되어서 발생하는 사이버 공간에서 공격이 주목받고 있습니다. 아마도 미래에 사이버 공간에서의 전쟁 수행을 어떻게 하느냐가 전쟁의 승패를 장악하는 핵심이 될 가능성이 높습니다. 최근에 AI를 장착한 무인무기가 등장하며 유인 시스템과 무인 시스템이 복합된 전투체계에 대한 논의가 있는데, 문제는 만약 인간이 자율 전투로 프로그램해놓은 무기가 해킹 공격을 받아 아군을 향해 겨누게 될 수 있기 때문에 위험이 증폭될 것이라는 것입니다. 또한 자율무기체계는 해킹에 대한 취약점뿐만 아니라 버그, 소프트웨어 결함 등 기계적인 결함에 취약할 수 있습니다. 소프트웨어 크기와 규모가 커지고 기술의 복합도도 늘어나면서 악의적으로 침투하지 않아도 사고가 발생하거나 오작동 가능성이 있기 때문에, 이에 대한 대비가 필요할 것입니다. 또한, 딥페이크 처럼 스크린 조작을 활용하여 인간 자체가 가지고 있는 인지적인 취약점들을 겨냥한 사이버 공격도 넓은 의미에서 사이버전으로 간주되고 있습니다.

한편, 사이버전과 전자전의 결합되고 있습니다. 우리는 현재 다양한 종류의 정보통신 시스템을 활용하며 살고 있는데, 전쟁이 발생하면 그 유닛들 간의 작동이 복잡하고 중요해집니다. 전자기파 공격, 에너지 지향성 공격, 에너지 레이저 무기를 사용한다면 전자전이 되는 것인데, 이런 전자전의 요소들이 사이버전과 결합되는 양상이 되고 있습니다. '발사의 왼편(Left on Launch)'이 가장 대중적으로 알려진 용어로, 발사 이전 단계인(왼편) 발사준비에서 미사일 기지나 이동식 발사대를 무력화하는 것을 뜻합니다. 영국의 어느 일간지 보도에 따르면, 2010년대 초반 오바마 행정부 시절 북한이 미사일 발사 장소를 계속 옮겨가면서 발사했는데, 이러한 북한의 미사일 이동과 발사형태에 대한 고민이 미국이 가했던 전자 공격 또는 전자전과 연동된 사이버 공격 때문에 그랬다는 것입니다. 다음으로 이러한 복합적인 전쟁 양상은 우주전으로 이어집니다. 인공위성의 인공지능 시스템 자체가 해킹되어 궤도가 바뀌어 서로 충돌하게 할 수 있으며, 우주 파편이 부딪혀 인공위성 체계를 파괴하는 시나리오들도 논의가 되고 있습니다. 실제로 현재 위성 항법 시스템, GPS 교란이 문제가 되고 있습니다.

사이버전은 최근에 핵무기와 연결되고 있습니다. 이러한 맥락에서 최근에 사이버 안보 복합 넥서스, 사이버 안보가 전쟁과 관련된 다양한 부분들과 연결되는 경향으로 진화하였습니다. 냉전시대에 만들어진 핵무기 시스템이 아날로그 시스템을 바탕으로 한 부분적 전자 시스템이었다면 이제는 전체적으로 네트워크화된 시스템을 구축하고 있어, 해킹 공격이 가해질 경우 더 큰 위험을 초래할 수 있습니다. 한반도의 맥락에서도 북한의 핵 문제나 미사일 발사가 이루어지는 현실 속에서 사이버전과 관련된 양상들이 어떻게 연결될 수 있을 것이냐에 대한 논의들이 이루어지면서 그야말로 비대칭 전쟁의 맥락 속에서 핵과 사이버를 어떤 식으로 관장할 것인지가 주요한 쟁점이 되고 있습니다. 더 나아가서는 사이버 안보와 관련된 공격력의 역량이 오늘 내지는 내일 미래 국제 질서의 양상을 변화시킬 수 있을 것입니다. 어떻게 보면 냉전 시대에 만들어진 과거의 질서는 핵을 기반으로 강대국들이 중심이었지만, 오늘날은 사이버 안보 이슈가 핵과 연결되고 또 다른 다양한 이슈와 연계되며 우리가 알고 있던 국제 질서의 모습들을 변화시키게 되는 가능성이 커지면서 이를 규제하는 새로운 규범의 필요성이 제기되고 있습니다. 19세기 후반에 핵 규범에 대한 논의가 주요 쟁점이었다면 앞으로는 핵과 연결되어진 또는 다른 이슈와 연결되는 사이버 규범이 주요한 쟁점이 되리라 짐작하며, 결론적으로 복합지정학적인 시각에서 본 국제정치학적인 쟁점들이 현재의 현실이지 않을까라는 생각을 하게 됩니다.

필자 소개 김 상 배 (서울대 정치외교학부 교수)

학력
인디애나대학교 정치학 박사
서울대학교 외교학과 석사
서울대학교 외교학과 학사

경력
서울대학교 정치외교학부 교수
서울대학교 국제문제연구소 소장
한국국제정치학회 회장(2022년도)

저서
『미중 디지털 패권경쟁: 기술-안보-권력의 복합지정학』(한울, 2022)
『버추얼 창과 그물망 방패: 사이버 안보의 세계정치와 한국』(한울, 2018)
『아라크네의 국제정치학: 네트워크 세계정치이론의 도전』(한울, 2014)
『정보혁명과 권력변환: 네트워크 정치학의 시각』(한울, 2010)
『정보화시대의 표준경쟁: 윈텔리즘과 일본의 컴퓨터산업』(한울, 2007) 외 다수