

ISSUE BRIEF

2017 - 062

여시재 - 협력연구기관 공동 기획: 각국의 싱크탱크 동향

각국의 신안보이슈 - 미국

‘새로운 전쟁’과 미국의 대응:

기술 우위 속에서 규범 확립 고심

2017. 12. 06

나지원(동아시아 연구원)



전쟁과 군사는 어느 시대에도 기술 발전의 촉매이자 경연장이 되었다. 하지만 그 때문에 이전 시대에 발전된 전술과 교리는 다음 전쟁에서 대개 무익하거나 심지어 역효과를 내기도 했다. 때문에 강력한 군대를 육성하기 위해서는 첨단기술을 반영한 장비를 빠르게 도입하는 것만큼이나 그것을 효과적으로 배치하고 활용하는 무형의 기술, 즉 훈련, 전술, 작전 등을 갱신하는 것도 필수적인 과제가 된다. 의심의 여지없이 현존하는 세계 최강의 군사력을 자랑하는 미군 또한 이런 고민에서 예외가 아니다. 오히려 어느 나라보다 거대한 군 조직이 급변하는 전투 환경과 전쟁 양상에 기민하게 대응하지 못하는 상황에 대한 염려의 목소리도 들린다.

지난 2016년 데이비드 페트레이어스(David Petraeus) 육군 대장과 군사안보 전문가 마이클 오핸런 교수가 미국의 향후 국가 과제를 논의하는 브루킹스의 “Big Ideas for America” 시리즈의 일환으로 집필한 국방 관련 보고서에서는 첨단기술 발전, 특히 사이버공간, 우주, 대량살상무기 관련 기술을 미군의 약점을 키우는 위협으로 지목하고 있다. 같은 맥락에서 미국의 외교안보 싱크탱크와 전문가들이 주목하는 ‘새로운 전쟁’의 두 축은 바로 자동화(무인화)와 사이버 전쟁이다. 전자가 기존 전쟁의 양상 변화를 의미한다면 후자는 완전히 새로운 시공에서 펼쳐지는 전쟁을 대표한다고 할 수 있을 것이다.

보이지 않는 위협: 사이버 안보 전략

우선 이른바 사이버 안보(cybersecurity)에 대해서는 이미 2010년대 초반부터 행정부 차원에서 대응책이 논의되었으며 지난 2015년 1월 백악관이 공공기관과 민간기관이 사이버안보 관련 정보를 공유할 수 있도록 허용하는 법안을 제출했다. 국가가 사이버공간에 대한 통제력을 강화하고 민관군이 국방을 위해 공조하는 체제를 사이버공간에도 적용하겠다는 것이다. 안보에서 물리적 대비만큼이나 심리적 안정 또한 중요하다. 이러한 조치의 의의를 찾을 수 있다. 손에 잡히지 않고 눈에도 잘 띄지 않는 이러한 새로운 전장에서 어떤 ‘전쟁’이 벌어지고 있는지 가늠하기 쉽지 않은 대중들은 오히려 사이버 위협(cyberthreat)의 파괴력에 막연한 두려움을 품고 있기 때문이다. 실제로 브루킹스 연구소의 2015년 조사에 따르면 미국 대중들이 느끼는 최대 공포 요인 중 3개가 기술 관련 공포였으며 특히 사이버테러리즘이 2위를 차지했다는 점은 그 방증이다. 특히 사이버 공간의 비정형성, 비가시성은 사이버테러리즘, 사이버범죄, 사이버전쟁의 명확한 구분을 어렵게 만들기 때문에 자연스럽게 무법지대의 양상을 보이게 된다는 점에서 문제는 더 복잡해진다.

패권국의 역할이자 권리가 세계 질서와 규범을 주도하고 상당 부분 좌우한다는 점에서 이러한 사이버 위협의 확대는 미국에게 실질적인 안보위협이다. 무엇보다도 (잠



재적) 경쟁국들의 사이버전 역량이 나날이 강해지고 있다는 점은 이러한 위협을 가중시키고 있다. 미국 국방과학위원회(Defense Science Board, DSB)의 사이버 억지 태스크포스(Cyber Deterrence Task Force)가 지난 6월 발표한 보고서 또한 타국의 사이버 (공격)능력이 미국의 사이버 방어 능력을 추월하고 있다는 점을 핵심 결론으로 제시하면서 총체적인 사이버 전략의 필요성을 역설했다. 특히 미군은 이미 다수의 무기과 장비가 전자, 통신 기기를 통해 서로 연결된 ‘사물인터넷(Internet of things)’이 되었기 때문에 향후 사이버공격은 미군에 대한 물리적인 타격을 줄 수도 있다고 경고하고 있다.

이러한 위협에 대해 보고서는 세 가지 대책을 제시하고 있다. 첫째로 핵무기 타격 체계와 재래식 장거리 무기 체계의 원상복구 능력에 우선적으로 투자하고, 둘째로 핵심 기간시설에 대한 침투 저지능력 강화로 테러 단체 및 (북한, 이란 등) 소국의 사이버 공격 위협을 낮추며, 마지막으로 중대한 사이버 공격에 대한 대응 매뉴얼(playbook)을 개발해야 한다는 것이다. 미국-유럽 관련 외교안보 전문 싱크탱크인 대서양 평의회(Atlantic Council) 또한 향후 사이버 공격 예방에 관한 제언을 통해 사이버 역량이 큰 주요 국가들이 가칭 국제사이버안정위원회(International Cyber Stability Board)를 구성할 것을 제안하고 있다. 이 보고서는 창립 회원국으로는 미국을 필두로 캐나다, 프랑스, 독일, 영국, 한국, 일본, 호주를 제시하면서, 위원회가 인터넷의 중추를 구성하는 핵심기간시설을 보호하고 인터넷의 취약점을 보호하는 기준을 수립하며 사이버 첩보, 정치공작, 범죄활동에 대한 국제적 대응 공조를 주도하는 역할을 담당할 것을 주문한다.

하지만 이러한 시도와 노력이 필요한 것과는 별개로 고려해야 할 현실적, 이론적 제약이 있다. 현실에서 잠재적 공격을 예방하기 위해 만들어진 억지 이론(deterrence theory)을 사이버 공간에서는 적용하기 어렵다는 점이다. 억지가 성립하기 위해서는 억지할 대상과 그 대상을 억지함으로써 보호받는 영역이 분명해야 하는데 경계와 형태가 불분명하고 규범조차 정립되지 않은 사이버 공간에서는 누구를 대상으로 억지를 실시해야 할지도 명확하지 않으며 그들이 어느 선에서 억지해야할지, 즉 어디까지는 공격당해도 괜찮고 어디부터 용납할 수 없는지에 대해 억지당하는 측(잠재적 공격자)이나 억지하는 측(잠재적 방어자)이 파악하기 어렵다는 점이 가장 큰 문제다.

사이버 공간에서 일어나는 어떤 행위에 대해 어느 수준까지 제재나 징벌을 가해야 하는가에 대해 합의한다고 해도 여전히 해결해야 할 문제가 있다. 이러한 집행(enforcement)의 비용을 누가, 얼마나 부담할 것이냐 하는 질문이다. 결국 이 부분에서는 미국이 주도적인 역할을 하고 우선적으로 비용과 수고를 부담해야 할 공산이 크다. 현실적으로도 미국이 그러한 집행의 가장 큰 수혜자가 될 것이며, 규범적으로도 국제질서 유지와 보호에 앞장설 것을 요청받는 국가이기 때문이다.



하버드 대학 케네디 스쿨 벨퍼 과학 국제문제센터(Belfer Center for Science and International Affairs)에서 사이버안보 프로젝트를 담당하고 있는 마이클 설메이어(Michael Sulmeyer) 소장은 이를 위해 세 가지 조치가 필요하다고 조언한다. 첫째, 동맹국들과 보다 명확한 공동대응책을 마련하고 시민들에게도 상세한 정보를 제공하는 소통이 필요하다. 둘째, 의회(정부)와 민간 부문이 협력해야 한다. 셋째, 사이버공격은 전통적 테러리즘만큼이나 예측불허이며 맞서 싸우기 어렵다는 점을 인정해야 한다.

세 가지 대응에 모두 유효할 수 있는 분야는 다름 아닌 국제법이다. 국제적 합의에 따른 공조를 가능하게 하고, 성문화된 규범을 통해 보다 분명한 경계선을 확립할 수 있으며 이러한 과정을 대중에게 알림으로써 인식을 제고할 수 있기 때문이다. 지난 3월 미국의 대표적 외교안보 싱크탱크인 외교평의회(Council on Foreign Relations, CFR)의 매튜 왁스먼(Matthew Waxman) 법률외교 선임연구원이 상원 국방위원회(Armed Services Committee) 청문회에 출석해 발언한 내용 또한 이러한 맥락이다. 그는 “여러 국제법적 문제들은 특정한 사례별 판례에 의존하고 있어 앞으로도 논란이 될 가능성이 크므로 미국이 다른 국가들의 행동을 효과적으로 통제하고 전략적 이익을 수호하려면 법 해석을 지속적으로 제시해야 한다.”고 조언했다.

그러나 트럼프 행정부는 이러한 사이버 안보 대전략 수립의 필요성과는 역행하는 움직임을 보이고 있다. 지난 7월 렉스 틸러슨 국무장관은 국무부의 사이버 문제 조정관실(Coordinator for Cyber Issues)을 폐쇄하고 담당 업무를 경제기업국(Bureau of Economic and Business Affairs)로 이관하기로 결정했다. 또한 이 소식이 나온 직후, 조정관 크리스토퍼 페인터(Christopher Painter)가 사직서를 제출하면서 사실상 부서가 해체되어버렸다. CFR의 사이버안보 선임연구원인 데이비드 피들러(David P. Fidler)는 트럼프 행정부가 사이버 문제의 중요성을 낮춰보고 있는 증거라고 평가하면서 이러한 조치를 강하게 비판했고, 브루킹스 연구소의 캐머런 케리(Cameron F. Kerry) 선임연구원 역시 오바마 행정부가 2011년 발표한 국제 사이버공간 전략(International Strategy for Cyberspace)를 바탕으로 구축하고자 했던 통합적이고 유기적인 사이버 전략을 무위로 돌릴 위험이 있다고 경고했다.

무인 전쟁: 축복인가, 재앙인가

사이버 안보가 전혀 새로운 전장(battlefield)을 창출했다면 이른바 전쟁의 자동화(automation)는 기존의 물리적 싸움터에서 전쟁이 수행되는 방식을 뒤바꾸고 있다.



드론(drone), 보다 정확히는 무인비행체(unmanned aerial vehicle, UAV)로 대표되는 무인, 원격 무기들은 공격자의 인명피해는 최소화하면서도 살상력과 파괴력은 극대화함으로써 첨단 무기를 보유한 공격자에게 압도적인 전력 우위를 가져다준다는 이점이 있다. 또한 지극히 낙관적으로 해석하면 무인무기가 보편화된 시대에는 군인의 목숨을 담보로 나라를 지킬 필요가 없어지고 경제적 측면에서도 기존 병력을 보다 생산적인 일에 투입할 수 있다는 장점이 있다. 특히 미국이 이라크와 아프가니스탄에서 벌인 군사작전을 통해 드론의 성능과 위력을 지켜본 세계 각국들이 그 이후로 군사용 무인기 도입과 개발에 박차를 가하고 있는 것은 주지의 사실이다.

그러나 전쟁의 자동화, 무인화는 이러한 잠재적 이점을 상쇄하고도 남을 만큼 크고 다양한 정치적, 법적, 도덕적 난제를 제기한다. 우선적으로 가장 많이 활용되고, 널리 알려진 무인공격기 ‘드론’의 법적 지위부터 논쟁거리다. 지난 2015년 미국 연방항공국(FAA)은 소형무인항공체계(UAS)가 항공기(aircraft)의 범주에 포함된다고 처음으로 언급했다. 그러나 이처럼 지나치게 포괄적인 해석은 무인항공기의 잠재적 효과와 이득을 심각하게 침해할 수 있다고 헤리티지 재단(Heritage Foundation)의 법률 전문가인 제이슨 스니드(Jason Snead)와 존-마이클 세이블러(John-Michael Seibler) 수석연구원은 지적한다.

무엇보다 무인항공체와 기존의 항공기는 기술, 운용방식, 용도 등 모든 면에서 차이점이 너무 많기 때문이다. 뒷마당에서 취미로 날리는 드론에까지 기존 항공 법규를 적용하는 식이라면 과범죄화(over-criminalization)이 생겨 시민의 자유와 기본권을 침해하는 부작용이 나타날 수 있다고 이들은 경고하고 있다. 또한 무인항공체에도 크기와 용도, 작동방식에 따라 수많은 차이가 있으므로 이러한 편차를 무시한 채 일괄적으로 ‘항공기’로 규정하고 법을 적용하는 데에도 자연히 무리가 따를 수밖에 없다. 따라서 드론 사용자와 업계, 대중, 정부가 우선적으로 무인기와 항공기는 다르다는 점을 인식해야 하고 의회 또한 “항공기”에 대한 법적 정의를 수정, 보완함으로써 무인항공체에 대한 불필요하고 과도한 규제를 막아야 한다고 조언하고 있다.

이처럼 무인기는 국내법상으로도 이미 상당한 논쟁을 초래하고 있지만 잠재적으로 더 심각한 논란의 소지가 있는 분야는 국제법, 특히 전쟁 관련 법규다. 물론 미국 내에서는 미국이 군사용 무인항공체 기술과 활용에서 압도적인 우위를 점하고 있는 현재 상황에서 굳이 법을 통해 제약을 가할 필요가 있느냐는 지적도 있다. 그러나 중국, 러시아, 이란과 같은 잠재적 군사 경쟁 상대는 말할 것도 없고 한국, 대만 등 동맹 세력까지 빠르게 군사용 무인기 개발과 배치를 추진하고 있는 상황에서 법령 마련을 미루다보면 오히려 미국의 국익에 큰 손해가 될 것이라고 CFR 수석연구원 미카 젠코(Micah Zenko)와 새라 크렙스(Sarah Kreps)는 경고한다. 특히 빈번한 무력 사태, 인권 침해 등의 우려가 있다는 것이다.



이들이 보고서에서 구체적으로 제시하고 있는 무인기 확산의 위험성은 세 가지로 요약할 수 있다. 우선 국제적으로만이 아니라 국내적으로도 무력 남용의 가능성이 높아진다는 점이다. 무인무기가 보편화되면 굳이 병력을 투입하지 않아도 은밀하고 비공식적인 ‘첩보 작전’의 형식으로 전쟁을 벌일 수 있게 되면서 국제정치가 대화와 협상보다는 무력 수단을 선호하는 양상으로 전개될 수 있다는 것은 쉽게 상상할 수 있다. 이는 통상적으로 인명 피해에 민감하기 때문에 전쟁을 자제하는 것으로 알려진 민주국가들의 경우에 문제가 된다. 하지만 이들은 여기에서 그치지 않고 국내적으로 정부나 테러 조직 등 무력 집단 또한 무인 무기를 활용하면 보다 손쉽게 적대적인 개인이나 대상을 제거, 파괴할 수 있다는 점에서 국내 안보에도 심각한 도전이 야기될 수 있다는 점에 주목한다. 이 문제는 특히 민주 국가보다는 권위주의 또는 독재 정권에서 부각될 수 있다. 국가가 이런 무기를 동원해 반정부, 반체제 인사들을 보이지 않는 방식으로 억압할 수 있게 되기 때문이다.

두 번째 문제는 오인식(misperception)과 갈등 고조(escalation)의 가능성 증가이다. 예를 들어, 한 국가가 자국 영공에 침입한 타국의 무인기를 격추시킨다면 이를 전쟁 행위(act of war)로 봐야하는지에 대한 질문에 명확한 답을 하기 어려워진다는 것이다. 무인무기와 관련하여 국가 간 합의와 공통 규범이 없는 상태에서는 사소한 도발이 오해를 부르고 대대적인 충돌로 이어질 위험이 커지는 것은 자명한 사실이다. 이는 병력 투입의 감소로 결정권자의 책임성이 낮아진다는 첫 번째 문제와 상호작용하면서 위험을 더욱 증폭시킨다.

마지막으로 이들은 대규모 살상의 위험이 증가할 수 있다고 지적한다. 이는 일견 앞서 병력 투입의 필요성이 줄어든다는 주장과는 배치되는 것처럼 보인다. 그러나 무인공격기가 확산되면 핵무기와 마찬가지로 적의 군사기지뿐만 아니라 도시, 기간시설 등 민간인이 집중된 지역에 대한 공격이 벌어질 가능성이 커지기 때문에 민간인 피해가 증가할 수 있다는 점을 간과해서는 안 된다고 이들은 지적한다. 따라서 이러한 문제들을 방지하기 위해서는 무인공격기 사용에 대한 군사교리와 함께 국제법적 지침을 마련할 필요가 있다고 결론짓고 있다.

물론 군사용 무인기를 규제할 수 있는 기존의 국제규범이 없는 것은 아니다. 1987년 체결된 미사일 기술 통제 레짐(Missile Technology Control Regime, MTCR)의 1항목(Category 1)은 적재하중과 비행거리에 따라 무인기를 구분하고 있다. 문제는 이 규범에 구속력이 없을 뿐만 아니라 군사용 무인기를 보유하고 있는 국가 중 상당수(이란, 이스라엘, 중국, 인도, 파키스탄 등)가 서명하지 않았다는 점이다. 게다가 규범 자체가 제시하고 있는 분류법 또한 자의적이고 현실에 맞지 않는다는 비판도 제기된다.



그럼에도 미국 군 당국자들과 안보 관계자들이 이에 대한 시정이나 새로운 규정 수립에 미온적인 반응을 보이는 것은 앞서 말한 대로 미국이 여전히 이 분야에서 독보적인 우위를 누리고 있기 때문만은 아니다. 핵무기와 마찬가지로 비확산(non-proliferation) 레짐이 초래하는 딜레마가 있기 때문이다. 즉, 기존 합의가 아무리 불완전하고 비효율적이라고 하더라도 이를 개정하려고 하는 과정에서 오히려 비확산의 틀 자체가 깨지는 최악의 결과가 나올 수 있다는 위험 때문에 설불리 손을 대지 못하고 있는 것이다.