issue BRIEF

하이브리드 전쟁의 위협과 대응

2019-28

박지영 선임연구위원

김선경 연구원

아산정책연구원

2019.12.05

하이브리드 전쟁은 기존의 재래식 무기와 더불어 모든 다양한 요소를 활용하여 상대를 공격하는 수단으로 이용하는 전쟁 형태이다. 하이브리드 위협에 대한 경각심은 2014 년 러시아의 크림반도 합병, 돈바스 전쟁 등에서 강화되었다. 유럽국가들을 중심으로 하이브리드 위협과 향후 펼쳐질 가능성이 있는 전쟁 형태 등에 대한 연구와 논의가 지속되고 있다. 현대 사회에 가해지는 위협은 국가 대 국가의 정규전보다 다양한 위협 주체와 대상으로 세분화되었다. 세분화된 주체와 대상으로 인해 어떤 위협은 국제법의 영역에 속하지 않기도 한다. 따라서 새로운 위협을 식별하고 대응하기 위한 전략을 세우는 것이 필요하며 우리사회에 대한 영향을 지속적으로 분석하는 것이 중요하다.

하이브리드 위협의 정체

하이브리드 위협이란 기술력, 정치력, 경제력, 군사력 등을 모두 망라한 형태라고 할 수 있다. 하이브리드 위협은 냉전 종식 이후 서방세계에 비해 상대적으로 자원이 빈약한 러시아가 중점적으로 활용할 것이라 예측되는 위협이었다. 정치공작, 경제침투, 정보탈취 및 교란 등을 이용하는 심리전과 사이버전의 비정규전과 함께 핵을 비롯한 정규전을 결합하는 것이

하이브리드전이다. 2013 년 러시아의 발레리 게라시모프는 하이브리드 전쟁을 "선전포고 없이 이뤄지는 정치·경제·정보·기타 비군사적 조치를 현지 주민의 항의 잠재력과 결합시킨 비대칭적 군사 행동"으로 정의했다. 이는 게라시모프 독트린으로 불리며 러시아의 하이브리드 전쟁을 수행하기 위한 군사전략 변화를 가져왔다. 러시아는 에스토니아, 조지아, 우크라이나 등지에서 사이버전과 분쟁개입 등을 통해 러시아에 유리한 상황으로 국면을 전환해 왔다. 경제적 영향력, 에너지 자원 등 가용한 자원을 결합하기도 했다.

하이브리드전은 비대칭전, 혹은 복합전쟁이라는 용어로 설명되기도 하는데 냉전시대 이후 미국이 독보적으로 우위에 선 군사력을 보유하게 됨으로써 부상하게 된 개념이다. 소련 붕괴 이후 러시아는 미국과 견줄만한 힘을 유지하지 못했고 이러한 비대칭적 상황에서 다른 전략요소가 필요하게 되었다. 이는 G2 로 급부상하며 미국과 신형 대국관계를 수립하고자 하는 중국에게도 매우 효과적이고 매력적인 대안이 되고 있다. 일본과의 센카쿠 영토분쟁에 따른 희토류 수출중단이나 관광제한, 필리핀, 베트남과의 남중국해 영토분쟁과 관광 제한, 우리나라 사드 배치에 따른 경제적 보복 등 중국은 적극적으로 비군사적 공격을 주변국에 감행하고 있다.

군사적 전면전이 드물게 행해지는 현대사회에서는 시간이 흐를수록 군사적 충돌보다는 비군사적, 비전통적 개념의 위협이나 전쟁의 중요도가 커지고 있다. 군사적 수단의 정규전과는 양상이 상이하지만 상호 상당한 피해를 야기시키는 다양한 공격이 일어나고 있다. 이러한 공격은 군사력이 본격적으로 동원되지 않았을 뿐 전쟁이라고 표현되고 있다. 하이브리드전의 공격목표는 군사력이나 권력집단이 아니다. 공격목표가 사회나 문화를 대상으로 하는 경우도 있어 사회적 가치와 규범이 대상이 되기도 한다. 이 결과로 사회적 혼란이나 분열이 조장될 수 있다. 특히 넘쳐나는 SNS 등 미디어를 이용한 고도의 심리전은 뚜렷하게 공격이라고 인지하지 못하는 가운데 심각한 타격을 받을 수 있는 위험요소이다. 비대칭적인 힘에 도전하는 도구로서의 하이브리드 위협은 효과적이다. 중동테러집단, 마약조직 등 집단이나 조직에 의해 생성되는 위협은 소재와 책임을 파악하기 쉽지 않고 행위자의 입장에서는 비용도 적고 명확한 주체 파악이 어려워 책임을 회피할 수 있으므로 좋은 수단이 된다. 위협의 수단도 점차 다양화되어 예측하기 어려워진다. 네트워크로 고도로

연결된 현대사회에서 시간과 장소에 구애받지 않고 위협을 감행할 수 있다는 점 때문에 하이브리드 위협에 대해서는 위기 이전에 대응능력을 구축하는 것이 중요하다.

하이브리드 위협의 종류

하이브리드전은 정치, 경제, 외교, 군사적인 수단을 모두 사용하며, 국가와 비국가 행위자를 모두 포함하는 복합적인 형태의 전쟁이다. 하이브리드 전쟁은 회색전(grey zone warfare)이라고도 불리는데 전쟁과 평화의 경계선을 모호하게 하기 때문이다. 하이브리드 위협의 종류를 사용하는 공격의 수단에 따라 아래와 같이 사이버전, 정보전, 경제로 구분하였다. 급속화되는 ICT 의 발전으로 하이브리드전에서의 사이버 활용 비중이 높아지고 있으며, 정교한 도구와 전략을 사용하는 정치적 레버리지로 부상하고 있다.

<표> 하이브리드 위협의 종류

하이브리드 구분	전략	예시
사이버전	사회불안 조장	• 러시아 우크라이나 전력망공격 • 북한의 디도스(DDos) 공격 (2009 년) • 언론·금융기관 전산망 마비 (2013 년) • 랜섬웨어 워너크라이 해킹 (2017 년)
	정치적 목적	• 북한의 소니픽쳐스사 및 영국의 지상파 방송국인 채널 4 (Channel 4)공격
	억제	• 미국의 이란 나탄즈(Natanz) 사이버 공격 • 북한에 대한 미국의 Left of launch(발사 직전 교란) 작전
정보전	정치적 개입	• 러시아의 2016 년 미국 대선 개입
	기업 기밀 탈취	• 중국의 미국 기업 해킹/ 정보 탈취
	비대칭전	• 북한의 한미 유사시 계획 등 국가기밀 해킹 (2016 년) • 테러 단체들의 조직원 모집, 프로파간다 전파
경제	외교적 압박	• 미중 무역 전쟁/ 미국의 화웨이 압박

- 중국의 사드(THAAD) 보복
- 일제강점기 강제징용자 대법원 판결에 대한 일본의 수출 규제

사이버전

사이버전은 컴퓨터 시스템에 대한 공격이라고 할 수 있다. 웜, 렌섬웨어, 말웨어와 같은 컴퓨터 바이러스 또는 해킹을 통해 시스템을 불능화 시키는 것이다. 가장 흔한 사이버전의 형태는 공공기관, 민간 시설과 주요 인프라 시설 공격을 통해 사회적 불안을 조성하는 것이다. 러시아는 우크라이나 크림 반도를 점령하기 전인 2015 년 12 월 크래시오버라이드(CrashOverride)라는 명칭의 악성코드를 이용하여 우크라이나 전력망을 공격하였다. 이로 인해 우크라이나 수도인 키예프 전력의 1/5 이 중단되었고, 키예프 주민 22 만 5000 명이 피해를 입었다. 사회적 불안을 조성함으로써 정치적으로 우크라이나를 압박하고 동시에 서방 세력에게는 경고의 메시지를 보냈다.

북한도 세계적인 사이버 강대국으로 부상하며 한국을 대상으로 수차례 사이버 공격을 시도하였다. 2009 년에는 디도스(DDos)라고 불리는 공격을 감행하여 한국과 미국의 주요 정부기관 등 총 35 개의 주요 웹사이트를 해킹하였다. 2013 년에는 한국의 언론과 금융기관을 해킹하여 KBS, MBC, YTN 등 주요 언론사가 피해를 보았고, 신한은행, 제주은행, 우리은행 등 금융기관 전산망이 일시적으로 마비되는 피해를 입었다. 2017 년에는 한국을 포함한 90 여개국의 컴퓨터를 워너크라이(Wannacry) 렌섬웨어에 감염시켜 전세계의 대기업, 국민건강 서비스, 병원, 정부기관 등의 인프라에 막대한 피해를 입히기도 했다. 이란의 사이버 군대(Iranian Cyber Army) 산하의 이슬람 혁명 수비군(Iran's Islamic Revolutionary Guards Corps)도 2013 년 뉴욕주 바우맨 댐 수위조절 컴퓨터 시스템을 해킹했다. 다행히 댐이 공사 중인 관계로 별다른 피해는 없었지만, 향후 댐, 발전소 등 국가 기간시설 제어 전산망을 상대로 해킹이 이루어질 경우 사회적인 혼란을 초래할 수 있다는 우려가 제기되었다.

한편 사이버 공격은 의사결정에 영향을 미치기 위한 정치적인 수단으로 활용되기도 한다. 2014 년 11 월 미국 소니픽쳐스는 북한 수뇌부를 제거하는 내용을 골자로 한 코미디 영화 인터뷰를 제작했다. 북한은 영화가 '최고존엄을 모독'한다는 이유로 강한 불만을 제기하며 소니픽쳐스사에게 경고를 보냈다. 소니픽쳐스사가 영화 상영을 그대로 진행하기로 결정하자 북한의 해킹 그룹은 미국 소니픽쳐스의 내부 네트워크 회로에 진입해 바이러스를 심고, 영화 출연자를 포함한 소니사 직원들의 급여 문건, '007 스펙터'의 각본 사본 등의 자료를 유출하여 공개했다. 결국 소니사는 영화 인터뷰를 제한적으로 상영하기로 결정을 내렸다. 당시 오바마 대통령은 소니사가 영화 상영을 중단할 경우 독재국가가 민주주의 국가의 표현의 자유를 제한할 수 있다고 비춰질 가능성에 대해 심각한 우려를 표명했다. 큰 피해는 없었지만, 사이버전이 민주주의를 위협할 수 있는 수단으로 사용될 수 있다는 점에서 심각한 우려가 제기되었다.

사이버전은 상대국의 군사력을 억제하기 위한 전략적인 예방차원에서도 사용되고 있다. 사이버전은 특성상 공격의 주체를 명확하게 밝히기 어렵고, 책임 규명이 어렵기 때문에 민감한 외교적/군사적 사안에 대한 하나의 대안으로 떠오르고 있다. 미국은 이란의 지속적인 우라늄 농축과 핵 개발을 저지하기 위해 2010 년 이란 나탄즈 핵 시설에 바이러스 코드를 심었다. 이로 인해 나탄즈 우라늄 농축 시설의 원심분리기가 오작동하여 20%가 가동이 중단되었다. 당시 나탄즈에서 근무하던 핵과학자들도 원심분리기가 갑자기 중단된 이유를 밝혀내지 못했고, 시설을 재가동하기까지 수개월이 걸렸다. 이후 뉴욕타임즈는 오바마 정부가 스턱스넷(stuxnet)이라는 악성코드를 이용하여 이란 나탄즈 핵시설을 중단시켰다고 보도하며, 이스라엘의 디모나 비밀 핵시설에서 미국과 이스라엘이 공동으로 원심분리기 작동을 중단시키는 실험을 한 것을 근거로 제시했다.[1] 북한도 2016 년 원인을 알 수 없는 이례적인 미사일 실패를 겪는다. 그 해 북한은 6 개월 간 총 8 번에 걸쳐 무수단 미사일 실험을 했는데, 그 중 7 번은 실패로 돌아갔다. 실패한 미사일은 발사 직후 불과 몇 초 만에 폭발하였다. 미국의 하와이나 괌을 타격하겠다는 북한의 계획에 차질이 생길 수 밖에 없었다. 이에 따라 미국 오바마 정부의 left of launch(발사 직전 교란)[2] 작전이 실패의 원인이라는 주장이 제기되기도 했다.

정보전

하이브리드전의 또 한가지 구성요소로는 정보전이 있다. 정보전은 과거에도 강대국들, 특히 러시아가 전통적으로 사용해왔던 전략이다. 최근 사이버 공간이 여론 선동과 조작의 수단으로 정보전에 활용되면서 더욱 정교해졌다. 특히 과학기술의 발전에 따라 정보 접근이 용이해졌고 개발 비용도 비교적 저렴하며, 불특정다수에게 접근이 가능하다는 점에서 효율적인 전략으로 자리잡고 있다.

국가 주도의 정보전을 가장 활발하게 사용하는 국가는 러시아다. 러시아는 우크라이나를 점령하기 위해 반군 세력들에 대한 가짜 뉴스를 배포하고, 음모론을 통해 사회적인 혼란을 조장하였다. 뿐만 아니라 우크라이나 내 러시아 소수 민족의 독립운동을 부추기는데도 정보전을 이용하였다. 2016 년 러시아는 다방면에서의 사이버/정보전을 통해 미국의 대선에 직간접적으로 개입하며 대선 결과에 영향을 줌으로서 민주주의 절차에 대한 불신을 심고, 민주주의의 근간을 흔들 수 있다는 것을 보여주었다. 로버트 뮬러 특검은 2016 년 러시아연방보안국(FSB) 및 러시아정보총국(GRU)을 배후로 둔 해커 Guccifer 2.0 가 연계그룹 민주당 전국위(Democratic National Committee)와 대선 유력 후보였던 힐러리 클린턴의 이메일을 해킹하여 탈취한 문건을 위키리크스(Wikileaks)에 유출했고, 위키리크스는 민주당 전당대회(Democratic National Convention)가 열리기 3 일전 20,000 건의 이메일과 다른 자료들을 사이트에 공개했다고 밝혔다.[3] 이 사건으로 인해 유력한 대선 후보였던 힐러리 클린턴은 큰 타격을 입었고, 트럼프가 대통령에 당선되는데 유리하게 작용하였다.

러시아는 또한 쇼셜미디어 플랫폼에 가짜뉴스를 배포하여 트럼프 후보에게 유리한 방향으로 여론을 조장했다. 미 상원 사법위원회에 제출한 증언에서 페이스북 관계자는 러시아가 2015-2017 년 사이 120 개의 페이지에 80,000 건의 게시물을 게재했고, 대선 기간 동안 미국인 1 억 2,600 만명에게 직간접적인 영향을 미쳤다고 진술했다.[4] 러시아 정부 연계 단체는 사회/정치 분열 메시지를 내포한 3,000 건 이상의 광고물을 페이스북에 게재했으며 페이스북 사용자 1,000 만명 이상이 그 광고를 접한 것으로 나타났다. 구글도 러시아와 연관성이 의심되는 4,700 달러 규모의 광고물들과 18 개의 유튜브 채널을 발견했고, 트위터

역시 러시아 정보원과 연계된 2,752 개의 계정을 발견했다고 밝혔다. 미국 정계에서는 이 사건을 미국 사회의 혼란과 분열을 초래함으로서 표현의 자유와 민주주의 체제의 존립을 위협할 수 있는 중대한 사안으로 보았다.

급격한 경제 발전을 이룬 중국은 미국의 기술혁신 속도를 따라잡기 위해 정보전을 펼쳐왔다. 기술 의존도가 높은 미국의 약점을 이용하여 중국의 부족한 기술력과 군사력을 지원하는 도구로 사용하였다. 특히 관련 기술을 보유한 미국의 기업들을 해킹하여 군사, 기술 관련 데이터를 포함한 기업 기밀을 탈취하는 방법으로 중국 기업들의 기술 발전을 도모하였다. 2009 년 중국은 로히드 마틴사에서 탈취한 F-35 합동타격전투기(Joint Strike Fighter)의 제작과 관련된 데이터를 토대로 2012 년 F-35 와 비슷한 J-31 을 자체적으로 제작했으며,[5] 2014 년에는 보잉사의 C-17 군용수송기를 포함한 미국의 방산업체의 기밀을 탈취한 혐의로 중국인이 기소되기도 했다.

북한, 이란과 같이 경제력이나 군사력이 상대적으로 약한 국가들도 비대칭전의 수단으로 정보전을 활용하고 있다. 북한은 2016 년 한국 국방부 통합 데이터 센터에서 김정은 참수작전을 담은 미국의 작전계획 5015 (OPLAN 5015)를 포함한 182 GB 의 정보를 빼돌렸는데, 이중에는 한미 동맹과 한국군의 군사 계획도 포함되어 있었다. 북한의 입장에서는 한미의 주요 군사 작전을 미리 파악하고 대비할 수 있는 중요한 정보를 얻은 셈이다.

국가뿐 아니라 비국가 행위자들(non-state actors)도 사이버 공간을 적극 활용한 정보전에 나서고 있다. 테러 단체들은 세력을 확장해나가기 위해 정보전을 이용한 정교한 전술을 구사하였다. 알카에다는 온라인과 소셜 미디어를 통해 프로파간다를 전파하였고, 탈레반도 알레마라(Al-Emarah)라는 텔레그램 채널을 만들어 운영한 바 있다. 알카에다의 분파이자 이슬람 극단주의 무장조직인 ISIS 는 소셜미디어를 통해 110 국에서 40,000 명이 넘는 외국인 조직원들을 모집했다.[6] ISIS 는 대원을 모집하거나 프로파간다를 전파할 때 페이스북, 트위터, 유튜브와 같은 소셜미디어 플랫폼을 활용하면서 빠른 속도로 영향력을 확장해 나갔다. 다양한 소셜미디어 채널을 통해 전세계적으로 외로운 늑대(lone wolf)와 같은 사회적

소외계층들을 유인했고, 개인정보보호 문제로 활동이 자유로운 사이버 공간을 악용하여 세계 각지에서 테러 공격을 모의하기 위한 플랫폼으로 활용하였다. 또한 자칭 이슬람국가 사이버군대(Islamic Cyber Army)로 불리는 해커들은 소셜미디어에서 수집한 정보들을 바탕으로 살인 명부를 작성하기도 했다. 표현의 자유와 민주주의 확산에 긍정적인 영향을 미칠 것이라는 예상과는 달리 소셜미디어는 테러 단체들에 의해 악용되면서 사이버 공간에서의 안보 문제가 제기되었다.

경제

냉전 이후 미국은 자유주의 국제 질서를 확립하고 이를 유지하기 위해 앞장섰으나, 트럼프 행정부 출범 이후 미국과 중국을 중심으로 정치전이 강화되고 있는 양상이다. 트럼프 행정부는 미국 우선주의와 공평한 무역을 앞세워 자유주의 경제 체제를 외교적인 압박 카드로 활용하고 있다. 미국은 중국을 견제하고 압박하기 위해 중국에 대한 대대적인 수입 관세를 부과하였고, 안보 문제를 거론하며 화웨이에 대한 압박 공세를 이어가고 있다. 한국, 유럽, 일본을 포함한 동맹국들에게도 안보에 대한 대가로 각종 청구서를 요구하고 있다. 한국도 작년 방위비분담금을 8.2% 인상했고, FTA 도 재협상하였으며 다시 천문학적인 방위비분담금 인상을 요구 받고 있다.

중국은 2017 년 한국의 사드 배치에 대해 경제 보복 조치를 감행했다. 중국에서 반한 감정과 한국산 상품 불매 운동을 부추기고, 중국 관광객의 한국 방문을 중단시켰다. 특히 사드 부지를 제공한 롯데에 대해 중국에서 운영한 99 개 점포 가운데 87 개 점포에 영업 중지 조처를 내렸다.[7]

일본도 최근 일제강점기 강제징용자에 대한 한국 대법원의 판결에 대한 보복으로 반도체 소재 등 3 개 품목에 대한 수출 규제를 실시하면서, 정치적인 압력을 넣기 위한 수단으로 경제적인 의존성을 이용하는 경향이 미국을 중심으로 전세계적으로 확대되고 있는 추세다.

한국의 상황과 도전

한국은 주변국들의 하이브리드의 위협에 취약한 국가다. 세계 최고수준의 정보통신 기술과 인프라를 보유한 데에 비해 보안 수준은 낮아 사이버전과 정보전에 무방비로 노출되어있다. 특히 한국은 북한이라는 변수가 있기 때문에 사이버 공격의 위협은 더 클 수 밖에 없다. 북한은 2001 년부터 인민무력부를 설립하며 사이버, 정보전과 같은 비대칭전력/비정규적인 능력을 향상시키는데 심혈을 기울여왔고, 2000 년대부터는 한국의 민간·공공 주요기반시설, 국방, 그리고 국회 등을 대상으로 사이버 공격을 수십 차례 감행하였다.[8] 심지어 올해 남북정상회담 전과 싱가포르 북미정상회담 기간 중에도 스피어피싱 공격을 하는 등 북한의 사이버공격은 여전히 진행 중이지만 한국 정부는 북한에게 이 문제를 공식적으로 제기하지 않고 있다. 초연결 사회에 본격적으로 진입하면서 북한은 비군사적 접근방식으로 사이버전/정보전을 복합적으로 구사하는 하이브리드 전략을 사용할 가능성이 높다. 북한이 가짜뉴스를 퍼트려 한국 내 남남갈등을 조성하고, 북한에게 유리한 방향의 여론을 조성하는 등 간접적인 방법으로 한국의 정치적 상황에 개입할 가능성도 배제할 수 없다.

정부도 국가안보에 심각한 도전이 되고 있는 사이버 안보 위협의 중요성을 인지하고 체계적으로 대응하기 위해 컨트롤 타워 마련에 나섰다. 현재는 청와대 국가안보실이 국가 컨트롤 타워 역할을 수행하고 있다. 국가안보실 2 차장 산하에는 사이버 안보비서관과 정보융합비서관을 통합한 사이버정보비서관을 두고 있어 사이버 범죄 관련 대응 역량을 강화할 방침이다. 국방부 산하에는 사이버사령부가 있어 사이버 안보역량 강화와 사이버 공격의 단계별 다중 방어체계를 구축하는 역할을 담당하고 있다.[9] 그러나 아직까지 사이버 공간이 사이버사령부의 통합방위작전 관할 구역[10]에 포함되지 않았다는 점에서는 한계가 있다. 이 외에도 각 중앙행정기관 부문별로 보안관제센터를 운영하고 있고, 지역정보보호지원센터도 7 개에서 10 개로 확대할 예정이다.

국가안보실을 주축으로 정부는 올해 4 월 최초로 국가 사이버 안보 전략을 발표했다. 대한민국 최초로 국가차원에서 목표, 기본원칙, 전략 과제를 토대로 큰 틀에서의 국가 사이버 안보 전략 지침서를 내놓았다는 점에서는 의의가 있다. 그러나 추후 국가 사이버

기본 계획과 국가 사이버안보 시행계획을 통해 구체적인 안보 전략 계획과 이행 방안을 마련하겠다고 한 부분은 아쉬운 대목이다. 이와 함께 정부는 정보보호 관련 예산을 2022 년까지 8,485 억원을 투입하고, 정보보호 시장은 14 조원 규모로 확대[11]한다고 발표하는 등 사이버 대응 역량을 꾸준히 강화해나가고 있다.

사이버 안보 관련 법령으로는 대통령 훈령인 국가사이버안전관리 규정이 유일하며, 정보보호 법령으로는 정보통신망 이용 촉진 및 정보보호 등에 관한 법률, 정보통신기반보호법, 정보보호산업진흥법이 있다. 그러나 현존하는 법령은 국가 차원의 사이버 정책이 아닌 국가 정보통신망 침해 사고에 대한 관리 감독에 초점을 맞췄기 때문에 사실상 공공과 민간 부분을 모두 포함하는 사이버 테러 방지법은 없는 실정이다. 사이버위협에 대응하기 위한 입법 마련 논의는 19 대 국회 때 제기되었고, 2017 년에는 국가사이버안보에 관한 법률안이 발의되기도 했다. 그러나 국정원의 불법사찰에 대한 우려로 인해 논의 조차도 제대로 이루어지지 않고 있다. 미국, 일본, 유럽은 이미 국가사이버안보전략과 사이버안보법을 제정하여 자국의 국가 핵심정보자산을 보호하고 안전한 사이버 공간을 구축하기 위한 기반을 마련했다. 우리나라도 점점 커지는 사이버 위협에 효율적으로 대응하기 위해서는 구체적인 제도적·법적 근거 마련이 시급하다.

북한이라는 상수적인 위협 외에도 최근에는 주변국들(미국, 러시아, 중국, 일본)의 하이브리드적 위협에 대한 취약성이 증대되고 있다. 중국의 적극적인 대외 영향력 확대 의지, 전세계적으로 번지고 있는 국수주의와 미·중간 패권 경쟁이 심화되면서 한국에게 새로운 위협으로 다가오고 있다. 특히 한국은 지정학적으로 강대국들 사이에 위치해 있어 강대국들의 하이브리드전에 말려들기에 최적화된 나라다.

이같은 하이브리드 위협은 2016 년 박근혜 정부가 미국 사드 배치를 결정하면서 수면 위로 떠올랐다. 중국은 한국의 사드 배치에 대한 보복으로 중국인의 한국 관광을 금지했고, 중국에 진출해있는 한국 기업들에 대한 규제를 강화하는 등 중국에 대한 경제적인 의존도가 높은 한국의 약점을 이용하여 안보 상황에 대한 압박을 가했다. 국제 자유무역주의 질서를 주도하던 미국도 트럼프 행정부 이후 자국의 이익을 얻기 위한 수단으로 미국의 경제적인

영향력을 하나의 외교적인 카드로 이용하고 있다. 트럼프 행정부는 미국이 제공하는 모든 안보 보장, 무역관계를 '공평'하게 재설정할 것을 요구하며 이에 대한 대가를 요구하고 있다. 한미 동맹의 의존도가 높은 한국에게는 매우 곤란한 상황이 아닐 수 없다. FTA 재협상뿐만 아니라 작년 방위비 분담금을 8.2% 인상한데 이어 올해에는 5 배 이상 증가한 액수를 요구하고 있어 난관이 예상된다.

올해 6 월 G20 회의 때 까지만 해도 자유무역과 다자주의를 지지하던 일본도 경제 압력을 정치적 외교적 문제에 대한 보복으로 한국 경제를 타격 하고 있다. 2016 년 한일 위안부 협정 파기부터 레이더, 최근 일제 강점기 강제징용자 대법원 판결에 이어 일본이 한국의 반도체에 핵심적인 3 품목에 대해 수출 규제를 발표하였다. 역사적인 문제로 인한 갈등은 새로운 일이 아니지만, 일본이 보복으로 경제 카드를 꺼내든 것은 이례적이다. 이에 대해 우리 정부가 한일간 군사정보보호협정(GSOMIA) 연장을 거부함으로써 각국의 힘 다툼은 역사, 경제, 군사정보 등 영역 없이 복합적으로 전개되고 있다. 올해 7 월 이후 중국과 러시아가 한국 상공 영공을 침범하면서, 한국은 강대국들의 하이브리드 전략 실험장으로 전락하는게 아닌가 우려도 제기된다. 한국을 둘러싼 하이브리드전의 위협은 향후 더 심화될 것으로 보인다.

결어

초고도 네트워크 사회로 진입하면서 전쟁에 있어 정규전과 비정규전의 경계가 모호해지고있다. 지금까지의 전쟁에서는 비정규전이 정규전을 도와주는 역할에 머물러 있었던 반면 지속적인 안보환경의 변화로 비정규전의 영향력은 더 커질 수 밖에 없다. 인공지능과 인터넷의 발달은 재래식 무기 이외의 다양한 형태의 공격을 가능하게 했으므로 전쟁에 대한 인식변화와 대응이 요구된다.

북한은 이미 국가수준의 하이브리드 위협을 도구화하여 사용하고 있다. 하이브리드 위협은 방대한 양의 정보와 정확한 잠재 대상을 타겟팅 할 수 있는 능력으로 위협적이며 인공 지능

개발과 네트워킹 기술이 성숙함에 따라 위험도가 증가한다. 이러한 위협에 대응하기 위해서는 하이브리드 위협에 대한 인식을 향상해야 한다. 하이브리드 활동을 감지하고 표시하기 위해 지속적으로 정보를 수집하고 공유하며 평가하는 것도 필요하다. 사회 기반이 되는 각종 인프라 보호, 사이버 방호 등 각 분야에 대한 점검과 유기적인 대응이 필요하다. 위협에 대비하기 위한 의사 결정과 지휘체계, 군사적 및 비군사적 대응책도 함께 모색해야 한다. 사회, 정치, 군사 등 모든 분야에 걸쳐 신속하고 정확한 판단과 대응을 위한 논의와 대비가 요구된다.

---

[1] 이란 핵시설 공격 스턱스넷(Stuxnet·악성코드)은 이스라엘·美 작품, 조선일보, http://news.chosun.com/site/data/html_dir/2011/01/17/2011011700132.html

[2] 사이버 해킹 등을 이용하여 상대국의 미사일 발사를 무력화시키는 방안

[3] How the Russians hacked the DNC and passed its emails to Wikileaks, The Washington Post, https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html?utm_term=.7ad9bc06f509

[4] Russia-backed Facebook posts 'reached 126m Americans' during US election, The Guardian, https://www.theguardian.com/technology/2017/oct/30/facebook-russia-fake-accounts-126-million

[5] Catherine A. Theohary, "Information Warfare: Issues for Congress", Congressional Research Service, March 5, 2018. https://fas.org/sgp/crs/natsec/R45142.pdf

[6] Antonia Ward, "ISIS's Use of Social Media Still Poses a Threat to Stability in the Middle East and Africa", The RAND Blog, Dec 11, 2018.

[7] FT "중국의 韓사드 보복은 자해적 행동", 연합뉴스, https://www.yna.co.kr/view/AKR20170323108900009

[8] "청와대 안보실 10 년만에 펴낸 보고서, 미국에 10 년·일본보다 5 년 늦어", 중앙일보, https://news.joins.com/article/23444687

[9] 「국방개혁 2.0」, 국방부

[10] 현재는 지상, 해상, 공중만 포함하고 있다.

[11] "문 대통령 "2022 년까지 정보보호 예산 8485 억원 투입"", IT 조선, http://it.chosun.com/site/data/html_dir/2019/07/10/2019071001600.html