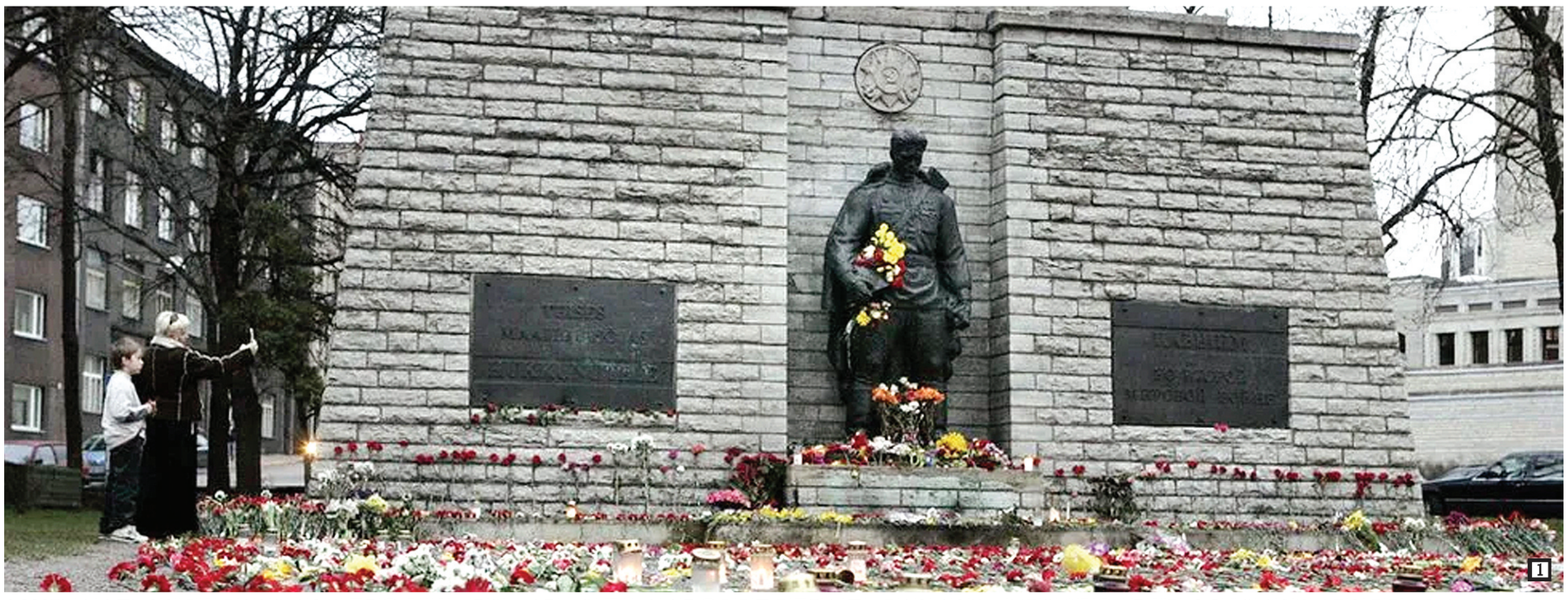
제3전선, 정보전쟁 진화하는 사이버 정보전

러, 에스토니아 민관사이트 공격 국가기능 3주 마비되기도

〈2007〉

최성규
고려대 연구교수



1 2007년 에스토니아에 대한 러시아의 사이버 공격을 촉발한 탈린의 구소련 군인 동상. 이 사건을 계기로 미국과 나토는 러시아 사이버 정보전의 위력을 실감했다. 2 최초의 사이버 스파이 마커스 헤스.

지난 1월 우크라이나 정보국(SSU)이 국민들에게 인터넷과 연결된 IP카메라 사용을 중단하도록 긴급 요청했다. 키이우의 민간아파트 관리자가 아파트 관리를 위해 IP카메라를 설치했는데, 러시아가 이 카메라를 해킹해 키이우의 방공망 정보를 수집하여 미사일 공격에 활용한다는 이유에서다. 이에 따라 우크라이나 전역에 설치된 1만여대의 IP카메라 사용이 일시 중단됐다. 사이버 정보전이 실전 무기로 진화하고 있는 모습이다. 이 뿐 아니다. 중국은 해킹으로 미국인들의 건강기록, 신용카드, 여권 정보를 수집해 중국내 미국 스파이를 찾아내거나, 미국에 중국 스파이를 심는 데 활용하고 있다.

다른 나라 국민들의 개인정보를 비밀 정보활동에 활용하는 새로운 발전이다. 사이버 정보전의 영향력도 국가간 역학관계를 변화시킬 정도로 커지고 있다. 사이버를 통한 중국의 경제·기술 정보 탈취를 "금세기 최대 부의 이동"이라고 비유한 키스 알렉산더 전 미 국가안보국(NSA) 국장의 말은 정곡을 찌르고 있다. 사이버 공간에 허위조작정보를 유포해 경쟁국의 국정운영을 방해하거나, 사이버로 다른 나라의 인프라시설을 공격해 사회를 혼란시키는 것은 이제 더 이상 놀랄 일이 아니게 됐다. 가히 사이버 정보전이 국가운영의 비밀병기가 되고 있다. 사례를 하나씩 살펴보다 보면 그 실상이 드러난다.

러, 동상 이전 놓고 갈등 생기자 외교보복

사이버 정보전의 역사는 비교적 짧다. 1980년 소련 국가보안위원회(KGB)가 동독 과학자 마커스 헤스를 고용해 미국 컴퓨터를 해킹해 보도록 주문한 것이 지금까지 알려진 최초의 사이버 스파이다. 성공하면 5만4000 달러를 주는 조건이었다. 헤스는 독일 브레멘대학 네트워크를 사용, 400대의 미 군사시설과 방산업체 컴퓨터를 해킹해 반도체, 인공위성, 우주 기술 등을 훔쳤다. 이처럼 사이버 정보전의 역사는 정보수집에서부터 출발했다.

이후 사이버 정보전은 문어발처럼 영역을 확장해 나갔다. 국가가 필요로 하면 어디든 빈틈을 찾아 역할을 했다. 에스토니아에 대한 러시아의 외교보복도 그 중 하나다. 2007년 4월 27일 에스토니아가 수도 탈린에 있는 구소련의 2차대전 참전기념 군인 동상을 외곽의 공동묘지로 이전키로 발표했다. 이 동상은 에스토니아가 러시아에 통치당했다는 불명예의 상징이었기 때문이다. 그러나 에스토니아의 러시아계 주민에게는 나치와 싸우다 전사한 구소련의 영웅을 상징했다. 그래서 동상 이전을 격렬히 반대했다. 이 과정에서 사상자가 발생하는 등 외교분쟁으로 비화되자, 러시아는 에스토니아의 대통령궁과 정부, 기업 웹사이트를 마비시키는 대규모 사이버 공격을 단행했다. 이 공격으로 에스토니아의 국가기능이 3주간 정지됐다. 사이버 정보전을 통해 에스토니아에 무서운 보복성 경고를 날린 것이다.

사이버 정보전은 선거 개입에도 동원된다. 러시아 정보당국의 배후지원을 받는 해커단체 APT28과 APT29가 2016년 미국 대선과 2017년 프랑스 대선에 개입한 것이 좋은 예다. 특히 프랑스 대선에서는 투표일 이틀 전에 에마뉘엘 마크롱 후보의 e메일 2만개 이상을 유출시켜 선거 정국을 극도로 혼탁하게 만들었다. 당시 테레사 메이 영국 총리가 보복 사이버 공격을 경고할 정도였다. 2022년에는 중국 정보당국이 전세계 100여개 정당 도메인을 훑고 다녀, 미 NSA가 긴장했다. 올해 1월에는 러시아 해커조직이 핀란드 대선을 앞두고 디도스 공격을 위협했고, 인도네시아에서는 해커들이 선관위를 디도스 공격해 사이트가 다운되는 상황이 발생했다. 또한 추적이 어려운 다크웹에 리비아의 선거 시스템 접근 권한을 판매한다는 게시글이 올라와 리비아 당국을 긴장시켰다. 사이버 선거 개입의 그림자가 여기저기서 어른거리고 있다. 오는 6월 선거를 앞둔 유럽 의회가 외부의 사이버 선거개입 차단을 위해 강력한 정보보안 시스템을 정비한 것은 이 같은 우려 때문이다.

선거에도 사이버전 동원

프랑스 대선, 마크롱 e메일 유출돼

인도네시아선 선관위 디도스 공격

군사분야에서도 날로 진화

총성보다 먼저 사이버전 가동

AI까지 가세하면 파괴력 무한대

북한의 사이버전 위협

북, 세계 4대 위협국 분류될 정도

4월 총선에도 가만있지 않을 것

미국 국가안보국(National Security Agency, NSA)
중앙정보국(CIA), 연방수사국(FBI)과 함께 미국 3대 정보기관으로 전화, 컴퓨터, e메일, 암호 등 신호정보와 사이버정보를 책임진다.

작전준비 환경(OPE)
사이버 공격에 앞서 사전에 제반 환경을 점검하고 준비하는 행위로, 영어로는 Operational Preperation of Environmnet라고 한다.

휴민트(Humint)
스파이 등 인간을 통한 정보활동 방법으로 인간(Human)과 정보(Intelligent)의 합성어이다.

군사분야 사이버 정보전도 날로 진화하고 있다. 1990년 걸프전 당시 미국이 컴퓨터 바이러스를 통해 이라크 방공망을 마비시킨 것은 이제 고전이 됐다. 오늘날은 상대의 전쟁 의지를 꺾어 놓기 위해 사이버 정보심리전이 발전하고 있다. 2008년 러시아가 조지아를 침공할 때 정부 사이트를 먼저 공격해 국가기능을 일시 마비시켜 놓고 군사력을 동원했다. 전쟁 시작 전, 먼저 사이버 정보전을 통해 혼란과 공포감을 증폭시켜 전쟁 의지를 약화시키는 고도의 사이버 정보심리전이다. 전쟁의 시작은 총성이 울리는 순간이 아니라, 사이버가 움직이는 순간으로 변하고 있다.

사이버 정보전은 미래까지도 내다본다. 미래 분쟁에 대비해 사이버 공간에 미리 공격포인트를 은밀하게 확보해 놓는 단계로까지 발전하고 있다. 미래의 '작전환경 준비(OPE)'라고 부른다. 가령, 보안이 취약한 소규모 사무실을 해킹해 지하철, 에너지, 통신 등 사회 인프라시설에 침투할 수 있는 통로를 미리 확보해 두는 것이다. 특히 통신회사를 집중 공략한다. 통신회사를 해킹해 작전환경을 미리 준비해 두면 유사시 사이버 공격 범위를 훨씬 더 넓힐 수 있기 때문이다. 사이버 선진국들은 다른 나라의 사이버 시스템 취약점을 파악해 극비로 관리하고 있다.

1월 28일 러시아 해커조직이 핀란드 대통령 선거 직전, 핀란드 인터넷 포털 사이트들에 대해 디도스 공격을 감행했다고 주장했다.
[사진 해커조직 NoName057(16)의 텔레그램 채널]

지도자들 대응 전광석화처럼 빨라야

이와 같이 사이버 정보활동은 짧은 역사에도 불구하고 급속한 발전을 이룩했다. 가상의 사이버 공간이 최적의 정보활동 환경을 제공해주고 있기 때문이다. 무엇보다 사이버 공간은 국경이 없어 누구나 자유롭게 드나들 수 있으며, 익명성이 보장되므로 비밀 유지가 쉽다. 또한 사이버 공간을 통하면 언제 어디서든 전 세계를 실시간 접근할 수 있다. 다른 나라 영토에 직접 들어가지 않고서도 원경 정보활동이 가능하며, 따라서 정보활동이 시공의 제한을 받지 않는다는 의미다. 이뿐만 아니다. 사이버 공간은 '정보의 보고'이다. 개인과 기업은 물론 국가도 중요한 문서를 대부분 컴퓨터나 클라우드 등 사이버 공간에 보관하기 때문이다. 그런데 이 같은 장점에도 불구하고 비용과 위험은 휴민트를 통한 전통적 정보활동보다 오히려 낮다. 한마디로 최고의 가성비다. 이런 이유들 때문에 사이버 공간이 정보의 새로운 전쟁터가 되고 있는 것이다. 여기에다 인공지능(AI)까지 가세하면 사이버 정보전이 어디까지 발전할지 상상하기조차 어렵다.

더욱 어려운 것은 이 같은 사이버 정보전이 가져올 여러 가지 숙제들이다. 무엇보다 사이버 시대·디지털 시대는 지도자들의 결단이 전광석화처럼 빨라야 한다. 마이클 헤이든 전 미국 중앙정보국(CIA) 부장의 말처럼 사이버전은 엄청난 속도와 기동력 때문에 순식간에 국민안전과 국가안보를 위협할 수 있다. 그러므로 사이버전 대응은 머뭇거릴 시간이 없다. 스탠포드대 에이미 제가트 교수의 비유는 흥미롭다. 1962년 쿠바위기 당시 케네디 대통령이 결단을 내리는 데 걸리는 시간은 13일이었고, 2001년 911 당시 부시 대통령이 대(對)테러전쟁 결단을 내리는 데 걸리는 시간은 13시간이었다. 그렇다면 앞으로 전면적 사이버 공격을 받을 경우 미국 대통령은 단 13분 안에 결단을 내려야 할지도 모른다고 제가트 교수는 말했다. 또한 제도적 완비 못지않게 지도자들의 사이버전 이해와 리더십도 중요함을 잊지 말아야 한다. 그래야만 신속하면서도 옳은 결단을 내릴 수 있기 때문이다.

사이버 정보전이 더 격렬해질 경우의 파장을 관리하는 것도 만만치 않다. 사이버 공간을 통한 악의적인 여론 조작과 해킹 등이 심해질 경우 국가간 반감을 초래해 평화와 협력의 국제질서를 해칠 수 있고, 건전한 사이버 생태계도 위협한다. 특히 민주주의의 근간인 선거제도 공격은 부지불식간에 민주주의에 대한 회의와 불신을 불러와 자유 민주체제를 심각하게 위협할 수 있다. 권위주의 체제가 노리는 궁극적 목표다. 이에 대한 대비는 아무리 강조해도 지나침이 없다.

우리가 가장 신경을 써야 할 대상은 북한이다. 북한의 사이버전 위협은 미국이 러시아, 중국, 이란과 함께 세계 4대 위협국으로 분류할 정도로 우려할 수준이다. 어릴 때부터 사이버 영재를 집중적으로 육성하고 있는 점을 감안하면 과장이 아니다. 우리는 이미 북한으로부터 날카로운 사이버 공격을 수차례 받은 경험이 있다. 당장 코앞으로 다가온 4월 총선에 북한이 가만히 있지 않을 것이란 예측이 나오는 이유이기도 하다.

〈광주일보와 중앙 SUNDAY 제휴 기사입니다〉

최성규 국가정보원에서 장기간 근무하며 국제안보 분야에 종사했다. 퇴직 후 국내 최초로 비밀 정보활동의 법적 규범을 규명한 논문으로 고려대에서 박사학위를 받았다