제3전선, 정보전쟁 사이버 정보전

# 클릭 한 방으로 국가기능 마비, 원폭보다 무서운 '사폭'

〈사이버 폭탄〉

최성규
고려대 연구교수

1 2010년 미국 메릴랜드주 포트 미드에 있는 국가안보국(NSA) 본부의 조감도. 2 2004년 이전한 영국 정부통신본부(GCHQ). 두 기관은 각각 1952년, 1919년 설립됐다. 〈로이터=연합뉴스〉

2023년 미 국가정보장실(ODNI)이 랜드(RAND)연구소에 의뢰해 미국의 사회기반시설이 사이버 공격을 받는 시뮬레이션을 실시한 적이 있었다. 그런데 충격적인 결과가 나왔다. 전기·통신·수도 등 핵심 기반시설들이 연쇄적으로 정지돼 도시 전체가 마비되는 것으로 나타났다. 공격자가 누군지 모습을 드러내지 않아 반격도 어려운 것으로 나타났다. 속수무책이 된다는 것이다. 특히 누가 공격했는지보다 왜 못 막았는지에 대한 논란이 사회·정치적 분열로 이어져 위기를 더욱 악화시킬 수 있다고 경고했다. 한마디로 전면적 사이버 공격은 국가기반 전체를 정지시키는 '조용한 핵무기'가 될 수 있다고 봤다. 미 중앙정보국(CIA) 헤이든 전 국장이 사이버전의 파괴 잠재력은 히로시마 원폭급의 치명적 수준이라고 경고한 것을 재확인해 주었다.

### 5년 이상 국가 시설에 잠복해있다 적발

이처럼 사이버 정보전이 기업과 개인정보 탈취 수준을 넘어 이제는 국가기능을 마비시킬 정도로 진화했다. 1986년 컴퓨터를 통해 원격 정보 탈취가 가능한지를 알아보기 위해 시작된 사이버 정보전이 반세기도 안돼 급속히 발전하면서 정보 지형을 변화시키고 있다. 밝혀진 실상은 빙산의 일각에 불과하지만 그 일각만으로도 변화의 흐름을 충분히 알 수 있다.

사이버 정보전의 첫발은 비밀 정보수집에서 시작됐다. 1986년 소련 국가보안위원회(KGB)가 미국방부 컴퓨터에 침투해 정보 탈취에 성공하면서다. 이후 1996년 러시아가 또다시 미 패터슨 공군기지 컴퓨터에 침입해 비밀정보를 대량으로 탈취했다. 이번에는 3년 동안 잠복하면서 본격적으로 정보를 수집했다. '달밤의 미로(Moonlight Maze)' 사건으로, 사이버 공간을 통해 대량의 정보수집이 가능하다는 것을 확인했다.

당시만 해도 사이버 정보가 무엇인지 잘 몰라 세상은 관심을 보이지 않았다. 그러나 정보 당국은 향후 사이버 공간이 정보전의 신세계가 될 것이라고 보았다. 가상의 사이버 공간은 물리적 경계가 없고 시공의 제약이 없어 24시간 언제 어디든 정보 침투가 가능하기 때문이다. 특히 개인과 기업은 물론 국가도 비밀정보를 사이버 공간에 보관해 두기 때문에 '정보의 바다'가 될 것으로 봤다.

사이버 공간의 정보 잠재력을 간파한 정보기관들은 이때부터 사이버 공간으로 몰려들기 시작했다. 2013년 세계를 발칵 뒤집어 놓은 '스노든 폭로사건'이 이를 잘 보여주었다. 미 국가안보국(NSA) 전직 직원인 스노든은 NSA가 구글·애플·버라이즌 등 IT기업과 통신사 서버에 접근해 수억 명의 정보를 수집했으며, 심지어 독일 메르켈 총리 등 우방국 지도자들까지 무차별 도청했다고 폭로했다. NSA는 국가안보를 위해 법원의 허가를 받은 합법적 활동이라고 주장했지만, 국제적 비난을 피하진 못했다. 정보전의 일그러진 자화상을 보여주었지만, 동시에 사이버 공간이 글로벌 정보전의 새로운 수단이 될 수 있다는 것도 보여주었다.

러시아는 사이버 정보전을 전쟁의 영역으로 확대하는데 탁월한 능력을 보였다. 전쟁 개시 전 레이더를 해킹해 방공망을 무력화시키거나 사이버 심리전을 통해 적의 사기를 꺾는 등 전쟁 무기로 활용했다. 2008년 조지아 침공, 2014년 크림반도 합병, 2022년 우크라이나 침공 당시 모두 전쟁 개시 전 사이버 공격을 감행해 기선을 제압했다. 전쟁은 총알보다 키보드에서 먼저 시작되는 새로운 시대를 열었다.

### 정보기관 공격적 사이버전 뒷받침 필요

최근 사이버 정보전은 소리 없이 국가기능을 마비시키는 고도단계로 들어서고 있다. 중국 정보당국이 배후 조종한 것으로 알려진 볼트 타이푼(Volt Typhoon) 사건이 그 예다. 2024년 2월 7일 미 정보당국은 볼트 타이푼 해커조직이 미국의 통신·전기·수도 등 주요 기반시설에 침투해 5년 이상 잠복해 있었던 것을 적발했다고 발표했다. 그런데 침투 목적은 정보 수집이 아니라, 미국 사회기반시설 내부에 침투해 잠복해 있다가 미·중 충돌 등 유사시에 미국의 국가기능을 마비시키기 위한 것이라고 밝혔다. 미래에 대비해 디지털 지뢰를 심어놓았다는 의미다. 사이버 정보전이 점점 전통적 전쟁과 맞먹는 위협이 될 수 있다는 가능성과 경고를 동시에 보여주었다.

이처럼 공격이 진화하자 방어도 진화했다. 보복, 역해킹, 이중스파이 침투 등 모든 수단이 동원되고 있다.

2021년 러시아 해커조직인 '다크사이드(Darkside)'가 미국 송유관회사인 콜로니얼 파이프라인(Colonial Pipeline)을 해킹한 사건에서 그 일단을 볼 수 있다. 해커조직이 송유관 가동을 멈춘 후 500만 달러를 요구하자, 미국은 어쩔 수 없이 돈을 지불한 후 즉각 보복에 나섰다. NSA는 해커그룹의 통신을 감청하고, CIA는 전 세계 해커집단에 침투시켜 놓은 협조망을 통해 관련 정보를 수집했다. FBI는 지불한 돈의 흐름을 실시간 파악했다. 국토안보부의 사이버보안국(CISA)은 해커의 기술분석을 통해 공격자가 누구인지 추적했다. 이후 다크사이드의 서버가 마비되고 암호계좌도 텅텅 비었다. 그러나 누가 그랬는지 밝히지 않고 흔적도 남기지 않아 다크사이드는 답답해했다. 한참 지난 후 FBI가 '다크사이드의 개인 키에 접근했다'고 짤막하게 밝혔다. 정보·수사·행정 당국이 모두 나서 보복했음을 미 국민에게 보고한 셈이다. 다크사이드도 은퇴하겠다며 항복을 선언했다.

**러, 2008년 조지아 침공 때부터 총알보다 키보드로 전쟁 개시**

**중, 미 국가 주요 기반 시설 해킹 충돌 시 터트릴 디지털 지뢰 심어**

**유심 해킹 조종한 국가 있을 수도 러와 밀착하는 북 철저 경계해야**

**사이버 정보전 개념**
사이버 수단으로 정보우위를 확보해 적을 제압하는 현대정보의 요체로, 자국 정보와 인프라를 보호하는 방어전과 적에 침투해 정보를 수집하고 인프라를 무력화하는 공격전으로 구분된다.

**국가 사이버군 (National Cyber Force : NCF)**
2020년 영국이 국가 사이버전 역량을 혁신하기 위해 창설한 정보·국방 합동조직이다. 경찰과 민간도 실질적 파트너로 참여하고 있다.

2 영국 국가사이버군(NCF) 본부 전경

올 3월 미 법무부가 중국의 아이순(I-Soon) 해커조직을 기소했을 때도 공격적 방어전의 일단을 보여주었다. 역해킹이나 이중스파이가 없으면 알 수 없는 내용들이 기소장에 상세히 적시돼 있었기 때문이다. 아이순이 중국 정보당국의 지시를 받아 미 정부·기업을 해킹하고 대가로 건당 1만~7만 5000달러를 받은 사실, 정보당국이 해커들에게 지시한 메모 내용, 심지어 아이순에 위장 침투한 중국 정보요원의 신상정보까지 파악해 놓고 있었다. 사이버 방어를 위해 평소 해킹, 이중스파이 침투, 내부협조자 확보 등 공격적 정보활동을 꾸준히 하고 있다는 것을 밝힌 것이나 다름없다.

미국은 이 같은 공격적 방어를 예방적 방어 또는 전진 방어(defend forward)라고 명명해 합리화하고 있다. 눈에 보이지 않고 순식간에 이루어지는 사이버 공격을 방어하기 위해 먼저 공격원점을 찾아 제거하는 것이 최선이라는 것이다. '공격이 최선의 방어'라는 전략을 택하면서 공격과 방어의 경계도 점점 모호해지고 있다.

이처럼 사이버 정보전은 1986년 첫발을 뗀 지 반세기도 안돼 인류 정보사(史)의 새로운 역사를 쓰고 있다. 대량 정보수집(mass espionage)의 새로운 시대를 열었고, 시공을 초월해 언제·어디서든 정보활동이 가능한 시대를 열었다. 마우스 클릭 몇 번만으로 국가기능을 마비시킬 수 있는 세상도 열었다.

그러나 변화는 이제 시작에 불과하다는 것이 중론이다. 디지털 기술로 만들어진 사이버 세계는 앞으로 디지털 기술의 발전에 따라 어떻게 진화할지 미답의 영역이기 때문이다. 여기에다 인공지능(AI)까지 가세하면 사이버 공간은 AI 대 AI의 신시대로 접어든다. 이쯤 되면 사이버 정보전은 무엇을 상상하든 상상 그 이상이 되는 시대가 될 수 있다.

각국의 고민도 깊어지고 있다. 아날로그 시대의 관성적 방법으로는 미래 사이버전 대응이 어렵기 때문이다. 영국이 미래 사이버전 대응을 위해 아날로그식 칸막이를 허물고 정보·국방은 물론 민간까지 참여하는 융합형 사이버군(National Cyber Force)을 창설한 것은 그 예후다. 새로운 사이버 생태계 탄생의 예고편이다.

우리 고민도 만만찮다. 당장 SKT 사태의 배후를 밝혀야 한다. 앞서 볼트 타이푼 사건처럼 의도를 숨긴 채 배후에서 조종하는 국가세력이 있을 수 있어서다. 북한의 사이버 위협은 더 철저히 경계해야 한다. 우리 사이버 시스템에 깊숙이 숨어 있다가 언제, 어떻게 기습할지 모른다. 최근 북·러 밀착 시기에 러시아의 사이버 공격기술이 북한으로 넘어갔을 가능성도 있어 더욱 우려된다.

미래에 대비해 사이버 정보력을 꾸준히 강화하는 것도 중요하다. 먼저 사이버 정보전에 대한 냉철한 인식과 전략을 재정립해야 한다. 사이버 정보전은 앞으로 민간기술에 의해 좌우될 것이므로 민간이 참여하는 사이버 생태계도 새롭게 구축해야 한다. 정보기관에 대한 막연한 불신에서 벗어나 공격적인 사이버전 수행이 가능하도록 제도적 뒷받침도 필요하다. 조용한 사이버 전쟁에서 이기기 위한 최소한의 조치들이다.

〈광주일보와 중앙 SUNDAY 제휴 기사 입니다〉

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