전방위적으로 시도되는 북한 사이버 테러 실상

김승주
(고려대 사이버국방학과 교수)

세계적 화두로 떠오른 4차 산업혁명

요즘 4차 산업혁명 및 이와 관련된 기술들이 화두다. '4차 산업혁명'이라는 용어는 지난 2012년 독일의 '인더스트리(industry) 4.0' 정책에서 처음 등장해, 2016년 1월 스위스 다보스에서 열린 세계경제포럼(WEF, 다보스포럼)

의 주제로 선정되면서 전 세계적 화두로 떠올랐다. 1784년 영국에서 일어난 '1차 산업혁명'이 증기기관의 발명을 통한 육체노동의 기계화를 가능케 하였다면, 1870년 시작된 '2차 산업혁명'은 전기를 이용한 대량생산체계가 이루어진 시기로 생산성을 비약적으로 향상시켰다. 이어 1969년 이후 반도체와 인터넷을 필두로 한 '제3차 산업혁명'은 정보화 및 부분 자동화의 혁명을 불러왔으며, 이제 세상은 '4차 산업혁명'의 소용돌이로 들어가고 있다.

물론 아직 4차 산업혁명에 대한 개념이 확립된 것은 아니다. 혹자는 아직도 3차 산업혁명시대라고 주장하기도 한다. 하지만 그것이 3차 산업혁명의 최종단계든 4차 산업혁명의 시작이든 간에 최근의 비약적인 정보통신기술(ICT)의 발전은 우리에게 다가올 변화에 대한 준비를 요구하고 있는 것이 사실이다.

4차 산업혁명에 대해 다양한 정의와 예측들이 쏟아지고는 있지만, 필자의 생각에 이를 가장 잘 표현하는 키워드는 '사이버물리시스템(CPS, Cyber-Physical System)'이 아닐까 한다. 사이버물리시스템, 또는 우리에게 좀 더 친숙한 용어인 'O2O(Online To Offline)'란 사이버세계(cyber space)와 현실세계(physical space)가 완전히 통합된 세상을 뜻하는 것으로서, 우리가 살아가는 실제적인 물리세계와 컴퓨터상에 존재하는 가상세계가 인터넷을 매개로 물샐틈없이 연결돼 매순간 끊임없이 상호작용하는 초연결사회라 할 수 있다.

실제로 시장조사 전문업체 가트너에 따르면 인터넷에 연결되는 기기의 수가 2014년 37억5천만대에서 2015년에 49억대로 증가했고, 4차 산업혁명시대가 오는 2020년에는 250억대를 넘어설 것이라고 한다. 이중 스마트폰과 스마트TV를 필두로 한 가전분야가 131억7천2백만대, 커넥티드 카(connected car)로 대변되는 자동차분야가 35억1천1백만대로 2020년 전체 인터넷 접속 기기의 약 66.7%를 차지할 것으로 전망하고 있다. 또한 시장조사기관 IDC는 전 세계 사물인터넷(IoT) 시장을 2013년 1.9조 달러에서

2020년 7.1조 달러로 성장할 것으로 분석하고 있다.

장밋빛 미래에 숨겨진 심각한 사이버 해킹

그러나 이러한 4차 산업혁명시대의 장밋빛 미래 뒤에는 그에 따른 그늘 또한 존재한다. 2015년 7월 전직 NSA 출신 해커, 찰리 밀러(Charlie Miller)는 "모든 사람이 자동차도 PC처럼 사이버 공격을 당할 수 있는 대상임을 심각하게 받아들여야 한다"며 시속 130km로 달리고 있는 차량을 원격으로 해킹하는 시연을 방송에 공개했다. 이로 인해 세계적인 자동차 회사 피아트 크라이슬러는 해킹 취약점이 발견된 최신 자동차 140만대를 리콜해야만 했다.

스마트TV의 경우, 몰래카메라로 악용하거나 방송국 몰래 거짓뉴스를 내보내는게 가능하다는 것이 2013년에 고려대학교 연구팀에 의해 처음 시연됐으며, 작년 3월 폭로전문 웹사이트 위키리크스(WikiLeaks)는 미국 CIA가 영국 정보기관 MI5와 공동으로 개발한 악성코드를 삼성 스마트TV에 심어 도청장치로 악용해오고 있었음을 관련 문서와 함께 폭로했다. 이 악성코드는 TV의 전원을 끄더라도 주변에서 들리는 소리를 수집한 후 인터넷을 통해 CIA 서버로 전송할 수 있는 프로그램이라고 위키리크스는 전했다.

군도 예외는 아니다. 영국의 '영 · 미 안보정보협의회(BASIC, British American Security Information Council)'는 2017년 6월 발간한 '영국의 전략무기용 핵잠수함에 대한 해킹 위협 보고서(Hacking UK Trident : A Growing Threat)'에서 "핵잠수함과 같은 첨단 무기시스템들은 이미 너무나도 많은 컴퓨터 시스템들에 의존하고 있으며, 망 분리가 되어있다고는 하나 이는 제조단계, 소프트웨어 업데이트 과정 등에서 얼마든지 쉽게 우회가 가능하다. 이에 영국정부는 조속히 첨단무기 시스템들에 대한 사이버 공격에 철저히 대비해야 한다"고 밝힌바 있다.

4차 산업혁명시대에 접어들면서 북한의 사이버 공격 또한 전방위적으로

시도되고 있다. 우리 정부에 따르면 2016년 11월 기준으로 북한의 해킹인력 규모는 1,700명, 이들을 지원하는 인력은 5,000명 규모라고 한다. 또한 주요 공공기관을 대상으로 매일 평균 140만건 가량의 해킹 시도가 발생하고 있으며(물론 이것이 모두 북한 소행이라는 얘기는 아니다), 이는 꾸준히 증가하는 추세이다. 관계당국은 현재 북한의 사이버전 수행능력이 이미 세계 상급 수준에 도달해 있고 그 수법 또한 빠르게 고도화, 지능화돼 가고 있다고 판단하고 있으며, 공격목표도 과거 기밀 데이터나 개인정보 수집에 치우쳤던 것에서 벗어나 최근에는 4차 산업혁명의 대표적 이슈인 가상화폐 '비트코인(Bitcoin)'과 은행을 해킹하는 쪽으로 양상이 바뀌고 있다고 보고 있다.

전방위적으로 시도되는 북한의 사이버 테러

실제로 금융보안원이 공개한 '2017 사이버 위협 인텔리전스 보고서'는 국내 사이버 안전에 위협적인 북한의 3대 해킹그룹으로 '라자루스(Lazarus)', '블루노로프(Bluenoroff)', '안다리엘(Andariel)' 등을 꼽고 있다. '라자루스'는 북한이 배후로 추정되는 해킹그룹으로 상당한 기술력과 조직력을 갖춘 것으로 평가받고 있으며, 나머지 2개 그룹 '블루노로프'와 '안다리엘'은 라자루스에서 분화돼 활동하고 있는 것으로 나타났다.

이들은 ▲2013년 금융과 방송사를 마비시킨 3.20 사이버 테러부터 ▲2014년 미국 '소니픽처스 엔터테인먼트' 공격, ▲2015년 국내외 방산업체 대상 표적공격, ▲2016년 2월 방글라데시 중앙은행에서 8,100만 달러의 절도를 감행한 해킹공격, ▲2016년 6월 전 세계 100여개 국가에 있는 수많은 PC를 삽시간에 감염시킨 '워너크라이(WannaCry)' 랜섬웨어(ransomware, 몸값(ransom)과 소프트웨어(software)의 합성어로서 컴퓨터나 스마트폰 내의 데이터들을 암호화해 사용할 수 없도록 만든 뒤, 이를 인질로 금전을 요구하는 악성 프로그램) 공격, ▲2017년 2월 폴란드 금융감독원 홈페이지를

통한 워터링홀(watering hole, 표적 집단이 자주 방문하는 웹사이트에 악성코드를 심어 놓고 해당 웹사이트를 방문할 때까지 기다리는 해킹 수법) 공격 등의 배후로 지목되고 있으며, 최근에는 유럽과 한국에 있는 현금자동인출기(ATM) 회사와 빗썸, 코빗 등 국내 비트코인 거래소들을 노리는 공격에 집중하고 있다고 한다. 더욱이 지난 1월 8일에는 또 다른 가상화폐인 '모네로(Monero)'의 채굴을 지시하고 채굴된 모네로를 북한 김일성대학 서버로 송금토록 하는 악성코드가 발견되기도 했다.

이외에도 지난 2016년 7월 북한은 국내 인터넷 쇼핑몰 '인터파크'를 해킹해 개인정보를 빼내고 30억원 상당의 비트코인을 요구하기도 하였으며, 지난해 6월에는 인터넷 IDC업체 '나야나'가 정체불명의 해커로부터 랜섬웨어에 의한 해킹피해를 입기도 하였다. 해커는 당시 회사 규모와 연봉, 가족 등을 구체적으로 언급하면서 826.2비트코인, 당시 시세로 26억원 상당을 요구했으며, 업체측은 결국 13억원을 주기로 해커와 합의하고 복구작업에 나선바 있다.

이렇듯 비트코인과 금융기관에 대한 해킹이 증가한 이유로 전문가들은 미국 등이 주도한 대북 경제제재를 들고 있다. 대북제재로 인해 경제 성장이 정체되자 북한은 해킹을 통한 가상화폐 탈취 및 금융망 해킹을 통한 자금 탈취를 새로운 외화벌이 수단으로 삼고 있다는 것이다. 인터넷상의 가상화폐인 비트코인이나 모네로의 경우 일반 화폐와 달리 계좌 추적이 매우 어렵고 자금 세탁이 용이하기 때문에, 국제사회의 해외 송금 압류 및 차단과 외화벌이 송금 통로의 차단에서 비교적 자유로울 수 있다. 더욱이 최근 가상화폐의 가격이 천정부지로 올라감에 따라 북한의 사이버 공격 수위 또한 비례해서 증가하고 있는 실정이다.

사이버 공격은 유지비용이 타 전력보다 저렴하고, 전시와 평시를 막론하고 효과와 지속성이 보장되며, 은밀성과 비대면성이라는 특징 덕분에 북한과 같이 은밀하게 대남전략을 수행해야 하는 집단에는 최적의 공격무기이

한국인터넷진흥원(KISA) 인터넷침해 대응센터 종합상황실에서 직원들이 국내 주요사이트 디도스(DDos) 공격현황을 모니터링하고 있다.

다. 특히 북한이나 중국 보다 인터넷 의존도가 높은 우리나라나 미국은 사이버 공격으로 볼 피해가 더 클 수밖에 없으며, 전화기는 물론, TV, 자동차, 항공기, 화폐에 이르기까지 일상생활의 모든 것들이 인터넷에 연결돼 소통하는 4차 산업혁명시대에는 더욱 그러하다.

최근 우리나라는 사이버 보안분야에 있어 괄목할만한 성과를 내고 있다. 으레 법대나 의대에 진학하던 상위 1% 영재들이 사이버국방학과 등의 보안 관련 학과에 지원하고 있으며, 각종 국제해킹대회에서도 좋은 성적을 내고 있다. 특히 2015년에는 고려대 사이버국방학과 및 정보보호대학원 재학생들과 국내 보안업체 연구원들로 구성된 한국 연합팀 '데프코(DEFKOR)'가 세계 최고 권위의 국제해킹대회 '데프콘(DEF CON)'에서 아시아 국가로는 처음으로 우승을 차지하기도 했다. 그러나 세계는 벌써 차원이 다른 사이버전 준비를 하고 있다. 이제 우리 정부도 현재의 조그마한 성과에 자만하지 말고, 과거 컴퓨터 내 정보의 보호만이 보안의 전부라는 협소한 시각에서 벗어나 보다 더 넓은 관점에서 다가올 4차 산업혁명시대의 사이버 안보 위협에 치밀하게 대처해야 할 때다. 북한