한반도선진화재단
Hansun Foundation

한선 프리미엄 리포트
Hansun Premium Report

주 제 : 제4차 산업혁명 시대의 사이버 안보정책
발제자 : 김승주 고려대학교 교수
일 시 : 2016년 12월 1일(목) 오전 7시 30분
장 소 : 국회 의원회관 제3세미나실

241회 정책세미나 주요 내용

< 요약 >

☞ **12월 1일 정책세미나에서는 김승주 고려대학교 교수를 연사로 '제4차 산업혁명 시대의 사이버 안보 정책'을 주제로 논의했습니다.**

■ PC 모뎀으로 인터넷을 연결하던 시절이 있었다. 지금은 전국 곳곳에 와이파이가 설치되어 언제 어디서든지 스마트 기기로 인터넷 연결이 가능하다. 인터넷 연결이 용이해지는 만큼 개인 정보유출이 빈번하게 일어나고 있다. 전세계 10대 개인정보 유출사례 중 4건이 한국에서 발생하였다. 개인정보 유출사례가 속출하다보니 대중들은 문제의식을 잃은 지 오래다. 그러나 개인정보 유출은 2차 피해로 직결된다.

■ 제4차 산업혁명 시대로 진입하면서 인터넷과 연결되지 않는 기기는 전무하다. 사이버(Cyber) 공간과 물리적(Physical) 공간이 연결된 Cyber Physical 시스템의 지배를 받고 있다. 세탁기, 냉장고, 자동차 등 250억 개의 기기들이 연결되어 작동하고 있다. 이 기기들은 해커들의 공격대상이다. 인터넷과 연결되지 않는 기기는 전무하다. 방치되어 있는 공유기가 워낙 많아 무심코 와이파이를 연결하였다가 기기에 저장된 개인정보, 통화내역과 문자 내용이 유출될 수 있다. 오늘날 해커들은 'Hack Everything'을 좌우명으로 삼아 손쉽게 수많은 개인정보를 입수하고 있다. 해킹을 인터넷 개인정보 유출사고 수준으로만 이해하니 사이버 법안 효용범위가 협소하다. 개인정보 유출의 경로와 규모를 제대로 파악해야 하며 시대에 맞는 정책이 필요하다.

■ 2013년 4월 23일 미국 AP통신 트위터 계정 해킹사고가 발생하였다. “Breaking: Two Explosions in the White House and Barack Obama is injured”가 속보로 AP통신 트위터에 업데이트 되었다. 순간적으로 나스닥 주가가 폭락하였다 상승하였다. AP사례가 보여주었듯이 오보는 주식을 요동치게 하는 파급력을 갖는다. 국내 속보 자막이 해커들에 의해 조작될 경우 같은 결과가 초래될 수 있다. 홈쇼핑 방송화면에서 주문번호만 조작하여도 개인정보 도용은 물론 상당 규모의 피해액이 발생할 수 있다. 스마트 TV의 개인정보 유출 및 도용 방지를 위해 기업과 정부의 철저한 관리가 필요하다.

■ 2013년 미국 조지아공대에서 충전기로 아이폰이나 아이패드를 해킹하는 방법을 알아냈다. 단자를 연결하면 악성코드가 아이폰 안으로 유입된다. USB 포트를 이용해 전자담배를 충전할 때도 마찬가지로 악성코드가 컴퓨터에 유입될 수 있다. IoT(사물인터넷) 기기들이 보안관련 문제들을 일으킬 가능성에 대해 정부 대책 마련이 시급하다. 스마트폰 해킹을 감지할 수 있도록 최소한의 장치를 마련해주는 등의 조치를 취해야 한다. 한국과 일본이 스마트 가전시장의 선두주자라 하더라도 보안 기능을 제대로 갖추지 못하면 미국 시장에서 경쟁력을 잃는다. 미국의 보안관련 법률은 강화되고 있다. 정보 보안 보호대상이 단순 개인정보에만 제한되었던 Information Security에서 Cyber Defense로 확대되어야 한다. 전략전술개념으로 접근하여 사이버를 활용한 모든 것에 대한 법안을 마련해야 한다.

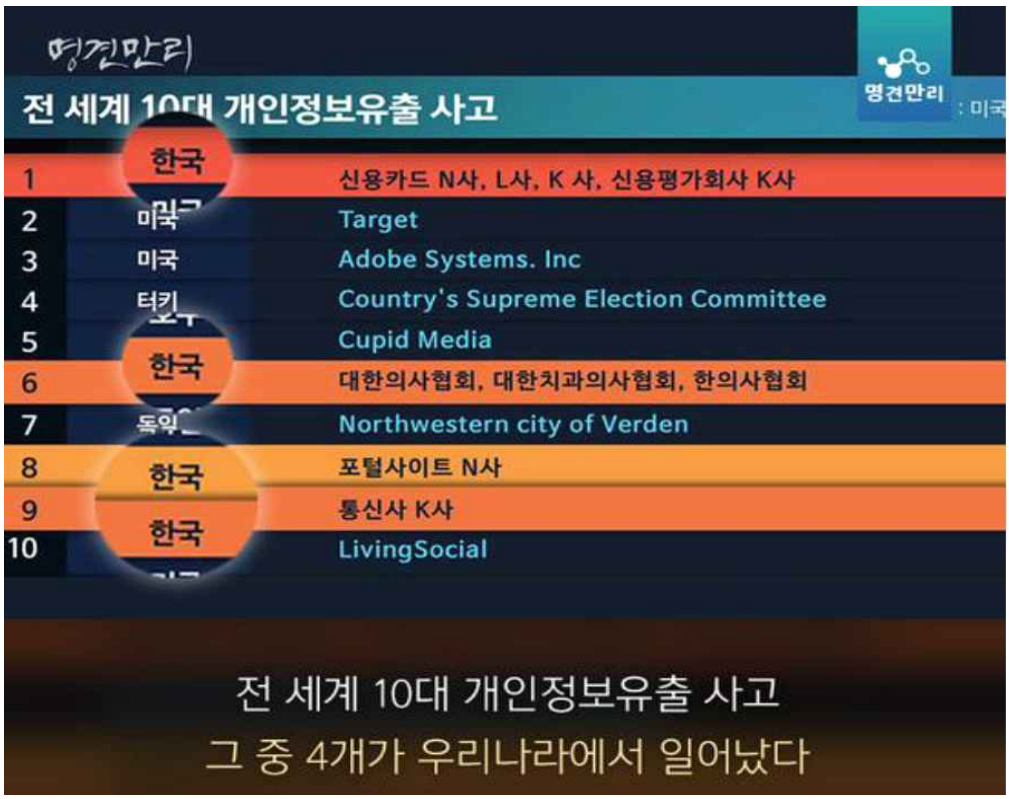
■ 미국 PAYPAL의 개인정보유출사고 발생확률은 하루 0.4%로 높은 편에 속한다. 반면, 우리나라 인터넷뱅킹의 사고 발생확률은 0.0009%다. 한국의 사고 발생률은 현저하게 낮아서 사고에 대한 손해배상 사례가 전무하다. 즉 방지대책은 잘 구축되어 있으나 복원력이 약하다. PAYPAL은 반대로 방지는 약하지만 복원력이 뛰어나 사고에 대한 손해배상과 대책마련이 빠르고 철저하다. 부실한 관리는 처벌받아 마땅하다. 공격 중에서는 미리 방지가 어려운 공격들이 있다. 취약점 노출 시 대중의 질책이 거세져 이러한 취약점들을 기업에서 미리 정부에 보고하도록 유도하고, 손해배상 대책 마련을 위한 동기 부여도 필요하다.

■ 미국은 신뢰성을 보안의 기준으로 삼는다. 항상 정상적으로 작동하는 시스템 도입을 목표로 한다. 드론과 인터넷 전문은행이 상용화되면서 민간에도 보안 시스템 도입이 확대되고 있다. 보안 교육도 철저히 시행되고 있다. 해킹과 시스템 문제가 발생해도 인명사고는 허용할 수 없다는 원칙을 가지고 있다. 스마트 기기자체에 보안 기능을 추가하게 되면 내부 시스템이 복잡해진다. 에러발생의 원인이 된다. 처음부터 설계를 어떻게 할지 고민하지 않으면 위험 현상이 지속적으로 발생할 수 있다. 초기 단계부터 이 점을 고려하여 제작해야 한다.

■ 제4차 산업혁명 시대의 사이버 보안 문제
: 인터넷 연결된 기기는 모두 해킹이 가능하다

- PC 모뎀으로 인터넷을 연결하던 시절이 있었다. 지금은 전국 곳곳에 와이파이가 설치되어 언제 어디서든지 스마트 기기로 인터넷 연결이 가능하다. 인터넷 연결이

용이해지는 만큼 개인 정보유출이 빈번하게 일어나고 있다. 최근 외국 보안업체가 개인정보 유출사고에 대한 통계자료를 발표하였다. 전세계 10대 개인정보 유출사례 중 4건이 한국에서 발생하였다. 개인정보 유출사례가 속출하다보니 대중들은 문제의식을 잃은지 오래다. 그러나 개인정보 유출은 2차 피해로 직결된다. 보이스피싱이 대표적인 피해의 예다. 상대방이 자신에 대해 속속들이 알고 있기에 피해자들을 설득하기 쉽다. 우리나라는 인터넷 뱅킹 시스템이 잘 구축되어 있어 인증번호 정보 하나로도 30분 이내에 통장의 모든 금액을 인출할 수 있다. 대부분 인출 시도는 현금 인출 안내문자가 전송되지 않는 새벽 2~3시경에 일어난다. 통장 잔액 인출 사고가 빈번하게 일어나고 있으나 피해자들이 손해배상을 청구하거나 사고를 신고할 수 있는 경로가 제한되어 있다.



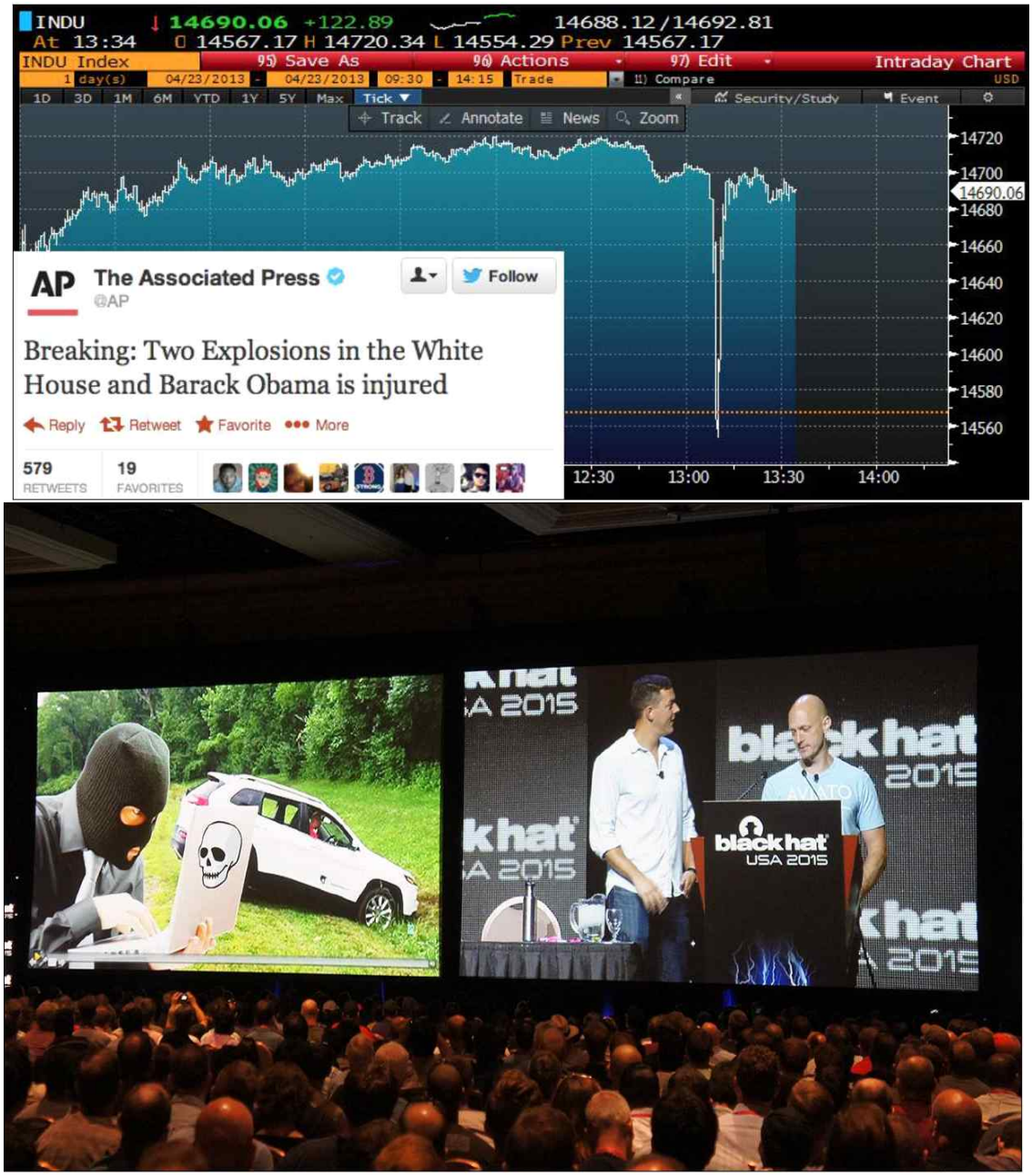
- 제4차 산업혁명 시대로 진입하면서 인터넷과 연결되지 않는 기기는 전무하다. 사이버(Cyber) 공간과 물리적(Physical) 공간이 연결된 Cyber Physical 시스템의 지배를 받고 있다. 세탁기, 냉장고, 자동차 등 250억 개의 기기들이 연결되어 작동하고 있다. 이 기기들은 해커들의 공격대상이다. 이전에는 해커가 기기를 하나씩 해킹하였으나, 이제는 무선 공유기 자체만 해킹하면 된다. 방치되어 있는 공유기가 워낙 많아 무심코 와이파이를 연결하였다가 기기에 저장된 개인 정보, 통화내역과 문자 내용이 유출될 수 있다. 오늘날 해커들은 'Hack Everything'을 좌우명으로 삼아 손쉽게 수많은 개인정보를 입수하고 있다. 해킹을 인터넷 개인정보 유출사고 수준으로만 이해하니 사이버 법안 효용범위가 협소하다. 개인정보 유출의 경로와 규모를

제대로 파악해야 하며 시대에 맞는 정책이 필요하다.

■ 스마트 TV, 자율주행 자동차, 스마트폰 해킹 사례
: 보안 기능이 갖춰지지 않으면 시장에서 경쟁력을 잃는다

- 잡지 『Bloomberg』 2015년 기사 'Hackers to Target Smart TV Sets After Phones, Kaspersky predicts'에서 스마트 TV가 해킹, 감시, 사기의 수단으로 사용될 수 있다고 주장했다. 당시 스마트 TV 개발 업체에서는 "스마트 TV와 인터넷이 연결되면 해킹이 용이해져 사건, 사고 발생 가능성은 있으나 당장 현실화되기는 어렵다고 입장을 밝혔다. 전원이 연결되어있는 스마트 TV는 배터리 제약이 있는 스마트폰보다 해킹이 용이하다. 스마트 TV에 부착된 카메라와 스피커로 촬영과 녹취가 가능하다. 스마트 TV는 CCTV로 이용될 가능성이 높다는 문제가 제기되자 국내 스마트 TV 제작업체는 카메라를 탈부착 형태로 바꾸기도 했다. 업체들은 리스크 전가(Risk Transfer) 전략으로 스마트 TV로 인해 발생하는 위험은 고객이 감수해야한다는 입장을 취했다.
- 해커는 리버싱(Reversing) 기술로 스마트 TV의 내부구조를 파악하여 취약점을 찾은 후 해킹코드를 만든다. 티비싱(Tvshing)은 단어 TV와 피싱이 결합된 용어로, 보이스피싱보다 더 큰 피해를 일으킬 것으로 보인다. 2013년 4월 23일 미국 AP통신 트위터 계정 해킹사고가 발생하였다. "Breaking: Two Explosions in the White House and Barack Obama is injured"가 속보로 AP통신 트위터에 업데이트 되었다. 순간적으로 나스닥 주가가 폭락하였다 상승하였다. 국내 연구기관에서 이 사례를 스마트 TV에 적용해 보았다. 방송사를 직접 해킹하여 송출을 시도할 경우 스마트 TV화면 자체 조작이 가능하다. AP사례가 보여주었듯이 오보는 주식을 요동치게 하는 파급력을 갖는다. 국내 속보 자막이 해커들에 의해 조작될 경우 같은 결과가 초래될 수 있다. 홈쇼핑 방송화면에서 주문번호만 조작하여도 개인정보 도용은 물론 상당 규모의 피해액이 발생할 수 있다. 스마트 TV의 개인정보 유출 및 도용 방지를 위해 기업과 정부의 철저한 관리가 필요하다.

- 제4차 산업혁명 시대에 대두되고 있는 유망 기술 중 하나는 자율주행 자동차(Connected Car)이다. '블랙햇 USA 2015'에서 한 유명 해커가 노트북으로 최신형 차를 해킹하여 조종하는 모습을 보여주었다. 자율주행 자동차는 도로주행에 필요한 정보를 통신기능으로 확보한다. 새롭게 도입된 인포테인먼트(Information과 Entertainment의 결합) 시스템이 통신기능을 갖추고 있으며, 해커들은 이 시스템을 매개로 자동차 내외부의 통신망을 조작한다. 미국에서는 자동차 자체를 제어하고 보안을 강화하기 위해 10년 R&D 사업에 착수했다. 'Government Vehicle'이라는 대응책을 정부가 직접 마련하고 있다. 보안기능이 탑재되지 않은 국내 자동차는 미국 시장에서 경쟁력을 갖지 못 하여 실패할 확률이 높다.



- 심장박동 조절장치는 심장에 이상이 있거나 심장박동이 불규칙적일 때 전기 충격을 주어 박동 수를 조절한다. 'Homeland' 라는 미국 드라마에서는 심장박동 조절장치를 조작하여 정치인을 암살하는 장면이 등장한다. 장치의 일련번호를 입수하지 않아도 원격으로 장치 조정이 가능하다. 비록 드라마의 한 장면이지만 현실가능성이 높다. 미국 정부는 의료기기에 대한 사이버 보안 강화에 투자하고 있다.
- 2013년 미국 조지아공대에서 충전기로 아이폰이나 아이패드를 해킹하는 방법을 알아내었다. 단자를 연결하면 악성코드가 아이폰 안으로 유입된다. USB 포트를 이용해 전자담배를 충전할 때도 마찬가지로 악성코드가 컴퓨터에 유입될 수도 있다. 컴퓨터는 어떤 기능을 실행하느냐에 따라 CPU에서 각기 다른 소음이 발생한다. 이

때 스마트폰은 그 소음을 감지하여 컴퓨터가 무엇을 시행하고 있는지 알 수 있다. IoT(사물인터넷) 기기들이 보안관련 문제들을 일으킬 가능성에 대해 정부 대책 마련이 시급하다. 스마트폰 해킹을 감지할 수 있도록 최소한의 장치를 마련해주는 등의 조치를 취해야 한다. 한국과 일본이 스마트 가전시장의 선두주자라 하더라도 보안 기능을 제대로 갖추지 못하면 미국 시장에서 경쟁력을 잃는다. 미국의 보안관련 법률은 강화되고 있다. 정보 보안 보호대상이 단순 개인정보에만 제한되었던 Information Security에서 Cyber Defense로 확대되어야 한다. 전략전술개념으로 접근하여 사이버를 활용한 모든 것에 대한 법안을 마련해야 한다.

■ 보안(Security)에서 정보 보증(Information Assurance)으로 : 개인 정보 보증을 위한 대책 마련 필요

- 현존하는 250억 개의 개인 정보를 사람이 관리하기에는 인력이 부족하다. 개인정보 관리를 최대한 자동화로 대체해야 한다. 보안 시스템만큼이나 자동화 방식도 중요하다. 미국은 3년 안에 자동으로 취약점을 찾아내는 인공지능을 보급할 예정이다. 자동 업데이트 시스템까지 갖춘 시스템을 향후 10년 내에 개발하고자 한다. CISCO는 IoT 시대에 대비하여 개인정보 관련 업무를 자동화하겠다는 포부를 밝혔다. 사이버 보안 피해방지와 대책 측면에서 미국과 한국은 10년 이상의 격차를 보인다. 미국 PAYPAL의 개인정보유출사고 발생확률은 하루 0.4%로 높은 편에 속한다. 반면, 우리나라 인터넷뱅킹의 사고 발생확률은 0.0009%다. 한국의 사고 발생률은 현저하게 낮으나, 사고에 대한 손해배상 사례가 전무하다. 즉 방지대책은 잘 구축되어 있으나 복원력이 약하다. PAYPAL은 반대로 방지는 약하지만 복원력이 뛰어나 사고에 대한 손해배상과 대책마련이 빠르고 철저하다. 부실한 관리는 처벌받아 마땅하다. 공격 중에서는 미리 방지가 어려운 공격들이 있다. 취약점 노출 시 대중의 질책이 거세져 이러한 취약점들을 기업에서 미리 정부에 보고하도록 유도하고, 손해배상 대책 마련을 위한 동기 부여도 필요하다.
- 미 국방부에서 'Hack the Pentagon' 대회를 개최하였다. 펜타곤 정보 시스템의 전체 취약점을 찾아내는 대회이다. 시작 13분 만에 한 팀이 전체 취약점 1,180개 중 138개가 위험하다는 해킹 결과를 보고하였다. 대회 시작과 동시에 찾아낸 것이 아니라 이미 알고 있던 사실을 제출한 것으로 밝혀졌다. 공개적으로 발표를 안 할 뿐 해커들은 미 국방부 해킹 경로와 취약점을 파악하고 있다. 미 국방부가 오히려 취약점을 스스로 밝히고 대책을 함께 마련하고자 하는 자세와는 다르게 우리나라 정부와 기업은 취약점을 숨기려 한다. 제4차 산업혁명 시대의 해킹 경로, 보호 대상인 개인 정보가 무궁무진하기에 소수 인력으로 해결이 불가능하다. 패러다임 전환이 필요하다.
- 미국 국가안전보장국(National Security Agency, NSA)의 구인공고 팜플렛을 살

펴보면 정보 보증(Information Assurance) 인력을 채용한다. 정보 보증 학위 수여자 중 우수한 성적을 거둔 학생에게 장학금과 인턴십 기회가 주어진다. 미국은 1998년 이후 정보를 보안하는 단계에서 정보 안전을 보증해주는 단계로 발전하면서 정보 보안(Information Security)을 정보 보증(Information Assurance)이란 표현으로 대체되었다. 정보 보증은 1996년 세계 최초 사이버전인 걸프전을 계기로 처음 표준화되었다. 보안 공학(Security Engineering)연구자들은 무기체계에 들어가는 DARPA'S HACMS(High Assurance Cyber Military Systems) Technology 소프트웨어를 개발하고 있다. 미국에서는 이미 작년부터 사이버 무기의 정의 및 평가 지침이 하달되어 평가가 시행되고 있다. 레이다, 드론, 무인장치를 포함하여 네트워크와 연동된 모든 무기체계는 군부대의 성능테스트로 검증을 받아야 한다. 우리나라는 사이버 무기 평가 체계도 잡혀있지 않고, 인프라도 전무하다. 지금부터라도 연구를 시작해야한다. 허나 실험실과 교육평가제도가 National Cyber Range 하에 완벽하게 갖추어진 미국을 따라잡기 쉽지 않다. 선제적으로 우리나라가 대응하지 못하면 뒤처지기 마련이다. 사이버 테러는 이미 발의되었으나 모두 좁은 시야로 문제를 지켜보고 있다.

- 미국은 신뢰성을 보안의 기준으로 삼는다. 항상 정상적으로 작동하는 시스템 도입을 목표로 한다. 드론과 인터넷 전문은행이 상용화되면서 민간에도 보안 시스템 도입이 확대되고 있다. 보안 교육도 철저히 시행되고 있다. 해킹과 시스템 문제가 발생해도 인명사고는 허용할 수 없다는 원칙을 가지고 있다. 스마트 기기자체에 보안 기능을 추가하게 되면 내부 시스템이 복잡해진다. 에러발생의 원인이 된다. 처음부터 설계를 어떻게 할지 고민하지 않으면 위험 현상이 지속적으로 발생할 수 있다. 초기 단계부터 이 점을 고려하여 제작해야 한다.

241회 정책세미나 질의응답

질문1 북한의 한국 정부 해킹 사례는 빈번하게 보도되지만, 역으로 우리나라가 해킹하는 사례는 왜 보도되지 않는 이유는 무엇인가?

답변 사이버테러방지법의 비례적 대응 전략 관점에서 살펴봐야 한다. 우리나라는 인터넷의존도가 높아 하루 사이버 공격받는 수가 평균 100만 건에 이른다. 북한은 인터넷 인프라가 잘 구축되지 않아 보복공격을 치를 곳이 없다. 국정원과 한국인터넷진흥원 중심으로 북한 해킹에 대응하고 있으나 인력이 부족하여 전부 막을 수가 없다. 사전 조치를 충분히 취하고 있으나 북한 인터넷에 대한 정보가 부족하다.

소니 픽쳐스가 해킹사건의 배후로 북한을 지목하였다. 일간지에서 청문회자료를 입수하여 발표하였다. '북한 시스템에 해킹 프로그램을 숨겨놓아 북한 정부에서 오고가는 대화들을 전부 듣고 있다'는 식으로 보도했다. 허나 이 모든 정보를 미국

NSA에서 입수한 것은 아니다. 한국이 포함된 동맹 국가로부터 정보 지원을 받는다. 우리나라 역시 북한 해킹 프로그램이 마련되어 있다. 북한 정부는 1700명의 해커들이 활동 중이며 해커 지원 인력이 5000명에 육박한다. 우리나라는 30명이 전부다. 인센티브를 도입하여 지원 인프라를 개발해야 한다.

질문2 **우리나라 사이버 무기체계는 어떻게 구축되고 있는가?**

답변 국방부에서 사이버 무기에 대한 정의를 내렸다. 미국은 안보와 관련된 모든 정책을 군부대에서 이끌고 책임진다. 우리나라는 국가정보원이 이끌고 있다. 국내 군부대의 사이버 무기체계는 매우 열악한 상황이고, 예산도 최근 삭감되었다. 전쟁에 대한 인식을 미국처럼 전환하여 사이버 무기 관련 예산을 국방부에서 확대해야 한다. 국방부 내에서 연구 체제가 하루빨리 구축되어야 하고, 일정 수준 이상의 민간 기관과 협력하여 기술력도 발전시켜야 한다.