

# 北, 통신線 연결 안돼도 ‘電波로 해킹’ 연구 중… 한국軍도 뚫릴 가능성

〈전파〉

## 세계는 사이버전쟁중(下)

북한의 사이버 공격 기술이 고도화되는 가운데 그동안 정부와 군(軍)이 절대 뚫리지 않는다고 공언해온 내부망(인트라넷·Intranet)마저 북한 해커에게 가까운 시일 내에 뚫릴 가능성이 크다는 지적이 나왔다. 사이버전 전열(戰列) 재정비가 시급하다는 것이다.

보안이 최우선인 군과 원전 등의 전산망은 외부의 인터넷망(網)과 아예 통신선(線)을 분리한 인트라넷을 사용한다. 해커가 들어올 출입문을 없앴으니 안전하다는 것이다. 하지만 최근 통신선이 연결되지 않아도, 소리, 열(熱), 빛 등으로 데이터를 주고받는 최신 기술이 등장했다. 전문가들은 기술적으론 인트라넷에 대한 사이버 테러가 가능해졌다고 보고 있다.

고려대 사이버국방학과 윤지원 교수팀은 지난 17일 인터넷에 접속하지 않은 두 대의 PC에서 자료를 전송하는 기술을 시연했다. 컴퓨터의 내부 정보를 소리로 바꿔 스피커로 내보내고, 다른 컴퓨터의 스피커에서 음성 신호를 인식해 다시 데이터로 바꾸는 방식이다. 윤 교수는 “기술적으론 망을 분리해도 해커가 침입해 시스템을 장악하는 공격이 불가능한 일은 아니다”고 말했다.

실제로 북한은 몇 년 전부터 ‘광자기 도파기’라는 인트라넷 해킹 기술을 연구하고 있다. 광자기 도파기는 광(光)케이블의 배선 근처에 갖다놓으면, 케이블 안에 흐르는 데이터를 미세한 전파 신호로 바꿔 인



이태동 기자

지난 17일 서울 고려대 인촌기념관에서 열린 정보보호 콘퍼런스에서 윤지원 교수 연구팀이 외부 인터넷과 차단된 컴퓨터를 해킹하는 모습을 시연하고 있다.

### 北, 新해킹기술 연내 성공 목표 보안 위해 외부 인터넷망과 아예 통신선을 분리한 ‘한국軍 인트라넷’ 뚫기 혈안

### 한국, 컨트롤타워도 부재 사이버 안보비서관 올해 초 신설했지만 부처간 異見에 제 역할 못해

라넷에 접속한다. 탈북자인 김흥광 NK지식인연대 대표는 “올해 말까지 광자기 도파기 연구과제를 성공한다는 게 북한의 목표”라며 “쉽지 않은 기술이라 연내 개발은 실패할 수도 있지만, 북한이 인트라넷을 표적으로 한다는 건 분명한 사실”이라고 말했다.

북한은 전 세계적으로 인트라넷 공격용 바이러스로 악명 높은 스텑

스넷(Stuxnet) 기술도 확보한 것으로 알려졌다.

하지만 이 같은 상황에 대응해야 할 우리 정부는 사이버 전쟁 발발 시 이를 지휘할 사령부조차 제대로 꾸리지 못하고 있는 실정이다.

정부는 지난 3월 사이버 전쟁에 대응하는 컨트롤타워 역할을 목적으로 청와대 국가안보실에 사이버 안보비서관을 신설했지만 국정원 등 관련 부처의 반발과 법령의 미비로 역할을 제대로 수행하지 못하고 있는 것으로 알려졌다.

정부 소식통은 24일 “지난 5월 국가안보실 주관으로 국정원, 군, 경찰, 미래부, 행자부 등 13개 부처 고위 관계자들이 모여 청와대 국가안보실을 사령탑으로 정부 여러 부처가 역할을 분담해 사이버전 대응을 강화하는 방안을 논의했다”고 말했다. 이 소식통은 “하지만 국정원 측이 법적 근거가 부족하다는 이유 등으로 강력 반발해 회의가 유야

→ 인트라넷(Intranet)  
군(軍)이나 기업 등이 내부 직원들만 접속해 쓸 수 있도록 만든 자체 인터넷망(網)이다. 외부 인터넷망과 연결된 물리적인 통신선(線)을 없애 해커 입장에선 출입문에 도달할 수 없어 해킹으로 문을 따는 행위 자체가 성립되지 않는다. 하지만 최근 통신선이 아닌 소리나 빛 등을 이용해 내부 정보를 빼내는 첨단 기술이 속속 등장하고 있다.

무야뚼으며 국가안보실의 개선 방안 추진도 지지부진한 상태”라고 말했다.

현재 우리 정부의 사이버전 대응은 국정원 국가사이버안전센터가 총괄 책임을 맡고 있다. 사이버 안보 비서관을 신설하면서 청와대를 사령탑으로 하고 국정원·군·경찰 등이 역할을 분담하는 방안을 추진했지만 국정원의 반발에 부딪혀 진전이 없었다는 것이다.

전문가들은 그동안 국정원이 맡아온 것은 개별 사건에 대응하는 ‘사이버 안전’ 차원이었으며 국가 전체 차원에서 접근하는 ‘사이버 안보’는 청와대가 컨트롤타워 역할을 하는 것이 바람직하다고 했다.

유용원 군사전문기자·성호철 기자

### 사이버전 국제 교전규칙 ‘탈린 매뉴얼’

특징: 사상 첫 사이버전 국제 교전규칙 (법적 구속력은 없음)

경과: 2007년 에스토니아 전체 인터넷이 2주간 마비된 사건을 계기로 수도 탈린에 세계 전문가들이 모여 사이버전 교전규칙 3년 이상 논의, 2013년 3월 발간.

구성: 총 7장 95개 규칙

주요 내용
-피해국은 가해국에 대해 비례적 대응 조치 가능
-무력 공격 수준의 사이버전 피해국은 고유의 자위권 행사 가능
-자위권 차원 무력 행사 시 필요성과 비례성 조건 충족해야
-자위권 차원 무력 사용권은 사이버 무력 공격 시 또는 임박 시 발생
-UN헌장 제51조에 따른 자위권 행사 국가는 UN 안보리에 즉각 보고해야

※우리나라는 아직 사이버전 교전규칙, 작전예규 등이 없는 상태

### 인트라넷 해킹 시연

## ‘사이버戰 전사’ 천재 해커들, 국정원 가기 꺼려

〈戰士〉

사이버 전쟁에서 가장 중요한 무기는 해커다. 사이버전은 그 특성상 최고 수준의 해커 한 명이 수백명의 해커 부대와 맞서 비등한 전쟁을 치를 수 있기 때문이다. 현재 우리나라 최고 해커는 병역 특례 중인 이정훈(22)씨로 알려져 있다. 2년 전 세계적인 해커들이 참가하는 해킹 올림피아드 ‘테프콘’에서 3위를 차지, 세계 해커계에 이름을 알렸다. 올 3월 구글(웹브라우저 크롬)·애플(사파리)·마이크로소프트(익스플로러 11)를 차례로 모두 해킹했다. 이전까지 십여명씩 모인 세계 최고 해킹팀도 해내지 못한 일을 단독으로 뚫어 화제가 됐다. 이정훈씨가 뚫은 해킹 경로는 구글 등에 전달돼 취약점을 보완하는 데 쓰였다. 해킹계에선 ‘차세대 세계 최고 해커 후보 중 1인’으로 꼽힌다. IT 업계에선 올 10월 병역 특례가 끝나는 이씨를 영입하기 위해 국가정보원이 나섰다

### 해킹과 무관한 일 시키거나 정식 입사 직원과 승진 차별 ‘차세대 톱 해커’ 이정훈 국정원 대신 삼성 선택

문이 무성했지만 이씨는 결국 삼성에 입사하기로 했다.

사이버 전쟁의 최전선인 군(軍) 사이버사령부와 국가정보원은 이씨와 같은 최고 수준의 화이트 해커(사이버 공격을 방어하는 선의의 해커)를 확보하지 못해 발을 구르고 있다. 15년 차 해커인 심준보씨는 “사이버사령부에 소속된 해커 부대 500여명은 해커 입장에서 보면 제대로 된 해커로 볼 수 없다”며 “이미 만들어진 해킹 도구를 활용해 공격하는 수준이기 때문”이라고 말했다.

해커들이 정부로 가길 꺼리는 이유는 사이버사령부·국정원과 같은

일선 부처에선 사이버전(戰)의 핵심 전력인 해커라면서도 입사하면 해킹과 상관없는 업무를 맡기거나 정식 입사한 직원과 차별하기 때문이다. 한 해커는 “국정원 같은 데서 일해보야 어차피 우리 같은 해커는 승진도 잘 안 된다”고 했다.

급해진 정부는 최근 화이트 해커 육성 계획을 내놔야. 실력이 뛰어난 해커 영재의 경우 수능 성적과 상관없이 고대 사이버국방학과 등 3개 주요 대학에 입학할 수 있게 했다. 사이버국방대학을 졸업하면 장교로 임관, 7년간 의무 복무토록 해 사이버 전력의 중추를 맡긴다는 것이다.

사이버국방학과 김승주 교수는 “군에 복무할 때도 단지 조금 장교라는 계급에 국한돼 단순 반복 업무만 시킬 것이 아니라 이들에게 충분한 자극이 되도록 다양한 과제를 부여할 필요가 있다”고 말했다.

성호철·박순찬 기자

## 국회서 잠자는 ‘사이버 테러 방지법’

### 野, 사생활 침해 우려로 반대

세계 각국이 사이버 공간에서 날마다 치열한 전쟁을 치르고 있지만 우리는 사이버 안보에 관한 기본 법률조차 없는 상태다. 현재 국내 사이버 안보 관련 법제는 대통령 훈령으로 만든 ‘국가사이버안전관리규정’이 전부다. 그나마 사이버 위기 상황 전파 등에 관한 내용 위주여서 실질적 응전(應戰)에는 미흡하다는 평가다. 정부 관계자는 “정보통신기반보호법 등에 사이버 안전 관련 규정 이 산재해 있지만 이는 일상적인 정보 보호에 중점을 둔 것이어서 치

명적이고 전문적인 북한 해커들의 공격에 대응하기에는 역부족”이라고 말했다.

국회에는 ‘사이버테러방지법’이 계류 중이지만 야당이 개인 사생활 침해 우려 등의 이유로 처리에 반대하고 있다. 17~18대 국회 때도 비슷한 법안이 제출됐지만 여야, 관련 기관 간 입장이 대립하면서 국회 임기 만료와 함께 자동 폐기됐다.

공안 당국은 사이버전에서 우위를 점하기 위해서는 통신 사업자에게 감청 장비 설치를 의무화하는 통신비밀 보호법 개정안도 반드시 통과돼야 한다는 입장이다. 북한과 연결된 국내

대공(對共) 용의자 수사를 위해 합법적 감청이 필요하다는 것이다.

현행 통합방위법을 손봐야 한다는 지적도 있다. 이 법에는 군이 ‘영토, 영공, 영해를 수호한다’고 돼있지만 사이버 공간은 포함돼 있지 않다. 미국의 경우 주요 기반 시설을 겨냥한 사이버 공격에 대비한 ‘사이버안보보호법’, 사이버 전쟁 시 민간 협력을 규정한 ‘사이버안보강화법’ 등 5개 관련 법률을 제정·시행하고 있다. 일본도 작년 11월 사이버 전쟁 시 정부·기업·개인 등 주체별 책무를 규정한 ‘사이버시큐리티기본법’을 제정했다.

황대진 기자

〈광고〉대한의사협회 의료광고심의필 140618-중-60827

# 골반·엉치 통증은 안강병원에서!

골반 및 엉치 통증을 비수술로 바늘을 이용한 ‘FIMS’로 치료

### ▶ 안강병원 치료는, 골반 엉치 통증의 여러 원인 중에 허리부터 먼저 살펴서 치료

**골반통증** | 배꼽 아래 부분의 통증을 통칭하며 골반통증은 자궁, 난소, 요도, 성기 등 장기의 문제로 인해 통증이 생기는 경우와, 원인을 모르는 경우도 많습니다. 원인을 모르는 골반통의 상당수는 근골격계의 문제때문에 발생합니다. 요추가 흔들리면서 골반으로 이어진 신경이 마찰돼 골반통증이 생기는 경우가 많으며, 그 중에서도 허리 윗부분의 척추나, 골반을 지나는 신경, 혈관의 문제인 경우가 많습니다.

**엉치통증** | 엉덩이 부위의 통증을 말하며, 대부분 허리의 병 때문에 생기는 경우가 많습니다. 조금만 걸어도 엉치가 아파 허리가 저절로 구부러지고, 허리를 펴려고 하면 ‘악’ 소리가 납니다. 엉치통증이 지속 되면 허리가 굽고, 팔자 걸음이 될 수도 있습니다. 허리를 지나 엉치로 가는 신경은 특히 마찰이 잘되며, 엉치통증을 유발하는 신경은 여러개가 있습니다. 골반통증은 신경보다는 내부 장기에 문제가 있을 가능성이 더 높은 반면, 엉치통증은 허리를 지나는 신경에 문제가 있는 경우가 많습니다. 따라서 골반·엉치통증은 어디가 문제인지를 확인하는 것이 치료의 첫걸음입니다.



### ▶ 안강병원은 골반·엉치 통증을 MRI와 더불어 촉진(손으로 느껴서) 진단

골반통증은 여러원인에서 비롯됩니다. 허리, 내장, 고관절, 근육 등 여러 부위의 문제를 고려해야 정밀한 진단을 할 수 있습니다. 안강병원은 우선 고관절이 움직이는 범위를 체크하여 무엇이 문제인지를 파악합니다. 사타구니쪽을 지나는 근육을 통해서는 힘줄이나 근육이 손상됐는지를 알 수 있는 경우가 많고, 허리를 만져보면 척추의 병을 알 수 있는 경우가 많고, 하복부를 만져보면 내장에 문제가 있는지를 알 수 있는 경우가 많습니다. 엉치통증은 대부분 허리에 관련된 신경의 문제가 많으므로, 안강병원에서는 허리 문제를 우선적으로 생각합니다. 허리를 지나서 엉치로 가는 신경은 흔히 마찰이 심해 문제를 많이 일으킵니다. 허리를 지나는 신경은 주로 다리를 향하지만, 일부 신경은 엉치나 고관절 부위를 지배합니다. 이런 경우, 안강병원에서는 MRI 검사와 더불어 손으로 직접 만져보고, 움직임을 살펴서 문제가 있는 신경을 찾아내고 있습니다. 안강병원은 촉진과 문진을 통해 진단하고 영상촬영은 이를 확인하는 도구로 활용합니다.

### ▶ 특수 바늘로 골반·엉치 통증을 치료하는 안강병원의 비수술적 치료인 ‘FIMS’

‘FIMS’는 비수술 통증 치료법입니다. 신경이나 힘줄, 관절의 움직임에 방해를 주는 요소를 찾아내어 특수 바늘로 유착된 조직을 박리하고 신경, 힘줄, 관절이 잘 움직이게끔 도와줍니다. ‘FIMS’는 병변이 되는 원인을 치료하고, 현류를 증가시켜 조직의 재생 및 조직의 강화를 유도하여 재발을 막는 치료법으로 추정됩니다. 또한 비수술, 비절개로 치료하여 흉터 문제가 거의 없습니다. (단, 시술 후 일시적인 어지러움, 구토, 오심, 통증이 있을 수 있습니다.)



**안강병원**  
신로 내과 척추 관절

**상담 예약 1899-3210**