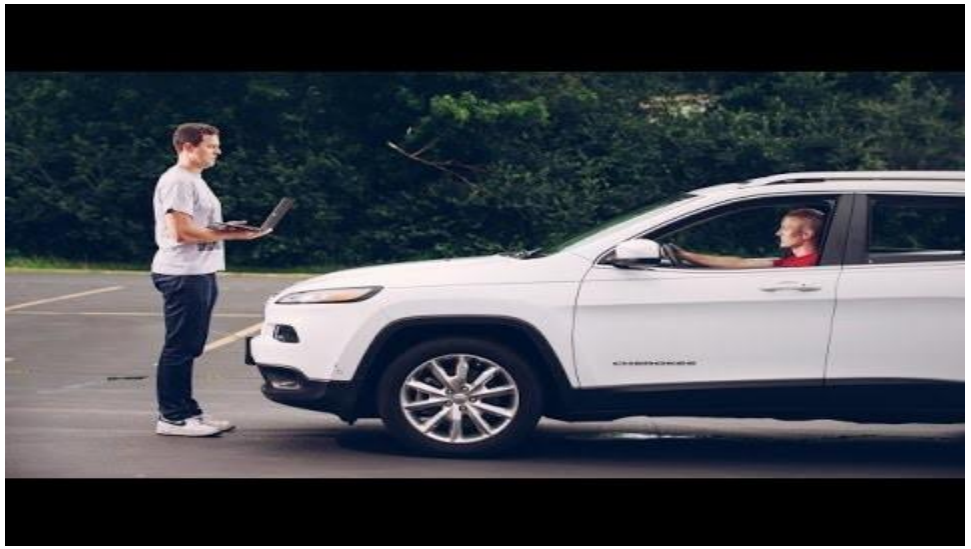
해킹수사의 헌법적 한계

박경신

kyungsinpark@korea.ac.kr

www.opennet.or.kr 이사

해킹이란 무엇인가? http://youtu.be/MK0SrxBC1xs



악성코드를 심는 방법

- 사회관계의 이용 – 익숙한 발신자로 가장한 메일 보내기
  →국정원이 예를 들어 한국전력을 가장하는 경우 사회적 신뢰의 문제
- 웹페이지 감염 – 악성 이미지파일 등을 통해 방문만으로 감염
  → 감시대상이 아닌 사람들도 방문만으로 감염
- 중간자 공격 – 특정URL에 대한 신청을 중간에서 가로채서 악성코드에 감염된 파일을 제공함. 웹브라우저 플러그인 등의 형태로 제공됨.
  → 암호화되지 않은 웹 트래픽을 감시하게 됨
- 직접 탈취 – 기기를 비밀리에 탈취하여 코드를 심고 반환함.

해킹수사의 해악

- Privacy International and Open Rights Group (진보넷-GCHQ 소송 → Equipment Interference Code of Practice→)

1. 한번 감염된 기기는 누구든 기술만 있다면 이용할 수 있음. (비교: 집에 침입하면서 잠금장치를 부숴놓고 누구나 볼 수 있는 CCTV를 설치해놓고 가는 것)
2. 감염기기에서 발견된 증거의 신빙성 문제 – 제3자침입가능성
3. 악성코드가 감염기기에 보관된 다른 파일들을 손상시키며 발생하는 재산권 문제
4. 악성코드 배포를 통제하지 못하는 문제. 피싱메일이나 감염 URL링크가 포워드되는 경우 등등 → 인터넷 전체의 보안을 위협
5. 보안상 결함 시장의 형성 – 정보기관들이 “Zero-day”결함을 구매함. → Hacking Team: 다수의 Zero-day보유.

해킹수사 허가 요건 I:

- Privacy International and Open Rights Group

1. 중대한 범죄나 국가안보에 대한 구체적 위험이 발생했거나 발생할 확률이 높은 경우에만 → 감청보다 더 높은 기준 (미국 텍사스 연방지법 2013년 결정, 2008년 독일연방헌법재판소 판결)
2. 위 범죄나 안보위협의 증거가 해당기기 접근을 통해 취득될 확률이 높은 경우에만.
3. 정보수집은 위 2의 증거로만 한정되도록 하기 위한 조치 필요
   - 영장 상의 명확한 적시 및 범위초과수집 시 수집된 증거 전체 무효화 (최근 2015/7/27 대법원 판결).
4. 다른 방식의 증거수집이 불가능할 때만.

해킹수사 요건 II:

5. 감염기기의 보안수준을 저하시키는 방식은 지양해야함.

6. 기간은 1개월 이상이 되어서는 안되며 해킹종료시 상대방에게 통지해야 함. 영장발부 판사가 진행상황에 대한 정기적인 검토.

내국과 외국의 구분은 무의미함. 외국인의 서버에 내국인의 정보가 포함될 수 있으며 외국통신망의 해킹을 통해 내국인의 정보를 탈취할 수 있음. 동일한 기준이 적용되어야 함. 특히 외국인에 대한 감청이 쉽게 허용되면 이를 겉으로 내세우면서 내국인감청이 이루어지는 경향

7. 해킹활동에 대한 독립적인 감독기구 설립

해킹수사 요건 III

8. 상호법적지원협약(MLAT) 절차를 우회하는 방식으로 이용되어서는 아니됨. → 해외소재기기의 감염에 대해서는 해당지역 법원이 발부한 영장이 필요함. 국내소재 외국인? → "내국인 끌려들어가기" 문제의 회피

9. 취득된 정보는 영장이 적시한 목적으로만 이용되어야 함.

10. 전세계의 부당한 해킹피해자의 손배청구권 보장 – 해킹대상에 대한 통지의 중요성

법률개정의 필요성 – 행정입법으로는 통제를 할 수 없음

독일 2008년 “연방트로이목마” 사건

- 테러리즘 수사를 위한 Trojan코드 이용

- “정보기술시스템의 비밀성과 무결성에 대한 헌법적인 권리”의 창설
- 근거: 정보기술시스템은 개인의 가장 은밀하고 민감한 정보저장
- 근거: 정보기술시스템을 통해 통신상대방의 프라이버시도 침해
- 근거: 클라우드나 통신기기를 중심으로 삶이 집중적으로 구조화
- 범위: 사물인터넷 – 특수목적기계도 일반정보저장 기능 수행
- 결정: 해킹은 감청 보다 더욱 높은 기준을 충족하는 경우에만 허용되어야 함. 현재의 법률은 그러한 기준을 충족시키지 못함. → 실질적으로 해킹을 금지함.

미국연방 텍사스지법 2013

- 해외IP주소로부터 금융사기 공격 → “해킹” 압수수색영장 기각
- 근거: 영장은 법원관할 내에서만 적용됨. 해외에 있는 컴퓨터를 감염시키는 것은 불가능. 역외영장은 테러리즘 수사를 위해서만 허용됨.
- 근거: 해당IP주소의 컴퓨터가 범죄용인인지 알 수 없음 (VPN, Proxy Server) → 영장의 구체성
- 근거: 카메라 원격가동기능을 포함하면 압수수색이 아니라 감청 영장이 필요함. (최근 국정원의 “해킹은 감청과 다르다 " 는 설명과 배치됨)

통신감시에 대한 국제인권원칙 - www.necessaryandproportionate.org

- 전세계 400여 단체가 서명
- UN 인권이사회 보고서에서 언급
- UN 표현의자유특별보고관 보고서에서 언급
- 국내감시와 국외감시 모두 영장주의 적용
- 통신의 내용 감시 = 통신사실확인 감시 = 통신자신원 감시에 모두 영장주의 적용
- 영장주의 내용의 핵심: 피감시자에 대한 통지, 감시수행자에 대한 독립적인 감독기구, 법원에 의한 영장발부

국내의 입법과제

1. 해킹수사에 대한 별도 입법
2. 통신비밀보호법 상의 피감시자 통지 (17건 기 발의)

- 수사종료 후→ 감시종료 후

3. 통신자료제공제도 개선 (10건 기 발의)

- 통신상대방을 보호할 필요
- 통신자 신원정보를 비밀로 인정할 필요

http://www.huffingtonpost.kr/kyung-sin-park/story_b_7883654.html