ITU: ICT 분야와 사이버공간의 신뢰 구축 (ITU: Building trust in ICTs and cyberspace)

ITU 는 2014 년 말까지 인터넷 사용인구가 거의 30 억 명에 달해, 정보통신 접근의 새로운 가능성이 열릴 것이라고 예상합니다. 그러나 이와 동시에 보안문제와 네트워크·서비스의 취약성으로 인해 사용자들은 어디서든 더욱 치밀해지는 사이버 위협에 노출되고 있습니다. 신분 도용, 스팸, 악성프로그램, 아동 및 여러 취약한 계층들에 가해지는 착취·위해 등은 글로벌 경제에 초래되는 연간 4000 억 달러의 추정 손실을 넘어서, 실제 세계에 심각하고 끔찍한 결과를 초래할 수 있습니다. [1]

정보통신기술(ICT)은 주요 국가 기반구조로 자리잡았기 때문에 지장이 초래되는 경우 필수 서비스의 중단은 참사 수준의 결과를 가져올 수 있습니다. 항상 연결되어 있고, 언제 어디서든 연결할 수 있는 브로드밴드 기술의 특성을 고려할 때, 공격자는 완전히 다른 지역에 있으면서도 한 개 국가 또는 그 이상의 국가들에게 공격을 가할 수 있습니다.

사이버위협은 최고의 기술을 보유한 선진국을 비롯하여 모든 국가들에게 위험요소로 떠올랐습니다. 국제적인 협력 증대는 사이버위협을 완화할 수 있습니다.

증가하는 국제적 위협

- 2013 년 사이버위협 피해자는 약 4 억 명.
- 2013 년에는 표적공격이 91% 증가. 침해 사례는 62% 증가했으며, 모바일 사이버범죄를 경험한 모바일 이용자는 전체의 38%에 해당.
- '개인정보 노출' 사례는 2012 년 9300 만 건에서 2013 년 5 배 이상 급증하여 약 5 억 5200 만 건으로 증가.
- 표적 공격의 위협에 가장 많이 노출된 세 분야는 정부, 채굴업계, 제조업계. (Symantec 2014 Internet Security Threat Report)

모바일 이용자들은 종종 민감한 파일을 온라인에 저장하며(52%), 업무 관련 정보나 개인적 정보를 동일한 온라인 계정에 저장하고(24%), 자주 로그인 및 패스워드를 가족과 공유하거나(21%) 친구와 공유하여(18%) 자신의 데이터와 회사의 데이터를 위험에 노출시킵니다. ITU 파트너사인 Symantec 에 따르면, 이용자 중 단지 50%만이 기본적 보안 조치를 취하고 있습니다.

[1] MacAfee

'사물인터넷(IoT)'이 현실화 됨에 따라, 상호 연결된 수백만 개의 기기들이 사람의 개입 없이도 기기간의 정보를 교환하고 있으며, 물리적 세계와 사이버 세계는 더욱더 밀접해지고 있습니다. ITU 는 글로벌 파트너십 관계에 있는 각 이해관계자들을 하나로 모아 사이버보안 문제 대응을 위한 기술 및 정책 솔루션 제공에 앞장서고 있습니다.

주요 성과 중 하나는 국제 협력 프레임워크인 ITU 글로벌 사이버보안 아젠다(GCA)의 수립입니다. 글로벌 사이버보안 아젠다는 국가들의 사이버위협 대응 지원에 필요한 ITU 의 기술 역량 증대 노력을 촉진하고, 사이버보안 및 기술에 관한 국제 표준을 권고하고, 지식과 공공정책을 논의하는 장입니다.

국가 차원의 사이버 공격 대응

국가 차원의 사이버 공격은 주요 인프라에 큰 위험을 주고, 은행 계좌 접근을 차단하거나 교통망에도 지장을 주고 있습니다. 이 밖에도 정전, 통신 중단 등의 피해를 끼치는 등 국민 생활에 직접적인 영향을 미칠 수 있습니다.

이 때문에 사이버 침해사고 및 공격에 대응할 수 있는 효과적인 제도적 구조가 필요합니다. ITU 는 국가 및 지역 차원의 역량 강화 능력을 효율적으로 활용하고자 회원국들과 지역들, 업계 파트너와 함께 협력하고 있습니다.

ITU 는 폭넓은 트레이닝 및 지원 프로그램을 통해 역량과 전문성을 제고하고 있습니다. 주요 내용은 다음과 같습니다.

- 50 개 회원국이 자국의 사이버보안 준비태세와 대응 역량을 평가하도록 지원합니다. ITU 는 7 개 회원국의 국가컴퓨터침해사고대응팀(CIRT) 설립을 지원했으며, 추가적으로 7 개 국가에 대한 지원을 확정하였습니다.

- 현재까지, 60 개국 이상이 참여한 CIRT 사이버 훈련이 7 차례 실시되었습니다. 이 훈련들은 설립된 CIRT 의 핵심 기능이 국제 표준 및 모범사례와 일치하는지를 평가합니다.

- 국가 사이버보안 전략 수립은 적절한 법적/규제적 프레임워크가 부족하고 사이버위협 파악 및 관리·대응에 있어 인적역량, 전문성, 재정적 자원이 부족한 최빈 개도국들에게는 더욱 쉽지 않은 일입니다. ITU 의 "최빈 개도국의 사이버보안 향상" 프로젝트는 최빈 개도국이 그들의 사이버보안 역량을 강화하여 자국의 인프라 보안 능력을 향상시키고 사회·경제적 혜택을 극대화 할 수 있도록 지원합니다.

- 지역 차원에서는 ITU 지역 사이버보안 센터를 통해 추가적인 지원을 제공합니다. 이 센터는 회원국이 주관하는 센터로서 사이버보안 문제에 대한 ITU 의 지역 포컬 포인트 역할을 합니다. 아랍 지역 사이버보안 센터는 현재 오만에 있으며, 나이지리아에 아프리카 지역 사이버보안 센터가 설립될 예정입니다.

- ITU 는 사이버보안의 법적인 측면에 대해 회원국들의 이해를 높이고자 회원국들의 법적 프레임워크의 조화를 추구하고 이러한 프레임워크가 국제적으로 적용가능하고 상호운용 될 수 있도록 지원합니다.

- 서비스 부문에서 ICT 역할은 보건, 교육, 금융 및 상거래 등 다양하게 확대되고 있으며 이로 인해 사이버 보안 시스템이 완벽히 갖추어진 환경 조성의 필요성이 높아지고 있습니다. 하지만 상대적으로 적절한 자격을 갖춘 사이버보안 전문가는 전 세계적으로 부족한 현실입니다. 이 격차를 줄이기 위해 ITU 는 1.900 여명의 전세계 정부관료, 규제 당국자, 공공 및 민간분야 ICT 전문가들을 대상으로 사이버보안 훈련 워크숍을 기획하였습니다.

온라인 아동 보호(COP)

아동은 온라인 상에서 가장 취약한 계층 중 하나입니다. '디지털 원주민'으로 불리는 신세대는 온라인상에서 개인정보를 드러낼 가능성이 훨씬 높기 때문에 범죄자와 해커들에게 손쉽게 표적이 될 수 있습니다.

최근에는 온라인 세상과 물리적 세상을 분리하는 장벽이 점점 무너지고 있으며, 이는 아동의 정신 및 신체 건강에 심각한 영향을 미칠 수 있습니다. 최근 조사에 따르면 지난해 13 세에서 17 세 사이 10 대 청소년의 절반 가량이 사이버 폭력(cyberbullying)을 경험했다고 응답했습니다. 더욱 심각한 것은 실제 오프라인에서 성매매에 연관되었던 청소년들 중 75% 가량이 가해자들을 온라인에서 만났다는 것입니다.

ITU 의 온라인아동보호(COP) 이니셔티브는 국제 협력 네트워크로서 전세계 아동이 직면한 사이버공간의 위험성과 취약성 파악 및 인식을 제고하고 자원을 공유하며, 위험성을 최소화하고 책임 있는 디지털 시민의식을 높일 수 있는 실질적인 문제 해결을 위해 고안되었습니다. COP 이니셔티브는 정부, 민간분야, 시민사회, 학계, 국제기구로부터 참여한 54 개 이상의 국제 파트너들이 문제 해결을 위해 협력합니다.

기술 표준(권고)

권고라고도 알려진 ITU 의 기술표준은 온라인상의 이용자 보호에 매우 중요한 역할을 합니다. ITU-T 연구반 17 은 전기통신 보안과 개인정보 관리에 관한 주도 연구반으로서, 일차적으로 ICT 이용에 관한 신뢰 및 보안 구축에 초점을 맞추고 있습니다.

보안은 ITU 권고와 표준에 매우 중요하며, ITU 의 모든 연구반들은 보안 관련 문제들을 전 분야에서 검토하고 있습니다. 지금까지의 성과로는 인터넷 프로토콜(IP) 네트워크·차세대(NGN) 표준에 관한 기술 권고와 현재 및 미래 모바일 네트워크에 적용되는 명확한 보안 관련 규칙 수립 등이 있습니다. 이 중 가장 눈에 띄는 사례는 바로 공개키기반구조(PKI)와 권한관리기반구조(PMI)에 대한 ITU-T 권고 **X.509** 입니다. X.509 는 공개 키 인증서에 대한 표준 형식과 인증서 폐지 목록, 속성 인증서 등을 명시하고 있습니다.

글로벌 다자이해관계자 차원의 접근

- 최근들어 최빈개도국(LDC) 내 ICT 의존도가 높아지면서 사이버 보안은 중요 한 이슈로 부각되고 있으며, 여러 조사들을 통해서도 사이버 범죄 및 사이버 위협 측면에서 개발도상국의 취약성이 가장 높다는 사실을 알 수 있습니다. ITU 의 LDC 내 사이버보안 향상 프로젝트는 정책 수준 지원을 실행하여 더 안전한 인터넷 만들기와 이용자 보호에 중점을 두고 있습니다.

- ITU 는 국가 사이버 보안 역량에 대한 기준을 마련하고 회원국들이 모범사례를 배울 수 있도록 글로벌 사이버 보안 지수(GCI)를 제공하기 위해 ABI Research 와 제휴를 맺었습니다.

- 또한 ITU 는 현재 부상하는 글로벌 사이버 위협 동향에 대한 정보를 정기적으로 공유하기 위해 Symantec 과 Trend Micro 와 같은 사이버 보안 기업들과 공식적인 협력관계를 수립했습니다.

- 현재 ITU 는 UN 체제의 타 기관 및 단체들과의 협력을 통해 UN 산하기구들의 사이버 보안 관련 회원국 지원 활동에 있어 기구들 간 내부 조정 개선을 위해 협의하고 있습니다.