2012

第二十八輯

治安論叢

治安政策研究所

第二十八輯

治安論叢

治安政策研究所

발 간 사

우리 경찰은 안전과 인권의 수호자로서 '국민이 믿고 의지할 수 있는 경찰'로 거듭나기 위해 지속적인 변화와 노력을 경주하고 있습니다.

이에 치안정책연구소에서는 국민과 현장을 만족하는 각종 시책을 발굴하여 정책방향을 제시하고 있으며, 특히 중장기 치안정책을 연구·개발하여 든든한 민생치안 확보를 위해 이론적 근거를 제공하고 있습니다.

이번 『치안논총 제28집』은 '지역경찰 순찰근무의 효용성 검토 및 적정 소요인력 산출' 등 4편의 논문을 엄선하여 수록, 발간하게 되었습니다.

그 동안 『치안논총』에 관심과 성원을 보내주신 분들께 감사드리며, 이번에 발간되는 제28집에 많은 사랑과 격려를 부탁드립니다.

아무쪼록 실무부서에서 알차게 활용되고 치안행정 및 경찰관련 연구분야에서 노력하고 있는 전문가들에게도 귀중한 자료로서 도움이 되었으면 합니다.

끝으로 그간 연구에 전념하여 훌륭한 논문을 완성하여 주신 연구진과 논총발간에 애써주신 관계자 여러분들께 깊은 감사를 드립니다.

2012. 10.

치안정책연구소장

총 목 차

개도국 사이버수사기법 교육훈련 프로그램 개발

≪研 究 陣≫

연구위원 : 최 정 호 (한국해양대학교 교수)

치안정책연구소

목 차

표 목 차

그 림 목 차

제1장 서 론

제1절 연구의 개요

1. 연구의 목적과 의의

정보사회의 발달에 따른 사이버범죄의 위협은 이제 우리의 일상 뿐 아니라 국가안보까지 위협하는 세계적인 문제가 되었다. 최근 유럽공동체 집행위원회는 EU 역내의 사이버범죄로 인한 손실을 7,500억 유로로 추산하였는데 이것은 이미 세계 GDP의 1%에 육박하는 것으로 그 위협이 이미 세계 마약범죄 규모를 넘어섰다고 하였고, 2010년 미·러·중 대표를 포함하는 유럽연합 정부전문가 그룹(Group of Governmental Expert, GGE)은 "정보보안 영역에서 현존하는 잠재적인 위협은 21세기의 가장 심각한 도전"이라고 보고[1]하고 있다.

이러한 사이버범죄에 대한 세계적인 대응에서 가장 먼저 언급되는 것 중의 하나가 경찰 등 법집행 기관의 역량을 확보하는 문제이다. 물론 이러한 역량을 확보하기 위해 우선되어야 할 것은 전문적인 인력의 확보를 위한 교육과 훈련이다. 1997년 주요 8개국 정상회담인 G8 법무·내무 각료회의에서 하이테크 범죄 대응을 위한 10대 원칙과 10개 실천계획을 채택하면서 10대 원칙의 하나로 "법집행관(수사요원)은 하이테크 범죄에 대처하기 위한 교육훈련을 받아야 하고 하이테크 범죄에 대처하기 위한 준비가 되어 있어야 한다."고 천명한 바 있다. 이러한 법집행기관의 교육훈련을 강조한 국제사회에서의 언급은 헤아리기 어려울 정도로 많다.

하지만 사이버범죄에 대응하기 위한 법집행기관의 체계화된 교육훈련은 쉽지 않다. 사이버범죄자들의 범행에 사용되는 기술은 이전의 법집행기관이 경험하지 못한 새로운 것

---

* 이 연구보고서는 한국해양대학교 해양경찰학과 최정호 교수와 경찰대학교 경찰학과 장윤식 교수가 함께 작성하였습니다.

1) UN General Assembly A/65/201:2

들이며, 대부분의 기존 수사 종사자는 IT 분야에 대한 전문지식이 매우 부족하다. IT 분야에 전문성을 지닌 인력을 신규로 채용하는 것은 예산 등의 이유로 그 한계가 뚜렷하다. 사이버범죄 수사에 대한 전문지식은 상당한 배경지식과 수사경험을 통해 서서히 형성되는 것인데, 기존의 경찰훈련은 특정 분야에 대한 단기 훈련인 소위 블럭(block)식 훈련에 머물고 있어 충분한 전문성을 갖추게 하는 훈련체계로 적절하다고 평가하기 어렵다. 많은 개발도상국가에서 이러한 어려움은 더욱 심각하다.

IT 강국을 지향한 국가의 정책에 따라 한국은 선진국 못지않게 인터넷 기반이 발달할 수 있었고, 덕분에 한국경찰은 일찍이 사이버범죄수사 분야에 대한 역량을 키워올 수 있었다. 현재 사이버범죄 전담수사인력의 규모가 약 1,000여 명에 이르고 있는데, 그 중 300명에 가까운 인력은 대학에서 IT 분야를 전공하고 관련 업종에 종사한 경험이 있는 경력자 출신이 수사관으로 특채된 경우로서, 한국은 세계에서도 손꼽히는 사이버수사역량을 확보한 국가 중의 하나가 되었다.

한국경찰은 스스로 무엇보다 전문인력의 양성에 최우선 과제를 두고 다양한 교육훈련 프로그램을 진행해 왔으며, 2000년대 초반부터는 경찰 뿐 아니라 국내 형사사법 전체의 어떤 분야보다도 더 활발하게 국제적인 사이버범죄수사 훈련을 제공하는 공여국으로 자리를 잡아 왔다. UN, 인터폴, ASEAN, UNIFEI 등 국제기구에 교관진을 파견하였고 국제기구의 국제훈련을 다수 국내 유치하였다. 또한 한국국제협력단(KOICA)의 개발원조(ODA) 사업 중 해외 공무원 초청연수사업의 일환으로 '국제 사이버범죄수사 과정'을 경찰대학 등에서 시행하고 있고, 다수의 국가로부터 초청을 받아 다양한 훈련프로그램을 제공하고 있다. 나아가 2010년에는 인터폴의 요청으로 사이버범죄 전문 교육훈련을 위한 국제기구를 국내에 유치하기 위한 연구까지 진행되었으나 여러 여건상 아직 구체적으로 추진되지는 못하고 있다.

이처럼 다양하게 국내외에서 사이버범죄수사와 관련된 교육훈련 프로그램이 실시되고 있지만 국제 사이버범죄수사 훈련, 특히 개발도상국가를 대상으로 한 훈련 프로그램은 여러 해 반복하여 실시한 결과 공통적인 문제점을 드러내고 있다. 이는 개발도상국의 열악한 현실에 덧붙여 고비용의 국제훈련 프로그램이 지닌 본래의 문제에다가 전통적 블럭

식 경찰 훈련의 답습 등이 결합되면서 나타나는 매우 복합적인 문제로 생각된다. 이와 같이 여러 해 동안 교육훈련 프로그램을 운영한 경험을 바탕으로 하여, 본 연구는 국제 사이버범죄수사 교육훈련의 문제점을 분석하고 이를 해결하는 방안으로서의 새로운 훈련 체계의 표준적인 모델을 구성하여 제시하고자 한다.

2. 연구 방법과 범위

가. 연구방법

당초 본 연구는 경찰청 및 소속기관이 주관하여 현재 시행하거나 향후 시행할 가능성이 높은 다양한 교육프로그램의 교과를 편성하는 것을 목적으로 기획하였다. 이를 위해 개도국의 훈련 수요를 파악하고 사이버범죄와 관련된 지식·기술·역량을 체계화하여 세부적인 훈련계획을 수립하고자 하였다. 하지만 연구과정에서 이러한 블럭식 사이버범죄 훈련이 여러 가지 분야에서 한계를 지니고 있으며, 이 문제를 해결하기 위해 보다 근본적으로 사이버범죄수사 훈련체계를 정비하기 위한 노력이 선행되어야 한다는 결론에 이르게 되었다. 전통적인 강의식 훈련의 한계를 극복하기 위한 방안으로 이-러닝(e-learning)을 활용하는 등 새로운 교육훈련 패러다임을 적용할 필요성도 절감하게 되었다. 따라서 다양하게 이루어질 수 있는 개별 훈련프로그램의 모델보다는 포괄적인 사이버범죄수사 훈련의 근간을 이루는 과정(process)과 이를 시행하기 위한 기반의 모델을 구축하는 것에 중점을 두게 되었다. 즉, 사이버수사 훈련을 개별 프로그램에 의한 단일 과정이 아니라 개인별로 전반적인 전문성을 향상시키기 위한 일련의 연속되는 과정으로 인식하고 이를 위한 체계의 모델을 마련하려는 것이다.

아쉽게도 기존의 문제를 발견하고 이를 해결하기 위한 방법으로 새로운 국제 사이버범죄수사 훈련체계를 구축하고, 이를 바탕으로 한 구체적인 훈련 프로그램을 기획하기 위해 참고할만한 선행 연구자료가 풍부하지 않았다. 또한 국제 사이버범죄수사 훈련의 수요(Needs)를 파악하기 위해 외국의 경찰관을 대상으로 훈련 참석 이전의 설문조사를 분석하였으나 수요자인 개발도상국 참석자들의 사이버범죄 문제에 대한 상당한 인식의 격차 등으로 인해 자료로서 활용하기 어렵다는 결론에 이르렀다. 따라서 무엇보다도 다양

한 국내외 사이버범죄수사 교육훈련에 참여한 연구진의 경험을 연구에 많이 반영하였다. 참고로 연구진은 UN, 인터폴, FBI, UNAFEI 등 다양한 국제기구 및 외국기관이 시행한 사이버범죄 국제훈련과 'Guidancesoft' 등 외국 전문 상업기관의 훈련 프로그램 및 국내의 프로그램에 강사 혹은 교육생 신분으로 참여한 바 있다. 또한 국제훈련에 경험이 많은 개도국을 포함한 외국 전·현직 경찰관과의 비구조화된 면담을 통해 연구내용을 정리하였다.

〈표 1〉 면담에 참여한 외국 경찰관

국 적	사이버수사 경력	교관경력	현 직	비 고
홍 콩	15년	12년	금융계(2010전직)	대면/이메일 면담
트리니다드 토바고	8년	2년	현지 경찰청	대면/이메일 면담
보츠와나	11년	없음	현지 경찰청	대면/이메일 면담
자메이카	7년	4년	현지 경찰청	이메일 면담

또한 무엇보다 가급적 다양한 해외의 교육 프로그램의 운영상황을 비교·검토하였다. 외국의 사례는 관련 문헌과 각 기관 등의 웹사이트의 자료를 수집하여 분석한 경우도 있고 연구진이 직접 훈련에 참여하거나 관계자를 통해 입수한 경우도 있다.

경찰청의 정책자료로 활용하기 위한 연구목적상 이 연구는 기존에 경찰청이 실시한 정책연구의 맥락과 같은 연속선상에 있다. 따라서 경찰청이 이미 보유하고 있는 기존의 경찰의 국제 교육훈련에 관한 사항이나 이에 대한 설문 등을 통한 평가, 또는 2010년에 실시한 용역연구를 통한 국제 사이버범죄수사 훈련의 의의와 한국경찰의 참여시 기대효과 등에 대한 검토는 필요 최소한의 범위에서 언급하였다.

나. 연구 범위

이 연구는 먼저 사이버범죄수사와 관련된 실무 직종을 일반적인 경우와 같이 크게 수

사관(investigator)과 디지털포렌식 분석가(digital forensic examiner)로 구분하여 두 직종의 교육훈련과 관련된 일반적 논의 및 국제 사이버범죄 훈련과 관련된 일반 문제를 검토한다.(제1장 서론 제2절)

일반적으로 범죄수사는 학문(science)라기 보다는 실무(art 혹은 craft)에 가까운 것으로 취급되어 왔으며 전 세계적으로 체계적인 교육훈련에 관한 연구가 축적되어 있지 못하다. 반면 디지털포렌식 분야는 법과학(forensic science)의 일부로 세계 많은 곳에서 대학의 교육프로그램으로 지난 수년간 신설되고 있는 상황이다. 일부에서는 디지털포렌식 분석가의 교육·훈련·자격을 포괄할 진로 모델이 개발되어 있을 정도이다. 하지만 한국경찰을 비롯한 많은 국가에서 사이버수사관과 디지털포렌식 분석가의 업무영역이 명확하게 구별되어 있지 않다. 따라서 디지털포렌식 분야 또한 여전히 대학에서 교육받지 않은 비전문가 출신이 전형적인 경찰훈련 과정을 통해 업무를 익혀 실무를 담당하고 있는 상황이다.

제2장에서는 국내외 사이버범죄 수사분야의 주요 훈련과정을 살펴본다. 많은 교과과정의 검토를 통해 분석된 내용은 실제 구체적인 훈련과정의 설계에 활용할 수 있을 것이며 훈련내용의 대부분이 기술적인 것에 집중되고 있는 것을 알 수 있다. 기술적인 문제의 상당 부분은 사실 경찰 업무분야에 고유한 것이 아닐 뿐 아니라, 매우 기초적인 내용에 많은 시간을 할애하고 있다. 특히 훈련프로그램이 국제기관 등에 의한 국제훈련으로 이루어질 때 또한 상업적 훈련이 아니라 공공적 성격을 지닐 때 이러한 경향이 심한 것을 알 수 있다. 그 이유는 국제훈련이 이루어지는 과정과 사이버수사 분야가 지니고 있는 특성 등이 복합적으로 작용한 것으로 이와 관련된 분석이 이어진다. 특히 유럽에서는 최근 이러한 문제점을 인식하고 이의 대안으로 훈련내용의 모듈화 및 대학에 의한 훈련프로그램의 개발·인증·시행을 하려는 노력이 이루어지고 있다.

이와 관련된 상세한 논의가 제3장에서 이루어진다. 앞선 기존 훈련프로그램이 가지는 문제를 분석하며 대안으로 유럽식 교육훈련이 만들어지는 취지를 좀 더 구체적으로 확인한다. 유럽공동체를 중심으로 이루어지는 유럽식 교육훈련 프로그램은 지역 법집행 협력체제 자체가 존재하지 못한 상태인 아시아권역, 특히 국내에서는 즉시 적용하는데 어려움이 있다. 따라서 현실적으로 기존 블럭식, 강의식 경찰훈련의 한계, 국제훈련 자체에 내재된 한계에 대한 대안으로서 교육철학적 개념으로는 구성주의, 교육공학적 방법으로

는 이-러닝과 멘토링, 경찰훈련의 방법으로는 블럭식이 아닌 점증적(incremental) 방법 등의 개념을 접목하고 교육훈련은 좀 더 측정할 수 있고 인증될 수 있는 프로그램으로 만들기 위한 패러다임 변화를 구상한다.

이 프로그램을 실행하기 위해서는 먼저 전제조건으로 현재의 교육체계 전반에 대한 재점검과 새로운 패러다임을 적용하기 위해 필요한 기반이 구축되어야 한다. 따라서 먼저 새로운 패러다임 적용을 위한 훈련 기반의 구축 모델이 제4장에서 검토된다.

다. 연구결과의 활용

본 연구는 무엇보다 경찰청에서 사이버수사기법과 관련하여 개발도상국가에 대한 지원이나 교류 및 새로운 관계 수립에 참고자료로 사용될 수 있을 것이다. 경찰청뿐만 아니라 각종 법 집행기관이 사이버수사의 최첨단에 서있는 우리나라의 위상을 알리고, 교육훈련을 통한 각 국가간 사이버수사 연락망을 구축함으로써, 국제적인 사이버범죄에 더 신속하고 공고하게 대처할 수 있는 기반을 만들 수 있으며, 사이버수사의 기본적인 규약을 통일화하여 법 집행에서 발생할 수 있는 불완전한 해석이나 오해 등을 사전에 막을 수 있는 기회를 제공할 수 있을 것이다.

아울러 개발도상국에서도 사이버수사 관련 법률이나 디지털 포렌식의 중요성에 대한 인식과 함께 이 분야에 대한 예산의 배분이나 인력의 모집과 배치와 같은 여러 측면에서의 배려가 이루어질 것으로 기대하고 있으며, 담당 부서에서는 장·단기의 정책의 수립과 집행, 각 정책에 있어 우선 순위의 결정에 참고가 될 것이다.

한편으로 사이버수사 및 디지털 포렌식이 단지 수사기관의 전유물이 아닐 뿐 아니라 수사기관의 입장에서도 이와 관계되는 정부부처 및 학계, 산업계에서의 지원을 필요로 하며, 무엇보다 사이버수사와 디지털 포렌식이 국가적인 차원에서 발전을 도모해야 한다는 측면에서 상호간의 이해와 협력에 본 연구가 다소간 도움이 될 것으로 기대된다.

제2절 사이버범죄수사 국제훈련에 관한 일반적 논의

1. 국제훈련 프로그램 개발 필요성

가. 사이버수사기법 국제교류의 필요성

국제교류란 인종·종교·언어·체제·이념 등의 차이를 초월하여 개인, 집단, 기관, 국가 등 다양한 주체들이 우호, 협력, 이해증진 및 공동이익 도모 등을 목적으로 공식·비공식적으로 추진하는 대등한 협력관계를 말한다. 따라서 그 범위는 매우 광범위하여 일률적으로 규정하기 어려운데, 이를 주체별로 구분해 보면 국제기구를 통한 다자간 국제교류, 국가간 교류, 경찰기관별 교류 뿐 아니라 개인 간 교류 등 공식·비공식적 활동을 모두 포함한다. 실무적으로 국제교류는 구체적인 개별사안에 대한 법집행을 위한 상호협력을 뜻하는 국제공조와는 구별되는 개념이다.

경찰은 조직의 구성(경찰기관)과 임무(경찰작용)에서 국가별로 다양한 차이가 있으나 법집행을 주된 내용으로 하는 경찰권은 국가의 영토고권(領土高權, territorial supremacy)의 중요한 부분이므로 영토를 벗어나 직접적으로 행사될 수 없는 것이 원칙이다. 따라서 필요한 경우 해당 국가의 법집행기관이 해당 국가의 법에 근거한 자발적인 협조만을 기대할 수 있을 뿐이다. 일반적으로 국제경찰로 알려진 인터폴이 수사권한을 전혀 행사할 수 없고, 인터폴을 매개로 공조수사 의뢰를 받은 회원국이 자국 법령이 인정하는 한도 내에서 그 권한만을 행사하는 것도 그 때문이다. 강제되지 않는 자발적인 협조를 이끌어 내기 위해서는 상호이해와 존중이 선행되어야 하며 이를 위해서 평상시 다양한 국제교류 활동이 필요하다.

한편으로 다양한 경찰조직의 구성과 활동, 관련된 제도나 지식·기술의 발전을 위해서도 교류협력은 매우 중요하다. 치안시스템은 빈곤퇴치 등 개도국의 경제적 발전을 직접 도모하기는 어렵지만 민주주의, 법치주의, 사회불안의 제거와 같은 정치·사회적인 발전을 통한 국가발전에 깊은 영향을 미친다. 보다 발전된 치안시스템을 구축하는 가장 효과

적인 방법 중의 하나는 다른 치안시스템을 적용하고 있는 국가의 사례를 연구·학습하는 것이니 교육 및 훈련의 효과는 즉시적이고 직접적이라기보다는 장기적이고 간접적으로 발전에 기여한다고 할 수 있을 것이다.

나. 개발도상국에 대한 지원 필요

전 세계 인터넷 사용인구는 2011년 3월 현재 20억 9천만 명(전체 세계 인구의 30.2%)을 넘어서고 있다. 전 세계의 인터넷 사용인구는 지난 2000년도 이래로 현재까지 무려 480.4% 증가한 것으로, 비교적 개발도상국가들이 많이 위치해 있는 아프리카(2,527.4%), 아시아(706.9%), 중동(1,987.0%), 라틴아메리카(1,037.4%) 등에서 그 증가추세가 더 두드러진다고 할 수 있다[2].

인터넷 사용인구의 증가에 비례하여 사이버범죄의 발생도 증가하리라는 것은 누구든지 예상할 수 있어 전 세계적으로 국제적인 사이버범죄에 공동으로 대응할 필요성이 있지만, 현재 이들 개발도상국에서는 국제적인 사이버범죄는 고사하고 자국 내에서 발생하는 사이버범죄에 대처할 수사역량도 부족한 형편이다. 사이버범죄의 특성상 국제적인 동반자적 대응이 무엇보다도 중요하며, 관련 법률이나 수사 등 혹시라도 어느 한 쪽 면에서 부족한 부분이 발견된다면 이를 악용하는 범죄집단의 속성에 따라 국제적인 공조수사의 망에 누수현상이 발생할 수밖에 없고, 이는 그동안 국제사이버범죄 수사사례에서 여러 차례 지적되어온 것이므로, 이들 개발도상국의 사이버범죄 수사역량을 강화하기 위한 지원이 꼭 필요한 요소라고 할 수 있다.

한국은 1986년까지만 해도 대외원조를 받아온 가난한 개발도상국이었지만, 1987년 처음 대외원조에 나선 이래로 국제적으로 그 발전사례가 거론될 만큼 원조하는 국가로 성공적인 변신을 하였다. 대외원조 초기에는 단순히 자금을 지원하는 형태였으나 이제는 개발도상국 경제 활성화뿐만 아니라 문화까지 '원조'하는 형태로 진화하였고, 건설·의료·교통 등 주요 사회간접자본(SOC) 분야에서 국내 기업의 해외 진출 교두보 역할을 하고 있다. 공적개발원조(ODA)[3]는 1987년 원조를 시작할 당시 2,000만 달러에 불과했지만

2) 세계 인터넷 통계 www.internetworldstats.com

지난 해 58.5배 수준(11억 7,000만 달러)으로 급증하였으며, 2015년에는 30억 달러에 달할 것으로 예상된다고 한다.

이제는 경제적인 원조뿐만 아니라 자본과 시설투자를 통한 개발도상국가의 문화발전에도 관심이 기울여지고 있다. 한 사례를 들자면, 필리핀 마닐라시 남부를 이어주는 통근 전철의 전동차 제일 앞 칸의 경우 여성들만 가득 채워지는데, 이는 이 통근 전철 개선 공사에 참여한 한국 기업(한진중공업)이 전동차도 함께 담당하면서 '여성·노약자 전용칸'과 같은 전철을 운영하는 방식까지 지원국의 문화를 받아들였기 때문이다[4]. 이와 같이 사이버범죄수사의 훈련프로그램도 개발도상국가를 대상으로 한 국제적인 지원을 통해 사이버범죄수사의 기술과 방법뿐만 아니라 한국의 발전된 사이버범죄 수사문화까지도 함께 전파할 수 있게 되는 것이다.

개발도상국의 치안문제의 해결은 점차 국제적인 관심사로 주목을 받고 있다. 2001년 OECD가 작성한 '분쟁예방 지침'은 많은 개발도상국들이 정치·사회적인 여러 분쟁들을 겪고 있으며 이로 인한 살상과 테러, 무질서 등 치안불안이 발전에 커다란 장애가 되고 있음에도 개도국 중의 상당수는 스스로 치안을 유지하지 못하고 있다고 밝히고 있다. 치안유지를 위해서는 법치, 인권 존중, 사회·경제 발전, 치안능력을 가진 민주적 시스템 구비 등이 필요하며 개도국이 이러한 능력을 갖출 수 있도록 경찰 등 치안 담당부서를 합법적으로 육성하는 것을 지원하는 등 공여국과 수원국 사이의 부서 간에 체계적이고 일관된 개발협력정책을 추진해야 한다.

이러한 치안의 개발협력에 대한 필요성은 점차 증가하고 있다. 1990년대 냉전의 종결

---

3) 공적개발원조(公的開發援助, ODA : Official Development Assistance) : 선진국에서 개발도상국이나 국제기관에 하는 원조. 공공개발원조·정부개발원조라고도 하며, 증여·차관·배상·기술원조 등의 형태를 갖는다. 개발도상국에 대한 공적자금 중 첫째, 정부 또는 정부의 원조기관에 의해 공여된다. 둘째, 개발도상국의 경제발전과 복지향상에 기여한다. 셋째, 자금 공여조건이 개발도상국에게 부담되지 않도록 무상 부분을 일정 비율 이상으로 한다는 조건을 갖춘 것을 말한다. 경제협력개발기구(OECD) 가맹국은 국민총생산(GNP)의 0.31%에 이르는 600억 달러의 ODA를 공여하고 있으나 국제연합(UN)은 일정 기간까지 0.7%로 늘리기로 결의하였다. 출처 : 네이버(www.naver.com)

4) 중앙일보 2011. 11. 28. 중앙경제 E9 기획, "한국 돈으로 지어준 마닐라 전철에 한국식 여성전용칸 - 베트남·필리핀·캄보디아, 한국 대외원조 국가를 가다" 김창규 기자

이후 국지적 무력충돌이 늘어나면서 수백만 명의 사상자가 발생하였고 최빈 개도국의 3분의 2이상이 분쟁에 휘말려 있다. 특히 미국 9·11 테러 사건과 아프가니스탄 지원 등을 계기로 빈곤과 테러의 관계, 그리고 평화구축의 중요성에 대한 국제사회의 관심이 고조되고 있다. OECD의 테러리즘 방지에 대한 개발협력(A Development Cooperation Lens on Terrorism Prevention, 2003)과 같은 프로그램들은 이러한 추세를 반영하는 국제기구의 많은 노력 중의 하나이며, 한국 또한 국제사회 일원으로 이러한 노력에 적극 참여할 의무가 있다고 하겠다.

개발도상국의 정보기술 발전상황 및 국가 여건에 따른 사이버수사기관의 수사역량을 고려한 표준화된 개도국 사이버수사관 교육 프로그램을 개발하여, 국제사회의 사이버범죄 발생 억제에 기여할 수 있고, 개발도상국 사이버수사관을 대상으로 체계화된 사이버수사기법 교육훈련을 실시하며, 교육 이수자를 상대국의 사이버범죄수사 담당자 및 국제협력 연락관으로 활용함으로써 사이버범죄에 대응하는 국제공조수사 역량을 강화하는데 일조를 할 수 있을 것이다.

현재 운영 중인 인터폴·국제협력단의 교육훈련 과정과 병행하여 개발도상국을 대상으로 체계화된 교육훈련 프로그램을 제공함으로써 해당 국가의 사이버범죄 수사역량을 제고하여 세계 각국의 사이버범죄 근절에 기여하고, 한국경찰에 대한 우호적 분위기를 조성할 수 있으며, 교육과정의 국제적 권위 확보 및 한국경찰의 우수성을 홍보하고, 각 수준에 맞춘 교육과정의 제공을 통해 사이버범죄 수사교육의 내실화 및 수요자의 시각에 맞춘 사이버수사교육의 공급이 가능하게 될 것이다.

그동안 정보인프라 부분의 발달로 국제적인 위상을 독보적으로 높여가고 있는 우리나라에서 개발도상국을 대상으로 발달한 사이버수사기법이나 교육내용을 전수함으로써 이에 따른 국제적인 이미지 제고에도 도움이 되리라 생각한다.

2. 관련 분야 국내 발전에 기여

인터넷 보급과 관련 산업의 성장에서 세계의 중심에 있는 한국에는 인구수 대비 엄청난 인터넷 사용량만큼이나 많은 수의 다양한 사이버범죄가 발생하고 있다. 연간 13만 건

을 넘나드는 숫자이다. 사이버범죄 단속에 관한 법집행기관의 통계에서 우리 경찰통계만큼, 아니 이와 어느 정도 필적할만한 범죄단속 건수를 나타낸 경우는 전 세계에서 유례를 찾을 수 없을 정도이다.

어찌 보면 당연하겠지만, 그간 경찰청은 사이버테러대응센터를 중심으로 단일 조직으로는 세계 최대 규모의 수사체계를 구축하였으며, 첨단의 사이버수사망인 NETAN HUB를 자체적으로 개발하여 전국 사이버수사관을 유기적으로 연결하고 수많은 국내 및 국제공조사건에서 그 역량을 인정받아 왔다. 최근에는 개발도상국가의 사이버수사역량 확보를 지원하는데도 많은 노력을 기울여 그 인지도를 높여가고 있다.

한편 국내적으로는 경제성장에 어울리지 않는 국제기여도를 높이고 법치질서를 바로 세워 국격을 높이려는 과제가 국가적으로 대두되고 있다. 무엇보다 국제적인 기여는 국제사회가 필요로 하는 곳에 이루어져야 국제사회의 요구도 우리가 뜻하는 국제기여의 의미도 만족시킬 수 있다. 국제경찰 인터폴은 글로벌한 이슈인 사이버범죄 문제 해결을 위한 중요한 역할을 한국경찰이 해줄 것을 기대하고 있다. 의도한 대로 국제적인 사이버수사기법에 대한 교육훈련 프로그램이 개발되어 개발도상국에 대한 사이버범죄 역량강화의 기폭제로 효과를 발휘한다면 국제사회는 그 성과와 기여를 인정할 것이다.

국내적으로 준법의식이 자리 잡지 못한 가장 큰 이유 중의 하나는 법집행기관을 비롯한 법을 수호해야할 집단에 대한 불신이 크게 영향을 미치고 있다고 분석된다. 최근에는 정당한 법집행과 뛰어난 성과에도 냉소적인 태도를 보이는 국민을 발견하는 것이 어려운 일이 아니다. 국제 법집행 사회에서 한국경찰에 대한 기대와 이에 응답하는 기여를 보게 된다면 이러한 국민들은 그간 보여 왔던 태도가 편견임을 확인하게 될 것이다.

하지만 사이버범죄 수사분야에 일부 강점을 가지고 있다고 하더라도 많은 부분에 있어서 우리나라 경찰은 아직 선진국의 수준에 미치지 못하고 있는 점이 적지 않음을 지적하지 않을 수 없다. 사이버수사기법 교육훈련에 대한 국제적인 프로그램을 개발하고 그 운영에 참여함으로써 그 과정에서 한국경찰의 글로벌화는 급격히 진척될 수 있을 것이고 선진의 시스템을 다른 어떤 방법보다도 빨리 경찰에 뿌리내리도록 할 수 있을 것으로 기대된다. 한국경찰이 가진 강점을 국제사회의 강점과 결합함으로써 목표한 바를 달성할 수 있을 것으로 충분히 기대할만 하다.

3. 사이버수사관의 교육과 훈련

가. 경찰 교육과 훈련의 일반적 이론

일반적으로 교육(education)은 개인의 사회적 발달에 필요한 지식이나 적합한 행동방식, 기술적 능력 따위를 가르치고 학습하는 모든 행위를 포괄하는 폭넓은 개념이라고 볼 수 있다. 하지만 일찍이 루소(J. J. Rousseau, 1721~1778)가 "우리가 태어났을 때는 갖지 못한 필요한 모든 것이 자라면서 '교육'에 의해 주어진다."고 설명한 것에서 보듯이 교육을 엄밀하게 정의하기는 쉽지 않다. 반면에 훈련(training)은 특정한 일을 하기 위해 필요한 지식과 기술, 능력을 가르치고 배우는 것으로 좀 더 한정적인 개념으로 사용된다.

직업적 관점에서 특히 경찰 등 형사사법 분야에서는 흔히 학위과정을 포함한 대학교육만을 교육으로 보며, 신규채용자에 대한 초기훈련, 지속적인 사격술 훈련, 새로운 기술에 대한 훈련과 같이 교육과 훈련을 구별해 왔다(Shafer 2007).

대학교육은 새로운 상황을 비판적으로 평가하고, 필요에 따른 새로운 학습을 수행하며, 심지어 필요한 경우 "사실"과 존재하는 지식의 규범에 대한 강조되는 가정에 대해 의문을 품도록 설계된다(Carter, Sapp and Stephens 1989). 반면 훈련은 직업에 직접적으로 전달될 수 있는 특정한 기술, 지식, 능력을 체계적으로 구성하는 것이다. 따라서 논의의 편의를 위해서 여기에서도 교육과 훈련을 이러한 관점에서 구별하도록 하겠다.

전문적인 직업을 수행하기 위해서는 직업별로 다른 지식(Knowledge), 기술(Skill), 역량(Ability, 혹은 태도 Attitude)을 필요로 한다. 흔히 KSAs라고 불리는 이러한 요건을 갖추는 가장 대표적인 방법이 교육훈련이다. 교육은 새로 고용될 때의 자격요건(qualification)인 경우가 흔히 있으며, 훈련은 특정한 분야의 직무수행에 필요한 지식·기술·소양 등의 습득정도가 일정한 기준과 절차에 따라 평가 또는 인정되는 것을 의미하는 자격(certification)의 지원에 있어서 요건이 되는 경우가 적지 않다.

어떠한 직업에 있어서 KSAs에 관한 공식적인 인정을 의미하는 자격(credential)에 있어서도 학문적 교육과 실무적 훈련의 이수 정도는 가장 중요한 판단 자료 중 하나이다. 따라서 교육훈련은 실질적으로 사이버수사에 있어 KSAs를 강화할 수 있는 최선의 방법이다. 반면에 한 개인에 있어 KSAs를 충분히 확보할 수 있도록 하기 위해서 교육훈

련의 기회가 필요에 따라 주어져야 하며 그 내용과 방법에 있어 정교하게 설계되고 이행되어야 한다.

문제는 KSAs를 확보할 수 있도록 진행되어야 할 교육훈련이 분야별로 인사제도, 예산 등 자원, 각 교육훈련간 또는 다른 전문성 확보를 위한 수단과의 관계, 교수법 등과 연계되어 매우 방대하고 복잡한 문제를 내포하고 있다는 점이다. 예를 들어 대부분의 국가에서 사이버수사관에게 대학교육은 필수적인 요건으로 여겨지고 있는데 이 때 요구되는 교육의 내용은 채용 이후의 훈련 내용에 직접적인 영향을 미치게 된다. 사이버수사 분야에 대한 인력수요는 사회적으로 보면 매우 소수에 지나지 않기 때문에 작은 규모의 변화에도 사이버수사 분야에는 큰 영향을 미치기 마련이다. 이는 가장 대표적으로 비수익적이면서도 공익과 밀접하게 연관될 수밖에 없는 사이버수사 분야에 대해 당사자 또는 관련 기관이 아닌 해당 제도와 관련된 모든 정부기관의 관심과 배려가 필요한 이유이기도 하다.

나. 사이버수사관의 Career Path와 교육훈련

1) 사이버범죄 수사 관련 직종 구분

많은 다른 전문적인 직종과 같이 사이버수사 분야에서 교육과 훈련은 그 직종에 종사하는 한 지속되는 평생학습의 과정이다. 교육훈련은 그 경력의 시작부터 끝까지 지속되어야 할 직업적 개발에 있어 매우 중요한 위치를 차지하기 때문에 전체적인 Career Path의 도식 하에서 설계되어야 한다.

사실은 사이버수사 업무는 단일 직종이 처리하는 업무가 아니다. 사이버수사와 관련해서는 실제 범죄사건의 수사를 주도하는 형사(detective 혹은 investigator)와 같은 수사관과 정보를 수집하여 분석하는 것을 주 업무로 하는 정보분석가(intelligence analyst), 디지털증거를 현장에서 수집하는 현장수사관(scene investigator), 수집된 디지털증거를 과학·기술을 활용하여 분석하고 이에 대해 전문가 의견을 제시하는 디지털 포렌식 전문가(digital forensic examiner) 등이 사이버수사와 관련하여 구분되는 직종이 될 수 있다. 이러한 직종은 업무수행에 필요한 KSAs에 상당한 차이가 있다. 하지만 세계적으로 사이버범죄 수사와 관련한 직종을 우선적으로 수사관(investigator)와 증거분석가(forensic examiner)로 양분하는 것이 일반적이다. 많은 훈련프로그램은 '사이버

수사 훈련' 혹은 '디지털 포렌식 훈련'으로 이름 붙여져 있다.

수사관과 포렌식전문가는 최근 대중매체를 통해서 널리 인식된 구분되는 직종이다. 무엇보다 근본적인 차이는 수사관은 범죄문제의 해결이라는 합목적성에 보다 관심이 크고, 포렌식전문가는 법과학자로 범죄의 해결에 앞서 과학적 진실, 객관성이라는 이치에 부합하려고 노력한다는 점에 있다.

2) 수사관과 법과학자의 교육훈련

전문직업으로서 수사관의 요건과 교육훈련에 대한 연구는 그다지 많이 이루어지지 않았다. 대부분의 국가에서 수사관은 일반적인 법집행관의 요건을 구비한 후 그리 길지 않은 단기 훈련을 거쳐 실무경험과 감독을 통해 업무에 능숙해지는 과정을 거치는 것으로 인식되어 왔다. 추가적으로 필요한 훈련은 단기의 집중적인 과정으로 주어져 왔으며 이는 흔히 블럭식 훈련이라고 불린다. 따라서 수사관에 대해 엄격하게 구조화된 교육훈련 과정이나 자격제도가 구축된 경우를 찾아보기 어렵다. 최근 수사관의 전문직업화와 관련하여 훈련제도와 자격제도에 대한 국가적인 변화를 활발하게 시도하고 있는 곳은 영국이다. 국가적으로 NPIA(National Police Improvement Agency)가 주도하는 수사전문화 프로그램(Professionalizing Investigation Programme: PIP)이 그것이다.

아래는 영국의 PIP에서 요구하는 상급 범죄수사관(Supervising Investigation Officer)의 요구기술이다(Tong, 2009).

〈표 2〉 상급 범죄수사관의 요구기술 : [초기 범죄현장 평가]

수 사 능 력	지 식 수 준
수사능력 · 수사선의 설정 시작 **정보평가** · "slow time" 만들기 · 현장 정보 융합하기 · 억측을 만들지 않기 · 범죄현장 정보해석의 시작 **전략적 주의** · 행동들의 연속성 파악하기 **적용** · 유연성 설명	**기반지식** · 절차 · 역할 지식 · 법적 과정 · 윤리적 적용 · 특수범죄형태의 지식

〈표 3〉 상급 범죄수사관의 요구기술 : [정보의 평가]

수사능력	지식 수준
수사능력 · 수사 전략의 설정 · 경험에서 배우는 능력 설명 **정보평가** · 들어오는 정보를 받아들이는 능력 설명 · 정보의 상관성과 유효성 파악 · '악마의 대변자' 역할 해보기 · 전문가 충고 검증 · 객관성 보이기 **적용** · 반동성 유지	**기반지식** · 팀의 강점·약점의 인식 · 역할들의 지식 · 절차 · 특수 범죄형태의 주요 지식 · 접근 가능한 전문 조언자 인식

〈표 4〉 상급 범죄수사관의 요구기술 : [적절한 수사선의 선택]

수 사 능 력	지 식 수 준
수사능력 · 미디어전략 설정 · 적절한 집중 유지 · 수사 가설의 개발과 검증 · 수사선의 우선 순위 설정 **정보평가** · 계속해서 객관성 보이기 · 들어오는 정보 평가의 계속 **전략적주의** · 행동들의 결과가 본부와 지역에 어떻게 영향을 줄 지 인식 **적용** · 특히 전문가의 조언에 개방된 자세유지 · 유연성 유지	**기반지식** · 절차 · 역할들의 지식 · 특수 범죄 형태의 주요지식 · 어떠한 자원이 필요한지 인식 · 어떠한 자원이 사용가능한가에 대한 지식 · 그러한 자원을 어떻게 획득할 것인가에 대한 지식 · 접근 가능한 전문 조언자 인식 **미래개발** · 수사분야에 현재 상태 인식 · 법률, 법과학, 기술의 변화 인식

〈표 5〉 상급 범죄수사관의 요구기술 : [수사 진행]

수 사 능 력	지 식 수 준
수사능력 · 모든 가능한 옵션 조사 **정보평가** · 수사 선 계속적 검토 · 정보의 검증 계속 · 추측 피하기 **전략적 주의** · 행동들의 결과가 본부, 지역, 희생자, 목격자에 어떻게 영향 줄지 파악 **적용** · 유연성 유지 · 개방 된 자세유지 **혁신적 형태** · 수평적으로 생각해보기 · 새로운 개발들을 수사에 포함	**기반 지식** · 절차 · 특수 범죄에 대한 주요 지식 · 접근 가능한 전문 조언자에 대한 인식 · 팀 구성원에게 동기부여 할 것 인식 **미래 개발** · 수사 분야에 현재 상태 인식 · 법률, 법과학, 기술의 변화 인식

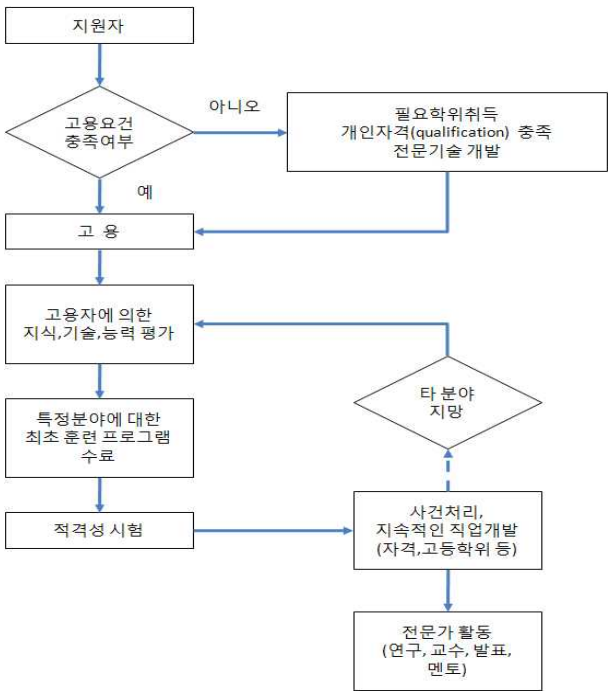
〈표 6〉 상급 범죄수사관의 요구기술 : [기소 후 사건관리]

수 사 능 력	지 식 수 준
수사 능력 · 가능한 피고측 주장 인식 · 모든 수사가 끝났다는 것의 확인 · 경험으로 배우는 능력 설명 **정보의 평가** · 법적 당사자에 대한 질문	**기반 지식** · 법적 과정 · 증거 제시를 위한 법정 조약 · 사실의 법칙 · 사건서류의 내용과 형태에 대한 지식 · 요구되는 역할의 지식 **미래 개발** · 입법의 변화에 대한 인식

국내에서도 범죄수사 전문화를 위해 가장 시급한 요소로 수사관의 전문화를 꼽고 있으며 이를 위해 범죄수사학 이론의 정립, 훈련의 강화 등이 추진되고 있다. 즉 아직 수사관이라는 직종의 교육·훈련·자격 제도에 대한 인식은 이루어졌지만 구체적으로 그것이 무엇인지를 알아볼 수 있는 표준적인 모델을 발견하기는 어려운 상태라고 할 수 있다.

반면에 법과학 분야의 전문성과 Career Path에 대한 논의는 수사관에 대한 그것보다 빠르게 진행되어 왔다. 그중에 가장 두드러진 작업은 미국 사법연구소에 의해서 이루어졌다. 지난 10년간 미국 내의 대학과 대학원에서 법과학 교육이 급증함에 따라 미국 법무부 사법연구소는 이러한 법과학 프로그램이 법과학 연구실의 업무에서의 요구수준을 충족할 수 있도록 교육 커리큘럼 구성에 대한 최적의 방안(best practice)을 마련하기 위한 연구를 진행하였고, 2004년 "법과학 교육훈련: 법과학 연구실, 교육기관, 학생들을 위한 지침(Education and Training in Forensic Science: A Guide for Forensic Science Laboratories, Educational Institutions, and Students)을 발간하였다(NIJ 2004). 이 보고서에 포함된 법과학 분야 종사자에 대한 Career Path 모델은 〈그림 1〉 법과학 분야의 Career Path 모델 (NIJ 2004)과 같다

〈그림 1〉 법과학 분야의 Career Path 모델 (NIJ 2004)



법과학 분야에 대한 지원자의 모델과 Career Path 모델의 적용은 다음과 같이 정의되어 있다.

- 개인적 염결성(integrity), 자연과학 분야 학사학위(최소한), 추가적 KSA(Knowledge-지식, Skill-기술, Ability-역량)
- 개인적 특질 : 형사사법분야에 속하기 때문에 정직성, 염결성, 과학적 객관성 등이 매우 중요하며 법집행관들과 유사한 배경조사를 받아야 한다. 이를 위해 약물검사, 범죄경력, 사회단체활동, 거짓말탐지기 검사, 운전기록, 경력, 신용상태, 의학적·신체적 검사 등을 받아야 한다.
- 학력 : 자연과학에 대한 탄탄한 기본적 배경을 지니고 있어야 한다. 대개 인증된 교육기관으로부터 화학, 생화학, 생물학 또는 법과학 학위를 요구받는다. 잠재지문, 무기, 문서감정과 같은 패턴의 인식과 비교와 관련된 법과학자들에게는 과거에는 학위가 필수적이지 않았었지만 가능한 과학분야에 대해 학위를 보유할 것을 요구받는 추세이다.
- 직업적 기술: 비판적 사고(정량적 추리와 문제해결), 의사결정, 연구실 실무, 연구실 안전문제에 대한 인식, 세부적인 것에 대한 관찰과 주의, 컴퓨터 숙련성, 대인기술, 공적 연설, 구두와 문서 커뮤니케이션, 시간 관리, 업무 우선순위 부여 등이 포함된다.
- 고용전 준비: 고용에 되기에 앞서 준비된 예비 법과학자는 품질 보증(quality assurance), 윤리, 행위의 전문적 표준, 증거의 통제, 보고서 작성, 과학 방법론, 연역 및 귀납적 추리, 통계, 안전 등에 관한 KSAs를 보일 수 있다. 이러한 KSAs에 대한 과정수료나 실무적 경험에 대한 문서는 새로이 고용된 법과학을 평가하는 이에게 객관적인 정보를 제공해 준다.
- On-the-job 훈련: 대부분의 법과학 연구실은 고용 후 6개월 내지 3년간의 초기 훈련을 진행하고 적격성 심사(competency test)를 거친 후에야 실제 사건처리를 담당하게 한다.
- 자격증(certification): 개인의 적격성에 대해 독립되고 적절하게 권한을 부여받은 기관으로부터 자격인증을 받는 것은 매우 바람직한 것으로 여겨진다. 엄격한 법과학 연구실은 법과학전문성 인증위원회(Forensic Specialties Accreditation

Board) 등 공신력 있는 기관에서 수여하는 자격증을 받을 것을 요구한다. 경우에 따라 이러한 자격은 지원요건이 되기도 하며 전문가 증언의 신뢰도를 높이는 역할을 한다.

◦ 전문가 활동: 연구, 멘토링, 교수활동, 전문가 조직에 참여, 지역사회 활동 참여, 저술 등의 전문가 활동은 직업개발의 중요한 요소가 된다.

다. 사이버수사관의 훈련과 보수교육

1) 개요

사이버범죄수사는 일반 수사에 덧붙여 IT 분야에 대한 충분한 이해와 이것이 실제 범죄사건에서 적용되는 방식과 이를 해결하는 능력이 필요하다. 즉, 앞서 설명된 수사관의 역량이 기존의 물리적공간이 아닌 사이버공간에서 적용되는 문제에 대한 추가적인 해결능력을 필요로 하게 되는 것이다. 많은 국가에서 사이버수사관은 기존의 수사관에 사이버수사와 관련된 훈련을 거쳐 그 보직을 변경하는 형태로 이루어져왔다. 당연히 이는 사이버범죄의 기술적인 문제를 해결하기에 대부분 턱없이 부족한 교육훈련이 이루어져왔다는 것을 의미한다. 한국경찰의 경우 2000년부터 IT 분야를 대학에서 전공한 이들을 사이버수사관으로 매년 20~30명 채용해 이제 그 수가 300명에 육박하고 있다. 게다가 이렇게 특별히 채용된 사이버수사관은 2~3년의 관련 직종에 종사한 경험까지 요구하고 있기 때문에 그런 경력을 지니지 못한 사이버수사관과 IT 분야에 대한 이해도의 차이는 쉽게 극복하기 어려울 정도로 크다.

따라서 많은 사이버수사관의 훈련은 IT 분야의 기술적인 내용에 대한 이해를 도모하는 기초적인 훈련이 포함되어 왔다. 한국경찰의 경우 해킹수사나 악성코드 분석과 같은 보다 고급의 훈련내용이 개발되어 진행되고 있으나 이러한 체계를 지니지 못한 개도국 수사관이 많이 참여하는 국제훈련의 경우 그러한 경향이 더욱 심하다.

앞서 언급한 바와 같이 디지털포렌식 분야에 대해서는 좀 더 많은 발전이 있었다. 후술하는 바와 같이 미국을 중심으로 선진국에서 디지털포렌식 분야의 교육과 훈련에 대한 체계적인 연구가 상당히 진행되고 있다. 하지만 많은 국가에서 수사관과 디지털포렌식 직종의 완전한 구분은 이루어지지 못하고 있다. 이는 디지털포렌식을 제외한 법의학, 화

학, 물리, 지문, 문서감정, DNA 등 다른 많은 법과학분야가 소위 법과학실(Forensic Laboratory)을 중심으로 이루어져 수사분야와 상당한 분화가 이루어진 것과 상황이 다르다. 그것은 전문화 수준에 따른 이유와 함께 디지털 증거가 가지는 속성에 기인한 것이기도 하다. 즉, 디지털 증거는 그 자체가 독립적인 증거자료로서의 가치와 함께 정보라는 내용을 포함하는 것이기 때문에 항상 수사관은 그 정보를 다루고 그 의미를 파악하는 업무를 하게 되며 이는 포렌식과 완연히 구별되지 않기 때문이다. 예를 들어 특정한 웹페이지를 살펴보고 그 소스코드를 분석하여 연결된 링크에서 범죄의 출처를 추적하는 경우라면 이러한 수사과정 자체가 수사관의 업무 그 자체이기 때문에 법과학적 분석 업무와 구별하기가 곤란해지는 것이다. 이러한 수사관과 포렌식분석가의 업무구분은 전문화의 진행에 따라 점진적으로 이루어지고 있는 상태이며 아직 많은 수사관과 포렌식분석가의 훈련과정은 그 내용이 중첩되는 것들이다.

훈련은 그것이 목적하는 바를 달성하기 위해 잘 구조화되어야 한다. 앞서 언급한 이유로 아직 수사관에 대한 훈련의 필요체계는 많은 연구가 이루어져 있지 못하지만 법과학 훈련에 대한 요건들은 상당한 연구가 이루어져 있다. 훈련과 보수교육은 통상 채용 후에 이루어지기 때문에 소속기관에 따라 프로그램의 형태는 다양하기 마련이다. 여기에서는 훈련과 보수교육이 목표를 달성하기 위해서 어떠한 요소들이 기준을 충족하여야 하는 지에 대해 미 법무부 사법연구소(NIJ 2004)의 기준 모델을 살펴보도록 하겠다.

2) 수사관의 훈련요건

훈련에서는 훈련생의 참가요건, 프로그램의 구조, 훈련의 내용, 평가체제와 기록과 같은 요소들에 대해서 기준의 충족 여부가 검토되어야 한다. 아래 표는 미국 법무부 사법연구소가 제시한 법과학 훈련의 요건들을 정리한 것이다. 이를 사이버수사관의 훈련과 디지털포렌식 훈련의 일반적인 요건으로 볼 수는 없겠지만 적어도 해당 분야에 필요한 요건의 구조를 파악하는 데는 도움이 될 것이다.

〈표 7〉 법과학 훈련의 기준 (NIJ 2004)

항 목	내 용
참가요건	널리 인정된 동료집단이 정한(peer-defined) 표준에 부합하는 특정한 최소한의 학술적 혹은 경험적 요건 등
프로그램 구조	다음의 요소가 문서화되어 있어야 함 학습목표, 교관의 자격, 교육생 요건, 수행목표, 정기적 평가, 적격성 시험(competency test)
훈련내용	프로그램은 다음의 핵심요소와 분야별 내용이 포함될 수 있음 수행 표준 - 직업윤리훈련 포함 안전 - 생물학적, 화학적, 물리적 위해요소를 포함 정책 - 표준실행절차(SOPs), 품질보증, 인증(accreditation), 보안 등 행정적 실험실 정책을 포함 법률 - 전문가증언, 직위해제, 증거법, 형사법 및 민사법 절차, 증거의 인증(authentication) 등 포함 증거취급 - 증거의 인지, 수집, 보존 등 분야간 이슈와 증거연계기록(chain of custody) 포함 의사전달 - 보고서 작성, 증거서류, 공판준비 및 법정 보고 등 문서, 구두, 비언어적 의사 의사전달 기술 포함 분야별 내용 : 분야별 역사, 관계 문헌, 방법론과 검증(validation) 연구, 기구사용법, 통계학, 관련 분야의 지식, 증언
평가체제	훈련생의 발전정도는 다음과 같은 방법을 통해 적절한 간격으로 평가받아야 된다. 구두시험 필기시험 실험실 실습 및 연습 모의 법정 적절한 상급자에 의한 기술적 수행에 대한 평가
기록	훈련과 보수교육에 관한 사항은 해당 프로그램의 구조와 세부내용, 참여요건, 수행결과 등이 기재된 공식문서로 기록되어야 한다.

3) 보수교육

보수교육(continuing education)은 적격성의 유지와 기술 개발, 기타 전문적 활동의 여러 측면을 포함한다. 보수교육은 구조화되고 측정이 가능해야 하며, 기록되어야 한다. 미국 법무부 사법연구소가 제시하는 법과학 보수교육의 기준은 아래의 표에서 정리된 바와 같다.

〈표 8〉 법과학 보수교육의 기준(NIJ 2004)

항 목	내 용
구 조	◦ 학습목표 ◦ 교관 자격 ◦ 세부 교수 요목과 프로그램 설명 ◦ 평가 ◦ 기록
측 정	◦ 구두 시험이나 보고 ◦ 필기 시험이나 보고 ◦ 동료평가(peer-review)된 논문 등 발표 ◦ 교관 혹은 보고자 평가 ◦ 실험실 실습 및 연습 ◦ 기술적 수행의 관찰
기 록	보수교육에 관한 사항은 영속적, 공식적 기록으로 남겨져야 함 기록은 활동에 대한 설명, 형태, 수행결과에 대한 기록 등이 포함되어야 함

라. 현장수사관의 교육

수사관과 법과학자의 교육훈련에 관한 문제를 고려할 때 참고할 수 있는 것은 그 중간적 위치에 놓인 범죄현장수사(Crime Scene Investigation: CSI) 종사자에 대한 논의이다. 종래 범죄현장수사는 훈련받은 경찰관에 의해서 이루어져 왔으며 차츰 이는 보다 전문화된 교육훈련을 받은 범죄현장수사관의 독립된 직종으로 발전하고 있다.

범죄현장기술자(Crime scene technician), SOCOs(Scenes Of Crime Officers)은 국내의 경우 현장감식요원 등 다양한 이름으로 불리고 있는데, 현장수사관은 범죄현장에서 실질증거를 수집하고 처리하는데 있어서 일반적으로 중요한 역할을 수행한다. 현장에서 실질증거를 수집하고 처리하는데 있어서 전문가를 양성해야 한다는 논의는 이미 1950년대부터 있어 왔던 것(표창원 2000)으로 당연하게 여겨지지만, 국내외를 막론하고 현장에서의 부적절한 실질증거의 처리는 사이버수사가 해결해야할 주요 과제 중의 하나로 여전히 남아 있다.

미국의 경우 경찰관(sworn-officer)이 현장수사관으로 활동할 때 일반적으로 특수한

기술과 전문성이 부족하기 때문에 때로 경찰관이 아닌 특수한 훈련을 받은 일반직(non-sworn civilian personnel)이 이를 담당하는 것이 바람직하다는 견해도 있다. 사실 범죄현장의 중요성을 고려할 때 현장에 대한 조사는 사이버수사 분야에서 가장 뛰어나고 경험 많은 전문가가 관장하는 것이 바람직하겠지만 현실적인 제약 때문에 그렇게 되지 못한다는 점을 인정한다(Capsambelis 2007). 따라서 FBI를 포함하여 미국은 여전히 현장수사관의 상당수는 법집행관이 일정 수준의 훈련을 받은 후 배치되고 있다. 이에 따라 미국의 법집행기관에 대한 인증을 시행하는 법집행기관 인증위원회(Commission on Accreditation for Law Enforcement Agencies, CALEA)에서도 현장수사관은 직무훈련(in-service training)과 정기적인 보충교육을 받을 것만을 요구하고 있고 교육에 대해서는 제한을 두지 않고 있다. 법과학연구실에 대한 인증을 하는 법과학연구실책임자협의(ASCLD)의 인증위원회에서도 인증을 받고자 하는 연구실의 대부분의 인력에 대해서 자연과학 분야에 대한 학사 이상의 학위를 요건으로 하면서도 범죄현장 검사관에 대해서는 학력규정을 두지 않고 있다.

한편 현장수사에 분화되어 전문적인 영역으로 점차 인식되고 있는 혈흔패턴분석의 경우 FBI의 혈흔패턴분석에 관한 과학실무그룹(Scientific Working Group on Bloodstain Pattern Analysis)은 혈흔패턴분석가에 대한 교육훈련 최소요건 가이드라인에서 해당 분야의 학사학위 혹은 2년제 학위와 2년간의 경험, 혹은 고졸 이상 학력과 4년 이상의 경험을 최소한의 교육요건으로 제시[5]하여 점차 현장수사 분야도 전문화 및 보다 높은 수준의 정규 교육을 요구하는 추세를 볼 수 있다.

영국은 수많은 법과학 교육 프로그램을 지니고 졸업자의 취업경쟁이 치열하기도 하거니와 영국에서 현장수사를 담당하는 SOCOs는 국가적인 법과학 실무자 등록(CRFP) 범주에 들어갈 정도로 전문적인 영역으로 자리매김하고 있다. SOCOs의 상당수는 경찰관이 아닌 일반직(civilian)이며 대부분의 경찰기관에서 모집시 대학의 전문학위를 요구한다. 그럼에도 워낙 인기가 높아, 경우에 따라 1명을 선발하는데 100명 이상이 지원하기도 한다[6]. 종래 경찰은 대인기술(interpersonal skill)과 결합된 기본적인 인문교양(literacy)와 수리력(numeracy)만으로 현장수사에 충분하다고 보았지만 향후 점차 고

5) http://www.fbi.gov/hq/lab/fsc/backissu/jan2008/standards/2008_01_standards01.htm
6) http://www.kent.ac.uk/careers/forensicsci.htm

도화된 과학과 기술에 대한 지식과 이해가 요구될 것으로 보고 있다(Mennell 2006).

영국의 SOCOs는 채용 후 중앙 경찰교육기관인 국립경찰개발청(National Policing Improvement Agency)에서 9주간의 기초교육을 받고 1~2년간의 On-the-job 훈련을 필수적으로 받아야 하며 정기적으로 2주간의 보수교육과 지문감식, 화재감식, 주요재해, 안면인식기술 등 특화된 부분에 대해서 전문성을 강화할 수 있는 교육기회가 주어진다. 모든 과정을 성공적으로 이수하거나 SOCOs로 5년간 근무한 후에는 NPIA와 Durham 대학교와의 협정에 의한 범죄현장수사 학위과정에 참여할 수도 있다. 일반적으로 CRFP나 국립직업표준(National Occupational Standards)의 사법기술(skills for justice, SFJ) 분야에서 제시된 KSAs를 충족할 것이 요구된다.

영국과 미국의 프로그램 차이를 살펴보면, 운용하기에 따라 현장수사관이 상당한 교육의 수료를 필요로 하는 전문직종인지, 경찰관인지 일반직인지, 신분이 문제가 될 수 있는지, 혹은 선호도 등이 제도의 운용 방식 등에 의해 크게 바뀔 수 있다는 사실을 엿볼 수 있다는 점에서 우리에게 시사하는 바가 크다. 마찬가지의 논의가 사이버범죄수사 분야에도 적용될 수 있겠거니와 향후 이러한 문제에 대한 지속적인 연구가 필요할 것이다.

제2장 사이버범죄수사 교육훈련프로그램

사이버범죄 수사와 관련한 교육훈련은 훈련의 주체와 참가자, 비용의 부담자, 훈련의 목적, 내용 등 여러 측면에서 매우 다양한 형태로 이루어지고 있다. 이를 전반적으로 파악하기에는 어려움이 있겠으나 여러 훈련프로그램들을 살펴봄으로써 이러한 훈련과정들이 지니는 공통적인 특성과 차이, 그리고 장단점을 파악할 수 있을 것이다. 따라서 대표적인 국내외 사이버수사 훈련 프로그램을 정리해 보았다.

제1절 우리나라 교육훈련프로그램

1. 한국국제협력단 초청연수 실시 프로그램

2005년 경찰대학은 경찰에서는 처음으로 한국국제협력단(KOICA)의 국내초청연수 프로그램의 연수기관으로 선정되어 '국제공조 과정' 및 '사이버범죄수사 과정'을 개설하여 18개국 30명의 연수생에 대한 교육을 실시하였다. 이후 국제 사이버범죄 수사과정은 매년 1회 정례적으로 실시하여 2011년까지 45개국 117명이 이 과정을 수료하였다. 한국국제협력단은 매년 훈련과정의 종료 후 참석자를 대상으로 과정평가를 시행하며 그 결과와 수원국의 요청을 종합하며 매년 특정 훈련과정의 개설여부를 결정한다. 경찰대학의 사이버범죄수사 과정에 대한 참석자의 평가는 매우 좋은 편이며 수원국 요청 또한 많아 매년 실시되고 있다.

경찰대학 국제 사이버범죄수사 과정은 한국국제협력단 초청연수사업의 일환으로 이루어지며, 따라서 훈련목적은 사이버범죄에 대한 전문적인 역량의 전수 기본으로 하되 개발도상국의 공무원에게 한국에 대한 이해와 협력 증진, 한국 경찰에 대한 전반적인 소개 등 여러 가지 부가적인 목표를 염두에 두고 있다

〈표 9〉 경찰대학 국제 사이버범죄수사 과정 이수자 현황

국가별	2005	2006	2007	2008	2009	2010	2011	합계
Bangladesh				1				1
Belarus							1	1
Bolivia					2			2
Brazil	1							1
Cambodia	1						2	3
Cambodia				1				1
Cameroon						2		2
China		1						1
Colombia	1	1	1	1	1			5
Congo					1			1
Côte d'Ivoire						1	2	3
Dominican				1				1
Ecuador						3	1	4
Egypt	1	1	1	1	2			6
El Salvador		2	1	2				5
Ethiopia	1				2	2		5
Guatemala		1						1
Indonesia		2		1				3
Jamaica		1	1					2
Jordan					2			2
Kazakhstan		1						1
Kenya						4	2	6
Lebanon						2		2
Maldives			1		1	1		3
Mongolia		2			1	1	2	6
Myanmar							2	2
Nepal	1		1					2
Nigeria	1					2		3
Pakistan	2							2
Panama							1	1
Papua New Guinea		1						1
Philippines	1	2	1	1		3		8
Russia	1							1
Rwanda			1	1	1			3
Serbia-Montenegro		1						1
Sri Lanka	2	2	2	1				7
Tanzania	1							1
Thailand				1				1

Uganda							2	2
Ukraine	1			1			1	3
Vietnam	1	2					1	4
Yemen						2	1	3
Zambia			1					1
Zimbabwe			1	2				3
	16	20	12	15	13	23	18	117

훈련 내용 또한 아래 일정표와 같이 전형적인 경찰대학 내에서의 강의실 훈련 외에도 견학 프로그램과 산업시찰 등 여러 외부활동이 많은 비중을 차지한다. 3주간의 일정 중 주말을 제외하고 13일의 훈련기간 중에 실제 강의실 교육이 이루어지는 시간은 48시간인데, 이는 일일 8시간으로 이루어지는 전형적인 경찰훈련 프로그램으로는 6일 분량에 불과하다. 교육프로그램에 참여에 대한 독려나 엄격한 평가 및 수료제한 등이 없다는 점에서 비긴장형 훈련(non-stressful training)에 속한다고 할 수 있다.

〈그림 2〉 2010 경찰대학 국제 사이버범죄수사 훈련 일정

MON	TUE	WED	THU	FRI	SAT	SUN
2	3	4	5	6	7	8
Arrival Incheon Int'l Airport	**KOICA Orientation**	**•Opening Ceremony** **•Orientation about KNPU**	**L2:** Legal Countermeasures on Cybercrime(LAB)	**L4:** Practical Issues on Cybercrime Investigation(405)	**Free Time**	**Free Time**
		L1: Dynamics of Cybercrime Investigation (LAB)	**L3:** Infrastructure and Security(405) **Campus Tour (-1800)** **Home Visiting (-2300)**	**Country Report** (405) (-1800)		
9	10	11	12	13	14	15
Study visit Police Museum	**L6:** Cybercrime Scene Investigation(LAB)	**L8:** Mobile Forensics -- Introduction and Practice(LAB)	**Field Trip** Ulsan	**Field Trip** Busan	**Field Trip** Kyeongju	**Free Time**
National Police Agency (L5: Korean Police's countermeasures to cybercrime)	**L7:** Internet Tracing(LAB)	**L9:** Forensic Examination and Application(LAB)				
16	17	18	19	20		
L10: National Cybercrime Deterrence Policies(405)	**L12:** Financial Network Security(405)	**Study visit** Asan	**Wrap up session**	**Departure**		
L11: Cyber Criminology(405)	**Group Workshop**	Samsung Electronics	**Closing Ceremony**			

AM : 09:30-12:30
PM : 14:00-17:00

On Campus

프로그램은 해마다 조금씩 변화하고 있는데 아래 보는 표와 같이 대부분의 강의를 외부전문가와 현장실무자가 담당하고 있다.

〈표 10〉 강의구성 사례('09년 사이버범죄수사 과정, 경찰대학)

제 목	강 사	비 고
사이버범죄수사 역학	내부 교수	강의
현대 컴퓨팅과 네트워킹	외부 교수	실습병행
디지털포렌식 개관	외부 교수	실습병행
한국의 사이버범죄수사 실무	내부 교수	
사이버범죄 추세와 전망	실무전문가	
네트워크 수사기법 1,2	실무전문가	실습병행
사례연구	실무전문가	
포렌식 기술 응용 1,2	실무전문가	실습병행
사이버범죄 법률과 국제협력	외부 교수	

위와 같은 형태로 이루어지는 경찰대학 훈련과정은 사이버범죄수사 전문 훈련과정으로는 여러 가지 문제점을 지니고 있다. 먼저 훈련생의 배경이 너무 다양하여 특정한 부분에 전문화된 훈련을 실시하기에는 어려움이 적지 않다. 일부 훈련생은 기초적인 사이버범죄수사 기술을 이미 가지고 있어 좀 더 고도화된 프로그램을 요구하는 반면 더 많은 훈련생은 기초적인 수사기술조차 이해가 어렵다고 호소를 하고 있다. 하지만 이러한 모든 요구를 충족하기에는 시간이 부족한 대신 너무 전문적인 내용 위주로 진행하여 산업시찰 등 여러 다양한 경험을 할 수 있는 기회를 포기하지 않을 수 없다. 훈련생의 수준을 요구사항(requirement)으로 엄격하게 제한하는 것도 개발도상국에서 해외 연수의 기회가 매우 드물기 때문에 국가별로 임의적으로 선정되는 관행을 어느 정도 인정하지 않을 수 없다.

기본적으로 경찰대학 훈련과정은 2006년 이래 매년 이루어지고 있지만 개인별로 자기계발의 전후관계를 고려하지 않은 전형적인 경찰의 블록형태의 훈련과정이다. 따라서 참석자의 기대와 훈련내용을 유기적으로 연계하는데 상당한 어려움이 있다. 이러한 문제점은 국가별 요청에 의해 이루어지는 대부분의 다른 국내외 훈련과정에서도 공통적으로 나

타나는 문제이다. 따라서 교과는 그 때 그 때 필요에 의해 만들어지며 교과를 만든 후에 해당 분야의 전문가를 초빙하여 강의를 일임하고 있는 상황이다. 2010년 과정 중 경찰대학 전임교수에 의해서는 단 한 강좌(3시간) 강의만이 이루어져 외래교수 비율이 압도적인 형편이다.

이러한 교과의 편성은 다양한 분야의 주제들을 폭넓게 다루어볼 수 있다는 장점이 있지만 훈련생에게 뚜렷한 목표를 제시하고 특정한 지식이나 기술, 역량을 갖추도록 훈련 효과를 기대하는 데에는 한계가 있다. 사이버범죄 수사분야에 영어와 강의가 가능한 전문인력이 부족하며 이러한 인력이 경찰청 사이버수사부서 등 현업에 종사하고 있어 충분히 강의준비를 하기에는 시간 등 자원이 충분히 제공되지 않는 것도 문제이다. 이러한 문제 역시 다른 국내에서 시행되는 국제 훈련과정에서도 대부분 공통적으로 발견되는 현상이다. 후술하는 유럽의 사이버범죄 훈련체계는 이러한 문제들이 국내에 고유한 문제가 아니라 국제 사이버범죄 훈련에서 공통적으로 나타나는 현상이며 이 문제를 어떠한 식으로 해결하려고 노력하고 있는 지를 잘 보여준다고 생각된다.

2. 국제형사경찰기구 주관 국제훈련 프로그램

경찰은 1999년 136개 회원국에서 940여 명이 참여한 가운데 국제형사경찰기구(인터폴)의 가장 중요한 행사인 제68차 인터폴 총회를 개최한 것을 비롯하여 주요한 국제 인터폴 회의와 교육훈련 프로그램을 주관하여 진행한 바 있다.

〈표 11〉 경찰의 주요 인터폴 행사 유치 현황

기 간	행 사 명	참가자(국/명)
1999. 11. 8	제68차 인터폴 총회	136/940
2002. 4. 23	한·중·일 경찰(인터폴) 회의	3/24
2002. 10. 15~17	제5차 인터폴 국제컴퓨터범죄회의	37/150
2002. 10. 18~19	제4차 인터폴 아·태지역 IT범죄수사 실무회의	12/30
2004. 7. 19~21	제2차 인터폴 아·태 IT범죄수사훈련 세미나	8/60
2004. 11. 8~12	제1차 아·태 IT범죄수사 교관양성 교육	10/16
2007. 6. 25~29	제5차 아·태 IT범죄수사 교관양성 교육	8/17
2007. 9. 17~20	제6차 아·태지역 인터폴 요원 워크샵	35/88
2008. 11. 14	제10차 인터폴 아·태 IT범죄수사 실무회의	12/30

이외에도 2008년 11월 인터폴과 경찰청이 공동으로 '사이버범죄대응 심포지엄'을 서울에서 개최하는 등 점차 참여의 폭을 확대하고 있다. '사이버범죄대응 심포지엄'은 2002년부터 매년 경찰청이 주관하여 서울에서 개최하는 국제행사로 2009년의 경우 36개국 400여 명이 참석하여 최신의 사이버범죄 동향과 수법, 수사기법 등을 발표하고 대책을 논의한 바 있다. 후술하는 인터폴의 교육프로그램에 수사관 등 전문가를 교관으로 파견하는 것 또한 일반적인 국제기구와 관련된 교육지원 형태로 볼 수 있다.

가. 교관 파견

교육과정을 운영하거나 관련 행사를 개최하는 것 외에 또 다른 교육지원의 중요한 형태는 특정한 분야에 교수역량을 지닌 전문인력을 파견하는 것이다. 경찰은 다양한 형태의 인터폴 교육 등에 교관을 파견하고 있는데 이중에 최근에는 사이버범죄 수사 분야에 대한 교관 파견 수요가 두드러지고 있다. 아래는 최근 이루어진 사이버범죄 수사 분야 교관 파견 실적을 정리한 것이다.

- 2004년 이후 매년 1~2회 실시되는 아·태 IT범죄수사 교관양성 프로그램 및 2007년부터 실시되는 디지털 포렌식 교관양성 프로그램에 교관 파견
- 2005. 5. 23.~29. 국제협력단 전문가 파견 프로그램으로 말레이시아 동남아 대테러 센터에 2명 파견
- 2006. 6. 19.~23. 초청으로 태국 국제법집행기관 교육센터(ILEA)에 2명 파견
- 2006. 10. 9.~20. 국제협력단 전문가 파견 프로그램으로 베트남 공안부에 4명씩 2개조 8명 파견
- 2008. 6. 26.~7. 8. 멕시코 정부 초청으로 멕시코 경찰학교에 3명 파견
- 2009. 8. 7.~8. 19 멕시코 정부 초청으로 멕시코 경찰학교에 사이버수사 분야 2명, 과학수사 분야 3명 파견

사이버범죄수사 분야는 이외에도 경찰청 전담부서인 사이버테러대응센터가 영국(NHTCU, 2005), 프랑스(OCLCTIC, 2005), 미국(FBI, 2006), 독일(BKA, 2007) 등 주요 국가의 사이버범죄 전담부서와 부서간 업무협정을 체결하고 2008년에만 38개국 169명이 동 센터를 방문하는 등 타 분야에 비해 두드러지게 활발한 국제교류 활동을

이어가고 있다.

나. 외국경찰관 초청 단기연수 프로그램

경찰청은 2009년 7월부터 6개월간 10개국 13명의 외국경찰관을 초청하여 경찰전문화와 한국어 등에 대한 심화교육 프로그램을 진행하였다.

〈표 12〉 경찰청 외국경찰관 초청 단기연수 프로그램 개요

기 간	2009년 7월 13일 ~ 12월 20일
참가국(인원)	10개국 13명 멕시코, 아르헨티나, 예멘, 우즈베키스탄, 키르기스스탄, 몽골, 필리핀, 베트남(2명), 캄보디아(2명), 태국(2명)
교 육 분 야	경찰전문화교육(과학수사 등 치안시스템 전반) 한국어교육(한국외국어대학교)

이 프로그램은 기존의 교육훈련 프로그램이 대부분 1~3주 내외의 짧은 기간에 이루어져 왔고 한국국제협력단 등 외부 예산을 활용하여 이루어진 것과 달리, 비교적 장기간의 교육을 경찰청이 별도의 예산을 확보하여 진행했다는 점에서 특색이 있다. 이 교육에는 2009년 3월 예멘에서 발생한 한국인 대상 테러사건에서 현지 경찰과의 긴밀한 협력의 강화 필요성에 대한 양국의 공감을 토대로 현지 경찰관을 교육대상에 포함시켰는데, 이는 교육을 통한 인적교류가 실질적인 국제공조의 강화에 긍정적인 영향을 미친다는 경험을 토대로 한 것이다.

3. 경찰청 사이버범죄수사 훈련

세계적인 수준을 자랑하는 경찰청 사이버테러대응센터(CTRC)에서도 IT 기술의 발달에 따라 지능화·첨단화하는 사이버범죄에 대한 수사역량을 제고하기 위해 계속적으로 분야별 전문교육을 시행함으로써 최첨단 범죄에 대응하는 사이버 수사전문가 양성하고 있다. 현직 사이버수사요원을 대상으로 한 교육훈련 과정을 살펴봄으로써, 현재 진행 중인 사이버수사 및 교육훈련의 흐름을 파악할 수 있고, 개발도상국 사이버수사 교육훈련 프로그램의 개발에도 좋은 모범을 제시할 수 있을 것이다.

가. 사이버범죄수사관 전문화 교육계획(2007년)

경찰 내부에서 실시하는 교육만으로는 IT기술 발달에 따라 지능화・첨단화하는 사이버범죄에 대응하기 어려워 외부의 전문기관에 위탁하여 실시하는 특별한 형태의 교육이 필요하다. 이 교육은 사이버수사관의 입직경로, 수사경력, 교육이수 분석 및 사전이해도를 미리 점검하여 각 수준 및 분야에 따라 시행하였다.

1) 교육과정

총 8개 과정으로 327명에 대해 실시하였으며, 교육 대상자를 엄격하게 선별하여 교육효과가 사장되지 않도록 체계적 관리하고, 이들 교육 이수자들을 추후 사이버수사 관련 전수교육 강사로 활용하도록 진행하였다.

〈표 13〉 2007년 사이버범죄수사관 전문화 교육

구 분	연 번	과 정 명	주 요 내 용	기 간	인 원
총 계		8개 과정			327명
사이버 범죄 수사	1	해킹·악성코드 대응 전문과정	해킹·악성코드 대응기법	3주	20
	2	DB분석 고급과정	Mssql, Oracle 등	5일	15
				5일	15
	3	인터넷추적 고급과정	VoIP, IPV6 등	5일	15
				5일	15
	4	IT 기초과정	자격증 지원 등	연간	200
디지털 증거 분석	5	파일시스템 교육과정	NTFS 등	3일	10
	6	Encase 고급과정	고급과정	4일	15
	7	물리복구 고급과정	하드 디스크 물리 복구	5일	2
	8	모바일 과정	분석 및 복구	2일	20

2) '해킹・악성코드' 분석과정 위탁교육

해킹·악성코드가 지능화됨에 따라 범죄수사를 위해서는 네트워크, 해킹방법, 프로그래밍 등 IT에 대한 종합적 전문지식이 필요하게 되었다. 따라서 사이버테러에 대한 국가적 차원의 전문 수사인력을 양성하기 위하여 경찰 내부에서 시행할 수 없는 교육을 민간에 위탁하여 추진하였다.

경찰대학 사이버수사교육장에서 '이지스원 시큐리티' 김태일 팀장 등 2명이 고급과정과 중급과정으로 나누어 20명씩 교육하였으며, 사이버특채자로 수사경과자인 자이거나 사이버수사 분야(교육기관 포함)에서 근무 중인 자 중에서 근무경력이 3년 이상인 사이버수사관을 대상으로 수준 테스트를 실시한 후 반을 편성하여 교육을 하였다.

〈표 14〉 '해킹 · 악성코드' 분석 고급과정 교육내용

과정명	일 차	교 육 내 용
해킹 기법 분석I	1일차	해킹사례연구 1. Mass SQL Injection, Backdoor, Keylogging, HTTP tunneling, NetBIOS Bruteforcing
	2일차	해킹사례연구 2. Cross Site Request Forgery, CSRF, Malicious Code Injection, Reverse Shell, SSH tunneling, Database Backdoor
	3일차	해킹사례연구 3. Cross Site Scripting XSS를 이용한 이메일 유출, Proxy를 이용한 방화벽 우회, HTTP tunneling, SQL Injection
	4일차	해킹사례연구 4. 악성코드를 이용한 공격 Excel 취약점을 이용한 악성 코드 배포, ARP Cache Poisoning, SSH Version Rollback, SSH MITM
	5일차	해킹사례연구 5. Wireless Hacking WEP/WPA Cracking, DNS zonetransfer, SSL MITM, Web Shell Upload, 익스플로이팅, NetBIOS Cracking
리버스 엔지니어링	6일차	Architecture : 명령어 실행 사이클, Segmentation & Paging, IA32 기본 커맨드 MOV, MOVZX, MOVSX, MOVS, AND, OR, XOR, SHL, SHR, LEA, ADD, SUB, MUL, DIV, CALL,JMP 등 함수 호출 규약 : Call Stack, Frame Pointer Omission, 함수 호출규약, 함수 호출 방법, PE File Format
	7일차	PE 파일 포맷 : DOS Header, DOS Stub, PE Header, PE Optional Header, Data Directory, Section Table, Exporting & Importing Mechanism 디버깅 기초 : 디버깅 절차, 브레이크 포인트의 유형 및 사용방법, Step Over/Step Into/Step Out, 메모리, 레지스터 내용 조사 및 변경, 프로세스, 쓰레드, 핸들정보 조사, Windbg & OllyDbg 주요기능
	8일차	디스어셈블링 기초 : IDA 기본 사용법, 지역변수/전역변수/파라미터 식별, 배열, 구조체 식별, 클래스 식별, IF/IF-ELSE/SWITCH-CASE 문식별
	9일차	Anti Reversing 기법의 이해 Anti Disassembling 기법, 디버거 탐지 및 무력화, 브레이크 포인트 탐지 및 무력화, TLS Callback
	10일차	Packing & Unpacking : Packing 의 원리, Manual Unpacking 의 원리 및 실습

악성 코드 분석I	11일차	Shadowbot Malware Analysis (IRC bot, DLL injection)
	12일차	감염 시간 및 감염 경로 파악, DLL injection의 이해, 감염된 PC로부터 Shadowbot 탐지 및 추출, 임포트 테이블 및 스트링 분석, 악성코드 런치 포인트 분석, C&C 식별, 봇넷 유형 파악 및 봇넷 시뮬레이션(IRC Botnet), 명령어 리스트 추출, 악성코드 기능 분석, 전파 메커니즘 파악
	13일차	Black Enery Malware Analysis (HTTP bot, DKOM) 감염 시간 및 감염 경로 파악, DKOM 을 이용한 Process Hiding의 이해, 메모리 덤프 분석을 통한 Hiding의 이해, 메모리 덤프 분석을 통한 Hidden Process 탐지, 감염된 PC로부터 Black Energy 탐지 및 추출, 악성코드 런치 포인트 분석, C&C 식별, 봇넷 유형 파악, 봇넷 프로토콜 분석 (HTTP Botnet), 명령어 리스트 추출, DDoS 공격 기법의 이해, 악성코드 기능 분석, 전파 메커니즘 파악
	14일차	Buffer Overflow의 이해 : Buffer Overflow 의 기본 개념, Trampoline Technique, SEH Overwriting
	15일차	익스플로잇 분석 case study : PDF, Excel 익스플로잇 페이로드 식별, 페이로드 추출 및 분석, PDF 취약점을 이용한 익스플로잇 분석, Excel 취약점을 이용한 익스플로잇 분석

〈표 15〉 '해킹 · 악성코드' 분석 중급과정 교육내용

과정명	일 차	교 육 내 용
해킹 기법 분석 II	1일차	해킹사례연구 1. 리버스 엔지니어링 : Active X 리버싱을 통한 웹 쉘 업로드, HTTP tunneling, 익스플로잇팅, Keylogger, Database Backdoor(1)
	2일차	해킹사례연구 2. htaccess 설정 취약점을 이용한 웹 쉘 업로드, SNMP 이용 방화벽 설정변경, SSH tunneling
	3일차	해킹사례연구 3. 악성코드를 이용한 해킹 악성 코드 배포, keylogging, VPN Client 해킹, DB Client 리버싱, Database Backdoor(2)
	4일차	해킹사례연구 4. Wireless Hacking Caffe Latte Attack, DTP attack, NetBIOS Cracking 등
	5일차	해킹사례연구 5. 비즈니스 로직 분석 Proxy를 이용한 방화벽 우회, CSRF, Business Logic Analysis, 악성코드
루트킷 및 악성 코드 탐지	6일차	Rootkit 개요 : Rootkit 기술, User Mode Rootkit, Kernel Mode Rootkit Hooking : IAT Hooking, Inline 함수 Hooking, SSDT Hooking, IDT Hooking, SYSENTER Hooking Runtime Patch : Detour Hook, Jump Template
	7일차	Direct Kernel Object Manipulation DKOM 이용한 프로세스 은닉, DKOM 이용 디바이스 드라이버 은닉, DKOM 이용권한상승 Covert Channel : TDI·NDIS 이용 루트킷, 네트워크 패킷변경, TCP/IP Protocol Spoofing
	8일차	악성코드 탐지 : Live System 분석 프로세스 모니터링 및 분석을 통한 비정상 프로세스 식별, 파일시스템 조사를 통한 비정상 파일식별, 패킷 분석을 통한 비정상 트래픽 및 관련 프로세스 식별
	9일차	악성코드 탐지 : 메모리 덤프 분석 메모리 덤프 작성, 메모리 풀 분석을 통한 커널 오브젝트 식별, 프로세스 & 쓰레드 리스팅 및 스캔 기법, Kernel 심볼릭 링크 스캔 기법
	10일차	

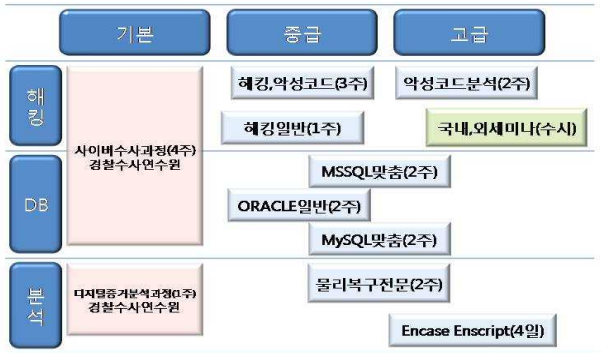
악성코드 분석 Ⅱ	11일차 12일차 13일차	악성코드 case study : ZxShell (C&S bot, IRP Hook, 재감염 및 변종 생산) 감염 시간 및 감염 경로 파악, IRP Hook의 이해, IRP Hook 탐지, 감염된 PC 로부터 ZxShell 탐지 및 추출, 임포트 테이블 및 스트링 분석, 악성코드 런치 포인트 분석, C&C 식별, 봇넷 유형 파악 (C&S Bot), 통신 프로토콜 분석, 명령어 리스트 추출, 악성코드 기능 분석, 전파 및 재감염 메커니즘 파악
	14일차	악성코드 case study : zhelatin (P2P bot, SSDT/IRP Hook, DDos/Spam) 감염 시간 및 경로파악, SSDT Hooking의 이해, SSDT Hook & IRP Hook 탐지, 악성코드 추출 및 매뉴얼 언패킹, 임포트 테이블 및 스트링 분석, 악성코드 런치 포인트 분석, P2P Botnet의 이해, 통신 프로토콜 분석, 명령어 추출, DDos 공격 기법의 이해, DDos 공격 메커니즘 분석, Spambot 이해, Spamming 분석, 전파 및 재감염 메커니즘 파악
	15일차	악성코드 case study : conficker(자동업데이트, 다양한 감염 전략, 자기방어) 매뉴얼 언패킹, 암호화된 페이로드 복호화, 임포트 테이블 및 스트링 분석, NetBIOS를 이용한 감염 전략 분석, USB 저장 매체를 이용한 감염 전략 분석, 자기 방어 메커니즘 분석, HTTP pull을 통한 업데이트 기능 분석, NetBIOS push를 이용한 업데이트 기능 분석

나. 전문 사이버수사 교육(2008년)

사이버수사관이 보유한 IT 전문지식과 추적수사기법은 범인추적 및 증거확보에 결정적인 변수로 작용하게 된다. 따라서 IT 기술발달에 따라 지능화·첨단화하는 사이버범죄에 대응하기 위해서는 지속적으로 신기술 습득을 위한 교육이 필요하다.

경찰청에서는 경찰수사연수원에서 실시하는 일반적인 사이버범죄 수사교육 이외에 추적수사기법 개발이나 분석프로그램 개발 등 전문교육을 실시하고, 디지털증거분석과 관련하여 국내·외 최고 수준 기관의 심층 및 고급 교육을 실시하는 등 총 3개 분야 8개 과정에서 117명을 교육하였다.

〈그림 3〉 2008년 전문 사이버수사 교육개요



1) 해킹·악성코드범죄 대응과정

금전을 목적으로 하는 민생 침해적인 해킹·악성코드범죄가 전국적으로 발생하고 있기 때문에 경찰청뿐만 아니라 각 지방경찰청에도 수사가 가능한 전문인력을 집중하여 양성하기 위한 과정이다. 2007년 해킹·악성코드 전문대응과정(20명, 3주)을 고급, 중급, 일반과정 등 수준별로 세분화하고 대상 교육인원을 20명으로 확대하였다.

악성코드 분석을 중심으로 고급과정은 2주 동안 20명을, 해킹·악성코드 분석 전반을 다루는 중급과정은 3주 동안 20명을, 침해사고분석 등 일반 IT 교육기관 개설과정은 1주 동안 10명을 교육하였다.

2) DB 분석과정

사이버범죄 및 일반범죄에서 현장에 있는 컴퓨터 서버의 증거자료를 압수할 경우 또는 유효한 증거 추출의 기반기술이 되는 데이터베이스(DB) 관련 심화교육을 실시하였다. 데이터베이스(database)는 대용량 자료를 빠르게 처리하는 프로그램으로서, 현재 가장 많이 쓰이는 데이터베이스 프로그램 중 MSSQL 분석, MYSQL 분석은 전문기관에 맞춤교육을 2주 동안 20명에 대하여 실시하였고, ORACLE 분석은 오라클사(社) 일반과정에 2주 동안 4명을 교육하였다.

3) 디지털증거분석 물리복구과정

디지털 기기가 파손 또는 훼손된 경우 기기에 포함된 자료를 복구하기 위한 기반기술로서, 정보통신에서 주로 이용되는 USB 저장장치, 노트북 컴퓨터, 개인용 컴퓨터 등의 파일시스템 등에 대한 심화교육을 물리복구 전문기관으로서 충북 청원군 오창면에 소재한 명정보기술 본사에서 2주간 10명에 대해 실시하였다.

4) Encase Enscript과정

2007년 교육한 Advanced 과정의 상위과정인 Enscript 과정 교육 통해 디지털증거분석과 관련된 역량을 강화하였다. Encase는 미국·영국·일본 등 각국 수사기관에서 가장 많이 사용하는 증거분석프로그램으로서 교육을 통해 분석능력에 대한 국제인증의 효과도 함께 가져올 수 있다.

Encase 프로그램 제작업체인 미국 GSI사(社)의 담당자를 국내에 초청하여 1주 동안

15명에 대해 강의를 실시하였다.

다. 디지털 증거 분석과정

해킹·악성코드가 지능화됨에 따라 범죄수사를 위해서는 네트워크, 해킹방법, 프로그래밍 등 IT에 대한 종합적인 전문지식이 필요하므로, 사이버테러에 대한 대응역량 제고를 위해 국가적 차원에서 전문인력을 양성할 필요가 있다.

〈표 16〉 2009년 디지털 증거분석과정 교육내용

일 자	교 육 내 용
1일차 미국 GSI 강사	• Encase 소프트웨어 개괄 및 업데이트 현황 • 기술연구 : multi-byte 값 해석하기, big endian, little endian • 파일포맷(NTFS) - 내부파일(Internal files), master file table(MFT), MFT attributes - 잔류 및 비잔류 데이터(resident/ non-resident data) - 조각난 파일 문서조사, NTFS상에서 삭제된 파일 - MFT 해석을 위한 Enscripts 사용하기(Using Enscripts to decode the MFT) - MFT를 정상적 수단으로 접근할 수 없을 때 데이터 복구하기
2일차 미국 GSI 강사	• RAID - RAID의 하드웨어 및 소프트웨어, RAID Levels, 포렌식 관점에서의 접근 - 하드웨어와 소프트웨어 RAIDs 해독을 위한 encase 사용하기 • 윈도우즈 이벤트 로그 - 이벤트 로그 포맷, 윈도우즈와 encase를 이용하여 이벤트 로그 해독하기 • NTFS $ LOGFILE - 용도와 작동, 잠재적 인공물(Potential artifacts) - Extracting $LOGFILE data using Enscript programs • 암호 - 역사와 용어(terminology), 암호화된 데이터의 위치, 암호해독을 위한 실습 - Encase EDS module, NT/2K/XP/2K3 패스워드 복구, NTFS의 암호화된 데이터
3일차 미국 GSI 강사	• 리눅스/유닉스 디스크 레이아웃 및 파일시스템 - 파티션 및 슈퍼블럭, Inode table, mounted volume, 디렉토리 구조 - 파일을 위한 데이터 위치 서류조사, symbolic/ hard links • 리눅스/유닉스 사용자 계정 및 권한 허용 • 리눅스/유닉스 패스워드 해독 : 패스워드/쉐도우 파일 • 리눅스/유닉스 : 쉘 히스토리, 시스템 로깅, 사용자 권한(UTMP/WTMP Files) • 리눅스 파티션 복구 - 슈퍼블럭 센터에서 문서화된 필드 사용하기(Use fields documented in superblock sector) - encase 프로세스에 정보 제공하기 • encase 리눅스 버전을 이용하여 포렌식 획득

4일차 미국 GSI 강사	• 매킨토쉬 파일시스템 - HFS/HFS+, 디스크 및 볼륨 조직, 파티션 지도, 파일시스템 구성요소 및 조직, 파일구조 • 매킨토쉬 포렌식 조사 : 이미징 • MAC OS 8,9 AND 10 artifacts - 시스템 폴더, 최근 접근된 파일 및 프로그램, 인터넷 다운로드 히스토리, 사용자 데이터 - 시스템 환경정보 • 필터/쿼리/상태 - 백그라운드/정의, 리소스 - Introduction to objects, classes, properties and methods - Building basic filters within the "ENTRIES/Home' view - Building a compound filter - combining filter to form queries - Using the conditions "wizard" to build conditions
5일차 교육사업업 체주관	• 디지털증거분석 장비 활용법 교육 및 교육평가 실시 등

라. 사이버테러 핵심 수사요원 위탁 교육(2010년)

해킹, DDoS 공격범죄가 국경을 초월하여 발생하고, 점차 조직화되면서 국가기관·금융·교통·행정 등 주요 기반시설을 집중 공격하는 추세로서 사이버테러가 지능화·첨단화하여 국가안보에 위협요인으로 등장하였다.

국제적 해킹사건을 수사하기 위해서는 해킹 분석기술과 범죄수사뿐만 아니라 외국어 능력까지 겸비한 전문인력이 필요하므로 최고 수준의 해킹 공격·방어·분석기법 습득하기 위해 미국·중국에 위탁교육을 실시하게 되었다. 특히 '중국발(發) 해킹사건'에 있어서 수사역량을 제고하기 위해 적극적으로 추진하여야 할 필요성이 있다.

사이버테러 수사과정 중 국내교육은 전문 교육기관에서, 국외교육은 미국 SANS·GSI사(社) 그리고 중국 연변과학기술대 부설 교육기관에서 실시하였다. CEIC 2010은 미국 GSI사에서 매년 개최하는 전 세계 디지털증거분석 분야 전시회 중 가장 인지도가 높은 전문 컨퍼런스로 전 세계 컴퓨터 포렌식 조사관, 사이버보안 전문가, 사법기관, 정부기관 등이 참여하며, SANS사, GSI사는 해킹공격·분석, 디지털포렌식 기술에서 세계 최고의 정보보안 교육업체이다. 또한 중국발 해킹사건의 약 50%가 중국 연변지역으로 나타남에 따라 해당 지역 내 전문 교육기관을 선정하여 교육을 추진할 필요성이 있다.

〈표 17〉 2010년 사이버테러 수사과정 교육내용

일 자	교 육 내 용
1주차	• Window Sever 해킹공격 방법론과 대응방어/ 정보보안의 위협요소 STRIDE 모델 • Window Sever 해킹공격 프로세스 7단계/ OSL 7 Layerdp Ekfms Window Sever 공격 패턴 • 일반적인 해킹공격 대응 방법/ 보안 솔루션 프레임워크 모델, SRMD • Window Sever 인프라 기반 정보보안 서비스/ Cobit 모델 기반의 MSRA • Window Sever의 해킹공격을 예방하기 위한 방법들 • osl 7 Layer 따른 해킹공격 대응을 위한 방어 보안 솔루션
2주차	• 리눅스/유닉스 시스템 서비스 / 프로세스, 이상, 시스템 서비스, 서비스 이상 모니터링 • 리눅스/유닉스 시스템의 파일시스템 분석 / 유닉스, 리눅스, 파일 시스템 구조 • 리눅스/유닉스 RAID 기법 및 디스크 가상화 / RAID 소개, 볼륨 복구 방법 등 • 리눅스/유닉스 파일시스템 복구 방법/ 장애대처 및 증거 수집을 위한 디스크 백업 • 파일 삭제 원리, 삭제 된 파일 복구 방법, LOST+FOUND 폴더의 삭제된 파일 분석 • 디스크 SLACK 공간 점검 방법/ 리눅스/유닉스 네트워크 서비스 / 네트워크 서비스 • 분석을 위한 유닉스 계열 명령어 / 시스템 점검을 위한 명령어, 시스템 분석을 위한 명령어
3주차	• 데이터 베잇 보안 / SQL 구문. SELECT, DML, TABLE, VIEW, USER ASSES • 절차형 SQL, 트리거 및 저장 프로시스 • My SQL /기본구조도, 설치 및 테스트, 옵션파일 및 로그파일, 메타데이터 조회, 일반적인 보안이슈, MySQL 액세스 권한권리, MySql 유저 계정 관리, 트리거 및 저장 프로시저를 통한 감사기능 구현 • SQL Sever 기초, SQL Sever Forensics, SQL Sever 분석자료, SQL Sever 분석준비 • 침해탐지, 분석자료 수집, 분석자료 분석, SQL Sever 루투킷 • 오라클 보안/ 데이터 베이스 개요, 오라클 관련 파일 보안, 접속 및 인증과정 통제 • 오라클 네트워크 및 리스너 보안, 유저본안, 권한 및 룰 관리, 애플리케이션 보안
4주차	• 프로그램 핸들링을 통한 악성코드 분석, 악성코드 실행을 위한 환경 구성 및 실습 • 원격조정 프로그램 및 ZOMBI 생성, 감지방법 • 지능화된 공격도구,방법, 악성 도구 탐지 및 분석 • 리버싱을 이용한 악성코드 분석/ 리버싱 엔지니어링 실습 기초 • 리버싱 엔지니어링 실습 및 KEYGEN 만들기 • Packing과 Unpacking

〈표 18〉 2010년 사이버테러 수사과정(미국)

기 간	교 육 과 정	교 육 내 용
1주차	디지털포렌식 (컨퍼런스)	• 해킹공격 디지털 포렌식 기술(패킷위조, Spoofing, Tunneling, 위장 AccessPoint) • 악성코드 분석도구를 활용한 역공학 분석기법 • 고급 은닉기법 분석 • Entropy로 인한 악성코드의 실행 • DDOS 등 BotNet 공격기술 • Case Study

2주차	Malware Analysis (악성코드 초급분석)	• 시스템 물리 메모리 이미징 • 휘발성 시스템 테이터 획득 • 원격 증거 수집 • 악성코드 분석 • 가동 중인 윈도우 시스템의 물리적 메모리 채증 및 분석 • Registry Key 접근 및 파일 수집 • DLL 침입 및 보안침해 프로세스 수집 • Dropper (악성코드 컴포넌트) • 탐지 회피 기법
3주차	Malaware Reverse Engineering (악성코드 고급분석 - 역공학기법)	• 악성코드 분석 체계 구성 • 악성 윈도우 코드 행위 분석 • 코드 레벨 역공학분석 • Flash Program 역공학 분석 • Java Script& VBScript 분석 • MS 오피스 및 PDF 문서 분석 • 악성코드 분석 도구 활용법 (IDA Pro, Malzilla 등)

〈표 19〉 2010년 사이버테러 수사과정(중국)

기 간	과 정	교 육 내 용
1주차	공격방법 소개	• Backdoor 도구 • DDOS 도구 • 자주 사용되는 해커 공격수단
2주차	WEB 공격	• Web-SQL 도구 • Web-Scan 도구 • Web 서버 보안
3주차	공격도구	• Web-Shell 도구 • Sniffer 도구 • 자주 사용되는 네트워크 공격 방식 • 스캔공격, 트로이 목마, 이메일공격, DDOS 공격
4주차	악성코드 분석도구	• 악성코드 분석 도구 습득 • 디버거, 디스어셈블러, 기타 도구 • 해킹 및 보안 유틸리티 소개 • 해킹 및 보안 기초 이론 학습
5주차	악성코드 초급분석 실습	• 트로이목마 등 원격 조종 프로그램 • 각종 악성코드 샘플분석 및 분석보고서 작성실습 • 보고서 작성 실습
6주차	악성코드 고급분석 실습	• 원격서버 패킷 캡쳐 • VPN 프록시 소개, 트로이목마 프로그램 • XML 웹서비스 트로이목마 • 프로젝트 - 개인별 악성코드 분석 보고서 작성

제2절 외국 대학의 교육훈련프로그램

1. 미국의 대학과정

미국에서는 훈련받은 디지털 포렌식 전문가에 대한 수요가 폭발적이며, 심지어 전통적으로 이 분야의 수요를 창출하고 발전시키는데 중요한 기여를 했던 법집행기관에서는 상대적으로 낮은 보수 등으로 인력부족이 심각하다. 퍼듀대학교와 같이 잘 알려진 디지털 포렌식 과정을 졸업한 학생(석사)들은 최초 85만에서 100만 달러의 연봉을 제시받으며, 그렇지 못한 대학들도 50만에서 60만에서 시작하지만 3~4년 안에 150만 달러 가까이 연봉이 증가한다고 한다[7]. 이러한 상황은 미국에는 디지털 포렌식에 대한 대학에서의 교육을 폭발적으로 증가시키고 있어 이미 2006년도에 그 수가 100여 개 코스에 이른다고 한다.[8] 그 목록의 일부는 E-evidence Information Center 웹사이트에서 확인할 수 있다.[9] 일반적으로 대학에서의 교육은 컴퓨터 공학, 형사정책(Criminal Justice), 경영학 과정 등에서 한두 개의 일반적인 코스를 제공하거나 자격 혹은 석사과정에서 예닐곱 개의 집중적 과정을 제공하는 형태로 진행된다.

대학 외의 포렌식 훈련은 특정한 소프트웨어 업체의 훈련, 산업계의 훈련, 또한 전문기관의 훈련 등으로 구분될 수 있다. 이러한 교육과 훈련제도에서 가장 큰 쟁점은 누가 급변하는 디지털 포렌식 분야를 전문가를 양성해야 하며, 어떠한 표준이 적용되어야 하는 것이다.

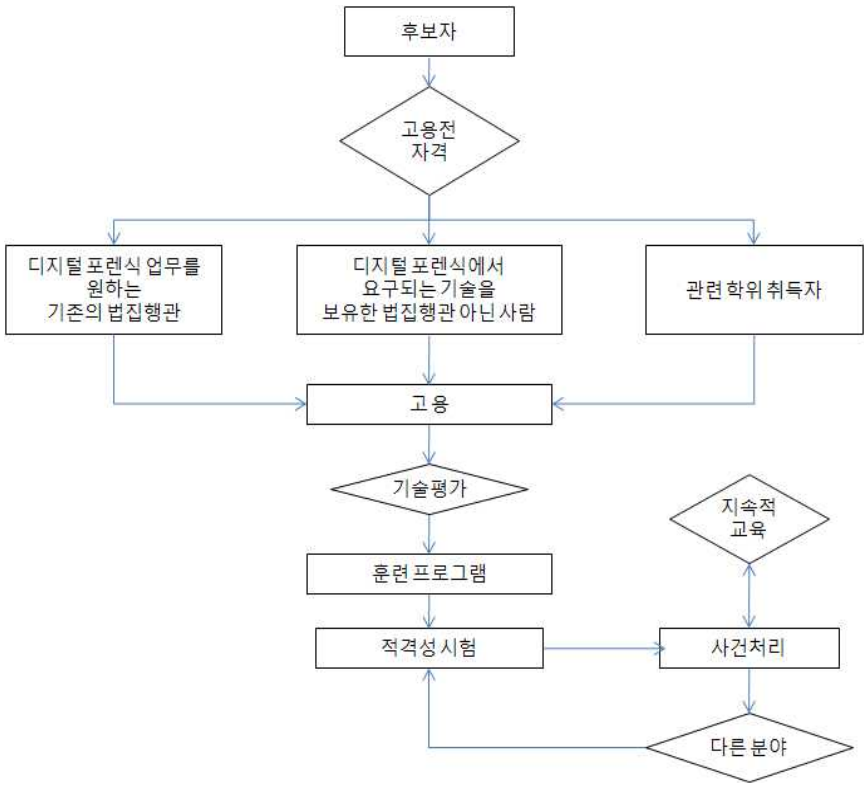
가. 대학에서의 사이버수사 교육

미국에서는 국립사법연구소를 중심으로 법과학 교육 품질을 향상시키기 위한 노력을 경주하고 있다. 2004년의 법과학 교육을 위한 TWGED의 가이드라인에 포함시키지 못한 디지털 포렌식 분야에 대한 교육훈련을 위한 TWGED(Technical Working Group

7) C. Taylor, B. Endicott-Popovsky, A. Phillips, "Forensics Education: Assessment and Measures of Excellence", proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE 2007), 155-165, 2007.
8) http://www.usatoday.com/tech/news/techinnovations/2006-06-05-digital-forensics_x.htm. 참조
9) http://www.e-evidence.info/education.html 참조.

for Education and Training in Digital Forensics)의 보고서가 작성되어 국립사법연구소에서 출간을 기다리고 있다.[10] 동 보고서에서 디지털 포렌식 실무가의 경력개발의 경로는 〈그림 4〉와 같다.

〈그림 4〉 디지털 포렌식 실무자의 경력개발



이에 따르면 디지털 포렌식 실무자가 되기 위한 지원자는 세 가지의 경로를 따를 수 있는데, 기존의 법집행관, 법집행관이 아니지만 기술이 있는 사람, 학위를 지닌 사람 등이다. 하지만 그 경로와 관계없이 개인적 염결성(integrity)과 함께 지식, 기술, 능력(Knowledge, Skills, Abilities, KSAs)은 지니고 있어야 한다.

개인적 염결성(integrity)과 관련된 개인특성의 요구사항은 일반 법과학의 경우와 같

10) 동 보고서는 http://www.aafs.org/pdf/NIJReport.pdf 참조.

다. 대학교육(academic qualification) 측면에서 역사적으로 디지털 포렌식 분야에서는 학위를 요구하지 않았지만 점차 추세는 학위, 특히 과학 분야에 대한 학위를 요구하는 것으로 바뀌고 있다. 참고로 ASCLD/LAB 인증요건에 부합하려면 디지털 포렌식 실무자들은 최소한 자연과학 분야의 학사학위를 지니고 있어야 한다. 기술적, 전문적으로 요구되는 사항들은 〈표 20〉과 같다.

〈표 20〉 디지털 포렌식 실무가에게 요구되는 기술적, 전문적 능력

기술적 요건	전문적 요건
• 컴퓨터하드웨어와 아키텍쳐(Computer hardware and architecture) • 저장매체 (Storage media) • 운영체제(Operating systems) • 파일시스템(File systems) • 데이터베이스 시스템(Database systems) • 네트워크 기술과 정보통신기반(Network technologies and infrastructures) • 프로그래밍과 스크립팅(Programming and scripting) • 컴퓨터 보안(Computer security) • 암호(Cryptography) • 소프트웨어 도구(Software tools) • 검증과 시험(Validation and testing) • 타 분야에 대한 인식(Cross discipline awareness)	• 비판적사고(Critical thinking) • 과학방법론(Scientific methodology) • 정량적 추리와 문제해결(Quantitative reasoning and problem solving) • 의사결정(Decision making) • 랩실무(Laboratory practices) • 랩안전(Laboratory safety) • 세부사항에 대한 주의(Attention to detail) • 대인기술(Interpersonal skills) • 공적말하기(Public speaking) • 구두, 서면 커뮤니케이션(Oral and written communication) • 시간관리(Time management) • 작업우선선위선정(Task prioritization) • 디지털포렌식 절차의 응용(Application of digital forensic procedures) • 증거보존(Preservation of evidence) • 검사결과의 해석(Interpretation of examination results) • 수사절차(Investigative process) • 법절차(Legal process)

동 보고서에서는 검토사항을 토대로 2년제 전문대 연계 과정(associate degree), 학사학위과정, 대학원 과정, 대학에서의 자격공인 과정, 훈련 및 계속 교육으로부터 각 교육의 커리큘럼과 교육에 필요한 자원 등 요구사항을 기술하고 있다. 이 중에 다른 과정과 달리 학사과정의 경우 구체화된 모델 커리큘럼을 제시하고 있는데 그 내용은 〈표 21〉과 같다.

〈표 21〉 디지털 포렌식 학부과정 커리큘럼 모델

구 분	과 목
대학 일반 교육 (36~40학점)	대학의 요구사항에 따라 언어, 인성, 사회과학, 수학, 공적 연설 등을 포함할 수 있음 학생들이 과학 방법론과 전자기학 기초를 접할 수 있는 6학점의 과학코스가 여기에 포함되어야 함 일부 컴퓨터 포렌식 과학/디지털 증거 학위 코스는 이 요구를 충족할 수 있음
핵심 컴퓨터 및 정보과학 (24학점)	컴퓨터와 저장매체 개론, 응용 파일시스템과 운영체제 기초 컴퓨터 네트워킹과 네트워크 보안, 프로그래밍 I, 컴퓨터 아키텍쳐, 데이터베이스/응용프로그램 정보 보안, 이산수학
핵심 법과학 (6학점)	법과학개론 법과학 전문 실무a
추가적 필수코스 (16학점)	기초 법률 문제(증거), 범죄수사, 공적 연설, 기술적인 글쓰기, 졸업 프로젝트 (Capstone Project) 디지털 포렌식의 쟁점 (1 학점 세미나)
핵심 디지털 포렌식 랩 (12학점)	기초 컴퓨터 포렌식(3학점 + 1시간 실습) 파일시스템과 운영체제 증거복구와 검사(3학점 + 1시간 실습) 디지털 매체, 저장 장치와 응용프로그램 분석(3학점 + 1시간 실습)
상급 포렌식 코스	
고급 핵심 디지털 포렌식 (필수: 11학점)	고급 컴퓨터 포렌식(3학점 + 1시간 실습), 네트워크 포렌식(3학점 + 1시간 실습) 저장 시스템(3학점)
기술 선택 (필수: 9학점)	개인 전자장치(PED) 포렌식(3학점 + 1시간 실습) 임베디드 장치 포렌식(3학점 + 1시간 실습) 사고대응(3학점) 역공학기술과 대응(3학점) 멀티미디어 포렌식(3학점) 통계학(3학점) 개별 연구(3학점) 디지털 포렌식의 고급 법률 문제(3학점) 민사법문제(3학점)
대학 일반 선택 (6학점)	자유선택(인턴쉽 포함 가능)
a. 이 과정은 윤리, 법정 증언, 증거, 증거연계관리(chain of custody), 안전 등을 포함함. b. 여기서 기재된 선택과목은 한정되는 것이 아니라 관심 분야에 따라 조정될 수 있음.	

대학원 과정의 경우 커리큘럼은 교육기관의 임무나 시설, 관심과 학생과 교수의 능력에 따라 다를 수 있으며 연구 프로젝트에의 참여가 권장되고 있다. 커리큘럼에 포함될 수 있는 영역에 대한 분류는 〔표 22〕와 같다.

〈표 22〉 대학원 과정의 커리큘럼 모델

구 분	내 용
디지털 포렌식 방법론 개발	• 단일 혹은 다중의 장치나 시스템을 포함한 복잡한 시나리오를 받아 이에 대한 해결방안을 제안, 개발, 검증하는 것
고급 운영체제 분석	• 실시간 시스템 • 트랜잭션 처리 시스템
디지털 포렌식 행정	• 범죄현장 관리 • 포렌식랩 관리 • 사건관리 • 품질보증(Quality assurance) • 윤리 및 전문가 책임
증거보존	• 통제와 검증 절차 • 증거역학: 보존에 있어 자연, 인간, 도구, 시간의 영향과 디지털 증거의 복구
민·형사법률문제	• 법정증언 • 법정에의 증거제출 • 고급 법률문제/규제 • 컴퓨터 압수수색 • 모의재판 • Electronic Discovery • 증거법
복잡(Complex) 데이터 분석	• 관계분석 • 디지털 증거와 물리적 증거의 연결 • 시계열 분석: 데이터와 관련된 날짜와 시간의 상관관계 • Understanding Data Structures
복잡 사례연구 /시뮬레이션	• 상관관계를 확인하기 위한 다량의 사건에서의 디지털 증거의 비교 • 대량 데이터 세트에 대한 검사 • 기업 시스템 • 중복 관할과 국제 수사에 있어 증거 문제
데이터 통신과 네트워크 시스템	• 패킷과 프레임 분석 • 네트워크 보안의 이해 • 네트워크 트래픽 재구성과 추적

컴퓨터 포렌식 분야는 과학적 분야로 인식되기 위한 교차점에 있다.[11] 아직 대학과 대학원 과정에 대한 FEDAC 등의 인증절차는 확립되지 않았으며 인증이 이루어지지 않

11) M. Rogers, K. Seigfried, The future of computer forensics: a needs analysis survey, Computer & Security(2004), 23, Elsevier, 12-16.

고 있다. 따라서 실제로 대학에서 이루어지는 교육의 커리큘럼은 다소간 차이가 있을 수 있다. 〈표 23〉에서는 미국 미주리남부대학 컴퓨터정보과학 및 형사사법과학(컴퓨터 포렌식 옵션) 학사과정 커리큘럼[12]을, 〈표 24〉에서는 퍼듀대학교 사이버포렌식 석사과정 커리큘럼[13]을 정리하였다.

〈표 23〉 미주리남부대학 컴퓨터정보과학 및 형사사법과학(컴퓨터포렌식 옵션) 학사과정 커리큘럼

1학년		**2학년**	
1학기	학점	1학기	학점
프로그래밍 I	3	DBMS I	3
범죄수사 I	3	컴퓨터 네트워크	3
대수학	3	형사법	3
영작 I	3	인터뷰와 보고서 작성	3
Lifetime Wellness	2	물리학 개론	5
오리엔테이션	1		
2학기		2학기	
프로그래밍 II	3	정보시스템 I	3
형사절차	3	데이터 구조론	3
미국경제	3	범죄수사론 II	3
영작 II (WI)	3	체육	1
생물학	4	화법	3
		일반 선택	3
3학년		**4학년**	
1학기	학점	1학기	학점
UNIX 시스템 관리	3	운영체제	3
정보시스템 II	3	선택과목	3
자산보호	3	국제관계	3
문학과 인성	3	미국사	3
미국사	3	선택과목	3
2학기		2학기	
컴퓨터 포렌식	3	DBMS II	3
선택과목	3	선택과목	3
선택과목	3	선택과목	3
문학	3	예술	3
일반 심리학	3	미국 정부조직	3
		전체	124

12) 출처: http://www.mssu.edu/schtech/criminaljustice/BSForensics.htm
13) 출처: http://cyberforensics.purdue.edu

〈표 24〉 퍼듀대 사이버포렌식 석사과정 커리큘럼

전 체	필수과목 (6학점), 전문화(15학점), 선택과목(6시간), 논문(6시간)
필수과목	산업·공학에서의 측정과 평가, 또는 통계, 또는 심리학 (3)
	산업·공학에서의 연구 분석 (3)
전문 과목 (15 hrs)	기초 사이버포렌식 (3)
	사이버포렌식에서 고급 연구 주제 (3)
	소형 디지털 장치 포렌식 (3)
	최신 토픽 (3)
	파일시스템 포렌식 (3)
	전문가 증언 (3)
	필수 하드웨어 필수 (1)

아직까지 100여 개에 이르는 미국 내 대학에서 디지털 포렌식 관련 교육의 상당수는 학위과정 보다는 법집행관 등 실무자들을 대상으로 한 자격과정인데, 위 보고서에서는 동 자격과정에 대한 커리큘럼과 요건 등에 대해서도 언급하고 있다. 하지만 역시 이러한 자격과정에 대한 인증제도는 아직 존재하지 않는다.

나. 훈련과 지속적 전문성 개발

위 TWGDE의 가이드에 따르면 훈련(training)은 디지털 포렌식 실무자들이 특정한 디지털 포렌식 분석을 수행하는데 요구되는 일정한 수준의 과학적 지식과 경험에 이르게 하는 공식적이고 구조화된 과정이다. 적절한 훈련과 전문성은 개인이 독립적인 사건처리를 할 자격이 주어지기 이전에 필요한 요소이다.

지속적 전문성 개발(continuing professional development)은 현재 상태를 유지하거나 더 높은 전문성, 특기, 혹은 책임의 진보를 가져올 수 있는 체제를 말한다. 조직은 지속적인 전문성 개발에 대한 지원과 기회를 주어야할 지속적 책임이 있다. 이러한 훈련과 전문성 개발과 관련된 사항은 적절하게 문서화되며 항구적으로 보존되어야 한다.

적격성, OJT(on-the-job), 및 지속적인 전문성 개발에 필요한 모델 기준은 핵심요소와 분야별 프로그램으로 구분된다. 핵심요소에는 수행표준(전문가 윤리 훈련 포함), 안

전, 정책, 법률, 증거처리, 커뮤니케이션 등이 포함되며, 분야별 요소에는 분야별 역사, 관련 문학, 방법론과 검증 연구, 하드웨어・소프트웨어・기타 디지털 매체, 관련 분야에 대한 지식, 법정 증언, 특정 범죄형태에 대한 훈련, 법적 측면에 대한 지식 등을 포함한다.

이러한 형태의 계속적인 훈련은 많은 기관에서 의무사항이다. 예를 들어 FBI CART는 연간 64시간, ASCLD/LAB은 40시간, IACIS는 연간 60시간의 보수 교육과 자격을 유지하기 위해 매 3년 마다 적격성 시험(competency examination)을 볼 것을 의무화하고 있다.

다. 자격인증제도

인증(accreditation)이 포렌식 랩에 대한 자격제도라면 개인 또한 자격공인(certification)을 받을 것이 요구된다. 자격제도는 크게 필요로 하는 기관에 의해 직접적으로 훈련과 연계하여 이루어지는 경우, 전문적인 기관에 의해 이루어지는 경우, 특정한 업체가 자사의 제품을 기반으로 하여 인증하는 경우 등 다양하다.

1) 주요 기관의 자격인증 제도

디지털 포렌식 자격위원회(DFCB, Digital Forensic Certification Board)에서 각 기관의 대표자를 대상으로 파악한 주요 연방기관별 자격제도는 다음과 같다.[14]

〈표 25〉 미국 주요기관의 포렌식 검사관 자격제도

조 직	국 세 청(IRS)
자격명	"Computer Investigative Specialist"
응시요건	학사학위(B.A., B.S.) 선임 특수요원, 범죄수사; 13등급
심사방법	3단계 훈련:P-CERT A-CERT (ENCASE, I-LOOK) B-CERT (Networks) 숙련도 시험 : 각 단계의 실기 테스트

14) The National Center for Forensic Science The Certification Roundtable Meeting, Draft Final Report, (http://www.ncfs.org/dfcb/CERT%20ROUNDTABLE%20REPORT%20(DRAFT%20V%206-07-04).pdf.), 2006.

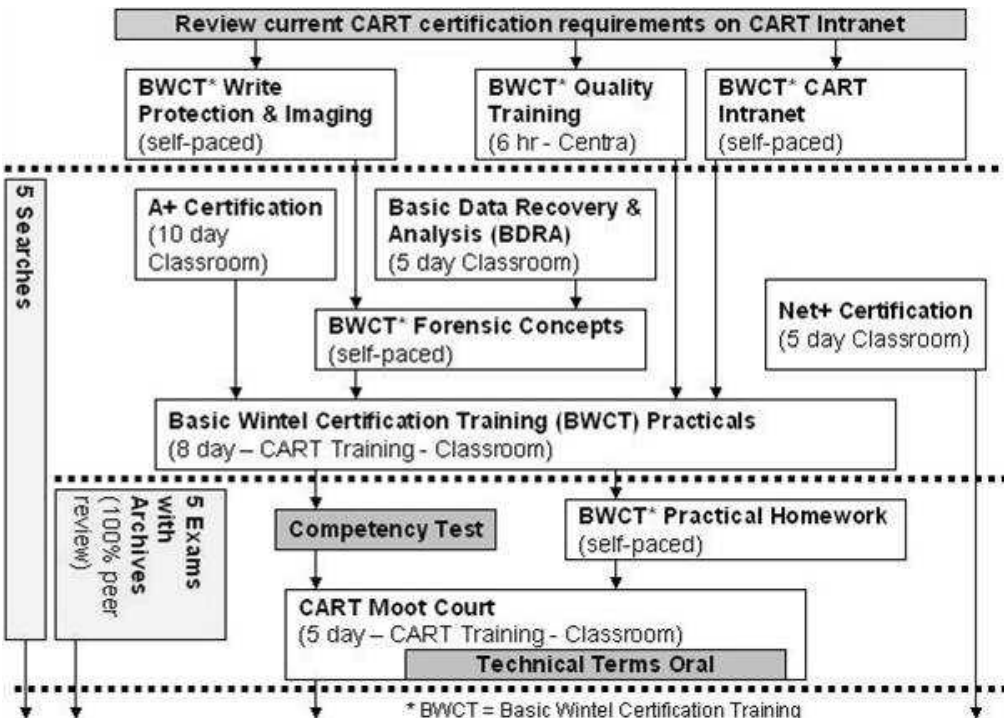
갱신 필요	있음
1인당 비용	$30,000
자격을 받은 인원	200
조직	United States Secret Service (USSS)
자격명	Electronic Crime Special Agent Program
응시요건	USSS 특수요원
	학사학위(B.A., B.S.), 2쪽의 질문지
심사방법	기초자격: 최소 연간 30개 시험
	고급자격: 최소 연간 30개 시험
1인당 비용	$80,000
조직	FBI/Cart
자격명	CART Forensic Examiner
응시요건	학사학위를 받은 FBI요원, 지원인력, RCFL 파견자
심사방법	A-plus certification (기초 전산관련 자격시험) Net+ 검정, 기초 데이터 복구, NWCE CART 기초 시험 훈련, OJT, 모의법정, 구술시험, 숙련도 시험, 매년 재심사
갱신 필요	있음 GIAC GCFA (매4년) 자격마다 필기시험
1인당 비용	최초 심사(코스별 $250-500)
	갱신 ($120.00)
자격을 받은 인원	현재 250명, 누적 350명

이러한 자격제도가 생겨난 이유 중에 하나는 수사기관이 능력 있는 검사관 수요를 감당할 수 있는 전문인력을 기존의 대학교육과 일반적인 자격제도 하에서 수급할 수 없었기 때문이다. 이중에 CART의 Forensic Examiner 훈련 및 자격심사를 좀 더 깊이 살펴보겠다.

CART의 Forensic Examiner는 압수수색지원/디지털증거분석/법정증언 등 임무수행의 임무를 수행한다. 훈련과정의 커리큘럼은 〈그림 3〉과 같다. 자격심사는 Wintel(Windows OS, Intel Architecture)과정에만 7~24개월 소요되며, Unix/Linux, Macintosh, PDA, 휴대전화 등 다른 분야에 대해서는 추가적인 훈련과 심사를 받아야 한다. BWCT(Basic Wintel Certification Training)는 Wintel에 사용가능한 모든 허용된 도구 사용하여 8일간 5개의 시험을 치루며, 이외에도 개별 밀착지도(coaching), 교재를 이용한 개별학습, 개인 탐구활동, 온라인강의, 강의실교육을 병행하는 등 다양한 교육방법을 활용하는 것이 특징이다. 또한 시뮬레이션으로 능력시험(하드드라이브를 주고 증거

를 찾는지, 절차를 따르는지, 수사관과의 효과적으로 대화, 법적인 문제에 대응능력, 수사관이 이해하기 쉽게 자료작성) 및 모의법정 심사를 통과해야 한다. 모의법정은 1.5~2시간 가량의 구두 증언으로 이루어진다.

〈그림 5〉 CART forensic examiner certification curriculum (2004. 2월 현재)



FBI에서는 이와 같은 훈련의 성공요건으로서 CART 및 RCFL 등 현장과는 분리된 교육 전담부서가 존재하는 것이 핵심이며, 대신에 그러한 현장부서와 적극적인 의사소통을 통해 현장감 있는 교육을 실시하며 훈련 전문가를 배치하는 것을 꼽고 있다[15].

15) A. Corrigan, How To Make a Forensic Examiner, 2004 HTCIA International Training Conference & Expo, presentation 자료를 정리한 것임.

2) 전문기관에 의한 자격 제도

소수의 전문기관에 의한 자격인증제도가 존재하는데 이러한 자격제도의 특징은 기간이 대체로 짧아 실제로 포렌식 실무가의 적격성을 완전히 판단하는데 활용되기 보다는 최소한의 기초수준의 능력을 판단하는데 사용될 수 있다.[16]

〈표 26〉 주요 전문기관의 포렌식 검사관 자격제도

자 격 명 칭	자격인증 기관	특 징
공인 컴퓨터 검사관 **Certified Computer Examiner(CCE)**	International Society of Forensics Computer Examiners	인정된 훈련과 경력 필요 3개 모듈의 필답 및 실기시험 현재 가장 널리 알려짐
GIAC 공인 포렌식 분석가 **GIAC Certified Forensics Analysist(CFA)**	Global Information Assurance Organization	75개의 질문으로 이루어진 2개의 온라인 시험
공인 컴퓨터 포렌식 기술사 **Certified Computer Forensics Technician(CCFT)**	High Tech Crime Network	공인 컴퓨터범죄 수사관, 검사, 변호사 등 자격시험 병행
공인 포렌식 컴퓨터 검사관 **Certified Forensic Computer Examiner(CFCE)**	International Association of Computer Investigators	회원, 혹은 실제 데이터를 대상으로 외부 시험 2주간의 교육과 병행
사이버보안 포렌식 분석가 **Cyber Security Forensics Analyst(CSFA)**	Cyber Security Institute	제품 중립적인 시험 실제 사건 시나리오를 객관식으로 시험

이외에도 Encase나 FTK와 같은 포렌식 제품에 기반한 제조업체에서 운영하는 교육훈련과 자격제도는 매우 다양하다. 하지만 이러한 자격제도의 범람은 사회적으로 승인된 디지털 포렌식의 핵심 지식과 훈련 및 평가 방법의 부재 등에 기인한 면이 크며, 따라서 이러한 자격들이 실제로 포렌식 실무자들의 적격성을 검증하는데 충분한 것으로 여겨지지 않는다.

16) C. Taylor, B. Endicott-Popovsky, A. Phillips, Ibid.

3) 적격성 및 숙련도 시험

적격성 및 숙련도 시험(Competency and Proficiency Test)은 전문적인 능력의 보유 여부를 지속적으로 평가하기 위한 것으로 포렌식의 품질관리를 위해 매우 중요한 것이다.

숙련도 시험(proficiency test)은 랩 관리자나, 법 집행기관 혹은 포렌식 랩에 의해 디지털 포렌식 검사관의 현재의 지식(knowledge), 기술(skills), 능력(abilities)을 평가하기 위한 것이며, 적격성(competency) 테스트는 일반적으로 디지털 포렌식 검사의 특별한 응용에서의 검사관의 지식, 기술, 능력을 평가하는 것이다. 예를 들어 훈련이 끝난 후에 관리자는 검사관이 그 훈련 내용을 마스터하고 배운 것을 실제 증거에 적용할 수 있는 지를 결정하기 위해 적격성 테스트를 부과할 수 있다. 숙련도 시험은 특정한 작업(task)에서의 검사관의 기술을 측정하고 검사관의 기술을 평가하고 또한 일상적인 관점에서 검사관의 기술 뿐 아니라 랩의 품질관리시스템 및 절차가 지속적으로 상태를 유지하는 것을 보증하기 위해 이루어진다.

ASCLD/LAB의 경우에 모든 인증받은 랩은 매년 한번 외부기관이나 ASCLD/LAB에서 승인한 테스트 서비스 제공자에 의한 외부 숙련도 검사를 받을 것을 요건으로 하고 있다. 하지만 적격성 테스트에 대해서는 그러한 요구가 없다.

미국 남부플로리다 대학교의 National Center for Forensic Science(NCFS) 및 평생교육부와 연계한 Digital Forensic Quality Solutions(DFQS)사는 최초로 외부 Competency와 Proficiency test를 시행할 계획임을 발표하였다. 이는 ASCLD/LAB이 2007년 10월 컴퓨터 포렌식 숙련도 시험에 대해 승인을 함으로써 이루어지게 된 것이다.[17]

2. 더블린대학 사이버범죄수사 교육

가. 교육센터

정식명칭은 더블린대 '사이버보안 및 사이버범죄수사센터(UCD Centre for Cybersecurity & Cybercrime Investigation, 이하 UCD CCI로 칭함)'로 2006년 설립되었다. UCD CCI는 정보보안 분야 민간인을 대상으로 한 디지털수사 및 포렌식

17) Digital Forensics Quality Solutions (http://www.ncfs.org/dfqs/index.html) 참조

컴퓨터 과정과 경찰 등 법집행기관 종사자를 위한 온라인 교육 기간의 석사 및 자격 과정 등 교육과정(과정별 약 30~40명)을 운영하고 있다. 이러한 자체 정규 교육과정 외에도 특히 EU와 인터폴, IMPACT 등 국제기구 및 기관과 사이버범죄 및 디지털 포렌식 분야 교육·훈련 및 협력에서 중요한 역할을 수행하면서 ECTEG(European Cybercrime Training and Education Group), AGIS cybercrime investigation training projects(현재는 ISEC), 2CENTRE(Cybercrime Centres of Excellence Network) 등 사이버범죄의 교육훈련과 관련된 다양한 사업을 진행하고 있다. 석사과정을 비롯하여 상당수의 강의는 온라인을 통해 이루어지며 시험기간에만 대학을 방문하면 된다.

나. 교육기반

위 교육과정을 담당하기 위해 UCD CCI에는 실습실과 각종의 첨단 사이버 포렌식 수사장비와 소프트웨어를 구비하고 있다. 포렌식 소프트웨어에는 매우 고가인 EnCase Enterprise 등 상용 포렌식 툴과 원격 증거분석 실습을 위한 VMware network를 구축하는 등 설비를 완비하고 있다. 특히 실습교육을 위한 모의사건의 다양한 이미지(image)를 만들어 두어 다양한 교육에 활용하고 있다. 온라인 강의는 대학이 자체적으로 보유한 멀티미디어 방송 제작실에서 이루어지고 있으며 온라인 강의와 집체 강의의 간극을 없애기 위해 온라인 실습교육이 제대로 이루어질 수 있도록 많은 노력을 기울이고 있다.

〈그림 6〉 그룹강의실 (주 강의실로 사용됨)

〈그림 7〉 일반강의실(모의 현장수사 장면)

〈그림 8〉 포렌식실습장

다. UCD CCI의 훈련모듈

UCD CCI에서는 2011년 10월 현재 15개의 훈련모듈을 마련하고 있다. 앞서 살펴본 바와 같이 이러한 사이버범죄 훈련 모듈은 Falcone 프로젝트로부터 이어진 성과물이며 이제는 대학과 E.C.T.E.G를 중심으로 만들어지고 있다. 〈표 27〉에서 보는 바와 같이 각각의 모듈은 석사과정/졸업인정과정/수료과정(MSc/Dip/Cert)와 계속교육(CPD), 포렌식 컴퓨팅전문가 모듈, 사이버범죄수사 전문가 모듈로 구분되어 각각 주제별 모듈의 과정별 적용여부가 다르다. 학점은 유럽표준에 따라 1학점당 20~25 시간의 학습이 필요하게 되어 5학점 과목이라고 하면 대략 100~125 시간의 학습시간이 소요된다.

〈표 27〉 더블린대학의 사이버범죄수사 교육훈련 모듈

모 듈 명	학 점	MSc/Dip/Cert	CPD	Forensic Computing Specialist Modules	Cybercrime Investigation Specialist Modules
Introduction to Programming for Cybercrime Investigators	10	Yes	Yes	Yes	Yes
Advanced Computer Forensics	10	Yes	Yes	Yes	
Case Study	10	Yes		Yes	Yes
Advanced Scripting	10	Yes	Yes	Yes	
VoIP and Wireless Investigations	10	Yes	Yes		Yes
Open Source Intelligence	5	Yes	Yes		Yes
Money Laundering Investigations	5	Yes	Yes		Yes
Computer Forensics	10	Yes	Yes	Yes	
Network Investigations	10	Yes	Yes		Yes
Hacking and Malware Investigations	10	Yes	Yes		Yes
Mobile Phone Forensics	5	Yes	Yes	Yes	
Linux for Investigators	10	Yes	Yes	Yes	Yes
Live Data Forensics	5	Yes	Yes	Yes	Yes
Research project	30	Yes			
Investigation of Sexual Abuse of Children on the Internet	5	Yes	Yes		Yes

제3절 국제기구의 교육훈련프로그램

1. 유럽의 국제 사이버범죄수사 교육훈련

가. 개관

유럽은 국가별 훈련과정 뿐 아니라 다수 유럽국가가 참여하는 교육의 필요성을 일찍이 인식하였다. 이러한 인식은 유럽집행위원회나 유럽평의회, 유로폴 등의 기구들을 통해 확인되었으며 이에 따라 국제교육은 국제기구들을 중심으로 뚜렷한 방향성을 지니고 진행되어 온 것이 두드러지는 큰 특징이라고 할 수 있다. 그 결과 많은 투자 끝에 단계별 사이버범죄 훈련 프로그램이 만들어졌고, 대학과 연계하여 이를 인증하는 체계를 가지게 되었으며, 상시 훈련 프로그램에 논의를 할 수 있는 국제적 워킹그룹이 결성되었고, 사이버수사 훈련 문제를 전담할 고등연구소 네트워크가 창안되었다. 특히 이러한 유럽국가의 움직임에는 UN과 인터폴 등 글로벌 기구의 호응을 받아 유럽을 넘어 세계적인 영향력을 끼치고 있다.

물론 단시간 내에 이에 직접적으로 한국경찰이 적극 참여하거나 아시아권역에서 유사한 형태의 프로젝트를 수행하기를 기대하기는 쉽지 않을 것이다. 유럽의 프로그램에 대한 비판이 전혀 없는 것도 아니다. 하지만 유럽의 프로그램들이 만들어질 때 국제 사이버범죄 훈련 과정에서 일반적으로 인식되어온 문제들에 대한 해결을 위한 상당한 노력이 이루어졌다는 점은 국내 프로그램을 준비하는 과정에서도 시사하는 바가 매우 크다고 본다.

나. Falcone 프로그램

유럽집행위원회(European Commission)와 아일랜드 경찰(Garda)는 EU 지역의 법집행기관의 사이버범죄수사 훈련의 모범실무(best practice)에 대한 연구 프로젝트인 Falcone 프로그램을 2002년 개시했다. 이 프로그램에는 10개 회원국의 전문가가 참여했으며 2002년에 3차에 걸친 회합을 통해 EU 회원국 첨단범죄 수사관 훈련에 대한 권고안 등 3개의 보고서를 작성했다.

Falcone 프로그램의 결론은 아래와 같이 정리할 수 있다.

- 유럽 지역의 사이버범죄 훈련의 조화를 이룰 것
- ① 기초과정(수료) ② 중급과정(졸업장) ③ 고급과정(석사학위과정) ④ CPD(Continuing Professional Development)/비전문가 과정 등 4개 수준의 과정을 구분하여 개발할 것
- 대학과 협력하고 특히 대학이 훈련과 교육과정에 대한 인증(accreditation)을 할 것
- 과정을 모니터할 단일 기관을 정할 것. 유로폴(Europol)이 적절할 것으로 보임(이는 2007년도 Europol Cybercrime Investigation Training Harmonization Group으로 이어짐)

다. AGIS 프로그램[18)]

Falcone 프로그램의 결과로 영국 첨단범죄훈련센터(UK National Hi-Tech Crime Training Centre, 현재 National Police Improvement Agency)가 관리를 맡고 불가리아, 덴마크, 핀란드, 독일, 아일랜드, 스페인, 영국, 포르투갈 등 유럽국가와 유로폴, 인터폴이 참여하여 AGIS 프로그램이 실행되었다. 이 프로그램의 목표는 Falcone 프로그램에서 제 1단계인 기초과정의 시범과정을 만들어 시행하고 평가하는 것이었다. 이 과정은 2004년에 시행되어 성공적이었다는 평가와 함께 계속해서 아일랜드 경찰 및 아일랜드 더블린 대학과 협조하여 제2단계인 졸업장을 수여하는 중급과정을 지속할 것을 권고했다.

2005년에는 2004년도에 참가한 국가 외에도 벨기에와 이탈리아가 추가되었으며, 2005년과 2006년에 제 2단계로 3개 모듈(Internet Investigations, Network Investigations, NTFS Forensics)이 개발되어 시범적으로 실시되었다. 이 모듈들은 더블린대학 Forensic Computing and Cybercrime Investigation 석사과정의 일부로 개발되어 인증(accredited) 되었다. 이 과정에 대한 평가를 통해 제 2단계 과정을 지속하여 추가로 3개의 중급과정을 영국 NPIA 및 더블린대학 CCI(Centre for Cybercrime Investigation)와 협력 하에 개발할 것이 권고되었다. 2006년에는 오스트리아, 프랑스, 그리스, 라트비아, 네덜란드, 말타 등의 국가 외에 민간기업인 마이크로소프트가 민간기업으로는 처음으로 참여하게 되었다. 이에 따라 2006/2007년에 추가로 3개 중급과정(Linux

18) AGIS 후술하는 ISEC과 더불어 조직범죄에 대응하기 위한 유럽집행위원회의 "범죄 예방과 투쟁" 프로그램에 붙여진 이름이다. 사이버범죄는 ISEC에서 정해진 16개 대상 범죄의 하나이고, 2007-2013간 ISEC에 투입되는 자금은 6억 유로이다.

Forensics, Mobile Telephone Forensics, Wireless LANS and VOIP)이 개발되어 시범적으로 실시되었다. 이 과정 또한 더블린대학의 석사과정의 일환으로 개발되어 인증되었다. 이 과정에 대한 평가의 결과로 추가적으로 3개 중급과정과 고급(석사)과정을 유로폴, 인터폴, 산업계, 더블린대학, 유럽법집행기관들이 참여하여 개발할 것이 권고되었다.

라. ISEC 프로그램

AGIS에 이어 ISEC이 시작된 2007년 3개 모듈(Advanced Scripting, Live Data Forensics, Microsoft Vista Forensics)이 역시 더블린대학 석사과정의 일환으로 개발되었다. 이에 따라 2006년 1월에 개설된 더블린대학 사이버범죄센터 석사과정을 수료한 6명(영국, 이탈리아, 오스트리아, 노르웨이 및 인터폴에서 참석한 2명)이 2006년 12월 더블린대학에서 처음으로 Forensic Computing and Cybercrime Investigation (FCCI) 과정으로 석사학위를 받게 되었다.[19] 2007년 입학생은 영국, 네덜란드, 프랑스, 독일, 그리스, 아랍 에미리트, 홍콩 등 20명으로 늘어났다. 따라서 평상시 재학생은 30~40명 선을 유지하고 있다. ISEC의 많은 과정의 교육은 온라인을 기반으로 이루어지고 있다. 일종의 e-Learning이라고 할 수 있는데 이는 단일 시스템이라기보다는 웹사이트와 원격강의, 원격실습 등이 이루어지는 여러 시스템과 그 훈련체계의 전체적인 집합적 개념이다. 이중 가장 기본이 되는 것은 〈그림 9〉 ISEC 훈련 홈페이지이다.

〈그림 9〉 ISEC의 http://www.cybercrimetraining.eu의 초기 화면

19) http://www.ucd.ie/news/0712_december/071207_cyber_crime.html

〈그림 10〉은 ISEC 훈련 홈페이지에 개설된 과정을 보여준다. 앞서 설명된 훈련 모듈을 기본으로 과정들이 구축되어 있음을 알 수 있다. 이 홈페이지는 교육과정 관리시스템(course management system) 내지 이-러닝 플랫폼으로 자유롭게 사용할 수 있는 오픈소스 프로젝트인 무들(http://www.moodle.org)을 이용하여 구축되어 있다.

〈그림 10〉 http://www.cybercrimetraining.eu의 과정 목록

〈그림 11〉에서 보는 것은 2009년 사이프러스(Cyprus)에서 실시된 ISEC 기초과정, 즉 Introductory IT Forensics and Network Investigations 과정의 화면이다. 이 과정 자체는 온라인 과정이 아니라 집체교육이며 사이트는 주로 교육일정표와 강의자료 등을 강사 상호간 혹은 강사와 훈련생간에 주고받는 용도로 사용되었다.

〈그림 11〉 http://www.cybercrimetraining.eu의 다마스커스 기초과정

ISEC의 기초과정은 다수의 유럽국가와 남미국가, 인도 및 호주 등에 유럽 혹은 인터폴 사이버범죄 훈련의 일환으로 제공되었다. 유럽의 교육자료는 인터폴 아시아 사이버범죄 교관 훈련 프로그램 등 타 지역 프로그램 개발에도 기초자료로 활용되고 있다. ISEC의 중급 이상의 과정은 주로 대학에서의 교육과정으로 진행되며 주로 큰 역할을 하는 곳은 더블린대학이다.

마. E.C.T.E.G.

AGIS 프로그램 시행의 평가과정에서 지속적인 국제 사이버범죄 훈련 프로그램 조화로운 개발을 위한 집단의 필요성이 제기되어 2007년 유로폴 주도로 Europol Cybercrime Investigation Training Harmonization Group이 결성되었다. 이 워킹그룹의 주된 목표는 활성화되고 지속가능한 훈련 프로그램의 개발과 시행을 통해 사이버범죄에 대응하

는 국가의 역량을 구축하는 기회를 확인함으로써 사이버범죄 훈련의 조정을 강화하는데 경험과 지식을 전하는 것으로 정의되어 있다. 2009년 11차 회의에서 워킹그룹의 명칭은 European Cybercrime Training and Education Group(E.C.T.E.G.)로 변경되었다.

E.C.T.E.G.는 유럽연합 회원국 및 지원국의 법집행기관, 국제기구, 학계 및 산업계 구성원에게 참석자격이 주어지고 유로폴의 첨단범죄센터(High Tech Crime Centre)에서 사무를 맡고 있으며 운영비 또한 유로폴에서 감당하고 있다. 즉, 현재의 ISEC 프로그램의 구체적인 사항은 E.C.T.E.G.가 중심이 되어 진행되고 있으며 대부분 교육과정의 강사가 E.C.T.E.G.에 참여하고 있다.

바. 사이버범죄 교육 고등연구소(2CENTRE)

더블린대학을 중심으로 사이버범죄 훈련과정이 모듈화되어 제공되다보니 자연스럽게 사이버범죄 훈련의 중심이 대학이 되게 되었다. 하지만 대학에 이러한 사이버범죄 훈련과정이 제공되는 경우는 많지 않으며 따라서 더블린대학과 같은 역할을 수행하는 고등연구소를 확대 설치하고 고등연구소간의 조정자 역할을 더블린대학이 하도록 하자는 보고서가 2009년 유럽집행위원회에 제출되었다.[20] 이러한 고등연구소에는 2CENTRE(Cybercrime Centres of Excellence Network for Training Research and Education)[21]라는 이름이 붙여졌다. 이 계획은 2010년 10월에 유럽집행위원회와 더블린대학의 CCI, 프랑스의 Troyes and Montpellier 1 대학의 계약에 의해 성사되었다.

아래 내용은 위 보고서의 주요 내용을 발췌한 것이다. 2CENTRE는 그간 Falcone으로부터 이어진 사이버범죄 교육훈련에서 가장 진보한 단계에 있는 것이라고 할 수 있다.

- 법집행기관과 산업계는 모두 현재의 사이버범죄 훈련들이 지속가능하고, 계량화할 수 있으며, 표준에 기반하고, 측정할 수 있는 기술들을 제공하지 않는다는데 공감하고 있다. 산업계는 또한 IT forensics에 경험 있는 기술을 갖춘 보안전문가를 고용하고 훈련하는 것이 어려우며 따라서 법집행관으로 유사한 방법으로 이미 훈련받아

20) Cormac Callanan & Nigel Jones, "Study: Co-operation between LE, Industry and Academia to deliver long term sustainable training to key cybercrime personnel", 2009. <http://www.2centre.eu/sites/default/files/LEA-ISP%20Training%20Strategy%20v1.0.pdf>

21) http://www.2centre.eu 참조

약간의 변형된 일을 할 사람들을 필요로 한다는 것을 깨닫고 있다. 법집행계의 훈련은 이런 요구를 충족하기에 충분하지 않다. 더불어 산업계에 대한 훈련은 법집행기관의 요구에 응해야 하는 서비스제공자의 법이나 IT관련 종사자들에게도 필요하다.

- 국제적인 수준에서 법집행 효과적인 사이버범죄 훈련을 개발하고 실행하기 위해서 학습기관 및 산업계와 연계하여 프로그램 및 학술적 안목 및 학문적 자격검증(qualification)을 책임질 네트워크를 구성할 필요가 있다.
- 이러한 학술기관은 사이버범죄와 관련된 기술과 자격검증의 발전을 촉진하도록 설계된 교육프로그램의 개발에 있어 그들의 상당한 연구와 교육자 풀(pool)을 활용할 수 있다.
- 2006년 아일랜드의 더블린 대학(University College Dublin: UCD)은 첨단시설을 갖춘 포렌식 랩과 법집행관에만 허용되는 포렌식 컴퓨팅과 사이버범죄수사의 석사과정을 만들고 사이버범죄수사에 대한 UCD 사이버범죄수사센터(UCD CCI, Centre for Cybercrime Investigation)를 설립했다. 더블린 대학은 전술한 사항에 대한 지속적인 활용과 지속적인 교육훈련 개발, 관리, 교육시행을 지원하기 위한 다섯 명의 교원에 대한 재원을 지원하고 있다.
- UCD의 포렌식컴퓨팅과 사이버범죄수사 석사과정(FCCI)은 법집행기관과 파트너십 하에 특별히 설계된 인증된(accredited) 프로그램이다. 이 프로그램은 비영리 기반이며, 법집행관만 대상으로 제한적으로 운영되고 있다.
- 이번 검토의 결론은 법집행기관과 산업계의 협력 하에 사이버범죄 포렌식수사관이나 정보시스템 보안에 초점을 맞춘 모듈형식의 학술적으로 인증받은 훈련을 제공하는 고등교육원(Centres of Excellence: CoE)을 지원하고 개발하는 즉각적인 필요의 존재이다. 이것은 특정 기준을 충족하는 CoE를 창설함으로써 가능할 것이다. 그러한 협력이 가능한 방법의 사례는 유럽집행위원회 Falcone과 Agis 프로그램의 후원하에 이루어지는 일련의 "사이버범죄 훈련" 프로젝트이다.
- 학술적으로 인증되고 수사관과 산업계의 보안직원에게 기술을 전수하도록 특별히 고안된 교육프로그램의 개발은 교육내용이 요구사항에 충족되는 것을 보장하기 위해 그러한 조직들의 이해관계인과의 협력 하에 설계될 수 있다.
- 그 CoE는 연구주제와 프로그램을 정의하고 이러한 주제에 대한 석박사 학위를 부여

하고 사이버범죄 연구를 인지된 적법한 연구분야가 될 수 있도록 노력해야 한다. 이것이 법집행, 산업계, 학계 등의 다양한 이해관계자들의 재능있는 사람과 프랑스 ANR, 산업계, 혹은 유럽집행위원회 프로그램 등의 보충적 재정지원을 유치하는데 도움을 줄 것이다. CoE 네트워크 자체의 재원과 기술은 종국에는 상당한 추진력을 갖추게 될 것이다.

- 유럽과 다른 세계 전역에 있을 수 있는 CoE는 CoE 네트워크로 문화적 언어적 민감성에 부합하는 지속성과 측정성을 보장하기 위한 네트워크의 다른 부분과 공유를 통해 노력의 최소한의 중첩과 고품질의 훈련과 연구를 보장할 것이다. 이는 다른 관할에서의 학습의 제한을 넘어 자격과 검증을 가능하게 하는 국경을 넘어선 지속가능한 훈련을 실현할 수 있을 것이다.
- 사이버범죄 훈련활동에 관여된 국제경찰조직이 매년 실행할 수 있는 훈련 횟수는 예산과 자원부족으로 인한 한계가 있다는 것이 인식되고 있다. 유로폴은 예를 들어 매년 사이버범죄 주제와 관련된 하나의 훈련 코스를 가지고 있다. 인터폴은 유럽에서 연간 2회의 사이버범죄 훈련과 이 분야에 불충분한 수의 효과적인 교관을 보충하기 위한 교관기술 개발 프로그램을 가지고 있다. 훈련은 이러한 조직들의 주요 역할이 아니며 그들의 노력이 가치 있다고 하더라도 행정적인 추가적 부담없이 CoE 네트워크의 창설에 의해 혜택을 받을 수 있을 것이다.
- CoE 네트워크의 창설에서 조정이 필요하며 이 역할을 수행할 '네트워크 조정센터' 선임을 제안한다. 네트워크 조정센터는 센터의 네트워킹에 필요한 유연성과 새로운 센터에 전달될 확고한 지식기반의 성취 사이의 바른 균형을 찾기 위해 노력할 것이다. 네트워크 조정센터는 유럽평의회, 유로폴, 인터폴, OSCE, UNODC, APEC, ASEAN, OAS와 같은 법집행 분야의 핵심적인 국제적 이해관계자와 EurolSPA, 지적재산권 그룹과 같은 산업계의 긴밀한 참여를 추구할 것이다.
- 네트워크 조정센터는 다섯 가지 핵심영역에 집중할 것이다. ① 각 센터의 탁월성을 촉진한다. ② 적절한 새로운 센터와 새로운 국가를 지원하기 위해 네트워크를 확대한다. ③ 국제적 기관과 활동과의 대외 관계를 지원한다. ④ 센터들과 네트워크의 업무를 촉진한다. ⑤ 제안된 ISEC 프로젝트 팀과 추가적인 프로그램 개발을 위해 협업한다.

- 네트워크 조정센터와 각 CoE는 식견과 조직의 전략에 대한 지침제공을 위해 법집행, 산업계, 학계의 관계된 이해관계인을 포함한 '자문위원회'를 결성할 것이다. 초기 단계에 네트워크 조정기능에는 산업계, 법집행, 하계의 참여자를 포함하는 것이 필요적이며 앞서 언급된 Falcone과 Agis 프로젝트 뿐 아니라 '유로폴 사이버범죄훈련 조화에 관한 실무그룹(Europol Working Group on Harmonization of Cybercrime Training)'의 작업에서 얻어진 지식을 기반으로 하여 구축하는 것을 추구하게 될 것이다.
- 2008년 6월의 '유로폴 사이버범죄 훈련 조화에 관한 실무그룹'에서 ISEC EC 재정지원 프로그램과의 프레임워크 파트너십 하에 CoE프로젝트 개발을 위한 입찰이 제안되었다. 이 연구의 권고사항은 '사이버범죄 훈련, 연구, 교육을 위한 고등연구원 네트워크(Cybercrime Centres of Excellence Network for Training, Research, and Education: 2CENTRE)'의 설립, 운영, 개발에 관한 입찰을 EC 재원의 ISEC 프로그램에 제출하는 것이다.
- 네트워크 조정의 역할은 전반적인 프로젝트와 프로젝트의 결론에서 네트워크의 지속성에 대한 핵심적인 요소이다. 2CENTRE는 최초의 CoE와 함께 하지만 중립적으로 분리된 소수의 지명된 인사들과 네트워크 조정센터를 시작할 것이다. 이 네트워크는 최초에 UCD에 기반을 둔 아일랜드 CoE와 트루아(Troyes) 공과대학에 기반을 둔 프랑스 CoE로 구성될 것이다. 하나의 '그룹'으로 그 네트워크는 다른 멤버들과 같은 조건에서 회원자격을 검증하기 위한 규칙과 절차와 최적실무를 개발할 것이다. 경험에 의하면 이러한 네트워크는 CoE가 그들의 자원을 교육의 개발과 실행에 집중하게 될 것이기 때문에 전임자 없이는 제한적인 성공만이 가능할 것이다. 네트워크 조정센터에 의한 대내 및 대외의 이러한 작업의 국제적인 조정이 노력의 중복을 줄여주고 다른 지역과 언어권에 신속하고 유연한 네트워크 확장을 가능케 할 것이다.
- 이러한 새로운 영역에서, 네트워크 조정자의 자체조직화와 주요 이해관계자의 참여에 대한 경각심을 높이는데 있어 EC의 도움이 필수적일 것이다. 새로운 멤버가 네트워크에 참여토록 초대받을 것이 그려지며 법집행기관과, 산업계, 학계가 ISEC 프로젝트 중에 프로젝트의 완성이전에 개발된 시스템이 검증될 수 있도록 최초의 센터

와 참여 혹은 협력하게 될 것으로 기대된다. 네트워크는 프로젝트의 결론에서 확대될 것이 승인될 것이며 최종 보고서가 유럽집행위원회에 제출되고 파트너 조직과 관심있는 이들에게 공개될 것이다.

2. 인터폴 사이버범죄 서머스쿨

가. 개요

2009년 4월 아일랜드 더블린대학(이하 UCD)과 인터폴은 사이버범죄에 관한 상호협력과 학술·교육 분야 교류확대를 위한 포괄적 내용을 담은 양해각서(MOU)를 교환하였고 이에 따라 UCD의 사이버보안·범죄연구센터(Centre for Cybersecurity and Cybercrime Investigation, 이하 CCI)에서 2011년 7월 2주 과정으로 제1회 인터폴 사이버범죄 서머 스쿨이 개최되었다. 이 교육에는 한국경찰 2명을 포함하여 17개국 법집행기관 종사자 25명이 참석했는데 참석자들은 인터넷 프로토콜인 TCP/IP와 파일시스템에 대한 충분한 지식이 있을 것이 요구되었다. 대부분의 인터폴 주도 훈련프로그램이 인터폴의 예산을 이용해 참가국 훈련생에 무료로 제공됨에 비해 이 교육은 교육비와 체제비 등 제반 비용이 더블린대학에 지급되는 유료과정으로 이루어졌다.

나. 훈련 내용

사이버범죄 서머스쿨의 훈련내용 또한 기존 UCD CCI의 모듈을 중심으로 설계되었다. 하지만 본래 모듈별로 필요한 시간을 학습할 시간이 부족하기 때문에 일부 모듈을 선택하여 각 모듈의 전반적인 내용을 짧은 시간에 다루는 형태로 훈련이 진행되었다. 하지만 대체적으로 각 모듈의 내용이 어떠한 것인지 가늠할 수 있으므로 전체 일정을 아래와 같이 정리해보았다.

〈표 28〉 제1회 인터폴 사이버범죄 서머스쿨 전체 일정

2011년 7월 25일 월요일 (Computer Forensics: Foundations)	
시 간	과 정 명
08:30-09:00	등록
09:00-09:30	개회식, 관계자 및 교수진 소개
09:30-12:00	컴퓨터포렌식 기초(Foundations of Computer Forensics) Time standards, time zones, and daylight saving time Sources of evidence in computer system ACPO Principles of Computer Based Electronic Evidence Forensic Disk Imaging, Disk Wiping, Write blocking Using cryptographic hashing for detection of data tampering
13:00-18:00	포렌식 분석 워크숍(Computer Forensic Analysis Workshop) Analysis of the sexual abuse victim's computer X-Ways Forensics Overview of Windows File System Layout Traces of Internet Usage (Email & Instant Messaging Forensics, Tools)

2011년 7월 26일 화요일 (Computer Forensics: Data Acquisition)		
시 간	과 정 명	
09:00-10:30	이미징 기술 리뷰(Review of Disk Imaging Techniques) To introduce some basic concepts of HDD technology To review practical aspects of disk imaging (Documentation, HDD interface)	
10:30-12:00	라이브포렌식 리뷰(Review of Live Data Forensics Techniques) A Brief Discussion of Live Data Forensics Concepts (Law, Platforms, Volatile Data, Persistent Data) Live Forensics Tools(FTK Imager, X-ways capture, Winen, Win32dd, mdd, Helix PRO)	
13:00-18:00	이미징 및 라이브포렌식 워크숍(Workshop: Disk Imaging, Live Forensics) Disk Imaging Practice (IDE, SATA, SAS, SCSI..) and Documentation In-situ disk imaging with Helix CD v1.9 and Documentation	

2011년 7월 27일 수요일 (Mobile Phone Forensics)	
시 간	과 정 명
09:00-12:00	모바일 포렌식 기초(Foundations of Mobile Phone Forensics) Mobile Device Examination Search and Seizure Consideration, Device Handling, Common Terminology(IMEI, IMSI, ICCID), Extraction Mobile Device Data Content (NAND/NOR, SIM/UICC)
13:00-18:00	모바일 포렌식 워크숍(Mobile Phone Forensics Workshop) Mobile Device Aquisition Practice by XRY(Mobile Phone, SIM Card) Exhibit Examination Overview

2011년 7월 28일 목요일 (Crime Scene Search and Seizure)	
시 간	과 정 명
09:00-12:00	압수수색 기술 리뷰(Review of Search and Seizure Techniques) Good Practice Principles for Electronic Evidence Pre-Search Preparation & Briefing Live Forensics Seizing, Labelling, Storage
13:00-17:00	압수수색 실습 과제(Search and Seizure Practical Assignment)
17:00-18:00	압수수색 실습 결과 발표(Debriefing of Search and Seizure Teams)

2011년 7월 29일 금요일 (Money Laundering)	
시 간	과 정 명
09:00-12:00	자금세탁 워크숍1(Money Laundering Workshop [Part 1]) Effects of money laundering Investigating Money Laundering FATF Introduction (The key issues that FATF recognised) Summary of AML measures Money Laundering Through Real Estate
13:00-18:00	자금세탁 워크숍2(Money Laundering Workshop [Part 2]) Money Laundering and Fraud (VAT Carousel Fraud) Countering Terrorist Financing (CTF) US Office of Foreign Asset Control Terror Funding and Operations

2011년 8월 1일 월요일 (VoIP and Wireless Investigations)	
시 간	과 정 명
09:00-12:00	VoIP와 무선인터넷 수사워크숍1(VoIP and Wireless Investigations Workshop [Part 1]) Explain what Bluetooth is Potential security risks associated with Bluetooth What a wireless LAN(WLAN) is Differences between ad-hoc and infrastructure WLANs Potential security risks associated with wireless networks Compare and contrast the use of traditional techniques for acquiring wireless information with the use of a custom built toolkit to perform the same. Discuss the benefits of using a custom built toolkit Use the Carabinieri toolkit to acquire information from a wireless connection
13:00-18:00	VoIP와 무선인터넷 수사워크숍2(VoIP and Wireless Investigations Workshop [Part 2]) Describe the popularity and penetration of Skype Cryptographic methods used to secure Skype communications Services provided by Skype Distinguish between P2P, SkypeOut and SkypeIn communication modes Information that can be requested from Skype Local and remote infection for Keylogging software Concept of Skype cloning Locate the Skype chat on different OSs Different techniques to rebuilt Skype chat Identify a Skype user by the email address Identify the IP used by the Skype user to geolocate it

2011년 8월 2일 화요일 (Malware Detection and Analysis Workshop)	
시 간	과 정 명
09:00-12:00	멀웨어 탐지 및 분석 워크숍1(Malware Detection and Analysis Workshop [Part 1]) Malware overview What is the main use of Malware? How much money did CyberCrime make last year? Malware Types, Malware Naming Conventions Setting up a Malware Test Lab Basic Lab Setup Professional Lab Setup Gateway - REMnux Virtual Machines(vmware, parallels, qemu...) Lab Setup Tips What tools to install?

13:00-18:00	멀웨어 탐지 및 분석 워크숍2(Malware Detection and Analysis Workshop [Part 2]) Malware Analysis Process Finding and Extracting the Malware (Scan the computer, Look for Rootkits, suspicious processes, system startup locations, Use System Information Collector) Static Analysis Blackboxing (Change Monitoring, Processes, Files, Registry, Ports, Networking) Internet Search Whiteboxing Results Rootkits Conclusion

2011년 8월 3일 수요일 (Cybercrime Investigation Contest)
2011년 8월 4일 목요일 (Cybercrime Investigation Contest)

사이버범죄수사 컨테스트: 사례 제시, 그룹별로 실제 수사를 진행해서 발표

다. 인터폴 사이버범죄 서머스쿨의 특징과 평가

1) 교육방식상의 특징

- 대부분의 모듈들은 오전에 강의(필요시 실습병행), 오후에 실습 위주로 편성[22]
- 강의와 실습의 상당 부분은 일반적인 형태의 것이었으나, 시나리오 기반의 일부 실습(현장 압수수색과 종합 수사실습)은 준비과정에 많은 시간과 노력이 필요한 것이라 인상적이었음
- 강사들은 ECTEG(European Cybercrime Training and Education Group) 멤버들 위주로 구성되므로, 전반적인 사이버범죄 훈련에 대한 이해와 강의 숙련도가 뛰어난 것이 큰 장점

22) 필자가 동 훈련과정에 참여한 후 경찰청에 제출한 보고서의 내용을 발췌한 것임.

2) 평가

- 전반적인 교육과정의 짜임새는 매우 훌륭했음. 특히, 대학에서의 경찰실무 훈련이 일반적인 훈련과 어떻게 다를 수 있는 지 보여주는 좋은 사례로 생각됨
- UCD CCI의 교육과정은 실무와 대학의 교육·연구 프로그램을 조화시키려는 노력이 두드러짐
- 그럼에도 불구하고 국제 사이버범죄 훈련에서 공통되는 가장 큰 어려움, 즉 참가자의 기술적 숙련도의 격차에 대한 문제 해결에는 그다지 성공적이었다고 보기 어려움
- 여러 참가자는 충실한 교육프로그램에도 불구하고 그 내용이 너무 초심자 중심으로 편성되어 있어 기대에 미치지 못하였으며 차기 프로그램에 각국 수사관의 참가를 권유하지 않겠다는 입장이었음
- 이는 개별적인 수사관의 전문성 훈련이라는 측면에서는 충분히 이해되는 반응이었으나 반면 국제적인 사이버범죄 대응을 위한 공동의 노력, 공감의 형성이라는 측면에서는 좋은 프로그램일 수 있음. 하지만 후자의 측면을 이번 교육은 크게 고려하고 있지 못하고 강사들의 일방적인 지식과 기술의 전달 위주로 편성된 바, 전후자 모두의 목적에 다소간 미흡한 결과가 되지 않았나 생각됨
- 인터폴에서 최초로 시도한 유료 국제교육 프로그램으로 지나치게 UCD CCI의 일방적인 주도로 프로그램이 마련되었으며 기존의 인터폴 교육경험이 많이 반영되지 못한 아쉬움과 그 비용이 많은 개발도상국에는 부담스러운 금액이었던 만큼 이러한 여러 측면이 차기 교육에는 반영되었으면 하는 바람
- 교육내용의 모듈화, 표준화, 강사진의 Pool 형성, 온라인 교육진행 기반의 구축, 훈련 컨텐츠의 재활용과 같은 여러 측면에서 사이버수사 교육 프로그램 개발에 참고할 만한 내용이 많았음
- 사이버범죄 교육훈련 프로그램의 국제표준화라는 측면에서 향후 UCD측과 긴밀한 협력을 유지할 필요가 있음

3. 유럽 ISEC 기초과정

가. 개관

유럽 ISEC 기초과정은 앞서 살펴본 바와 같이 "IT 포렌식 및 네트워크 수사 기초(Introductory IT Forensics and Network Investigations)"로 이름 붙여진 단일 과정으로 가장 많이 실제로 여러 국가에서 훈련이 이루어지고 있는 과정이다. 이 과정의 개괄적인 사항은 강사가이드(Trainer Guide)를 통해서 살펴볼 수 있다. 강사가이드는 도입, 교육일정 및 강의별 학습계획서로 구성되어 있는 87면의 적지 않은 분량이다. 국내에서 실시되는 많은 국제 사이버범죄 훈련과정에서는 이러한 정규적인 준비문서를 작성하지 않는 경우가 많다.

나. 강사 가이드(Trainer Guide)

1) 도입

역사, 목표, 개관, Trainer Guide 사용방법, 강의 플랫폼, 권고사항, 교육대상, 학습 주안점, 시험방법, 평가, 연락처 등 기재되어 있다.

2) 교육일정

아래는 2009년 다마스커스에서 실시된 ISEC 기초과정(2주)의 교육일정이다. 강좌별로 필요에 따라 1~2시간으로 구분되어 편성된 것을 알 수 있으며, 아침 9시부터 오후 5시까지 일정이 빠짐없이 편성되어 있다. 내용 자체는 사이버수사 기술에 중점이 주어지고 있음을 알 수 있다.

〈표 29〉 2009년 다마스커스에서 실시된 ISEC 기초과정(2주)의 교육일정

	09:00 - 10:00	10:00 - 11:00	11:00 - 12:00	12:00 - 13:00	13:00 - 14:00	14:00 - 15:00	15:00 - 16:00	16:00 - 17:00
Monday	1.1.1 Opening	1.1.2 Introduction to Computer Forensics	1.1.3 Demystifying Computer Hardware		LUNCH	1.1.4 Physical Characteristics of HardDisks ; CD/DVD & other Storage Media		1.1.5 Overview of Computer Data(Bits and Bytes)
Tuesday	1.2.1 Review of the day	1.2.2 Preparing a Hard Disk for Use-Partitioning and Formatting		1.2.3 Drive Letter Assignment	LUNCH	1.2.4 FAT File System	1.2.5 NTFS File System	
Wednesday	1.3.1 Review of the day	1.3.2 Deleted Files/Recycle Bin		1.3.3 Operating Systems	LUNCH	1.3.4 Working with a Command Line Interpreter	1.3.5 The Boot Process	1.3.6 Windows Shutdown
Thursday	1.4.1 Review of the day	1.4.2 Introduction to Networks1	1.4.3 Introduction to Networks2		LUNCH	1.4.4 Network Practical	1.4.5 WWW	
Friday	1.5.1 Review of the week		1.5.2 Assessment of the week		LUNCH	1.5.3 Linux Introduction	Travel	

	09:00 - 10:00	10:00 - 11:00	11:00 - 12:00	12:00 - 13:00	13:00 - 14:00	14:00 - 15:00	15:00 - 16:00	16:00 - 17:00
Monday	2.1.1 Wireless Networks & Security	2.1.2 Wireless Networks Practical	2.1.3 Internet Investigation		LUNCH	2.1.4 Network Live Investigation	2.1.5 E-Mai lBasics	
Tuesday	2.2.1 Review of the day	2.2.2 File Times & Dates	2.2.3 The Internet & Forensic traces		LUNCH	2.2.3 The Internet & Forensic Traces (Cont)	2.2.4 Basics of Encryption	
Wednesday	2.3.1 Review of the day	2.3.2 Forensic Tools		2.3.3 File Types & Signatures	LUNCH	2.3.4 Wiping & Counter Forensics	2.3.5 Capture of Digital Evidence Imaging & Hashing	
Thursday	2.4.1 Review of the day	2.4.2 Trojan & Trojan Defences	2.4.3 Basic Mobile Forensics		LUNCH	2.4.4 Search & Seizure		2.4.5 Presenting & Giving Evidence (Practical)
Friday	2.5.1 Final Review		2.5.2 Assessment of Week2		LUNCH	2.5.3 Course Closure, Review & Travel		

3) 강의 계획

문서화된 강의계획이 있다는 것은 매우 중요하다. 많은 법집행기관의 훈련프로그램은 대학에서 교수들이 자유롭게 강의를 진행하는 것과 달리 프로그램 자체의 인증과 평가, 강사가 바뀌더라도 일관된 훈련내용을 전달하기 위해 세부적인 강사용 훈련매뉴얼을 만드는 경우가 많다. ISEC 프로그램의 경우 시간별로 상세한 훈련매뉴얼은 없지만 훈련교재와 이 강의 계획이 그러한 역할을 한다고 볼 수 있다. 강의 계획은 강좌별로 필요한 교보재, 강좌의 목표, 간단히 정리된 세부 훈련 내용이 포함되어 강좌별로 1~2페이지 분량으로 작성되어 있다.

4. UN 온라인 사이버범죄수사 교육훈련 프로그램

UNODC와 한국형사정책연구원이 공동으로 추진하는 사이버범죄대응포럼(Virtual Forum Against Cybercrime)의 일환으로 사이버범죄 관련 형사사법 종사자를 위한 온라인 교육 프로그램이 있다. 이 프로그램의 가장 큰 특징은 거의 완전한 온라인 강의 프로그램의 형태를 지니고 있다는 것이다. 따라서 그 교육효과에 관심이 가게 되는데 이러한 온라인 강의에 대해서는 단지 지식이 아니라 실습이나 선험자를 통한 경험을 통해 익히게 되는 일반적인 법집행기관 집체 훈련과 비교하여 효과에 대해 회의적이라는 것이 사이버수사관 면담을 통해 공통적으로 인식되었다. 즉, 훈련내용이 온라인으로 전달되기만 할 뿐 그것을 주도적으로 이끌어주거나 경험할 수 없게 되므로 시중에 있는 교육자료를 살펴보는 것과 크게 다를 바가 없다는 것이다. 한 때 사이버범죄에 관한 훈련자료 자체가 태부족인 때가 있었지만 이제는 시중에서도 쉽게 그런 자료를 구해볼 수 있기 때문에 듣고 보기만 하는 훈련이라는 것은 어느 정도 한계가 있으리라는 것은 짐작할 수 있다.

이 프로그램은 기초과정으로 ① 과정 개요, ② 정보통신 기술의 이해, ③ 사이버범죄 법률의 이해와 고급과정으로 ④ 사이버범죄수사 - 절차와 기술 ⑤ 사이버범죄수사 - 디지털포렌식 ⑥ 특별주제에 대한 세미나 등 하위과정으로 구분되며, 하위과정별로 3개에서 13개에 이르는 모듈로 구분되어 있고 각 모듈은 최대 8개 레슨(레슨별로 대략 1시간 소요)으로 구성되어 있다. 따라서 ISEC의 프로그램이 주로 기술적인 측면에 많은 강조를 두고 있는 반면에 법률 등 다양한 주제들이 다루어지고 있는 점이 특징이자 장점이라고 할 수 있다.

〈표 30〉 UN 온라인 사이버범죄수사 교육훈련 프로그램 기본과정

Lesson No.	Course	Module
0-1-1	[0] Introduction to the Training Course of the Virtual Forum against Cybercrime	[0.1] Introduction to the Training Courses of the Virtual Forum against Cybercrime
0-2-1		[0.2] Cybercrimes in the global village (I)
0-3-1		[0.3] Cybercrimes in the global village (II)
1-1-1	[1] Understanding Information and Communication Technology	[1.1] Understanding emerging trends in ICT & cybercrime in the information age
1-1-2		
1-1-3		
1-2-1		[1.2] Structure of the internet & digital divide
1-2-2		
1-3-1		[1.3] Vulnerabilities of ICT
1-4-1		[1.4] ICT & network security
1-5-1		[1.5] Forms of intrusion & hacking
1-5-2		
1-6-1		[1.6] E-commerce & forms of electronic payment
1-7-1		[1.7] Digital evidence & digital forensics for non-forensic specialists
1-7-2		
2-1-1	[2] Understanding Cybercrime Laws	[2.1] Criminality – Definitions of cybercrime
2-1-2		
2-2-1		[2.2] Judicial issues in cybercrimes (I)
2-3-1		[2.3] Judicial issues in cybercrimes (II)
2-4-1		[2.4] Types of cybercrimes (I) - Cyber-property crimes
2-4-2		
2-5-1		[2.5] Types of cybercrimes (II) - E-commerce & e-banking crimes
2-5-2		
2-6-1		[2.6] Types of cybercrimes (III) - Cyber-terrorism
2-6-2		
2-7-1		[2.7] Jurisdiction – the roles of national & international law enforcement
2-7-2		
2-8-1		[2.8] International cooperation in the control of cybercrime
2-8-2		
2-9-1		[2.9] Compatibility of international conventions on cybercrime with domestic laws
2-10-1		[2.10] Mutual legal assistance : methods & problems – procedures & practices of online cooperation for law enforcement agencies
2-10-2		
2-11-1		[2.11] Digital evidence, preservation & presentaion of evidence for non-forensic specialists

〈표 31〉 UN 온라인 사이버범죄수사 교육훈련 프로그램 고급과정

Lesson No.	Course	Module
3-1-1	[3] Cybercrime Investigations – Procedure & Techniques	[3.1] Computer investigation techniques (I)
3-1-2		
3-1-3		
3-1-4		
3-2-1		[3.2] Computer investigation techniques (II)
3-2-2		
3-3-1		[3.3] Investigation system & procedure of developed countries
3-3-2		
3-3-3		
3-3-4		
3-3-5		
3-3-6		
3-3-7		
3-4-1		[3.4] Criminal procedure & digital evidence
3-4-2		
3-5-1		[3.5] Modus Operandi of cybercrime & investigation techniques (I) - Computer viruses, hacking & botnet
3-5-2		
3-5-3		
3-5-4		
3-6-1		[3.6] Modus Operandi of cybercrime & investigation techniques (II) - Cyberstalking & electronic vandalism
3-6-2		
3-6-3		
3-7-1		[3.7] Modus Operandi of cybercrime & investigation techniques (III – Computer fraud & phishing
3-7-2		
3-8-1		[3.8] Modus Operandi of cybercrime & investigation techniques (IV) - Terrorist use of the Internet
3-8-2		
3-9-1		[3.9] Preservation & presentation of digital evidence
3-9-2		
3-10-1		[3.10] Assessment Potential Threat of Anonymous Communication
3-10-2		
3-11-1		[3.11] Network Security
3-11-2		
3-11-3		
3-11-4		
3-11-5		

Lesson No.	Course	Module
3-11-6		
3-12-1		[3.12] Incident response teams – Priorities & team building
3-12-2		
3-13-1		[3.13] Investigative best practices – Case studies
3-13-2		
3-14-1		[3.14] Practicum – Project exercise
4-1-1	[4] Cybercrime Investigation – Digital Forensics	[4.1] Understanding and applying the rules of digital evidence
4-2-1		[4.2] Acquiring forensic images & preservation of digital evidence
4-2-2		
4-3-1		[4.3] Computer Forensics Tools Testing (CFTT)
4-3-2		
4-3-3		
4-4-1		[4.4] Analytical Procedures & Forensic Techniques (I) - Program analysis
4-4-2		
4-4-3		
4-4-4		
4-5-1		[4.5] Analytical Procedures & Forensic Techniques (II) - Network analysis
4-5-2		
4-5-3		
4-6-1		[4.4] Analytical Procedures & Forensic Techniques (III) - Database analysis
4-6-2		
4-6-3		
4-6-4		
4-6-5		
4-6-6		
4-7-1		[4.4] Analytical Procedures & Forensic Techniques (IV) - Digital evidence analysis
4-7-2		
4-7-3		
4-7-4		
4-7-5		
4-7-6		
4-7-7		
4-7-8		
4-8-1		[4.8] E-mail investigation
4-8-2		

Lesson No.	Course	Module
4-9-1		[4.9] Keyword analysis
4-9-2		
4-10-1		[4.10] Internet activity analysis
4-10-2		
4-11-1		[4.11] Encryption & stenography
4-11-2		
4-11-3		
4-11-4		
4-11-5		
4-12-1		[4.12] Computer security risks & remedies
4-12-2		
4-12-3		
4-12-4		
5-1-1	[5] Special Online-Seminars : Issues and Topics	[5.1] Privacy & data protection
5-1-2		
5-1-3		
5-1-4		
5-2-1		[5.2] Obscenity & offensive/racist materials
5-2-2		
5-2-3		
5-2-4		
5-2-5		
5-3-1		[5.3] Online game & gambling
5-4-1		[5.4] Assessment of potential threat from wireless technology
5-4-2		
5-4-3		
5-5-1		[5.5] ID theft & Online Fraud
5-5-2		
5-5-3		
5-6-1		[5.6] The challenge of Cybercrime
5-6-2		
5-6-3		
5-7-1		[5.7] Special topics issued by participants - Open forum on special cases

제3장 기존 교육훈련 프로그램 분석

제1절 기존 교육훈련 프로그램의 한계

사이버범죄 수사기법은 정보통신기술의 발달에 따라 그리고 사이버범죄의 다양성과 급변성에 따라 달라질 수밖에 없으므로 사이버범죄의 변천에 따른 교육훈련 프로그램의 구성 변화는 필연적이다.

아무리 뛰어난 교육훈련 프로그램을 개발한다고 하더라도 이미 사장된 정보통신기술을 사용하거나 또는 해당 개발도상국의 IT 상황에 맞지 않는다면 교육훈련 프로그램으로서 전혀 쓸모가 없기 때문에 해당 국가 각각의 세부적인 사정에 따른 적절한 교육훈련 프로그램의 구성 및 적용이 필요하다. 아울러 가까운 미래에 나타날 것으로 예상되는 사이버범죄의 진행 방향을 미리 예측하여 이에 따른 기술습득과 대응태세를 교육훈련 프로그램 내용에 포함하여야 하며, 기초 기술부터 최상급 기술까지 단계적으로 사이버수사기법 교육훈련 프로그램을 편성하여야 한다. 그런 점에서 한국의 사이버테러대응센터의 재교육 및 심화교육 프로그램들은 좋은 선례가 될 것이다.

개발도상국가를 대상으로 한 사이버수사기법 교육훈련은 앞서 살펴본 것과 같이 한국국제협력단의 공적개발원조의 일환으로 연수생 초청교육과 프로젝트 사업 등을 시작하면서 본격화되었고, 차츰 수원국 초빙 및 경찰청 자체 프로그램 등으로 다양화되었으며 양적으로도 팽창기에 있다고 볼 수 있다.

여러 교육사업을 진행한 후에 연수생의 교육에 대한 다양한 평가를 종합하면, 교과의 편성과 질적인 수준에서 만족도가 높은 편이지만, 대부분의 교육이 2~3주를 넘지 못하는 단기 프로그램으로 구성되어 있어 구체적인 지식·기술·역량을 배양하기 위해 좀 더 충분한 기간 동안 교육이 이루어질 것을 희망하고 있는 것으로 파악되고 있다.

교육의 분야별로 살펴보면, 지금까지 경찰의 국제교육 기여의 상당 부분이 사이버범죄 수사와 과학수사 두 분야에 집중되어 있다. 두 분야는 대단히 기술적인 분야라는 공통점

이 있으며, 이는 법집행과 관련된 제도 전반의 선진화보다는 상대적으로 발달한 과학기술의 기반 하에 비교우위에 있는 분야에 집중되는 교육수요와 교육서비스를 제공할 수 있는 역량의 두 가지 측면이 모두 고려된 결과로 파악된다.

교과편성 및 진행과 관련하여 대부분의 교육과정이 공적개발원조 자금에 의존하며, 이러한 사업이 매년 사업제안과 채택 및 실시와 같은 일련의 절차에 따라 비정규적으로 이루어지므로 전용시설의 확보나 체계적인 교과 및 교보재의 개발, 교수의 양성 등과 같이 상당한 기간의 투자를 필요로 하는 교육준비를 충분히 할 수 없기 때문에 교육품질에 있어 일정한 한계를 지닐 수밖에 없다.

또한 전문분야에 대한 강사의 경우, 대부분의 교육훈련 프로그램이 영어로 진행되는데 반하여 영어에 능통하지 않아 통역을 활용하는 경우도 적지 않아 원활하지 못한 의사소통으로 인한 교육효과의 반감 또한 해결해야할 문제로 보인다. 미국이나 캐나다를 비롯한 영어권 국가의 해외 법집행기관 종사자 참여 프로그램이 해외 참여자만을 위한 특별 프로그램이 아닌 내국인 종사자를 대상으로 하는 프로그램에 일부 해외 참석자를 포함시키는 방식으로 이루어지는 것이 가능한 것도 언어문제가 발생하지 않기 때문이기도 하다. 외국인만을 대상으로 하는 교육은 외국 손님을 대하는 일반적인 정서와 태도가 교육과정에 포함되지 않을 수 없기 때문에 교육을 받는 대상자의 입장에서는 보다 실질적인 교육효과를 기대하기가 그만큼 어려울 수가 있다.

경제개발 등 타 분야에 비해 비록 뒤늦은 감은 있지만, 국제적인 경찰교육 커뮤니티에서 한국이 리더십을 지니기 시작했다는 측면에서 사이버수사기법 교육훈련 프로그램의 개발은 그 의미가 크다. 교육은 단순히 알고 있는 지식과 기술을 전수하는 것이 아니라 성공을 위해서는 준비과정에서부터 평가에 이르는 일련의 준비와 절차를 지닌 매우 복잡한 과정으로 목표한 성과를 달성하기 위해 노력하는 과정에서 전반적인 교육서비스의 품질을 향상시킬 수 있는 부수적 효과가 있으며 종국에는 자국 내의 치안서비스를 향상시키는 데에 일조할 것으로 기대할 수 있다.

1. 단기 훈련 과정이 지니는 한계

대부분의 국제 훈련 과정은 1~3주의 기간을 넘기기 어렵다. 무엇보다 국제 훈련에 들어가는 비용 부담이 크기 때문이다. 사이버범죄 수사와 관련된 지식·기술·역량의 범위가 매우 넓기 때문에 짧은 기간 동안 학습할 수 있는 내용의 범위는 뚜렷한 한계를 지니기 마련이다. 따라서 많은 전문화된 훈련과정의 경우 보다 좁은 범위의 특정한 내용에 대한 집중적인 훈련이 이루어진다. 앞서 따로 검토하지는 않았지만 국제 훈련으로는 미국 SANS의 "웹 응용 침투시험 및 윤리적 해킹"(6일) 과정이나 'Guidancesoft' 등 제품을 기반으로 한 특정한 기술 훈련, 국내 훈련으로는 경찰수사연수원의 해킹범죄수사전문과정 등이 그렇다.

특정한 주제에 관한 집중 훈련이 아니라 광범위한 주제를 다루는 경우 사이버범죄수사나 디지털 포렌식 등에 대한 기초훈련인 경우가 보통이다. 국제훈련으로는 인터폴의 TTI나 TTF 훈련, 경찰대학의 '국제사이범죄수사과정', 국내훈련으로는 경찰수사연수원의 '사이버범죄수사과정', 유럽의 ISEC의 기초과정과 같은 것들이 그러하다. 폭넓은 주제를 다루는 기초과정이나 특정 주제에 대한 전문화된 훈련 모두 국제훈련을 실제 실시할 때는 여러 문제를 내포하고 있다.

가. 폭넓은 주제에 관한 기초과정의 문제

폭넓은 주제에 관한 기초과정은 무엇보다 현재 사이버범죄수사기술의 복잡성에 비추어 실제의 문제를 해결하기 위한 적절한 기술과 응용력을 배양하기에 충분한 시간을 확보하기 어렵다는 문제를 들 수 있다.

일부 훈련생은 이러한 기초적인 수사방법에 대해서는 이미 익히 알고 있기 때문에 자칫 훈련이 자신에게 꼭 필요한 내용을 알려주기에 충분하지 못한다고 느끼게 된다. 물론 사이버범죄 기술이 발달하지 못한 많은 개발도상국 참석자는 이러한 기초훈련조차 어렵다고 느끼는 경우도 적지 않다.

나. 특정한 주제에 대한 과정의 문제

이러한 단기 훈련과정의 경우 훈련 참석자가 충분히 해당 내용을 학습할 준비가 되어 있는 지가 훈련효과 확보의 중요한 관건이라고 할 수 있다. 하지만 인터폴이나 경찰대학 훈련 등 개발도상국가에 지원하는 형태의 훈련은 참석자의 배경지식을 특별히 요구하여 훈련생을 선별적으로 참석하게 하기가 쉽지 않다.

대부분의 특정 주제에 대한 과정은 훈련국가 또는 훈련생이 비용을 부담하는 과정이며, 이런 경우 훈련생이 스스로 훈련성과에 대한 고려를 하기 때문에 특정 주제에 대한 수강 준비가 더 잘 준비되어 있는 경우가 보통이다.

2. 훈련생의 기술적 배경지식의 격차 문제

앞서 언급한 바와 같이 인터폴의 TTI, TTF 등 훈련이나 경찰대학 등 기존 국내에서 실시된 국제훈련의 경우, 기초적이고 광범위한 주제들을 다루고 있으며 훈련생의 보유역량을 참가자격으로 엄격하게 제한을 두고 있지 않기 때문에 현실적으로 훈련생 개개인간의 역량에 큰 차이를 보이고 있고 이것이 적실한 훈련에 큰 장애가 되고 있다.

예를 들어 인터넷 추적기술을 훈련하기 위해서는 인터넷 프로토콜의 구조에 대한 이해가 선행되어야 하는데 많은 참석자들이 그렇지 못하기 때문에 실제 인터넷 프로토콜 구조에 대한 설명에 적지 않은 시간을 할애하여야 하며 이로 인해 실제 인터넷 추적기술에 대해서는 설명할 시간이 충분하지 않고, 실습을 다소 병행한다 하더라도 이제 막 인터넷 프로토콜 구조에 대한 설명을 들은 훈련생이 충분히 응용기술을 실습하기가 쉽지 않은 것이 현실이다.

반면, 배경지식이 충분치 못한 훈련생을 고려한 훈련과정은 배경지식을 이미 지니고 있는 훈련생에게는 매우 불필요한 것이 되기 쉽다. 인터넷에서 이러한 기술적인 격차가 상당한 학습과 이를 응용한 실무를 통해 보통 수년에 걸쳐서 생긴 것이기 때문에 단기간 내에 이를 극복하기가 쉽지 않다. 즉, 개발도상국가라고 하더라도 어떤 참석자는 IT 분야를 전공하고 수년간 사이버범죄 수사실무에 종사한 상태이고 어떤 참석자는 IT 분야를 거의 접해본 적조차 없는 경우가 있는데 이들을 대상으로 같은 사이버범죄 수사실무에

대한 훈련은 사실상 쉽지 않은 것이 당연하다고 하겠다.

〈표 32〉 2008년 국제 사이버범죄수사 과정 참석자 배경 조사 결과

	예	아니오	응답자수
사이버수사 전담부서 근무	3	12	15
사이버수사 관련 부서 근무	9	6	15
IT 전문교육 이수 여부	7	7	14
업무의 IT 기술 관련성	10	5	15
사이버수사 경험 유무	8	6	14
프로그래밍 가능 여부	6	8	14
포렌식 이미징을 아는지 여부	5	8	13

위 표는 2008년 경찰대학의 국제 사이버범죄수사 과정을 이수한 참석자의 배경에 대한 설문조사 결과로, 동 과정이 주로 사이버수사 분야에 관한 실무책임자를 주된 훈련대상으로 삼고 있으나, 아직까지 많은 국가가 사이버수사와 관련된 전담 부서를 아예 가지고 있지 못하기 때문에 훈련생이 속한 부서가 사이버범죄와 전혀 무관한 경우도 15명 중에 6명이나 되었고, 디지털 증거 취급에서 일반적으로 사용되는 포렌식 이미징(forensic imaging)이라는 용어가 무엇을 뜻하는 지도 모르는 경우가 이를 아는 경우보다 더 많았다.(13명 중 8명)

3. 사이버수사훈련의 주제 : 기술과 비기술적 요소

경찰 실무의 차원에서 기술적인 문제는 사이버범죄 수사의 가장 큰 장애요소로 많은 사이버범죄 훈련은 기술적인 문제에 집중된다. 앞서 설명한 것처럼 훈련생의 배경지식과 관련하여 기술적인 측면에서의 격차가 매우 심각하지만, 실제로 훈련생들은 기술적인 측면에 대한 관심이 매우 높다.

하지만 사이버범죄와 관련된 국제적 이슈는 전부 기술적인 문제만을 다루지는 않는다. 특히 개발도상국가의 역량강화(capacity building) 및 국제공조의 강화라는 측면에서 보면 실제로 비기술적인 많은 요소들이 훈련과정에 포함될 수 있다.

법률의 적용이나 조직의 운영, 범죄사건 수사실무 등 많은 비기술적 요소들이 그러하다. 여러 민간부분의 훈련은 침해사고 대응 등 사이버보안의 측면에서 유사한 주제들을 다루는데 이러한 다양한 관점에서의 접근방법이 실제 범죄사건의 수사에서 다른 분야와의 커뮤니케이션에서 필요하기도하고, 통상적으로 훈련의 수준이 더 높기 때문에 어떤 수사관들은 전형적인 사이버범죄 수사관 훈련보다 그런 외부 훈련을 선호하기도 한다.

4. 블록식 경찰훈련과 점증적 학습

많은 경찰훈련은 특정 분야에 대한 단기간의 집중 훈련, 즉 블럭식 훈련에 이해 이루어진다. 특히 수사와 관련된 훈련이 주로 블럭식 훈련에 의해 이루어지는 문제점은 앞서 언급한 바와 같이 널리 알려진 것이다.

이러한 블럭식 훈련은 수사관 개인별로 볼 때 훈련과정이 평생학습과정으로 점증적인 학습과정의 일부가 아니라 특별하고 동떨어진 경험이 되도록 하는 단점이 있다. 따라서 어떻게 하면 경찰훈련이 지속적으로 발전할 수 있는지에 대해서 고려를 하여야 한다. 특히 국제훈련은 많은 기회가 주어지는 것이 아니기 때문에 더욱 블럭식의 훈련이 이루어지는 것이 보통이다. 즉, 국내 훈련이나 외국의 민간기관의 많은 교육들은 단계별 훈련이 이루어지며 이를 통해 지속적인 역량 발전과 훈련을 어느 정도 접목시킬 수 있다. 하지만 단발성 국제훈련은 이런 발전 기회를 만들기 어렵게 한다.

5. 훈련방법의 문제

현재 이루어지고 있는 대부분의 사이버범죄 훈련과정은 강의실 기반의 접근방법(classroom-based approach)이다. 이른바 한 장소에 교관과 훈련생이 모여 이루어지는 집체식 훈련이다.

훈련 또한 실습을 병행한 강의형태가 대부분이다. 강사가 가진 경험과 지식을 전달하는 강의가 아닌 스스로 인지하게 하는 자기인지적 학습이나 직접 경험하게 하는 시뮬레이션, 숙련자의 보조를 통한 멘토링 같은 다양한 훈련방법이 그간 사이버범죄 훈련에는 거의 접목되어 오지 못했다. 최근 전통적인 강의실 기반 훈련방법 접근의 대안으로 많이

언급되는 온라인 기반의 이-러닝 또한 마찬가지이다.

훈련방법의 문제 또한 일면으로는 IT 분야에 대한 지식과 기술 위주로 편성된 기존 국제훈련 프로그램 자체에 내재된 문제일 수도 있다. 하지만 앞서 언급한 바와 같이 실제의 사이버범죄 수사실무와 국제공조를 위해서는 IT 기술뿐 아니라 다양한 능력이 필요하며 이를 위한 훈련 또한 필요하다.

6. 의사소통 수준의 언어능력

교육훈련과 정보의 공유를 가능하게 하기 위해서 가장 중요한 것은 의사소통이며, 국제훈련에서는 특히 언어적인 문제가 매우 크다. 보통 대부분의 국제훈련 프로그램에서는 영어를 사용하는데, 영어를 모국어로 사용하지 않는 교관과 훈련생 모두에게 언어문제가 발생한다.

경험상 모국어로 강의한 내용을 영어로 강의할 때 양측의 의사소통 문제로 강의분량은 절반을 넘지 못하며, 전달되는 수준은 그보다 더 떨어지게 되어 결과적으로 훈련생의 훈련 몰입을 방해하게 된다. 국제훈련의 질을 담보하기 위한 방법으로 무엇보다 우선적으로 교관들에 대한 영어강의 능력을 배양하여야 하고, 이와 더불어 교육훈련에 사용할 강의자료를 제작할 수 있도록 충분한 배려가 필요하다.

교관진의 경우 언어능력을 교관진 선정의 기준으로 삼을 수도 있겠지만 그렇게 할 경우 전문분야에 대한 강의역량을 지닌 교관 인력 자체가 제한적이기 때문에 어느 누구도 적임자를 선정하기 어려운 문제가 발생한다. 이에 따라 후술하는 새로운 훈련기반에서는 교관진을 별도로 편성하고, 교관진에 대한 언어학습을 포함한 훈련지원 프로그램을 운영하는 등의 방안을 모색해볼 필요가 있다.

훈련생의 경우에도 물론 상당한 언어 문제를 가지고 있다. 훈련생들에게 역시 후술하는 이-러닝 시스템을 이용하도록 하여 참석요건의 확인 단계에서부터 자연스럽게 언어 구사능력을 확인함으로써 집체훈련에서 원활한 의사소통이 이루어지도록 할 필요가 있다.

한편으로 언어능력이 단시간에 확보되는 것은 아니기 때문에 이러한 능력을 갖추지 못한 수사관에 대한 훈련지원을 온라인을 통해서 가능하게 하되 온라인 훈련 프로그램을 각국의 언어로 번역하여 쉽게 접근할 수 있도록 오픈소스 프로그램을 개발하듯 버전관리

시스템을 포함하여 개발하는 방안을 대안으로 생각해볼 수 있다.

7. 전임교관의 부재

훈련을 전담하는 전임교관을 많이 확보하고 있을 때 훈련의 질을 담보할 수 있는 것은 당연하다. 하지만 사이버범죄 수사기술이 많이 세분화되고 역량있는 수사관은 교육훈련보다는 우선적으로 수사 현업에 투입되기 마련이므로 전임교관을 확보하는 것은 쉽지 않은 일이다. 나아가 언어능력을 포함한 교관인력은 그 자체가 손에 꼽을 수 있을 정도의 소수의 인원뿐이다.

현재 경찰대학과 경찰수사연수원에 영어강의가 가능한 사이버담당 교수요원 각 1명 외에는 대부분의 강의를 경찰청 사이버테러대응센터의 수사관과 연구관이 담당하고 있는데 어느 형태로든 강의에 참여할 수 있는 역량을 갖춘 국내 경찰인력은 10여 명에 불과하다. 심지어는 사이버범죄와 관련된 전문분야에 영어강의가 가능한 사람은 민간에서도 분야별로 쉽게 찾을 수 없는 실정이다. 교육훈련 업무만을 전담하는 전임인력을 더 확보해야 하는 것은 물론 기존의 인력풀(pool)을 재구성하고 이를 종합적으로 관리하는 체계를 마련해야 한다.

제2절 국제 사이버범죄수사 훈련 기반 구축 방안

현재 경찰이 수행하고 있는 국제 사이버범죄수사 훈련은 모두 비상설로 이루어지고 있으며 훈련의 계획과 시행 전 과정에서 체계화가 이루어져 있지 못한 상태라고 평가할 수 있다. 당장 훈련을 체계적으로 실시하기 위해서는 여러 가지 기반이 구축되어 있어야 한다. 그 기반이 어떤 것인지 왜 필요한지는 무엇보다 유럽의 사이버범죄 훈련의 개발을 위한 그간의 논의와 진행과정을 통해서 어느 정도 확인할 수 있다고 생각된다.

하지만 유럽의 경우와 달리 우리는 국제기구로부터 직접적인 재정지원을 받을 수 없고 여러 국가의 역량을 집결시킬 수 있을 만큼 지역간 활동이 활발하게 이루어져 있는 상태도 아니다. 따라서 한국의 실정에 맞는 사이버범죄수사 훈련기반 구축을 우선적으로 고

려하되 향후 지역적인 국제훈련의 협력이나 유럽 또는 국제적 기구와의 협력 등의 발전을 염두에 두고 개발할 필요가 있다.

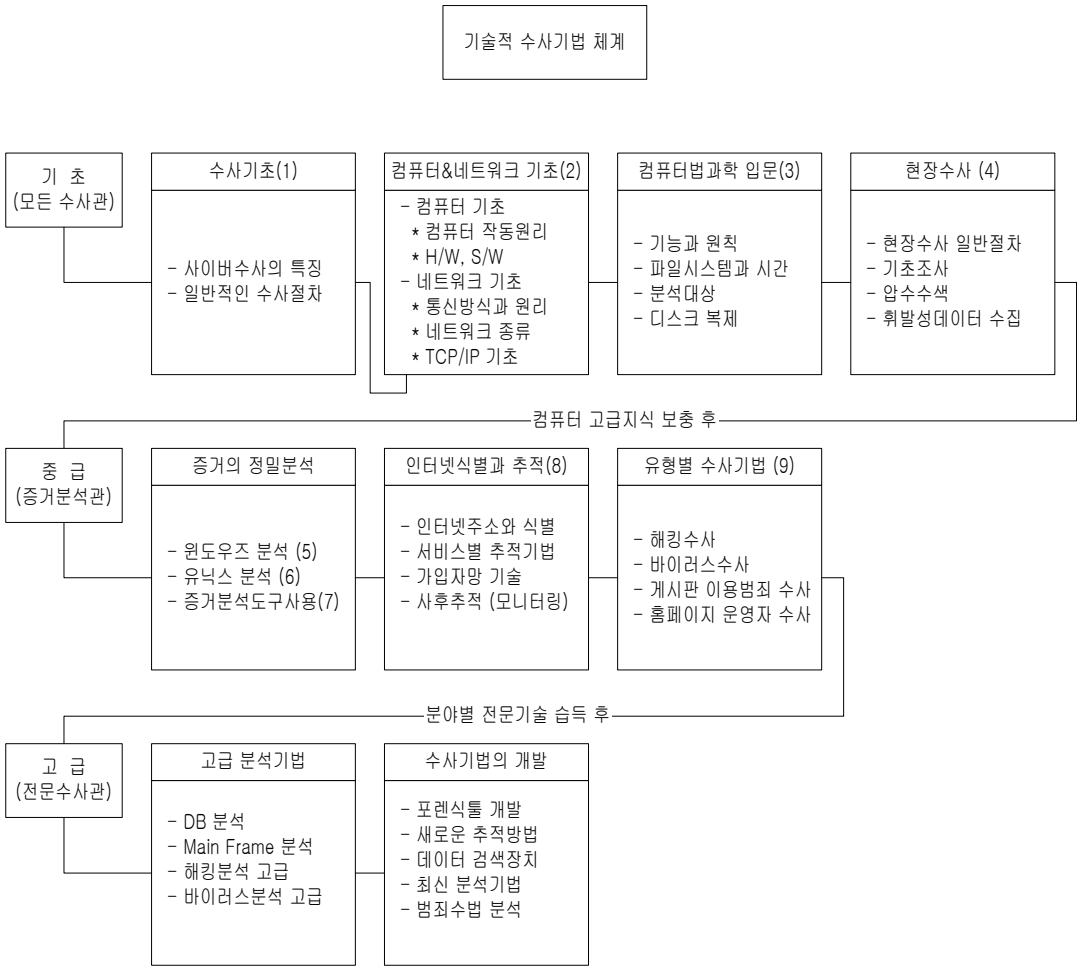
무엇보다 훈련내용의 표준화와 관리를 위해 사이버범죄 대응의 각 역영별로 훈련 내용의 모듈화 가능성을 검토할 필요가 있다. 이는 결국 무엇을 가르칠 것인가의 문제이다. 다음으로 어떻게 가르칠 것인가의 문제가 있다. 이를 위해 이-러닝과의 연계, 훈련방법 등이 논의되어야 한다. 이러한 훈련 내용을 계획하고 실제 가르칠 전문인력을 별도로 관리하여야 한다. 시설과 장비 등 물리적인 기반 또한 고려되어야 하며 이런 모든 기반들의 관리를 책임지고 수행하며 행정적 임무를 담당할 주체에 대한 고려도 있어야 할 것이다. 끝으로 국제 훈련을 완전히 별도로 하기 보다는 국내 훈련과 효율적으로 연계하여 훈련 소요비용을 낮출 수 있는 방안에 대해서 간략하게 검토해보기로 한다.

1. 교육내용의 모듈화

유럽의 경우와 같이 표준적인 교육내용의 모듈화는 매우 필요한 작업이라고 생각이 된다. 훈련내용의 준비와 이에 대한 평가 그리고 승인을 위해 훈련 내용은 매우 치밀하게 제작되고 검토되어야 할 것이다. 모듈화는 사이버범죄수사와 관련된 지식·기술·역량을 체계화하는 작업으로부터 시작되어, 시급하고 가능한 부분부터 순차적으로 진행될 수 있을 것이다.

2003년 경찰청은 '디지털증거의 수집과 분석' 매뉴얼에서 기술적 수사기법의 체계화를 〈그림 12〉와 같이 시도한 바 있다. 당시의 체계화는 현재의 국내외의 바뀐 상황과 실제 훈련에서의 적용을 고려하여 재편할 필요가 있다. 현실에서의 국제훈련 프로그램은 블럭을 쌓듯 모듈의 일부를 조합하여 해당 프로그램의 수요에 맞춰 진행하는 형태가 될 수 있을 것이다. 부분 모듈은 훈련의 내용, 방법, 강사진 등을 이미 포함하는 것이 되기 때문에 그것이 없는 상태에서 훈련 프로그램을 설계하는 것보다 훨씬 용이하고 다양하게 프로그램을 편성할 수 있는 장점이 있다.

〈그림 12〉 2003년 경찰청 사이버범죄 수사기법 체계



이러한 모듈화는 비단 국제 교육 뿐 아니라 국내 교육의 전 과정을 모두 포함하여 단일 체계를 가져가는 것이 혼선방지를 위해 필요하다. 구체적인 모듈화의 세부적인 내용은 후술하는 사이버범죄 교육훈련 전문가 집단의 공동 작업을 통해 하는 것이 바람직하다. 이는 전체적인 사이버수사의 내용을 완전히 파악하기 쉽지 않을 뿐만 아니라 부분별로 내용을 개발할 당사자 간의 협의를 통해 실현가능한 모듈화가 이루어질 수 있기 때문이다.

유럽식의 모듈화된 교육이 대학 측의 이해와 관련되어 대학입장을 주로 고려한 방법이기 때문에 면담에 참여한 일부 전문가는 시시각각 변화하는 법집행기관의 수요에 능동적

으로 대처하기 어려울 수 있다는 염려를 전달하기도 했다. 즉, 모듈화된 프로그램은 변화에 빨리 대응하기 어렵다는 것인데 이는 교육훈련 프로그램을 모듈화할 때 충분히 고려되어야 할 사항이다.

2. 이-러닝(e-Learning)과의 연계 방안

Elliott Masie는 이-러닝(e-Learning)을 학습(learning)을 디자인(design)하고 전달(deliver)·선택(select)하고, 관리(administer)하고, 확장(extend)하기 위한 네트워크 기술의 사용이라고 정의한다.

온라인 학습 그 자체는 전통적인 집체식 경찰훈련 방식이 가져오는 고비용의 부담을 해소하기 위한 대안으로 생각되었지만 훈련효과에 대한 불확실성 때문에 집체식 훈련을 완전히 대체하지는 못하고 있다. 하지만 오늘날 이-러닝은 과정의 관리, 다양한 정보의 제공, 네트워크를 통한 상호작용 등의 가능성으로 인해 집체식 훈련과 병행하여 실시하는 형태로 많이 활용된다.

이-러닝은 처음 교육훈련자료를 제작할 때의 비용은 높으나 교육내용을 재활용하기가 용이하여 효과가 확인된다면 훈련비용을 크게 낮출 수 있다는 장점이 있다. 게다가 뛰어난 접근성과 확장성으로 인해 고비용이 들어가는 집체적 국제훈련을 보완하는 방법으로 활용하기에 적합하다.

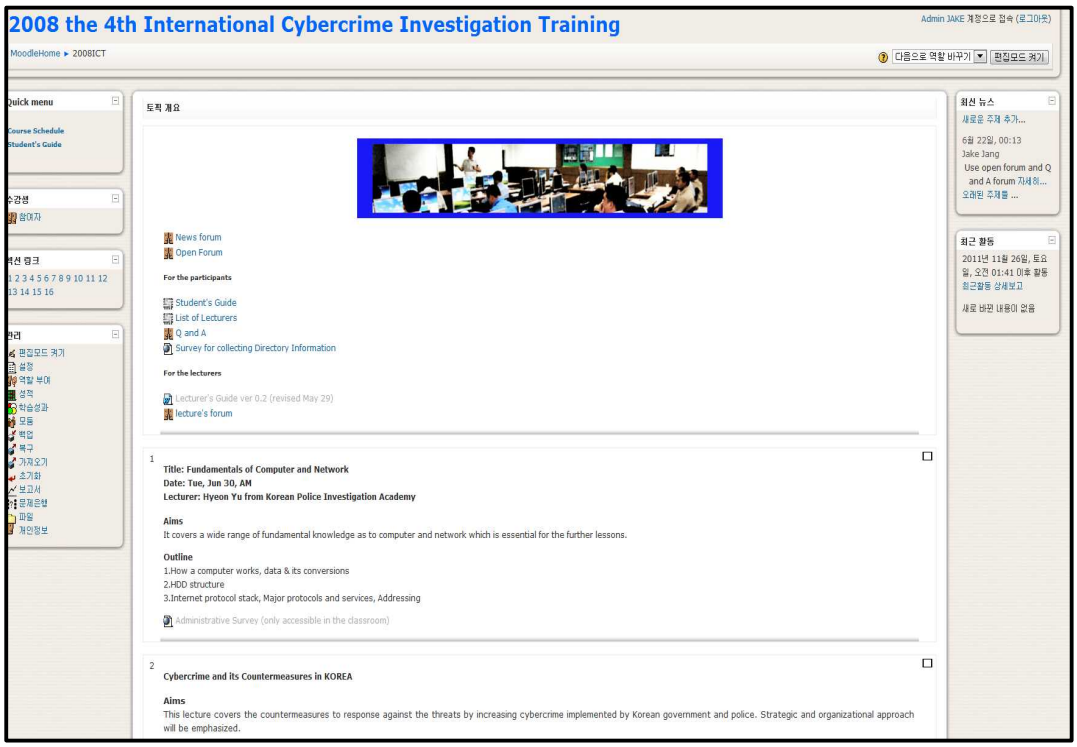
예를 들어 국제훈련프로그램에서 여러 차례 문제로 지적된 훈련생간의 역량 격차 문제를 해결하기 위해 이-러닝 시스템을 이용한 입교자격의 확인이나 선수학습 등을 사용하게 함으로써 그 격차를 다소 해소할 수 있고, 강의실에서 전달되지 못하는 자료를 지속적으로 제공하거나 의사소통을 강화하며, 교육 이후에 훈련생을 대상으로 손쉽게 설문을 시행하여 행정 비용을 줄일 수 있는 등 그 활용 가치가 무척 높다.

연구진은 경찰대학 사이버수사교육장의 시스템을 활용, ISEC에서도 사용한 교육과정 관리플랫폼인 'Moodle'을 이용한 이-러닝 시스템을 구축(이하 "CMS"라 칭한다)하여 국제 사이버범죄 수사훈련에서 보충적인 용도로 이를 활용하였다. 하지만 우선 결론적으로

언급하자면 이러한 시스템을 개발·운영하는 데에는 많은 시간과 노력이 지속적으로 투입되어야 하는데 그 개발이 조직적으로 이루어진 것이 아니라 개인적으로 시도된 것이라 뚜렷한 한계를 가지고 있다는 점이다.

하지만 조직적 차원에서도 이-러닝 시스템은 그것이 전체 훈련과정 개발의 큰 견지에서 그 일부분으로서 매우 정교하게 구성되어야 하는데 이러한 점에 대한 인식이 전반적으로 부족하여 개발 동기를 부여하기가 용이하지 않다.

〈그림 13〉 2008년 국제 사이버범죄수사 과정 CMS 홈페이지



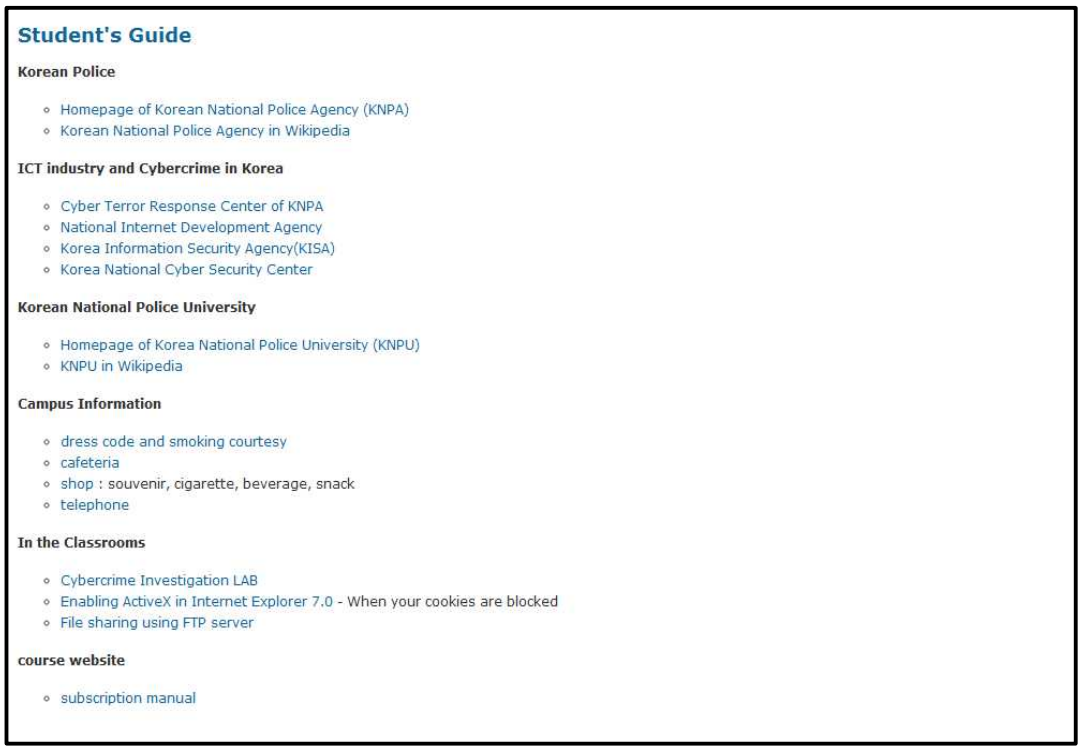
이런 오픈소스 프로젝트 형태의 프로그램을 이용하게 되면 여러 가지 장점이 있는데 그 중의 하나는 개발에 누구나 참여할 수 있기 때문에 가용성을 높일 수 있을 뿐 아니라 국제 훈련의 큰 장애 중의 하나인 언어 문제 해소에도 큰 도움이 될 수 있다는 것이다. 국제 훈련에서 언어문제는 UN의 형사사법 교육에서도 지적되는 문제이다.

'Moodle'의 경우 사용자 인터페이스가 수많은 언어를 지원하도록 하고 있기 때문에 만

약 그 컨텐츠 또한 오픈소스로 제작된다면 특정 컨텐츠를 필요한 국가에서 자신들의 언어로 번역하여 국내 목적에 맞게 사용할 수 있을 것이다. 교육컨텐츠 제작도구의 표준화 또한 상당히 이루어지고 있기 때문에 훈련 프로그램의 준비과정에서 이러한 기술을 반영하는 것을 적극 검토해볼 필요가 있다.

〈그림 14〉는 위키(wiki) 형태의 웹페이지로 구성된 교육생 가이드이다. 주요한 참조 웹사이트 뿐 아니라 교육생이 교육기관에서 생활할 때 필요로 하는 각종 정보를 제공하고 있다. 이에는 교육장과 시설의 이용지침 그리고 상세한 정보를 제공하여 시설보호와 사고방지에도 도움이 된다. 이러한 정보는 교육생에게 입국 전에 손쉽게 제공되어 편의를 도모함으로써 교육에 대한 전반적인 만족도와 교육효과를 제고할 수 있다.

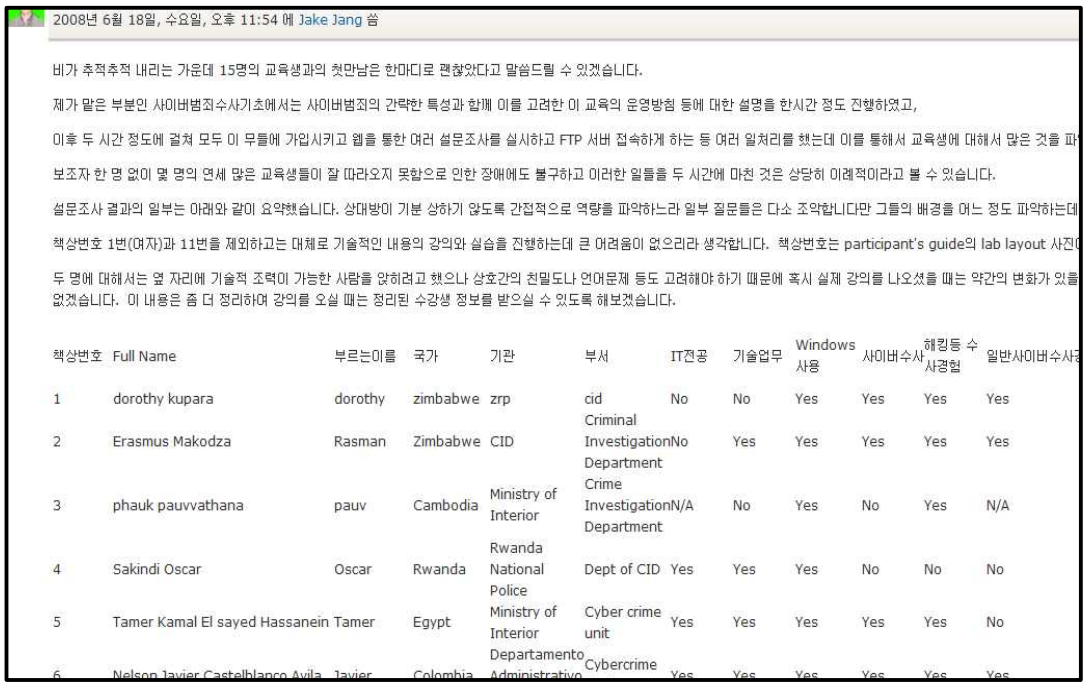
〈그림 14〉 CMS 교육생 가이드



〈그림 15〉는 게시판 기능을 이용하여 강사진을 위한 폐쇄 게시판을 운영하면서 훈련

준비와 시행과정에 의사소통을 하고 있는 모습을 보여 준다. 화면의 예에서는 과정 담당 교수가 교육생의 배경지식 등에 대한 조사결과와 수업진행 과정에서 기술적 문제의 이해도 격차 등에 대해 상세한 사항을 강사진에게 공지하고 있는데, 실제 교육생의 수업내용의 이해도와 수용태도는 효과적인 강의에 매우 필요한 사항이기 때문에 상당히 유용하게 활용될 수 있다. 후술하겠지만 전문강사진의 상설 그룹을 운영하게 되면 온라인 커뮤니티를 통해 상시 의견을 교환하고 협업하여 전체적인 사이버범죄수사 훈련 기반의 구축에 큰 도움이 될 수 있을 것이며 이런 온라인 커뮤니티는 별개로 구축되기 보다는 CMS의 일부분인 통합 형태로 가져가는 것이 더 효율적일 것이다.

〈그림 15〉 CMS 게시판



2008년 6월 18일, 수요일, 오후 11:54 에 Jake Jang 씀

비가 추적추적 내리는 가운데 15명의 교육생과의 첫만남은 한마디로 괜찮았다고 말씀드릴 수 있겠습니다.

제가 맡은 부분인 사이버범죄수사기초에서는 사이버범죄의 간략한 특성과 함께 이를 고려한 이 교육의 운영방침 등에 대한 설명을 한시간 정도 진행하였고,

이후 두 시간 정도에 걸쳐 모두 이 무들에 가입시키고 웹을 통한 여러 설문조사를 실시하고 FTP 서버 접속하게 하는 등 여러 일처리를 했는데 이를 통해서 교육생에 대해서 많은 것을 파

보조자 한 명 없이 몇 명의 연세 많은 교육생들이 잘 따라오지 못함으로 인한 장애에도 불구하고 이러한 일들을 두 시간에 마친 것은 상당히 이례적이라고 볼 수 있습니다.

설문조사 결과의 일부는 아래와 같이 요약했습니다. 상대방이 기분 상하기 않도록 간접적으로 역량을 파악하느라 일부 질문들은 다소 조악합니다만 그들의 배경을 어느 정도 파악하는데

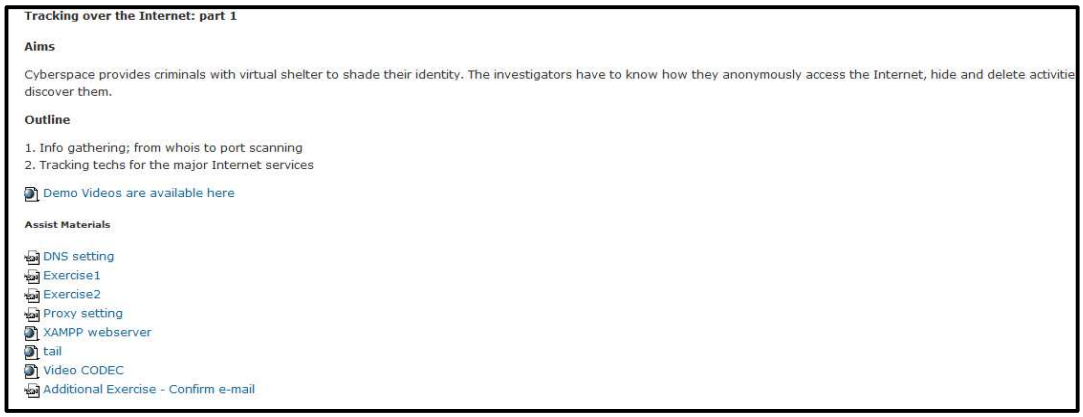
책상번호 1번(여자)과 11번을 제외하고는 대체로 기술적인 내용의 강의와 실습을 진행하는데 큰 어려움이 없으리라 생각합니다. 책상번호는 participant's guide의 lab layout 사진

두 명에 대해서는 옆 자리에 기술적 조력이 가능한 사람을 앉히려고 했으나 상호간의 친밀도나 언어문제 등도 고려해야 하기 때문에 혹시 실제 강의를 나오셨을 때는 약간의 변화가 있을 없겠습니다. 이 내용은 좀 더 정리하여 강의를 오실 때는 정리된 수강생 정보를 받으실 수 있도록 해보겠습니다.

책상번호	Full Name	부르는이름	국가	기관	부서	IT전공	기술업무	Windows 사용	사이버수사	해킹등 수사경험	일반사이버수사
1	dorothy kupara	dorothy	zimbabwe	zrp	cid	No	No	Yes	Yes	Yes	Yes
2	Erasmus Makodza	Rasman	Zimbabwe	CID	Criminal Investigation Department	No	Yes	Yes	Yes	Yes	Yes
3	phauk pauvvathana	pauv	Cambodia	Ministry of Interior	Crime Investigation Department	N/A	No	Yes	No	Yes	N/A
4	Sakindi Oscar	Oscar	Rwanda	Rwanda National Police	Dept of CID	Yes	Yes	Yes	No	No	No
5	Tamer Kamal El sayed Hassanein	Tamer	Egypt	Ministry of Interior	Cyber crime unit	Yes	Yes	Yes	Yes	Yes	No
6	Nelson Javier Castelblanco Avila	Javier	Colombia	Departamento Administrativo	Cybercrime	Yes	Yes	Yes	Yes	Yes	Yes

아래 화면은 Tracking over the Internet 이라는 강좌의 실제 컨텐츠이다. 개별적인 강의자료 인쇄물이 주어지지만 인쇄물 이외에 멀티미디어 자료를 제공하거나 과제의 제출, 워크샵, 온라인 실습 등 여러 기능을 CMS의 모듈 기능을 이용해서 수행할 수 있다.

〈그림 16〉 CMS의 강좌 컨텐츠



이러한 CMS는 훈련 과정별로 구축되기 보다는 경찰청 단위에서 지식관리시스템(KMS)과 연계하여 통합 사이버범죄수사 훈련 포털의 형태로 설치·운영하는 것이 바람직하다. 다만 설치시에는 표준화와 확장가능성, 국제교육과의 연계성, 언어적 문제 등을 모두 고려해 볼 때 'Moodle'과 같은 오픈소스 CMS 시스템을 실정에 맞게 최적화하는 것을 고려할 필요가 있다.

3. 강사진 구성을 위한 사이버범죄수사 전문가 그룹의 결성

가.필요성

현재 경찰에서 사이버범죄수사 교육훈련만을 전담하는 인원은 경찰대학과 경찰수사연수원에 각 1명이 있을 뿐이다. 하지만 이들조차 다른 과목 강의와 병행하여 사이버범죄수사 과목을 진행하고 있어 무엇보다 시급한 문제 중의 하나는 사이버범죄수사 교육훈련 실무를 전담할 전임교원을 확보하는 것이다. 따라서 현재 대부분 경찰 사이버범죄수사 훈련은 실제 사건수사나 증거분석 업무를 하는 실무자들이 전문분야별로 강의를 담당하거나 외래강의에 크게 의존하고 있다. 이는 교육훈련의 전문성과 함께 교육훈련의 품질을 크게 위협하는 요소라고 할 수 있다. 과정의 설계에서부터 훈련방법의 결정, 그리고 훈련의 내용은 서로 연계되어 통일되고 일관된 방향성을 지니고 있어야 하는데 이러한

모든 요소를 충족하기 위해서는 충분한 전담 전문교원의 확보가 긴요한 것이다.

하지만 전임교원의 확보에는 고질적인 인력부족 현상과 함께 우선적으로 실무자의 현장이탈 등의 문제가 있을 수 있으므로, 차선책으로 고려할 수 있는 것이 교육훈련에 강사로 참여하는 수준의 전문인력을 그룹화하여 특별히 관리하고 이들에게 교육훈련의 과정설계와 이와 관련된 지식자료의 관리, 강의를 전담하게 하는 것이다. 유럽의 E.C.T.E.G.와 같은 형태의 그룹이라고 할 수 있다.

나. 구성형태

전문가그룹에는 우선적으로 현재 여러 훈련과정에 출강하고 있거나 향후 출강 가능성이 있는 분야별 전문성을 갖춘 내부 인력이 포함되어야 할 것이다. 아울러 특정 분야에 대해서는 국내외의 외부 전문가 또한 이 그룹에 포함되어야 할 것이다. 이 중에 국제교육을 담당한 전문가는 영어 강의능력이 고려되어야 할 것이다. 인터폴 워킹그룹에서 교육분과가 존재하지만 교관양성과정 훈련 외에는 특별한 성과를 거둔 것으로 평가하기 어렵다. 이에 대해 동 워킹그룹에도 참여한 바 있는 면담대상 전문가는 아시아 지역에 별도의 사이버범죄수사 훈련 워킹그룹을 인터폴과 구분하여 독자적으로 추진할 필요가 있다고 지적했다. 그렇게 되면 경찰주도의 워킹그룹은 아시아 지역 워킹그룹의 결성을 주도하며 동시에 국내의 카운터파트(counterpart : 상대, 대응관계)가 되고 유럽의 2CENTRE나 E.C.T.E.G.와의 협력방안도 찾아볼 수 있을 것이다.

전문가 그룹은 앞서 언급된 모듈별로 전담을 두어 분야별로 책임성 있는 훈련설계가 이루어질 수 있도록 할 필요가 있다. 하지만 이러한 전문가그룹의 결성은 이미 경찰 내부에서 자발적인 참여를 전제로 결성이 시도된 바 있지만 활성화되지 못했다. 그 이유는 무엇보다 현업에 종사하는 참여자들이 적절하게 시간을 맞추어 활동을 하기 어렵고 주업무 외에 가외적인 교육훈련 문제에 기여할 인센티브가 따로 주어지지 않기 때문이다. 그러므로 이러한 문제가 해결되지 않고는 강제적인 그룹의 결성은 아무런 의미를 가지지 못할 것이다. 그룹의 운영과 관련된 자금은 경찰예산 뿐 아니라 민간의 참여 등을 통해 일부 해결하는 방안을 모색해볼 필요도 있다.

다. 전문가 그룹의 활동과 교육

전문가 그룹은 우선적으로 사이버범죄수사 훈련 과정의 설계와 시행에 관한 사항을 협의하고 실행에 옮기는 활동을 해야 할 것이다. 아울러 사이버범죄수사 훈련 포털의 운영과 관련해서 컨텐츠의 구성과 관리에 주도적인 역할을 수행할 수 있다. 나아가 사이버범죄 문제의 연구를 위한 학술활동으로 그 영역을 넓혀갈 수 있을 것이다. 다만 지식관리는 이제 너무도 방대한 양의 자료들이 사이버범죄의 주제 하에 다루어지고 있기 때문에 이를 집중해서 관리하기 보다는 위키와 같은 집단지성의 힘을 빌리는 것이 바람직할 것으로 보인다.

하지만 시스템의 구축과 기술적 관리는 별도의 관리 인력을 두지 않으면 운영이 쉽지 않을 것으로 생각된다. 정기적인 회의나 워크샵 형태의 모임과 온라인을 통한 상시 접촉 체계를 구축할 필요가 있다. 현재 각종 훈련의 강사로 활동하고 있는 수사관이나 연구관도 추가적인 교육을 받을 필요가 있다. 이들을 위해 별도의 교육을 통한 양성 시스템의 마련이 필요하다.

4. 훈련방법의 개발과 훈련매뉴얼의 작성

UN차원에서 효과적인 형사사법 교수법과 관련된 여러 논의가 진행된 바 있다. 조직화된 논의(모의 재판, 인권 논의 클럽), 시뮬레이션(인권 협의회, 유엔의 역사적인 모델), 롤 플레이(인권 협약), 실험, 그리고 서비스 학습(인턴십, 법률 상담), 사건 강의(변호사들에게 프레젠테이션), 실수를 통한 학습(무엇이 잘못되었는지), 영상 매체를 통한 학습(토론), 온라인 학습(가상 학습실), 번역을 통한 학습(대체 텍스트, 문화적 차이가 따르는 관점), 그리고 스마트보드 기술(구글 맵) 등이 그러한 예이다.

현재의 전형적인 훈련방법은 강의와 실습인데 이러한 전통적인 교수법에 대한 재검토가 필요하다. 물론 그러한 새로운 교수방법의 개발 자체에는 많은 시간과 노력이 필요하며 이는 교육시설 등 여러 기반과도 관계되기 때문에 전체적인 사이버훈련 체제의 일부분으로서 종합적으로 접근될 필요가 있다.

훈련매뉴얼은 훈련과정의 인증을 위해 또한 훈련시행 과정의 노하우를 집적하기 위해

필요하다. 훈련매뉴얼 또한 작성하기 위해서는 많은 시간이 소요되기 때문에 이를 전담하여 상당 기간 작업을 할 수 있는 환경과 비용이 조직적으로 지원되어야 한다. 훈련매뉴얼에는 과정 전체와 강좌별로 목표, 대상, 교보재, 훈련내용 및 가능한 한 상세한 훈련 시나리오가 포함되어야 한다. 보다 강화된 차원에서 훈련을 담당하는 교관은 훈련매뉴얼에 따른 교습이 가능한지를 직접 검증하여 교관 자체에 의한 인증제도를 두는 것도 바람직하다고 본다.

5. 훈련시설, 장비 및 소프트웨어 개선

훈련시설·장비·소프트웨어는 가장 기초적인 물리적 훈련기반이지만 현재 경찰 훈련기관의 시설과 장비는 매우 열악한 수준이다. 필요한 물리적 기반은 어떤 훈련 내용을 어떻게 가르칠 것인가에 대한 고려와 그것이 가져오는 효용과 기반을 갖추는데 소요되는 비용간의 비교분석을 통해 도입을 결정할 필요가 있다.

일부 기반은 구매가 불가능한 지적인 산출물이 될 수 있다. 예컨대 범죄사건을 재구성한 메모리나 디스크의 이미지와 같은 것들이다. 이러한 이미지는 시나리오 기반의 훈련에 다양하게 사용될 수 있으나 제작에 매우 많은 시간이 소요된다. 따라서 통상의 훈련과정에서 특별한 동기가 없다면 많은 시간을 들여 이런 이미지를 만들려는 노력을 기대하기 어렵다.

특히 이러한 이미지는 원격실습 시스템을 구축하게 되면 더욱 효과적으로 활용될 수 있다. UCD CCI의 경우 훈련과정에서 매우 많은 이미지를 활용하고 있으며 이것을 VMware Network 등을 통해 원격으로 분석하여 실습함으로써 온라인 교육으로서의 실효성을 확보하는 데에 매우 중요한 역할을 부여하고 있다. 원격실습과 이-러닝 시스템이 결합되면 훈련과정은 단일 집체교육이 아니라 집체교육-온라인교육 등이 결합된 종합적인 전문성 향상 프로그램이 될 수 있다. FBI의 Forensic Examiner 양성과정이 이러한 종합적인 전문성 향상 프로그램이라고 할 수 있다. 동 과정은 기초적인 지식에 대한 일반 자격과정, 멘토를 포함한 현장실무, 집체교육, 평가 등이 결합된 장기 과정으로, 개인별로 역량을 체계적으로 관리할 수 있는 장점이 있다. 국제교육에서도 일회성 집체교육을 벗어나 이러한 훈련서비스를 제공하는 방안을 모색해볼 수 있다.

6. 사이버범죄수사 훈련체제의 사무관리

지금과 같이 어떤 훈련과정의 개설을 결정하면 과정 설계 담당자가 개괄적인 교과를 편성하고 이에 따라 해당 분야의 강사를 섭외하여 훈련의 품질을 각 강좌별 강사의 개인 역량에 일임하는 식의 비체계적인 훈련은 많은 문제가 있다.

이와 같은 문제점을 제거하기 위해 교육훈련과정의 개설과정부터 강좌를 담당하는 전문가 그룹이 관여하여 이에 대해 물리적 기반을 포함한 준비과정을 거치고 이-러닝 시스템을 운영하며 또한 개별 훈련과정이 아니라 개인별 역량 개발 프로그램이 되게 하려면 상당한 행정력이 필요하게 될 것이다. 현재 경찰청에는 교육을 담당하는 직원이 있으나 교육 문제에 대한 전문성이나 인력은 매우 부족한 상태이다. 이는 교육기관의 경우도 마찬가지이다.

특히 행정인력 또한 사이버범죄수사 훈련 문제에 대해서는 일정 수준의 전문성이 있어야 하기 때문에 IT 문제에 지식이 많지 않은 일반 행정인력이 이를 감당하기 어렵다는 것도 문제이다. 따라서 최소한 경찰청에 전문가 그룹 행정업무 등을 담당할 사이버범죄수사 교육 전담관을 둘 필요가 있고, 경찰대학 등 교육기관에 일부 업무를 분산시켜 별도의 행정 및 연구지원 인력을 두는 방안을 고려할 필요가 있다. 사이버범죄수사 훈련 포털을 구축하게 된다면 이를 전담하는 별도의 IT 인력도 필요할 것이다.

우선적으로 국제 교육훈련 프로그램 전체를 조정하고 관리할 기능을 경찰청 내에 둘 필요가 있다. 미국 국토안보부의 연방법집행훈련센터(FLETC)의 관련 기능이나 법무부의 국제범죄수사훈련지원프로그램(ICITAP), 캐나다 왕립기마경찰대(RCMP)의 캐나다 정부명령 '외국에 대한 경찰지원'에 기반을 둔 경찰훈련 지원프로그램(Police Training Assistance Program)과 같은 전문적, 체계적, 포괄적인 국제지원 프로그램의 관리와 이를 처리할 부서 및 인력을 지정할 필요가 있다.

현재 경찰의 국제 교육프로그램은 국제업무라는 이유로 외사국에서 총괄하고 있으나 전문분야에 대한 교육업무의 관리역량을 충분히 확보하지 못하여 실제로 교육계획과 시행을 교육기관에 거의 일임하고 있는 형편이다. 이러한 체계는 지금의 비정규적이고 단기적인 훈련과정의 운영에는 크게 지장이 없을지 모르나 보다 장기적이고 전문화된 프로

그램으로 양질의 교육지원 사업을 운영하는 데에는 일정한 한계가 있다.

한편으로 흔히 선진국이라 부르는 나라에서 교육프로그램을 이수한 수료자들을 위한 연락처를 유지하고 동창모임 등을 정규화하여 지속적이고 긍정적인 자국과의 협력관계를 유지하고 친목을 도모하는 것과 같은 사후관리의 강화 또한 전반적인 국제교육 프로그램의 일환으로서 염두에 두어야 할 것이다.

또한 보다 실효성 있고 고도화된 교육 프로그램의 지원을 위해서는 상설화되고 전문화된 교육실시 기능의 확보가 긴요하다고 하겠다. 호주와 인도네시아 정부 등이 협력하여 설립한 자카르타 법집행협력센터(Jakarta Centre for Law Enforcement Cooperation), EU의 법집행기관 교육을 위한 교육기관 네트워크인 CEPOL, 미국이 태국 방콕과 헝가리 부다페스트 등 5개 주재국 정부와 협력하여 설치, 운영하고 있는 국제법집행학교(International Law Enforcement Academy) 등 세계에는 적지 않은 상설 국제 법집행교육기관과 네트워크를 통해 체계화된 국제 교육프로그램을 필요 국가 법집행기관에 제공하고 있다. 이러한 상설화된 교육기구가 있다면 더욱 양질의 교육을 실시할 수 있을 뿐 아니라 이를 통한 국가위상의 제고 등 부수적 효과측면에서도 현저히 개선된 효과를 기대할 수 있을 것이다. 훈련 프로그램 뿐 아니라 학위과정을 포함한 교육(education) 프로그램을 설치하는 것 또한 검토해볼 필요가 있다. 또한 외국인만을 대상으로 한 교육프로그램이 아니라 내외국인 모두 참여하는 개방형 교육프로그램이 개발된다면 교육의 직·간접적인 효과를 높이는 데에도 상당히 기여할 수 있을 것으로 기대된다.

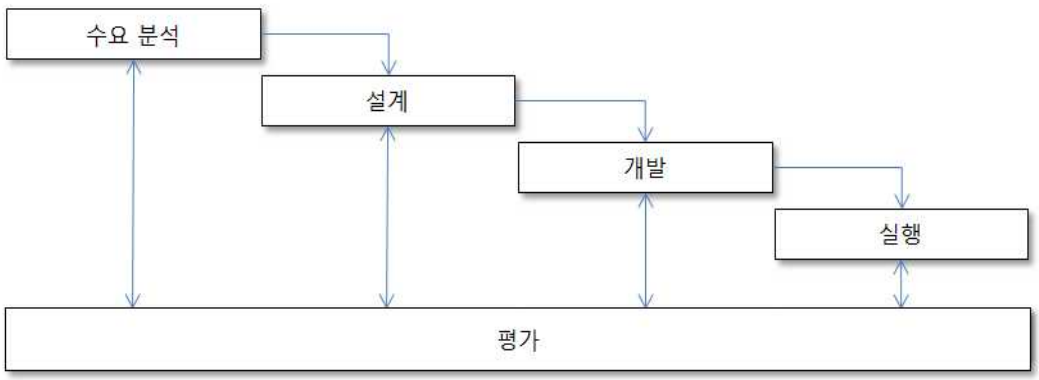
제4장 국제 사이버범죄수사 훈련 모델

제1절 훈련 절차 모델

1. 훈련과정의 일반적인 절차 모델

교육훈련과정은 통상 수요분석→설계→개발→실행→평가의 순환 프로세스로 설명된다. 무엇보다 현재 국내외에서 시행되는 국제 사이버범죄수사 훈련과정은 비정기적으로 실시되면서 이러한 프로세스가 각 단계별로 엄격하게 관리되기 보다는 과정마다 관여자의 직관에 따라 임의적으로 진행된다는 점에 문제가 있다.

〈그림 17〉 훈련과정의 일반적 절차



이전 단계에서 도출된 결과가 다음 단계에서 적절히 반영되도록 해야 하고 그 여부가 평가 단계에서 점검되어야 하는데 이러한 관점에서 보면 미흡한 면이 많다. 물론 그렇게 하기 위한 여러 장애요소도 적지 않다. 사이버범죄수사 훈련에 관해 단계별로 논점과 실행방안에 대해서 살펴본다.

2. 수요 분석(Needs analysis)

훈련 수요는 훈련의 제공자 측면에서 또는 수혜자 측면에서 매우 다양하게 파악될 수 있다. 특히 국가별 훈련이 이루어진다면 사이버수사기법 교육훈련 프로그램을 적용하기 위해서는 해당 개발도상국가의 정보통신기술 발전상태가 어느 정도인지, 사이버범죄의 발생비율과 이에 대한 수사기관의 대응태세는 어떻게 되어 있는지 등 개별 국가의 상황에 맞추어야 하므로 여러 분야의 수준을 고려하고 이를 평가할 수 있는 분석도구가 필요하다. 이에는 다음과 같은 여러 요소들에 대한 분석을 통해 수사관 및 디지털증거분석관의 직무역량 강화의 수요를 파악할 수 있다.

- 인터넷 사용률
- 무선 인터넷 보급률
- 개인용 컴퓨터 보급률
- 모바일 점유율
- 사이버범죄 발생률
- 사이버범죄 구성형태와 비율
- 사이버범죄 발생 추이와 검거율
- 인터넷 상거래 이용률
- 사이버범죄 수사기관 구성
- 사이버범죄 수사요원의 수와 능력수준
- 인접 국가와의 사이버범죄 관계

한편으로 개발도상국가의 사이버범죄 대응역량 및 국제공조 강화 측면에서 다음과 같은 요소들이 수요 판단요소로 검토될 수 있다. 이는 수혜국의 수요라는 측면에서 나아가 국제적인 개도국의 개발(development) 수요라고 할 수 있다.

- 법치주의의 확립
- 지도자의 사이버범죄에 대한 경각심(awareness)
- 사이버범죄 법률 정비
- 사이버범죄 수사조직의 구축

• 충분한 수사역량의 확보

훈련수요는 특히 다국적 국제훈련과정에서는 참석 국가별로 그리고 개인별로 수요가 매우 다르게 나타날 수 있다. 예를 들어 어떤 국가에서는 사이버범죄 수사조직이 이미 구축되어 운영되면서 그 조직의 구성과 운영방식에 대해서는 큰 관심이 없을 수 있는 반면, 또 다른 국가에서는 그 논의가 진행 중이거나 운영상의 문제로 이에 대한 관심이 높을 수 있다. 또한 조직의 관리자나 기획을 담당하는 입장에서는 이런 문제가 큰 관심사가 되지만 현장실무자에게 이런 문제는 당장 범죄사건을 해결하기 위한 현장기술보다 관심이 크게 떨어지는 문제가 될 수도 있다. 실제 아래와 같이 2008년에 실시한 설문에서 훈련 참석자 간에 관심사가 크게 차이가 나는 점을 볼 수 있다.

〈표 33〉 2008년 국제 사이버범죄수사 과정 참석자 주제별 관심도

훈련 주제	관심도(복수응답)
Legal Countermeasures on Cybercrime (국제 사이버범죄 법률)	11
Telecommunication Infrastructure and Security (정보기반 보안과 수사)	5
Practical Issues on Cybercrime Investigation (사이버범죄 수사 이론과 실제)	13
Korean Police’ s countermeasures to cybercrime (한국의 사이버범죄대응)	3
Cybercrime Scene Investigation (사이버범죄 현장수사)	13
Internet Tracing (인터넷 추적수사)	7
Mobile Forensics - Introduction and Practice (모바일 포렌식 기술)	4
Forensic Examination and Application (포렌식 조사와 응용)	3
National Cybercrime Deterrence Policies (한국의 사이버범죄 억제정책)	0
Cyber Criminology (사이버범죄학)	5
Financial Network Security (금융보안과 수사)	1

실제의 과정 설계에서는 어떠한 수요를 충족시킬 목적으로 훈련과정을 시행할 것인지 목표를 뚜렷하게 할 필요가 있고, 그것이 어떻게 가능할 것인지 충분한 검토와 실행방안에 대한 준비가 이루어져야 한다.

이는 훈련에 참석하는 입장에서의 수요이고, 국제훈련의 경우에는 훈련제공자의 입장에서의 수요 또한 고려할 필요가 있다. 많은 사이버범죄수사 관련 훈련이 상업성 훈련이지만, 국제훈련의 경우 상업성 훈련보다는 국제공조나 개발원조의 차원에서 무상훈련으로 이루어지는 경우가 많다. 따라서 이러한 훈련에서는 훈련 참석자 측의 수요 외에도 국제공조나 개발원조를 통해 이루고자 하는 목표가 수요가 될 수 있다. 예를 들어, 개발원조 차원에서 이루어지는 경찰대학 훈련과정의 경우 초청연수 전반을 담당하는 한국국제협력단 사업의 일반적인 형태와 같이 훈련 프로그램이 특정한 지식이나 기술훈련 외에도 수원국 국가 공무원의 일반적인 개발의식 고취를 위한 산업시찰이나 교류확대를 위한 문화탐방 등이 포함될 수 있는 것이다. 이러한 경우 교과과정을 특정 기술의 연마에 중점을 두는 것은 다소 부적절할 수 있다.

3. 과정 설계(Design)

과정의 설계 단계에서는 파악된 수요를 바탕으로 훈련의 목표를 설정하고 이를 달성하기 위한 실행계획을 수립한다. 확정적 혹은 잠재적 훈련대상자를 대상으로 훈련의 시기, 장소, 예산 등을 결정하고 훈련 일정을 정한다.

훈련 일정을 작성할 때는 과목별 혹은 시간대별 개별적인 내용과 교관, 훈련방법 등이 목표를 달성하기에 충분하도록 상호연계성을 고려하여 구성되어야 한다. 현재의 국제 훈련 과정의 설계는 흔히 과목의 개요를 정하고 교관을 초빙하여 실시하는 형태로 이루어지고 실제 내용의 개발은 교관에게 일임되고 있어 특히 관련 과목간의 연계성이 적절하게 확보되기 어려운 구조이다.

4. 개발(Development)

개발 단계에서 실제의 훈련을 위한 컨텐츠가 만들어진다. 구체적인 훈련방법에 따라

매체 및 자료를 선정하고 강의나 실습자료가 제작되며 세부적인 훈련계획이 만들어진다. 세부적인 훈련계획에는 각 과목별 목표와 일정이 포함된다. 많은 경찰훈련은 이러한 훈련프로그램이 담당 교관에 의해 만들어지는 것이 아니라 미리 만들어져 교관은 단지 만들어진 훈련프로그램을 실행하는 입장에 놓이게 된다. 그것은 훈련 자체를 평가하기 용이하게 하고 결국 훈련프로그램에 대한 대외적인 공신력을 확보하는데 도움이 된다.

훈련프로그램이 숙련도 검사나 자격제도와 관련이 되어 있다면 특히 프로그램은 그 진행의 세부사항이 미리 문서로 만들어져 외부의 검토와 승인을 받아야 한다. 많은 경우 이를 위해 훈련매뉴얼이 교관과 훈련생용으로 나누어져 제작되며 이를 제작하는 과정이 개발의 핵심으로 이는 별도의 사업으로 이루어지는 것이 보통이다. 현재 국내에서 실시되는 국제훈련과정은 이러한 별도의 훈련매뉴얼에 대한 제작과정이 없이 과목별로 교관이 선정되면 교관이 임의로 훈련자료를 작성하여 이를 시행하고 있는 형편이다. 교과목별로 미리 표준화된 훈련매뉴얼을 제작하는 것이 필요하다.

교관은 훈련프로그램을 적절하게 수행할 수 있는 지 역량이 확인되어야 하는데, 이를 위해 가급적이면 전문적인 전임교관이 충분히 확보되어야 한다. 현재 실시되는 각종 국제 사이버범죄수사 훈련의 가장 큰 문제 중의 하나는 다수의 교관들이 현업에 종사하다가 훈련 일정이 잡히면 형편에 따라 초빙되어 훈련내용을 개발하고 스스로 시행하기 때문에 전문성을 기대하기 어렵다는 점이다.

5. 실행(Implementation)

실행의 단계에서는 앞선 계획에 따라 훈련을 실시한다. 당연히 앞선 계획이 실제 실행에 적절히 옮겨질 수 있도록 이루어질 것이 요구된다. 하지만 실행과정에서 계획과 다른 변수들이 흔히 발생할 수 있어 실행과정에서 이러한 변수를 예측하고 이에 대응할 수 있는 준비가 되어 있어야 한다.

6. 평가(Evaluation)

평가 단계에서는 전체적인 훈련의 진행과정을 검토하여 발견된 문제점에 대해 이를 개

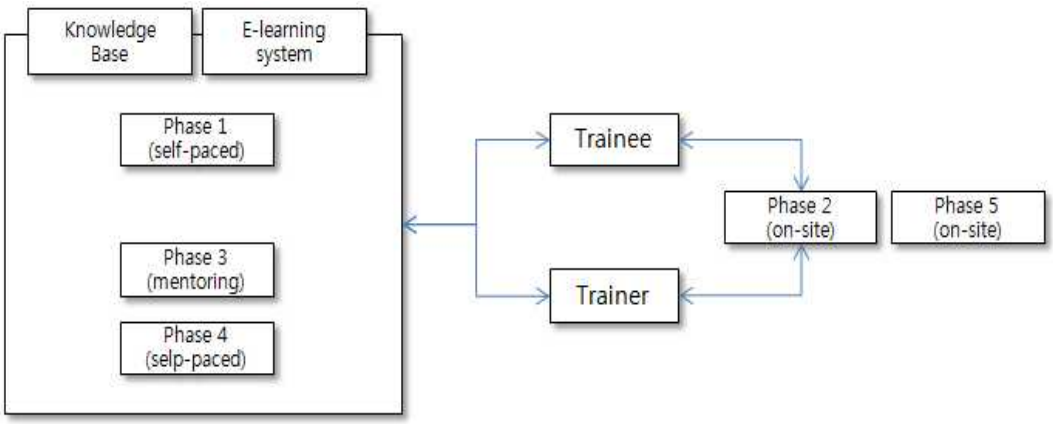
선할 수 있는 유기적인 순환구조가 이루어지도록 하는 것이 중요하다. 현재 많은 국제 훈련과정에서 이루어지는 설문형태의 평가가 이러한 목적에 맞게 잘 구성되어 있는지는 의문이다. 국제 훈련과정에서는 특히 훈련시행자에 대한 온정적인 평가가 이루어지기 십상인데 이는 현재 많은 국제 훈련과정이 개발도상국에 대한 지원의 성격을 지니고 있기 때문에 수혜자의 입장을 반영한 결과라고 판단되며 또한 교육시행자 입장에서는 긍정적인 평가를 받기를 바라는 경향이 투영된 것이라고 볼 수 있다.

제2절 새로운 국제 사이버범죄수사 훈련체제

훈련 절차 모델의 각 단계에 맞추어 개발도상국가에 적용 가능한 사이버범죄수사 교육훈련 프로그램을 제시한다. 연구의 목적 중의 하나로 각 개발도상국가별로 인터넷 기반 발전상황 및 사이버수사 역량 등의 수준을 고려하여 이에 적합한 사이버수사기법 교육훈련 프로그램을 제시하고자 하였으나, 다수의 개발도상국가 사이버범죄 수사관을 상대로 교육훈련 프로그램을 직접 실시해본 결과, 각 국가별 상황 보다는 사이버범죄를 수사하는 수사관 개인의 역량을 고려하여 교육훈련 프로그램을 개발하는 것이 훨씬 더 유효하고 의미있는 작업이라고 판단이 되었다. 따라서 국가별 수준이 아닌 사이버범죄 담당 수사관의 수준에 맞춘 사이버기법 교육훈련 프로그램을 제시하고자 한다.

우선적으로 새로운 훈련 모델을 적용하여 사이버범죄 수사기법 훈련과정을 '사이버범죄 수사관 양성 과정(CCIT : Comprehensive Cybercrime Investigator Training)'과 '디지털포렌식 전문가 양성 과정(CDFT : Comprehensive Digital Forensic Training)'으로 구분하고, 각 단계별로 필요한 내용들을 기술하고자 한다. 제시하고자 하는 사이버범죄수사 훈련체계는 〈그림 18〉과 같다.

〈그림 18〉 종합적인 사이버수사 훈련 모델



이 모델은 상시 세계에서 접속이 가능한 지식 베이스와 이-러닝 시스템, 추가적으로 과정관리시스템(course management system)을 구축하여 집체훈련에 참석하기 위한 요건을 충족시키고, 이를 확인하여 집체훈련의 성과를 높이며, 집체훈련이 끝난 후에도 지속적으로 멘토링과 자기학습을 통해 전문역량을 개발하여 보다 고급 수준인 다음 단계의 집체훈련에 참석하는 형태로 지속적인 발전이 가능하도록 설계하였다. 이는 현재의 국제훈련이 공통적으로 지니는 블럭식 훈련의 한계를 극복하기 위한 것에 주안점을 두었지만, 앞서 언급된 여러 기반이 구축되지 않으면 실행에 옮기기 어려울 것이다.

1. 지식기반과 이-러닝 시스템

지식기반시스템(knowledge management system)은 CMS가 포함된 이-러닝 시스템과 더불어 사이버범죄수사 훈련 포털로 구축된다. 이에는 사이버범죄의 수사와 관련된 다음과 같은 자료들이 포함될 수 있을 것이다.

〈표 34〉 사이버범죄수사 지식기반시스템(KMS) 내용 예시

구 분	종 류	예 시
공 통	참고자료	링크, 도서, 논문, 보고서 등
	동향	뉴스, 기술정보, 범죄동향
	표준, 매뉴얼	표준, 매뉴얼, 가이드라인
	교육자료	슬라이드, 문서, 강사매뉴얼, 비디오
	도구	Free Tool, H/W & S/W 정보
	자료요청	정보요청 사항 배포
	기타	Contact point, ISP Lists, Legal requirement
	협력기관 정보	IRT 등 타기관 정보 전파
수 사	범죄수법	MO
	수사기법	수사기법
	경보	수사상 경보, 통보, 관심 촉구(등급별)
	수사Briefing	공조사건 추적정보 보관 제공
기 술	Hash sets	악성코드, 아동포르노, 상용프로그램 등
	기술문서	분석기법,

앞서 언급한 대로, 사이버범죄수사 교육훈련을 받고자 하는 수사관이 기본 교육훈련을 시작하기 전에 사이버범죄수사와 관련하여 꼭 알아두어야 할 상식과 같은 내용을 미리 준비하도록 기준을 정해주는 것이다. 공통적으로 알아두어야 하는 인터넷이나 소프트웨어 이용법, 수사에 필요한 수사기법 등이 망라되어 있다. 이러한 내용들을 사전에 숙지하고 기초훈련 프로그램에 임한다면 교육생들의 이해 수준도 어느 정도 맞출 수 있고, 훈련프로그램도 원활하게 진행될 것이다.

2. 단계별 훈련 프로그램

가. Phase 1 : 온라인 기반 기초훈련

최초 단계의 훈련 프로그램으로서 온라인 기반으로 운영된다. 이는 지식기반시스템(KMS)에 포함된 기초적인 내용을 중심으로 학습을 진행하며 학습의 진행상황 확인과 시험 역시 온라인을 기반으로 이루어진다. 온라인 기반의 일부 실습이 진행될 수 있다.

〈표 35〉 사이버범죄수사 기초훈련(Phase 1) 교과 모델

과 목	학습시간	주요 내용
사이버범죄의 이해	6	사이버범죄의 정의와 역사, 사이버범죄의 특징
컴퓨터 기초	24	컴퓨터구조, 데이터, 운영체제, 데이터베이스 기초, 저장장치 기초, 프로그래밍의 이해
네트워크 기초	24	통신기술 개관, 인터넷 역사, 인터넷 프로토콜
포렌식 기초	12	법과학의 정의와 역사, 법과학적 조사기법 개관, 품질보증과 인증제도
주요 사이버범죄 이슈	24	해킹, 악성코드, 인터넷사기, 저작권침해, 아동착취
사이버범죄 국제공조	6	유럽사이버범죄협약, 국제기구 이니셔티브, 법집행 네트워크, 민간 사이버범죄 대응 협력
합 계	96	

온라인을 통해 프로그램을 이수하게 하거나, 부득이한 경우 나라에 따라 이를 집체식 교육훈련 프로그램으로 이수하게 한 후에 다음 단계인 상급 교육훈련 프로그램으로 나아갈 수 있도록 하게 한다. 기초훈련 프로그램에는 사이버범죄수사의 가장 기본이 될 수 있는 컴퓨터 및 네트워드의 기초와 같은 기술적인 교육뿐만 아니라 사이버범죄의 특징이나 국제적인 수사공조체계와 같은 정책적인 과목을 편성하여, 전체적으로 균형 잡힌 시각으로 사이버범죄수사의 전반적인 내용을 살펴볼 수 있도록 배려하였다.

Phase 1의 학습내용은 학습시간 기준으로 96시간을 산정하였으며, 따라서 하루 2시간씩 주 5일을 학습한다고 하였을 때 약 두 달 가량의 학습기간이 필요하게 된다. 이 이-러닝 과정은 UN과 한국형사정책연구원이 구축한 사이버범죄수사 훈련 프로그램의 일부 내용을 공동으로 활용하는 방안도 모색해 볼 수 있을 것이며, 그것이 실현된다면 교육과정 초기에 많이 소요되는 프로그램 구축 비용을 절감할 수 있을 것이다.

나. Phase 2 : 기초 집체훈련

이 단계에서는 사이버범죄 수사관과 디지털포렌식 분석가로서의 필수적인 실무역량에 대한 훈련 및 시험이 이루어진다. 반드시 기초훈련 프로그램을 이수한 수사관을 대상으

로 하고, 자격과정으로 병행할 수 있으며, 대학의 학점을 부여하는 과목으로 편성하는 것도 가능하다.

사이버범죄 수사관 과정(CCIT)과 디지털포렌식 전문가 과정(CDFT) 모두 기초 지식의 습득이 전제되어 있으므로 현행의 과정에서 기초강의를 제외하고 좀 더 심화된 수사 및 포렌식 기술 중심으로 편성하였고, 시간은 일일 8시간씩 주 5일의 2주 과정으로 총 80시간으로 편성하였다.

〈표 36〉 사이버범죄 수사관 양성 과정(CCIT) Phase 2 교과 모델

과 목	시 간	주 요 내 용
과정소개 및 행정	6	CDIT 소개, 입교식/수료식/평가
인터넷 추적기술 개요	9	일반적인 추적방법, 도구의 사용, 법률 문제
서비스별 추적기술	14	이메일, 웹사용자, 웹서비스제공자, Proxy, Tor, SNS, 휴대전화 사용자 추적
합법적 감청기술	6	감청원리, 감청기술, wireshark 이용, 감청표준
수사상 공개자원의 개발	3	각종 웹자원, 기관정보, 사이버범죄수사 관련 학회와 단체, 출판물 정보, Underground 정보
수사를 위한 고급검색	3	Boolean 검색, GREP, Google 검색 응용, Forensic 검색
정보의 통합과 분석	3	링크분석, 텍스트마이닝, 시계열분석, 사건의 재구성, 네트워크 관계 분석, 통합 분석도구 사용
국제공조 강화 워크샵	3	국제공조 강화를 위한 수사관의 역할에 대한 팀별 토론과 보고서 발표
사건 유형별 수사실무	15	인터넷사기수사, 아동포르노 수사, 해킹 및 악성코드 유포자 수사, 조직범죄 수사, 돈세탁
현장수사	12	압수수색 절차, 휘발성 증거수집, 포렌식 복제, 증거의 처리, 시뮬레이션
사례 연구	6	2~3건의 범죄사건에 대한 사례 집중 분석
합 계	**80**	

〈표 37〉 디지털포렌식 전문가 양성 과정(CDFT) Phase 2 교과 모델

과 목	시 간	주 요 내 용
과정소개 및 행정	6	CDIT 소개, 입교식/수료식/평가
운영체제 구조	3	운영체제 구조, 윈도우즈, 리눅스
윈도우즈 파일시스템	5	FAT, NTFS 등 윈도우즈 파일시스템
리눅스 파일시스템	5	Ext2, 3 등 리눅스 파일시스템
파일시스템 분석과 복구	5	파일시스템 분석, 파일시스템 복구, 숨겨진 파일찾기
인터넷 사용기록 분석	3	히스토리, 쿠키, 임시파일
응용 프로그램 분석	11	일반 응용프로그램, DB, 역공학 기초
암호와 스테가노그라피	11	암호 취약성과 분석, 스테가노그라피 탐지
휘발성증거와 메모리분석	5	휘발성 증거수집 기술, 메모리 덤프와 분석
포렌식 검색	5	키워드 개발, 검색기술, Hashsets
네트워크 분석	8	패킷캡춰와 분석 기술, 분석 도구
현장수사	5	압수수색 절차, 포렌식 복제, 증거의 처리, 시뮬레이션
보고서 작성	2	보고서 작성요령, 법과학적 의견
사례 연구	6	종합적인 포렌식 분석 사례 연구
합계	**80**	

다. Phase 3 : 온라인 기반 멘토링

Phase 2를 통해 교관진과 훈련생 사이에는 대면접촉을 통한 친교관계가 형성될 것이다. 많은 사이버수사의 초심자들이 겪는 어려움은 무엇을 어떻게 학습해야 할 지 모른다는 것이며 이러한 문제는 경험있는 교관들이 멘토로서 도움을 주면서 학습을 진행할 수 있도록 체계를 구성할 수 있다.

멘토링은 특정하게 정해진 내용에 대한 학습보다는 개인별로 겪고 있는 실무적인 문제의 해결을 중심으로 이루어지게 되며 온라인을 기반으로 이루어진다. 멘토링을 통해 프로그램에 참여하는 이들 간에 공통적으로 발견되는 문제들의 해결방식과 훈련 프로그램의 발전 방향을 발견하게 될 것이 기대된다.

훈련받은 멘티들은 해당 국가의 훈련받지 못한 다른 수사관들과 경험 많은 교관간의 커뮤니케이션을 촉진하는 역할을 한다. 흔히 훈련받지 못한 수사관들은 영어구사 능력이 떨어지는 경우가 있을 것이며 커뮤니티에 논의되는 내용은 다국어를 지원하기 위한 버전관리시스템을 채택한 훈련 포털에서 멘티들에 의해 다양한 언어로 번역될 수 있을 것이다.

라. Phase 4 : 자기학습

Phase 4의 자기학습은 Phase 5의 특정 분야에 대한 고급 전문훈련을 받기 위한 배경지식과 기술을 이-러닝을 통해 학습하는 과정이며 Phase 1의 경우와 같이 시험통과는 Phase 5에 참석하기 위한 요건이 된다. Phase 4의 내용은 Phase 5의 훈련 진행자들에 의해 구성되며 다양한 전문분야로 분류된다.

마. Phase 5 : 고급 분야별 집체훈련

Phase 5에서는 분야별 고급훈련이 이루어진다. 훈련과정은 사이버범죄수사 훈련모듈에 의해 수요에 따라 다양하게 이루어질 수 있다. 과정의 채택은 훈련 포털을 통해서 어느 정도 국제 사이버수사관 커뮤니티가 형성되었다는 것을 전제하므로 훈련수요에 대한 즉각적인 파악과 이를 반영한 훈련과정의 시행이 가능할 것이다.

우선적으로 CCIT와 CDFT만을 고려했지만 이러한 기본적인 구조는 다른 많은 훈련 프로그램에 다양하게 응용될 수 있을 것이다. 예를 들어 악성프로그램 분석 과정을 마련한다고 하면 먼저 이에 대한 수요가 발견된 후 이를 모듈화하여 프로그램을 구성하고 그 기초적인 내용에 대해서는 Phase 4의 내용에 포함시키고 이어 Phase5의 한 과정으로 전문화하여 편성할 수 있을 것이다. 이와 같은 전문화 과정의 예는 이미 제3장에서 기술한 것처럼 한국의 사이버테러대응센터의 교육방향이 모범이 될 수 있다.

제5장 결 론

2011년 11월 29일부터 12월 1일까지 부산 해운대구 소재 벡스코(BEXCO)에서 열린 '제4차 부산 세계개발원조총회'에서는 새로운 국제지원의 패러다임이 될 '부산선언'이 발표되었다. 이 선언에서는 '개발협력을 위한 글로벌 파트너십'이 채택되었는데, 그 주요한 내용으로는 '원조에서 개발협력으로', '서구에서 포괄적 파트너십으로', 'OECD에서 유엔으로', '공적원조에서 민간원조로' 방향이 선회되었음을 언급하였다. 즉, 지구촌 빈곤과 불평등, 분쟁과 환경위기, 질병과 실업, 차별과 배제를 극복하고 지구촌 99%의 삶의 질과 인권을 신장하기 위한 글로벌 파트너십 선언이 될 것으로 기대된다.

이 총회에 참석한 반기문 유엔 사무총장은 "원조는 자선 행위가 아닌 공동 번영과 안정을 위한 투자이자 시장 확대와 고용 창출을 위한 원동력이다. 금융위기로 원조 약속을 바꾸지 말아 달라."고 역설하였고, 세계 최대의 원조국가인 미국의 힐러리 클린턴 국무장관은 "개발원조는 이제 지엽적 문제가 아니라 외교·국방과 함께 미국 정책의 기둥이 됐다"고 강조하였다.

개발도상국가의 개발 정도 및 정보통신기술 발전 상황에 맞춘 수준별 사이버범죄 수사기법 교육훈련 프로그램을 개발하여 이들을 대상으로 사이버범죄 수사기법을 전수하여야 할 필요성은 누누이 언급되어 왔고, 현재 시행되고 있는 각종 사이버범죄수사 교육훈련 프로그램의 문제점을 분석하여 이를 해결하기 위한 새로운 사이버범죄수사 훈련 모델을 지식기반과 이-러닝 시스템 그리고 단계별 훈련 프로그램으로 제시함으로써, 이 프로그램을 통해 사이버범죄 수사에 있어서의 한국의 위상을 높이고 국제적인 역할을 담당할 수 있음을 검토하였다.

식상한 표현이기는 하지만 물고기를 잡아주는 방식의 교육훈련에서 물고기를 잡는 방법을 알려주는 방식으로의 교육훈련의 진화는 당연한 것이라고 할 수 있고, 각 국가의 발전 수준에 따른 교육프로그램의 적용방식도 중요하다고 할 것이다.

하지만 이제는 여기에서 한 걸음 더 나아가 국제개발협력의 패러다임에 변화가 시도되고 있다. 이제는 저개발국에 대한 단순 원조를 넘어 포괄적인 개발효과를 가져와야 하고 원조를 통한 국제개발협력의 틀을 새로 짜야 한다. 즉 각 나라의 문화에 맞는, 그 나라의 운영체계와 국민의 심성에 녹아들어가는 원조가 필요하다 할 것이다.

물고기를 잡는 방법의 전수뿐만 아니라 그 단계를 더 뛰어 넘어 물고기를 잡기 위한 설비나 잡은 물고기를 입맛에 맞게 보관하는 기술의 이전까지도 고려되어야 할 때이다. 단순한 교육훈련 프로그램 지원에서 그치지 않고, 더 나아가 교육훈련에 필요한 기반시설이나 교육관련 인력 및 교보재의 제공, 행정적인 처리지원도 뒤따라야 할 것이다.

이와 관련하여 신문기사의 내용을 한 번 살펴보자[23].

캄보디아 국립기술대는 한국이 당초 직업훈련원으로 자금을 지원한 곳이다. 2002년 2,770만 달러 지원 결정을 한 뒤 2005년 한국 기업이 건물을 완공했다. 하지만 한국은 이곳에 건물만 지원하지 않았다. 학교를 운영할 수 있는 교수진까지 지원했다. 그러자 캄보디아 정부는 이곳을 단순한 직업훈련원이 아니라 아예 국립대학으로 지정했고 그해 5월 국립기술대학으로 개교했다.

이 학교는 운영이 독특하다. 총장은 한국인과 캄보디아인 두 명이다. 한국인 총장은 외국인 교수 인사권과 교육 콘텐트 지원, 교수법 개발 등 대학 운영의 핵심 업무를 담당한다. 교수진 100여 명 가운데 27명인 한국인 교수들은 캄보디아 정부로부터 한 푼도 받지 않는다. 7명만 한국 정부의 지원을 받고 나머지 20명은 모두 자원봉사자다. 한국에서 은퇴한 교수나 안식년을 받은 현직 교수가 자원봉사 방식으로 이곳에서 강의를 하고 있다.

교수진 가운데 배대한(43) 전기·전자학부 교수는 “한국에서 학교 운영 노하우를 전수하고 있다”며 “자원봉사를 할 수 있는 교수 인력을 모집하기 위해 해마다 한국을 찾고 있다”고 말했다.

이 학교 졸업생이 몇 년 전에는 캄보디아 국비 장학생 시험에서 1위를 할 정도로 캄보디아 내에서 빠른 속도로 자리를 잡아가고 있다. 김성철 국립기술대 총장은 “학생들이 변화하는 모습에 뿌듯함을 느낀다”며 “무기력해 보였던 학생들이 이제는 나라를 생각하고 정의롭게 살기 위해 공부를 열심히 하려고 한다”고 전했다. 김 총장이 처음 이곳에 왔을 때 학생들이 함께 식사하는 모습을 볼 수 없을 정도로 학생 사이에 ‘더불어 산다’는 개념이 없었다고 한다. 김 총장은 “학생들이 자기 자신밖에 몰랐다”며 “하지만 학교 생활을 통해 더불어 사는 법을 익히면서 캄보디아의 국가 자산이 되고 있다. 그런 모습이 가장 기억에 남는다”고 말했다.

23) 중앙일보 2011. 11. 28. 중앙경제 E9 기획 하단, “캄보디아 직업훈련원→국립기술대로 바꾼 ‘한국의 힘’”

사이버범죄 수사 분야에서 국제공조수사의 중요성은 사이버범죄 개념이 나타난 초창기부터 계속 강조되어온 사항이다. 국경을 넘어 자행되는 또는 그 지역과 대상의 특정을 무시하고 횡행하는 현대적이고 조직적인 사이버범죄에 대해 어느 한 국가만의 또는 사이버수사역량이 강화된 몇몇 국가들만의 대비는 필연적으로 그와 대비되어 수사역량이 부족한 어느 나라로의 사이버범죄자들의 도피를 이끌어내게 될 것이고, 그렇게 된다면 전 세계적인 사이버범죄 대책은 그 효과를 거둘 수 없게 된다.

사이버공간의 특성상 전 세계적인 사이버수사 역량의 강화는 당연한 발전방향이라고 할 것이다. 따라서 개발도상국가들의 사이버수사 역량을 강화하기 위한 교육훈련 프로그램의 개발은 지금 당장 비용 면이나 인력 면에서 많은 노력이 요구된다고 하여도 간과할 수 없는 부분이다. 지속적인 교육훈련 프로그램의 개발이 필요하다고 할 것이고 이를 뒷받침 할 수 있는 인적 자원과 시설 등의 제공도 따라야 할 것이며, 단순한 기술적 내용의 전수에 그치지 않고, 수사와 관련된 기법 그리고 법률적인 보완도 함께 따라가는 문화적 전수의 방법도 고려할 때이다.

사이버범죄수사에 대한 개발협력은 국제사회에서 한국이 가장 모범적으로 기여할 수 있는 분야이고 가장 확실한 미래에의 투자이다.

참 고 문 헌

C. Taylor, B. Endicott-Popovsky, A. Phillips, "Forensics Education: Assessment and Measures of Excellence", proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE 2007), 155-165, 2007.

M. Rogers, K. Seigfried, "The future of computer forensics: a needs analysis survey, Computer & Security"(2004), 23, Elsevier, 12-16.

A. Corrigan, "How To Make a Forensic Examiner", 2004 HTCIA International Training Conference & Expo, presentation

Cormac Callanan & Nigel Jones, "Study: Co-operation between LE, Industry and Academia to deliver long term sustainable training to key cybercrime personnel", 2009.

UN General Assembly A/65/201:2

The National Center for Forensic Science The Certification Roundtable Meeting, Draft Final Report, (http://www.ncfs.org), 2006.

관련 인터넷 사이트

cyberforensics.purdue.edu

www.2centre.eu

www.aafs.org/pdf/NIJReport.pdf

www.e-evidence.info/education.html

www.fbi.gov/hq/lab/fsc/backissu/jan2008/standards/2008_01_standards01.htm

www.internetworldstats.com

www.kent.ac.uk/careers/forensicsci.htm

www.mssu.edu/schtech/criminaljustice/BSForensics.htm

www.naver.com

www.ncfs.org/dfqs/index.html

www.ucd.ie/news/0712_december/071207_cyber_crime.html

www.usatoday.com/tech/news/techinnovations/2006-06-05-digital-forensics_x.htm

중앙일보 2011. 11. 28. 중앙경제 E9 기획, "한국 돈으로 지어준 마닐라 전철에 한국식 여성전용칸 - 베트남·필리핀·캄보디아, 한국 대외원조 국가를 가다", "캄보디아 직업훈련원 → 국립기술대로 바꾼 '한국의 힘'"

治安論叢 (제28집)

2012년 10월 발행
2012년 10월 인쇄

발행인 : 한 광 일
발행처 : 치 안 정 책 연 구 소
경기도 용인시 기흥구 언남로 74
인쇄처 : JK Co.(제이케이컴퍼니)

이 책자에 게재된 내용은 연구자 개인 의견이며
치안정책연구소 공식 견해와 다를 수 있습니다.

제 28집 치안논총
2012 Police Science Journal

발간등록번호
11-1332522-000003-10

第 28 輯
ISSN 1738-2971

치안정책연구소

경기도 용인시 기흥구 언남로 74 T 031-285-0183 F 031-620-2989