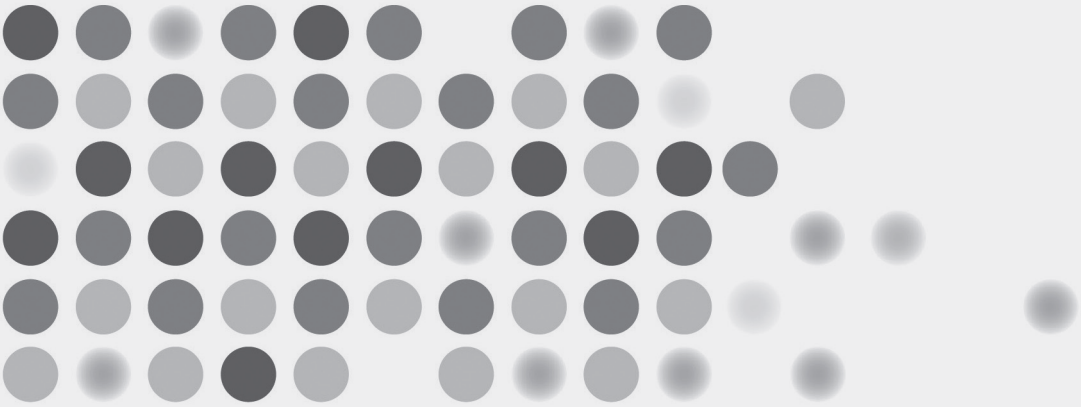
연구총서 15-B-13

사이버범죄방지 가상포럼(VFAC) 사업 정책성과 연구

김한균 | 승재현 | 나주원 | 조민정



KIC 한국형사정책연구원
KOREAN INSTITUTE OF CRIMINOLOGY

발간사

본 보고서는 2005년부터 2015년까지 한국형사정책연구원이 유엔 마약 및 범죄사무소(UNODC)와 공동개발하고 운영해온 「사이버범죄방지 가상포럼」(VFAC) 사업에 대하여 세부사업별로 기획과 실행과 평가의 내용을 분석함으로써, VFAC의 중장기적 비전과 지속적 발전 전략을 모색하는데 목적이 있습니다.

VFAC(Virtual Forum Against Cybercrime)은 개발도상국 형사사법공무원과 일부 일반인을 대상으로 하는 온라인 교육훈련프로그램의 개발과 보급에 중점을 두고 사이버범죄 및 사이버보안 분야의 전세계 전문가와 실무가들이 온라인상에서 사이버범죄 관련 동향과 정보를 공유하고 교류토록 하는 한편 이러한 정보를 데이터베이스화 하는 온라인 연구네트워크를 하기 위한 사업입니다.

VFAC 프로그램의 구체적 개발과정과 그 운영 성과 및 한계에 대한 분석과 평가를 바탕으로 축적된 경험과 성과를 향후 사이버범죄 및 사이버보안 분야 국제적 지역적 협력사업에 적극적으로 활용하는 방안을 제시할 것으로 기대합니다.

연구를 성실히 수행해준 김한균 국제협력센터장과 승재현 부연구위원, 나주원, 조민정 연구원의 노고에 감사드립니다.

2015년 12월

한국형사정책연구원

원장 김 진 환

목 차

표 차례

그림 차례

국문요약

1. 한국형사정책연구원은 2005년부터 사이버범죄방지가상포럼 (Virtual Forum against Cybercrime; VFAC)을 실시하고 있으며, 당해 포럼은 개발도상국가의 법집행 관계자들에게 사이버범죄 방지에 관한 교육훈련을 위한 온라인 강의와 동시에 사이버범죄에 관심 있는 학자, 실무진, 연구진들을 위한 포털 사이트인 연구 네트워크가 있다.

2. 사이버범죄 가상포럼 사업은 사이버범죄에 관한 범죄동향, 통계자료, 모범사례, 법률안, 국가적 국제적 대응정책, 전문가 및 사이버 연구기관 등 관련한 다양한 정보를 국내외 전문가와 일반인에게 제공하고자 만들어 졌으며, 국제사회의 사이버범죄를 비롯한 초국가적 범죄(transnational crimes) 현안 대응 역량 강화에 기여하고자 하는데 의의가 있다.

3. 본 연구에서는 VFAC의 온라인교육훈련사업과 연구네트워크 사업의 성과를 평가함으로써 온라인 교육훈련 프로그램의 발전적 활용방안을 탐구하고, 이를 토대로 국내적 사이버 보안 네트워크를 강화와 함께, 동북아지역 중점 사이버보안 연구협력사업과 UNODC의 사이버범죄 데이터 베이스 구축을 위한 발전적 과제를 제시한다.

4. 특히 10년간 유엔마약및범죄사무소와 교류협력관계에 있는 국내외 다수 연구기관 및 형사사법기관과의 공동작업을 통해 진행해 온 한국형사정책연구원 국제협력사업의 대표적 사례이자 성과인 만큼, 현재 시점에서 그 긍정적 성과와 부정적 한계를 객관적으로 살펴보고, 이를 바탕으로 중장기적으로 발전방안을 마련해야 마땅할 시점이다. 따라서 온라인 교육훈련프로그램의 실질적 보급확대를 위한 전략과, 그간 축적된 온라인 연구네트워크 데이터베이스를 여타 데이터베이스와 연계하여 그 내용의 질을 제고하고 그 활용도 역시 확장하는 방안의 모색하고자 한다.

5. 제2장에서 사이버범죄방지가상포럼 개발경과와 성과검토를 하고, 제3장에서 사이버범죄방지 가상포럼 연구네트워크 발전방안과 사이버범죄방지 가상포럼 교육훈련 프로그램의 성과를 평가한다. 사이버범죄방지가상포럼 개발경과는 2005 ~ 2009년 개발단계, 2010 ~ 2013년 운영단계, 2014 ~ 2015년 지속 발전 단계로 나누어 각각의 개발 단계에서의 특징을 기술하고, 사이버범죄방지 가상포럼 연구네트워크 발전방안에서는 사이버범죄방지 가상포럼의 사이버범죄 통계, 법률안 정리, 제2절 UNODC 사이버범죄 자료실 (Cybercrime Repository)과의 연계 발전 방향 그리고 VFAC리뷰의 지속적 간행에 대한 전략을 설명하였다.

6. 사이버범죄방지가상포럼 교육훈련 프로그램의 성과에서는 사이버범죄방지 가상포럼 온라인 교육 프로그램의 상황에 대하여 설명한 후 이를 오프라인 교육·훈련 프로그램 교육 교재 활용방안에 대하여 논의를 진행하였다. 특히 오프라인 교육·훈련 프로그램 교육 교재 활용방안과 관련하여 2015년 고려대학교 사이버법센터와 함께 '사이버범죄의 이해'라는 교재를 발간하였으며, 해당 교재를 조선대학교, 중국의 연변대학교 등지에서 사용하는 것을 적극적으로 검토하고 있다.

7. 사이버범죄방지 가상포럼사업은 국제사회의 사이버범죄를 비롯한 초국가적 조직범죄 대처역량 강화노력에 적극 기여하면서 주로 아시아, 아프리카 개발도상국가 형사사법공무원을 대상으로 한 사이버범죄 역량강화 교육훈련 프로그램, 전세계의 사이버범죄 전문가들의 토론장을 열어 주고 동 분야 최초로 사이버범죄 관련 정보를 축적하는 하나의 저장공간을 개설했다는데 상당한 의미가 있다고 자평할 수 있다.

8. 다만 이러한 대표적 국제협력사업으로서의 성과에 대한 높은 수준의 국제적 평가, 그리고 이를 위해 투입된 상당한 재정 및 인력자원을 고려해 보면 본 연구원 내에서의 객관적 평가와 역량지원에서는 미흡한 점이 있다. 본 VFAC 사업의 지속적 발전을 통한 결실을 맺으려면, 무엇보다도 내부적 이해와 협력이 절실하며, 이를 위해 본 사업의 성과에 대한 객관적 내용을 공유하여

이해도와 참여도를 높이고, 부정적인 오해와 불신의 장애요인을 극복해 나가야 할 것이다.

9. 현재 VFAC 사업은 개발과 운영단계를 넘어 중장기적인 지속적 발전전략을 모색하고 실천해 나가야 할 단계에 있다. 기존의 온라인 교육훈련프로그램은 그 교육대상과 보급방식을 혁신함으로써 확대발전되어야 한다. 급변하는 사이버범죄 환경과 사이버범죄 수사 및 대응의 전문성을 고려할 때 계속적인 온라인 교육훈련프로그램의 개발과 보완에는 엄연한 한계가 인정된다.

10. 특히 애초 개도국 형사사법공무원을 대상으로 실시한 바, 개도국의 경우 온라인 교육훈련 과정을 충실하게 이행할 만한 인터넷 인프라가 먼저 갖추어져 있지 않은 점을 고려하지 못하였다. 또한 언어적 장벽 또한 보급확산에 장애요인이라는 점도 인식하게 되었다. 이에 온라인 교육훈련과정 중에서 오프라인 교재화, 현지어 번역이 가능한 내용을 선별하여 일반인 또는 기초교육용 교재로 재활용하는 방안을 추진해 나가야 할 것이다.

11. 온라인 연구네트워크를 통해 축적된 사이버범죄동향과 사이버범죄대책 및 대응법제 정보는 사이버범죄 대응정책 연구개발에 매우 유용한 자료가 된다. 이를 고립적으로 운영하기 보다는 국내외 유사 데이터베이스 개발사업과 연계하여 시너지 효과를 모색하는 효과적 방안이 모색되어야 한다.

12. 한국형사정책연구원은 유엔마약및범죄사무소가 주도하고 있는 사이버범죄 저장소 데이터베이스의 초기 개발단계에 참여하여 공동개발자로서 기여할 수 있다. 이를 계기로 유엔마약및범죄사무소와의 사이버범죄 분야 협력관계를 한단계 높일 수 있다. 한국형사정책연구원이 사이버범죄 분야에서 국제적 연구기관으로서의 위상을 높일 수 있게 됨은 물론이다.

제1장

KOREAN INSTITUTE OF CRIMINOLOGY

서 론

김 한 균

제1장

서 론

본 연구는 2015년도 「국제 범죄방지를 위한 UN·국제협력 및 연구 사업」의 세부 과제 하나로 기획되었다. 또한 유엔 범죄방지 및 형사사법 프로그램 (UN Crime Prevention and Criminal Justice) 소속 연구기관으로서 14개국 34개 형사정책 연구기관 및 형사사법기관과 연구교류협력을 진행하고 있는 한국형사정책연구원 국제협력사업 중에서도 유엔 마약및범죄사무소(UNODC)와 사이버범죄 분야 연구 및 기술적 지원(technical assistance)협력 사업 추진성과를 정리하면서, 향후 과제를 발전적으로 제시하는데 목적이 있다.

제1절 연구의 의의와 목적

1. 연구의 의의

한국형사정책연구원이 2005년부터 UNODC와 공동개발하고 시행중인 협력사업인 사이버범죄방지가상포럼 (Virtual Forum against Cybercrime; VFAC)은 개발도상국가의 법 집행 관계자들에게 사이버범죄 방지에 관한 교육훈련을 위한 온라인 강의와 사이버범죄에 관심 있는 학자, 실무진, 연구진들을 위한 포털 사이트인 연구 네트워크로 구성되어 있다.

본 사업은 사이버범죄에 관한 범죄동향, 통계자료, 모범사례, 법률안, 국가적 국제적 대응정책, 전문가 및 사이버 연구기관 등 관련한 다양한 정보를 국내외 전문가와 일반인에게 제공함으로써 국가정책연구기관이자 유엔 범죄방지 및 형사사법 프로그램 네트워크 (UN Crime Prevention and Criminal Justice Pogramme Network)

소속 기관으로서 국제사회의 사이버범죄를 비롯한 초국가적 범죄(transnational crimes) 현안 대응역량 강화에 기여하고자 하는데 정책적 의의가 있다.

2. 연구의 목적

본 연구의 목적은 2005년부터 2015년에 이르기까지 진행되어 온 VFAC 사업의 축적된 성과를 정리·분석·평가하고 그 성과를 국내외에 적극 확산 보급하는데 있다.

즉 VFAC의 온라인교육훈련사업과 연구네트워크 사업의 성과를 평가함으로써 온라인 교육훈련 프로그램의 발전적 활용방안을 탐구하고, 이를 토대로 국내적 사이버보안 네트워크를 강화와 함께, 동북아지역 중점 사이버보안 연구협력사업과 UNODC의 사이버범죄 데이터 베이스 구축을 위한 발전적 과제를 제시해 보고자 한다.

특히 10년간 유엔마약및범죄사무소와 교류협력관계에 있는 국내외 다수 연구기관 및 형사사법기관과의 공동작업을 통해 진행해 온 한국형사정책연구원 국제협력사업의 대표적 사례이자 성과인 만큼, 현재 시점에서 그 긍정적 성과와 부정적 한계를 객관적으로 살펴보고, 이를 바탕으로 중장기적으로 발전방안을 마련해야 마땅할 시점이다. 따라서 온라인 교육훈련프로그램의 실질적 보급확대를 위한 전략과, 그간 축적된 온라인 연구네트워크 데이터베이스를 여타 데이터베이스와 연계하여 그 내용의 질을 제고하고 그 활용도 역시 확장하는 방안의 모색이 필요하다.

제2절 연구의 대상과 방법

1. 연구의 대상

본 연구의 대상은 2005년부터 2015년까지의 사이버범죄방지 가상포럼(VFAC) 사업이다. 즉 VFAC을 구성하는 두 가지 주요 사업이다. 그 하나는 개발도상국 형사사법 공무원과 일부 일반인을 대상으로 하는 온라인 교육훈련프로그램의 개발과 보급이며, 다른 하나는 사이버범죄 및 사이버보안 분야의 전세계 전문가와 실무가들이 온라인상에서 사이버범죄 관련 동향과 정보를 공유하고 교류하며, 이러한 정보를 데이터베이스화 하는 온라인 연구네트워크이다.

두 주요사업을 개발과 본격 운영, 그리고 후속 발전단계로 나누어 각각의 세부사업 기획과 실행과 평가에 걸친 사업내용을 정리 분석한다. 이를 바탕으로 VFAC의 중장기적 비전과 지속적 발전 전략을 모색하고자 한다.

2. 연구의 방법

본 연구 제2장에서는 VFAC의 개발경과와 성과를 검토한다. 즉 개발단계 (2005-2009년), 운영단계 (2010-2013년), 지속발전단계(2014-2015년)으로 각각 구분하여 성과를 정리하였다. 이는 지난 10년간 사업을 지속하면서 개별년도 성과분석에만 그친 점을 고려할 때 중장기적 발전전략을 모색하기 위해서는 체계적 분석이 필요하였기 때문이다.

제3장에서는 VFAC 연구네트워크의 발전방안을 검토한다. 이를 위하여 VFAC 웹사이트를 기반으로 운영해 온 연구네트워크의 사이버범죄 동향, 통계, 법률안 자료 데이터베이스 성과를 정리한다. 이어서 2015년 UNODC에서 개발하고 있는 사이버범죄 자료저장소(Cybercrime Repository) 사업과의 연계발전 방안을 제시한다.

제4장에서는 VFAC 교육훈련프로그램의 성과를 평가한다. 즉 온라인 교육훈련프로그램의 구체적 개발과정과 그 성과 및 한계를 분석한다. 이를 바탕으로 교육훈련프로그램 개발과정에서 축적된 교육교재를 적극적으로 활용하는 방안을 제시한다.

제2장

KOREAN INSTITUTE OF CRIMINOLOGY

사이버범죄방지 가상포럼 개발경과와 성과검토

승재현·나주원·조민정

제2장

사이버범죄방지 가상포럼 개발경과와 성과검토

제1절 개발단계 : 2005-2009년

1. 사이버범죄방지 가상포럼의 배경

초국가적 형태로 진화되고 있는 사이버범죄에 대한 효율적인 대응을 위해서는 국제기준에 부합하는 국제협약 및 규정과 형사사법체계의 확립이 중요하다. 신속한 범죄수사와 범죄인 인도 및 송환을 위해 국가적 차원에서의 형사사법기관 및 관계자들 간의 국제공조도 시급하다. 이에 대한 일환으로 유엔을 비롯한 국제사회는 사이버범죄 방지를 위한 여러 가지 대책들을 제시하였다. 그 중에서 가장 우선적인 대책으로 관련분야 공무원들에 대한 교육훈련 프로그램 개발과 이를 실행 할 수 있는 기반의 조성을 들고 있다.

한국형사정책연구원은 2004년 7월 29일 유엔마약 및 범죄사무소(UNODC)와 공식 양해각서를 체결하여 유엔범죄방지 및 형사사법네트워크(UNPNI)에 14번째로 가입하여 국제사회에서 범죄방지 및 형사정책 관련 전문 연구기관으로 공식 인정받았다.[1] UNODC는 2005년 4월 18일부터 25일까지 태국 방콕에서 열린 제11차유엔 범죄방지 및 형사사법총회 기간 중인 22일부터 23일까지 양일간 한국형사정책연구원 주관으로 '컴퓨터 관련범죄 대응방안(Measures to Combat Computer-related Crime)' 워크숍을 개최하였다. 동 워크숍에서는 사이버범죄의 발생추세 및 사이버범죄 문제의 보편성과 국제적 대응의 필요성, 사이버범죄방지를 위한 형사실체법과 소송법의 법적 조화, 사이버범죄 방지와 퇴치를 위한 국제협력, 사이버범죄 연구에 대한 국제협력,

1) 연성진 외 4인, 유엔 및 국제협력백서, 한국형사정책연구원, 2009, 16쪽.

컴퓨터 관련 범죄수사를 위한 기술적 지원 그리고 사이버범죄 퇴치를 위한 디지털 환경 내에서의 민관협력 전략에 대해 논의하였다.

제11차 유엔범죄방지총회는 급속한 세계화의 진전과 정보통신 및 컴퓨터기술의 발전이 범죄에도 악용되고 있음을 지적하고 첨단기술과 사이버 관련 범죄방지 및 수사의 역량강화를 위한 유엔의 지지를 촉구하는 방콕 선언(Bangkok Declaration)[2] 을 채택했다.

○ NF. 203/18, Chapter 1, paras. 16(2005년 제11차유엔 범죄방지 및 형사사법총회 결과 방콕 선언 중 일부)

16. 유엔회원국들은 세계화와 정보화시대에 있어 정보통신 및 컴퓨터기술의 급속한 발전에는 범죄목적의 기술악용도 뒤따름을 주목한다. 따라서 첨단기술과 컴퓨터관련범죄의 방지와 수사, 소추를 위한 노력이 강화되어야하며, 유엔차원의 기여가 필요하다.[3]

○ A/CONF.203/18,paras. 323 (2005년 제11차유엔 범죄방지 및 형사사법 총회문서)

F. 컴퓨터 관련 범죄 대응방안 워크숍

323. 4월 22일-23일까지의 제9차, 10차 회의에서 제2위원회는 컴퓨터 관련 범죄 대응방안을 주제로 한 워크숍을 개최했다. 이 워크숍은 한국형사정책연구원의 협력하에 구성되었다.[4]

---

2) 방콕선언 〈https://www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf〉참조.

3) 16. We note that, in the current period of globalization, information technology and the rapid development of new telecommunication and computer network systems have been accompanied by the abuse of those technologies for criminal purposes. We therefore welcome efforts to enhance and supplement existing cooperation to prevent, investigate and prosecute high-technology and computer-related crime, including through the development of partnerships with the private sector. We recognize the important contribution of the United Nations to regional and other international forums in the fight against cybercrime and invite the Commission on Crime Prevention and Criminal Justice, taking into account that experience, to examine the feasibility of providing further assistance in that area under the aegis of the United Nations, in partnership with other similarly focused organizations.

4) F. Workshop on Measures to Combat Computer-related Crime
323. At its 9th and 10th meetings, on 22 and 23 April 2005, Committee II held the Workshop on Measures to Combat Computer-related Crime. The Workshop was organized in cooperation with the Korean Institute of Criminology.

본 워크숍에서 사이버범죄의 발생추세, 사이버 문제의 보편성과 국제적 대응의 필요성, 사이버범죄 방지를 위한 형사실체법과 소송법의 법적조화, 사이버범죄 방지와 퇴치를 위한 국제적 협력, 사이버범죄 연구에 대한 국제적 협력, 컴퓨터 관련 범죄 수사를 위한 기술적 지원, 사이버범죄 퇴치를 위한 디지털 환경 내에서의 공공·민간 협력 전략에 대해 논의하였다.

○ A/CONF.203/18, paras. 340(a) (2005년 제11차유엔 범죄방지 및 형사사법 총회 문서 중 일부)

b. 결론 및 권고사항

340. 컴퓨터 관련범죄 워크숍에서는 다음과 같은 결론과 권고사항을 도출하였다.

(a) 유엔은 컴퓨터 관련 범죄에 대응하는 회원국들을 지원함에 있어 주도적인 역할을 해야 한다. 이와 관련하여, 전 세계 컴퓨터 관련 범죄 전문가들의 커뮤니케이션을 위한 포럼 또는 온라인 연구네트워크의 구성에 관해 심의하도록 한다.[5]

이를 계기로 2005년 5월 한국형사정책연구원은 UNODC로부터 사이버범죄방지를 위한 글로벌 프로그램에 참여해 줄 것을 제안 받았다. 제14차유엔 범죄방지 및 형사사법위원회(UN Commission on Crime Prevention and Criminal Justice)회의에서, 유엔은 사이버범죄 방지를 위한 국제적 차원에서의 지원을 촉구하였고, 특히 정보통신 강국인 대한민국에 대하여 사이버범죄 방지를 위한 국제적 차원의 참여를 독려했다. 이에 한국형사정책연구원은 UNPNI기관으로서 국제 형사사법 협력 네트워크 강화의 일환으로 2005년부터 2009년까지 UNODC와 함께 "사이버범죄 방지를 위한 가상포럼 (Virtual Forum Against Cybercrime, VFAC)"을 구축에 적극 참여할 것을 약속했다.

---

5) 340. The Workshop on Measures to Combat Computer-related Crime made the following conclusions and recommendations:
(a) The United Nations should play a leading role in assisting Member States in combating computer-related crime to safeguard the functioning of cyberspace, so that it would not be abused or exploited by criminals or terrorists. In that regard, consideration should be given to the establishment of a virtual forum or online research network to encourage communication among experts throughout the world on the issue of computer-related crime. 〈https://www.unodc.org/documents/congress//Documentation/11Congress/ACONF203_18_e_V0584409.pdf〉

E2005/30, paras.52 (2005년 제14차유엔 범죄방지 및 형사사법위원회)

[의제4] 주제: 제11차유엔 범죄방지 및 형사사법 총회 결론 및 권고사항 논의

참관인 자격의 한국형사정책연구원은 컴퓨터 관련 범죄 워크숍에 대해 발표하면서, 이 워크숍의 결과가 개발도상국 법 집행 관계자들에 대한 교육훈련과정 모델 개발을 포함하는 사이버범죄 방지 및 통제 프로젝트 기술지원으로 이어질 수 있음을 시사했다. 2006년 서울에서 개최되는 UNPNI 소속기관 및 민간부문이 참가하는 전문가그룹회의에서 개발도상국에 대한 교육훈련과정 모델 개발이 다루어질 예정이다.

또한 이 프로젝트에는 사이버범죄의 새로운 동향과 접근법에 대한 정보교환을 촉진하기 위한 UNODC 지원 전문가 포럼이 포함된다고 언급했다.

앞서 설명한대로 정보통신기술발달과 국제화에 따른 초국가적 사이버범죄의 증가에 따라 국제공조 및 협력의 필요성이 증대되었으며 특히, 사이버 범죄방지를 위한 국제협력네트워크의 강화를 위해서는 개발도상국가들의 사이버범죄방지대처역량강화를 위한 지원이 필요하다. 이러한 필요성에 따라 사이버범죄방지 가상포럼사업을 통해 아시아지역 개발도상국가들에게 온라인 사이버범죄관련 교육훈련프로그램을 연구 개발하여 제공함으로써 첨단범죄로서 사이버범죄에 대한 지식확산으로 인한 사이버범죄 예방환경조성 효과를 기대하였으며, 이를 위해 전문가 정보교류 및 대국민 정보제공이 가능한 온라인 네트워크를 구축하고자 했다.

2. 사이버범죄방지를 위한 가상포럼 구축사업 진행과정

한국형사정책연구원은 2006년부터 2008년까지 5차례에 걸쳐 사이버범죄방지 가상포럼구축을 위한 국제전문가 자문회의를 개최하고 온라인 교육훈련 프로그램과 연구네트워크 개발을 위한 단계별 작업을 진행했다. 제 1,2차 국제전문가 자문회의 및 조정위원회 회의는 사이버범죄방지 가상포럼 구축을 위한 사전준비회의로 역할별 구성원 분류 및 강의 형식안 제시와 예산 등을 논의했다. 제3차 조정위원회에서는 사이버범죄방지 가상포럼구축 착수단계로 가상포럼을 온라인 교육훈련 프로그램과

연구네트워크로 나누고 온라인 교육훈련 프로그램 강의 커리큘럼의 기본 특 구상 및 연구네트워크의 역할과 성격을 명확히 하였으며, 가상포럼 제작비 마련 등을 논의했다. 제 4.5차 조정위원회에서는 가상포럼 제작진행과 검토 및 사업확장 시기에 대한 논의가 있었다.

가. 제1차 사이버범죄방지 가상포럼 구축을 위한 사전준비회의

UNODC관계자 및 사이버범죄 전문가들이 참석한 사이버범죄방지 가상포럼 구축을 위한 사전준비회의가 2006년 6월 28일부터 30일까지 서울에서 개최되었다. 동 회의에서는 사이버범죄분야의 전문가들을 초청하여 가상포럼 구축을 위한 조정위원회 및 사무국 설립, 사업추진 계획안 및 교육훈련 논의 그리고 본격적인 프로그램 개발을 위한 2007년 개발 초안을 마련했다.[6]

나. 제2차 사이버범죄방지 가상포럼 조정회의

제2차 사이버범죄방지 가상포럼 조정위원회는 2006년 11월 8일부터 9일까지 경주에서 개최되었다. 동 회의에서는 구체적인 프로그램 개발 방안에 대한 논의와 플랫폼(platform)및 교육과정 구축을 위한 다양한 모델이 제시되었다. 또한 교육훈련 과정 시범 운용의 첫 번째 대상국가로 베트남을 선정하고 교육훈련과정 기획과 강의계획 구성을 담당할 국제전문가 자문위원회(International Consultant Group : ICG)를 구성했다. ICG는 크게 온라인 교육훈련 프로그램, 연구네트워크, 인프라구축의 세 분야로 나뉘었다. 그 밖에 교육과정 구축을 위한 소요예산 규모 제시 및 사이버범죄 연구네트워크 구성요소와 자원에 대한 논의가 진행되었다.[7]

다. 제3차 사이버범죄방지 가상포럼 조정회의

2007년 5월 14일부터 15일까지 서울에서 개최된 제3차 조정위원회 및 전문가 자문회의의 가장 중요한 성과는 온라인 강의 커리큘럼의 기본 틀 구축이다. 또한

---

6) 연성진 외 4인, 유엔 및 국제협력백서, 한국형사정책연구원, 2009, 17쪽.
7) 연성진 외 4인, 유엔 및 국제협력백서, 한국형사정책연구원, 2009, 17쪽.

ICG와 사무국 및 자문위원들의 역할에 대한 논의와 교육훈련 과정 첫 번째 대상국가인 베트남을 대상으로 시행될 시범사업과 온라인 교육과정 및 사이버범죄 연구네트워크개발에 대한 논의가 진행되었으며, 대한민국의 대표적인 인터넷 서비스기업인 ㈜네이버의 이전 상호명인 ㈜NHN 으로부터 500,000 달러 상당의 가상포럼 개발지원금과 기술적 지원을 제공받기로 합의했다.[8)]

라. 제4차 사이버범죄방지 가상포럼 조정회의

2008년 2월 21일부터 22일까지 서울에서 개최된 제4차 사이버범죄방지 가상포럼 조정회의에서는 첫 대상국가인 베트남에서 온라인 교육프로그램의 시범 사업 시행을 위한 계획을 논의했다. 전 세계 온라인 교육훈련 프로그램을 예시로 제시하면서 사이버범죄방지 가상포럼 구축 기본 구성안에 대한 논의와 시범시행을 위한 계획안 및 가상포럼 웹사이트 초안에 대하여 논의했다. 동 회의결과를 바탕으로 2008년 1월부터 6월까지 시범강의안 모듈 1.1부터 1.7까지 10개의 강의안 제작을 위해 국내외 사이버범죄 전문가를 강사로 초청하여 성균관대학교와 공동으로 개발했다. 또한, 교육훈련 과정 대상국가의 범위를 말레이시아, 인도네시아, 중국, 태국, 필리핀 등 아시아 개발도상국가들의 경찰, 검사, 판사 등 형사사법 실무자로 확대하기로 결정했다.

마. 베트남대상 시범사업 시행

한국형사정책연구원과 첫 번째 시범사업대상국인 베트남은 2007년부터 2년 간 시범사업 시행에 대한 지속적인 협의를 진행했다. 2007년 7월 2일부터 8일까지 베트남 경찰총국을 방문하여 시범사업에 관한 논의를 하였다. 또한 베트남 측의 사업 참여의사를 확인하고 온라인 교육훈련 진행을 위한 제반 현지시설 및 여건을 시찰했다. 베트남 방문을 통한 시범사업 대상기관을 확정하고 시범 온라인 교육 프로그램을 제작하여 2008년 6월 24일부터 27일까지 베트남 공안부 경찰총국의 실무자를 대상으로 시범 시행 및 평가를 실시했다.[9)]

---

8) 연성진 외 4인, 유엔 및 국제협력백서, 한국형사정책연구원, 2009, 17쪽.
9) 연성진 외 4인, 유엔 및 국제협력백서, 한국형사정책연구원, 2009, 18쪽.

바. 제5차 사이버범죄방지 가상포럼 조정회의

2008년 10월 30일부터 31일까지 양일간 개최된 제5차 조정위원회에서는 베트남 시범사업의 시행 및 평가를 바탕으로 온라인 교육프로그램을 아시아 개발도상국가 중 말레이시아(사이버시큐리티 말레이시아), 인도네시아(법무·인권부 국가입법기구), 중국(사법부 범죄예방연구소), 태국(법무부), 필리핀(초국가범죄대응특사청)으로 추가 확장시행하는 방안을 논의했다. 사이버범죄전문가 및 온라인 교육프로그램을 시행하고자하는 말레이시아, 인도네시아, 중국, 태국 등 아시아 4개국 대표단을 초청하여, 전체 온라인 교육프로그램 시행을 위한 논의와 대상 국가의 온라인 인프라 현황 및 본 사업에 대한 참여의사를 확인했다.[10]

3. 온라인 교육·훈련 프로그램 개발과정

가. 강사선정

사이버범죄방지 가상포럼 온라인 교육·훈련 과정은 입문과정과 고급과정, 세미나 과정으로 구분되어 총 137개의 강의로 구성되었다. 입문과정은 판사, 검사 및 경찰 등과 같은 법집행 관련 공무원들을 대상으로 설계되었으며, 사이버범죄 동향 및 사이버범죄 방지를 위한 법률 및 각 국의 정책 등에 초점을 두었다.

입문과정 코스1은 컴퓨터기술 및 새로운 커뮤니케이션 방법을 주요내용으로 총 6개의 모듈로 구성되었다. 입문과정 코스2는 사이버범죄에 초점을 맞추어 총 11개의 모듈로 구성되었다.

고급과정은 사이버범죄 수사의 실질적인 정보제고를 위한 전문가 양성과정을 목적으로 설계되었다. 고급과정 코스1은 사이버범죄 수사의 과정 및 기술, 코스 2는 디지털 수사를 다루고 있다. 세미나 과정은 전문가과정의 특별과정으로 제작되어, 사이버범죄 분야의 연구자 및 실무가들을 위해 사이버범죄 현안에 대해 논의할 수 있도록 구성되었다.

2008년 6월 입문과정 코스1의 강의내용에 대해 베트남 경찰청에서 시행한 온라인 교육프로그램의 시범사업 평가를 바탕으로, 2009년부터 본 사업을 위한 본격적인

10) 연성진 외 4인, 유엔 및 국제협력백서, 한국형사정책연구원, 2009, 18쪽.

준비절차가 진행되었다. 그 첫 번째 단계로 국내외 사이버범죄 전문가 인력풀을 확보하여 강사진을 선정했다. 5월부터 7월까지 3개월 간 본격적으로 온라인 교육프로그램 시행을 위한 강사선정의 작업을 거쳐, 학계 및 실무계의 사이버범죄 전문가 중 국내강사 12인과 미국, 독일, 호주, 일본, 인도, 홍콩 출신의 국외강사 9인과 계약을 체결했다.

나. 온라인 교육프로그램 개발업체 선정 및 개발과정

온라인 강의 콘텐츠 개발업체 선정을 위한 공개입찰을 통해 성균관대학교가 선정되었다. 콘텐츠 개발은 성균관 대학교가 10개의 시범강의를 포함한 136개의 강의에 대해 형사정책연구원과 논의 및 검토의 과정을 거쳐서 진행되었다. 강사들이 제출한 강의교재에 대한 검수를 과정 후 일부 내용 수정에 대해서는 강사와 최종 확인 작업을 거쳐 최종적으로 성균관 대학교에 전달하는 방식으로 진행되었다. 강의제작은 강사들이 직접 강의촬영을 하거나 원어민 성우를 고용하여 음성 녹음을 했다.

온라인 교육프로그램 개발을 위해 일부 국내외 강사들은 직접 촬영하였으며, 국외강사들은 초빙 또는 연구원에서 해당 국가를 직접 방문하는 방식으로 강의 내용을 촬영했다. 또한, 사이버범죄방지 가상포럼사업의 기본취지 및 개발목적, 강의구성 및 강의과목 등을 설명하기 위해〔Module 0〕을 신설·추가했다.

사이버범죄방지 포럼의 홈페이지 메인부분에 강사촬영과 음성녹음의 온라인 강의 제작 샘플을 탑재하여 온라인 강의 제작방식 및 구성에 대한 홍보를 진행했다. 2009년 12월 10일 이탈리아에서 개최된 UNPNI연례회의에서 온라인 교육프로그램 및 연구네트워크 시연을 진행하였다.

다. 대상국가와의 상호교류 협력

1) 상호교류협력(MOU) 체결 절차

온라인 교육훈련프로그램의 수강을 희망하는 대상 국가는 반드시 형사정책연구원(『사이버범죄 방지를 위한 가상포럼』사무국, 이하 사무국)과의 상호교류협력을 체결해야 한다. 대상 국가에서 체결 절차를 쉽게 이해할 수 있도록 간략한 순서를 정하였다.

① 사무국 측에서 대상국가의 해당기관에게 온라인 교육훈련프로그램의 목적과 주요대상, 강의 커리큘럼 등 강의에 대한 정보를 제공한다. 대상국가의 해당기관은 기관의 역할 및 주요기능 등 기관의 정보 및 온라인 교육 훈련프로그램을 담당할 부서와 담당자를 선정하여 사무국에 알려준다.

② 대상국가의 담당자는 해당기관의 인터넷 환경 등 온라인 강의 시청을 위한 제반 환경에 대한 정보를 제공한다. 또한, 사무국에서 준비한 상호교류협력 내용을 검토하여 수정사항이 발생할 시 상호의견을 조율하여 수정 및 보완한다.

③ 상호 동의하에 완성된 상호교류협력 문서는 기관장의 서명 후 각 1부씩 보관한다. 이후 대상국가의 담당자는 온라인 교육훈련프로그램 수강생들의 이력서(Curriculum Vitae)를 사무국에 제공한다.

④ 본격적인 온라인 강의시행에 앞서, 사무국은 대상국가 담당자에게 시범테스트를 할 수 있는 시범용 ID와 비밀번호를 발급하여 해당국가에서 온라인 강의가 제대로 수강이 가능한지 미리 확인한다.

⑤ 대상국가의 담당자는 강의 수강 완료 후, 수강생들의 의견을 수렴하여 사무국에 제출한다.

2009년 7월 30일 중국 베이징에서 개최한 한·중 국제학술회의에서 중국 사법부 예방범죄연구소와 사이버범죄방지 가상포럼에 관한 상호교류협력을 체결했다. 9월부터 말레이시아, 인도네시아, 태국, 필리핀과 상호교류협력체결 준비를 진행하여, 11월 16일 말레이시아 사이버시큐리티 말레이시아, 12월 8일 인도네시아 법무·인권부 국가입법기구, 12월 18일 필리핀 초국가범죄대응특사청과 온라인 강의 프로그램 시행을 위한 상호교류협력 각각 체결했다.

4. 연구네트워크

가. 연구네트워크 정보 업데이트

연구네트워크의 데이터베이스를 지속적으로 관리하고 관련 정보를 업데이트

하였다. 홈페이지 콘텐츠를 전문적으로 담당할 모더레이터를 고용하여, 연구네트워크의 구성항목인 사이버범죄의 최근동향 및 새소식, 사이버범죄 통계, 사이버범죄 전문가 및 관련저서, 사이버범죄 전문기관, 사이버범죄 대응을 위한 주요 국가들의 법률안 및 세미나 정보를 정기적으로 색인한 후 업데이트 하였다.[11]

나. 연구네트워크 보안점검

연구네트워크의 보안점검 방안은 지속적으로 기획 및 시행되었다. 자문위원단에게 초청장을 보내어 자문위원들이 연구네트워크에 가입하고 그들의 정보를 확인하게 한 후 2009년 6월 연구네트워크를 자문위원들에게만 시범 공개하였다. 시범 공개 이후 자문위원들의 의견을 반영하여 사이버범죄 방지 가상포럼 홈페이지의 내용 및 구성을 일부 수정하였다. 또한, 보안점검 전문 업체에 의뢰하여 연구네트워크 홈페이지의 보안테스트 및 웹 기능, 데이터베이스 등을 점검하였다.[12]

다. 연구네트워크 공식 개설

2009년 10월 16일 사이버범죄 방지를 위한 가상포럼 구축사업의 일환인 연구네트워크를 공식 개설하였다. 연구네트워크는 국제전문가자문단(ICG)과 홈페이지 구성 및 관리에 대하여 논의하였고, 이들에게만 제한적으로 시범공개를 하여 보완 및 개선 작업을 진행하였다. 연구네트워크는 사이버범죄 분야의 전문가들 뿐 아니라 일반인들이 정보를 공유하고 사이버범죄 현안에 대한 논의를 할 수 있는 토론의 장을 구축하는 데에 목적이 있다.[13]

라. 연구네트워크 홍보

2009년 10월 16일 연구 네트워크의 공식 오픈 후, 사이버범죄 분야의 학계 및 실무계 전문가 1000명에게 초청장을 발송하여 전문가로 활동할 수 있도록 하였다. 홈페이지 홍보를 위해 국내 인터넷 포털 사이트인 네이버, 야후, 구글 검색엔진에

---

11) 장준오 외 2인, 국제범죄방지를 위한 유엔·국제협력 및 연구, 2010, 70-72쪽.
12) 장준오 외 2인, 국제범죄방지를 위한 유엔·국제협력 및 연구, 2010, 70-72쪽.
13) 장준오 외 2인, 국제범죄방지를 위한 유엔·국제협력 및 연구, 2010, 70-72쪽.

'cybercrimeforum'으로 등록하였다. 또한, 적극적인 국내외 사이버전문가들의 참여 유도를 위해 e-journal에 홍보 광고 게재 및 배너광고를 통한 홍보를 추진하였다.[14]

제2절 운영 단계 : 2010년-2013년

1. 온라인 교육·훈련 프로그램

가. 온라인 교육·훈련 프로그램 공식 개설[15]

2009년 개발업체 공개입찰을 통해 선정된 성균관대학교와 지속적으로 강의를 제작했다. 2010년에 추가적으로 강사 체결한 강사들이 제공한 강의 및 제작 완료된 강의에 대한 교정 및 검토과정이 수행되었다. 또한, 연구원내에서 시행한 시범 테스트결과를 토대로 수정 및 보완과정을 거쳐 2010년 8월 2일 『사이버범죄방지 가상포럼』의 온라인 교육·훈련 프로그램을 공식 개설했다. 본 사업에 500,000달러 상당의 지원금 및 기술적 지원을 제공한 NHN측과 사이버범죄방지 가상포럼 온라인 교육·훈련 프로그램의 국내강사로 활동한 대검찰청, 경찰청, 경찰 대학교 등 사이버범죄 실무계 및 학계 관계자와 강의를 제작한 성균관대학교 측 등이 참석하였다.

1) 대상국가와 상호교류협력 체결

초창기에는 사이버범죄방지 가상포럼 온라인 교육훈련 프로그램 시행 대상국을 아시아 지역의 개발도상국들로 제한하였다. 그러나 전 세계적으로 사이버범죄방지 및 통제를 위해 더 많은 기관의 참여를 도모하고자 그 대상국을 아프리카 및 남아메리카 지역의 개발도상국으로 확대하였다.

〈표 2-1〉 2010-2011 년도 상호교류협력 체결 국가

	국가	기관	체결일
1	태국	법무부	
2	탄자니아	대검찰청	2011.04
3	에티오피아	법무부	2011.05
4	대한민국	국가기관	2011.06
5	태국	대검찰청	2011.07

14) 장준오 외 2인, 국제범죄방지를 위한 유엔·국제협력 및 연구, 2010, 70-72쪽.
15) 장준오 외 2인, 국제범죄방지를 위한 유엔·국제협력 및 연구, 2010, 70-72쪽.

2) 강의수강 진행절차

상호교류협력 체결 이후 곧바로 이어지는 강의수강을 위한 진행절차는 다음과 같이 마련되었다.

① 수강생들의 이력서를 토대로 입문과정 또는 고급과정 등의 코스 레벨을 지정한다. 사무국은 Student Selection Committee를 구성하여 수강 대상자의 수준에 맞는 강의에 배정하는 분류작업을 진행한다.

② 수강생들이 직접 온라인 교육 훈련프로그램에 접속할 수 있도록 개인용 ID, 비밀번호와 수강생용 매뉴얼을 제공한다. 이를 토대로 사무국의 LMS(Learning Management System) 관리자는 수강생들의 강의진행정도를 관리 및 감독할 수 있다. 진도가 뒤쳐진 경우, 경고 메시지를 발송하여 수강생들이 적극적으로 수업을 들을 수 있도록 유도한다.

③ 수강생들은 강의별로 제공된 퀴즈를 풀고 그 결과를 LMS 관리자에게 통보하여 다음 단계의 강의를 수강하도록 하는 등 수강생과 사무국간의 원활한 소통이 이뤄질 수 있도록 한다.

④ 입문과정, 고급 및 세미나 과정을 마친 수강자들에게 수료증을 수여한다.

3) 수강생 현황[16)]

2010년 8월 사이버범죄방지 가상포럼 온라인 교육훈련 프로그램을 공식 개통한 이래, 아시아 국가 및 아프리카 국가와의 상호교류협력 양해각서 체결 이후 수강이 진행되었다.

〈표 2-2〉 온라인 교육훈련 프로그램 수강현황 (2010.8.~2012.11)

대상국가	시작일	수강생	강의 코스
아시아·아프리카·중미 경찰 등	2010.8.5	아시아·아프리카·중미 등 11개국의 사이버범죄수사 담당 경찰, 군인 등 21인	법무연수원: "사이버범죄의 도전"

16) 장준오, 이윤미, 유엔협력사업·국제교류협력사업, 한국형사정책연구원, 2011, 53-54쪽.

대상국가	시작일	수강생	강의 코스
탄자니아 검찰 및 경찰	2010.10.4	탄자니아 사이버범죄수사 담당 검사 및 경찰 12인	"사이버범죄의 이해" "한국의 사이버범죄 통제시스템"
방글라데시 대법관	2011.4.6	방글라데시 법관 11인	입문과정
필리핀 특사청	2010.9.16.	필리핀 사이버범죄대응 특사청 수사관 2인	입문과정
태국 법무부	2011.1.12	태국 법무부 검사8인	고급과정
		태국 법무부 검사 23인	입문과정
한국 국가기관	2011.6.13	수사관 30인	입문과정
에티오피아 법무부	2011.6.20	에티오피아 법무부 20인	입문과정
탄자니아 대검찰청	2011.10.24	탄자니아 대검찰청 22인	입문과정
태국 대검찰청	2012.5.18	태국 대검찰청 16인	입문과정
2010.8~		총 누적 수강생 165인	

4) 번역사업[17)]

사이버범죄방지 가상포럼 온라인 교육훈련 프로그램은 기본적으로 영어로 진행되었다. 그러나 대상국가 수강생들에게 모든 강의 내용을 자국 언어 자막으로 제공하기 위해 2011년부터 번역작업을 진행하였다. 온라인 교육훈련프로그램 시행을 위한 상호교류협력 양해각서를 체결한 대상국가 중 한국어, 태국어, 베트남어로 전체 110개 강의에 대한 번역 작업을 실시하였다. 한국어는 2010년 말 번역 업체 선정 및 계약체결이 완료되어 2011년 3월 번역작업이 마무리되었다. 이후 약 7개월에 걸쳐 한국형사정책연구원 영문 에디터 2인이 감수작업을 실시하였다. 태국어의 경우, 태국 주재 UNODC아태지역센터의 추천을 받아 현지 번역회사를 선정하여 번역작업을 실시하였다. 이후 태국 대검찰청 소속 검사의 번역 감수과정을 진행하였다. 베트남어는 베트남 경찰총국의 추천을 받아 현지 번역회사와 계약을 맺고 번역작업 및 검수과정이 진행되었다.

17) 장준오, 이윤미, 유엔협력사업·국제교류협력사업, 한국형사정책연구원, 2011, 53-54쪽.

5) 추가강의 제작[18)]

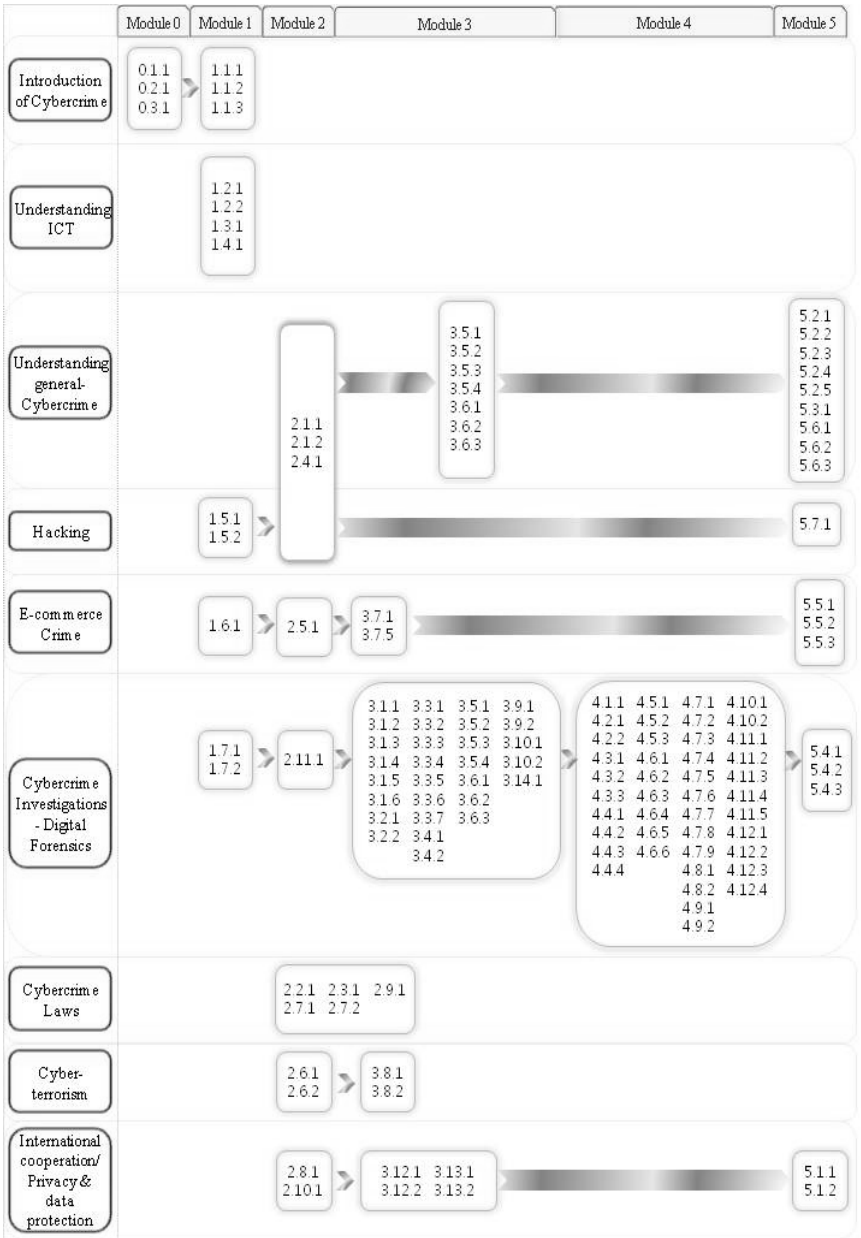
추가강의 제작을 위해 2010년도에 LG CNS소속의 이정아 강사, 서울 중앙지검 첨단범죄수사과의 조석영 검사, 홍콩 경찰청의 Frank Law강사와 추가적으로 강사 계약을 체결하였다. 2011년도에 추가로 제작된 강의 프로그램은 다음과 같다.

〈표 2-3〉 온라인 교육훈련 프로그램 추가 강의 제작 현황

강사	모듈	강의명
이정아	3-5-1	컴퓨터 바이러스: 범죄패턴 및 대응방안 Computer Viruses: Criminal patterns and countermeasures
	3-5-4	보트넷: 범죄패턴 및 대응방안 Botnet: Criminal Patterns and Countermeasures
조석영	5-7-2	경제적인 손해를 끼치는 스파이행위에 대한 조사 및 예방을 위한 훈련 Best Practices in Preventing and Investigating Economic Espionage
Frank Law	4-5-1	네트워크 분석: TCP/IP 및 그 외 프로토콜 등 1. Network Analysis: TCP/IP Protocol 2. Network Analysis: Other Protocols
	4-7-7	프린트 및 주변장치로부터의 증거복원 1. Recovering Evidence from Print and Spool Files 2. Understanding and Recovering Windows Restore Points
	4-8-2	메신저 프로그램 포렌식 1. AOL Instant Messenger Forensics 2. Yahoo and MSN Messenger Forensics

18) 장준오, 이윤미, 유엔협력사업·국제교류협력사업, 한국형사정책연구원, 2011, 55쪽.

6) Course Map [19)]



[그림 2-1] Course Map

19) 장준오, 이윤미, 유엔협력사업·국제교류협력사업, 한국형사정책연구원, 2011, 56쪽.

온라인 강의는 입문과정 모듈 0-1에서 모듈 2-11, 고급과정 모듈 3-1에서 모듈 4-12, 그리고 세미나과정 모듈 5-1에서 모듈 5-7까지 약 137개의 강의를 포함하고 있다. 수강생들의 강의 내용에 대한 이해도 및 각 모듈간의 연관성 이해도를 높이기 위해 강의간의 연관성을 도식화하는 작업이 진행되었다. 2009년도에 한 차례 Course Map 초안이 작성되었으나, 이후 강의 커리큘럼의 수정 및 보완작업으로 인해 Course Map 도 업데이트 되었다. 각 강의들은 총 9가지의 세부 주제에 따라 분류되어 있고, 그 주제들은 다음과 같다.

① Introduction of Cybercrime (사이버범죄의 소개)
② Understanding ICT (정보통신기술의 이해)
③ Understanding General Cybercrime (일반 사이버범죄의 이해)
④ Hacking (해킹)
⑤ E-commerce Crime (전자상거래 범죄)
⑥ Cybercrime Investigations: Digital Forensics (사이버범죄 조사기법: 디지털 포렌식)
⑦ Cybercrime Laws (사이버범죄 법률)
⑧ Cyber Terrorism (사이버 테러리즘)
⑨ International Cooperation/Privacy & Data Protection (국제협력/ 사생활 정보보호)

수강생들은 세부 주제에 따라 분류되어있는 Course Map을 따라 해당 강의들만 찾아서 수강할 수 있다. 이러한 서비스를 제공함으로써, 수강생들이 모든 강의 내용을 듣지 않고 모듈명만으로도 연관성 있는 강의 구조를 파악할 수 있게 하였다. 이러한 선택적인 수강을 통해 강의 수강의 효율성을 높이고자 하였다.

7) 온라인 강의 재검토 작업

정보통신기술의 급속한 발전과 변화에 따라 사이버범죄도 지능화 복잡화가 진행되면서 초기에 제작된 강의들은 기술적인 면에서 뒤쳐지고 시대에 부합하지 못했다. 사이버범죄방지 가상포럼 홈페이지 제작 초기 당시에는 존재하지 않았던 SNS (Social

Network Service) 및 스마트폰 등 등장으로 모바일 기기를 통한 제약이 존재하였다. 이에 따라 온라인 교육프로그램의 교육과정 중 시의적절하지 않거나 업데이트가 필요한 강의들을 선별하는 등 시대적 흐름에 맞게 수정 및 보완하기 위하여 사이버범죄 및 IT분야의 전문가들로 구성된 '사이버범죄방지 가상포럼 온라인 교육훈련 프로그램 강의 검토위원회'를 구성하였다. 교육훈련 프로그램 교육과정 커리큘럼 및 기 제작된 모든 강의들을 검토하는 작업을 의뢰하였다. 강의 검토 작업은 2011년 5월 2일부터 9월 30일까지 약 5개월 간 이루어졌으며 다양한 의견이 제시되었다.[20]

8) 사이버범죄방지 가상포럼관련 대외활동[21]

① 태국 법무부 및 대검찰청 방문

한국형사정책연구원은 2012년 3월 28일부터 31일까지 태국 법무부 및 대검찰청을 방문하였다. 동 방문을 통해 사이버범죄방지 가상포럼과정이 영문자막 뿐 아니라 태국어 자막으로도 접근이 가능해졌음을 알렸다. 태국 법무부 방문에서는 8명의 온라인 강의 프로그램 수료자들에게 수료증을 전달하였다. 태국 대검찰청 방문에서는 법무부의 사례를 설명하여 많은 수강생들의 수강을 권장하였다.

② 제21차 범죄방지 및 형사사법 위원회 참석

2012년 4월 23일부터 27일까지 오스트리아 비엔나에서 개최된 제21차 범죄방지 및 형사사법 위원회에 참석하였다. 회의 의제 7인 "제12차 범죄방지 및 형사사법 총회 후속조치 및 제 13차 범죄방지 및 형사사법 총회 준비(Follow-up to the Twelfth United Nations Congress on Crime Prevention and Criminal Justice and preparations for the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice)"[22]에 대한 논의자리에서 제12차 총회의 후속조치로 한국형사정책연구원이 사이버범죄와 관련하여 UNODC와 협력 하에 진행 중인 사이버범죄방지 가상포럼사업을 소개하였다.

---

20) 장준오, 이윤미, 유엔협력사업·국제교류협력사업, 한국형사정책연구원, 2011, 59쪽.
21) 김은경 외 9인, 2012유엔·국제협력사업 성과보고서, 한국형사정책연구원, 2012, 257쪽.
22) http://daccess-dds-ny.un.org/doc/UNDOC/GEN/V12/507/77/PDF/V1250777.pdf?OpenElement

나. 온라인 교육훈련 커리큘럼 및 진행현황[23)]

1) 온라인 교육훈련 커리큘럼

온라인 교육훈련 과정은 크게 입문과정과 고급과정으로 구성되었다. 총 130여개의 강의로 이루어진 입문과정은 모듈 0, 1, 모듈2로, 고급과정은 모듈3, 모듈4, 모듈5로 분류되었다.

입문과정은 전문적인 지식보다는 컴퓨터 관련지식을 필요로 하는 판사, 검사, 경찰 등과 같은 법집행 관련 공무원들을 위해 설계되었다. 컴퓨터 기술과 사이버범죄 동향에 초점을 둔 입문과정 모듈 1은 다시 총 7개의 모듈로 구성되었다. 사이버범죄 방지를 위한 법률 및 주요 선진국들의 정책에 초점을 맞춘 입문과정 모듈2는 총 11개의 모듈로 구성되었다.

사이버범죄 전문가를 위한 고급과정 중, 사이버범죄 수사 과정 및 기술을 다루고 있는 고급과정 모듈3은 총 14개의 모듈로, 디지털 포렌직 수사에 대한 내용을 다루고 있는 고급과정 모듈 4는 총 12개의 모듈로 구분된다. 전문가 과정의 특별과정으로 구성된 세미나 과정 모듈 5는 총 7개의 모듈로 구성되어 사이버범죄 관련 연구자와 실무가들이 현안엔 대한 논의를 할 수 있도록 구성되었다.

2) 온라인 교육훈련 진행 현황

사이버범죄방지 가상포럼 온라인 교육훈련 프로그램의 자료는 UNODC가 운영하는 시범 프로그램의 일부로 교육내용을 강화하기 위한 추가 자료로 사용되었다. 시범 프로그램은 온라인 사이버범죄 교육훈련 프로그램과 오프라인 프로그램이 혼합된 형식으로 개발도상국의 역량강화를 위한 프로그램의 효과성 평가를 위해 케냐에서 시행되었다. 그러나 오프라인 워크숍과 병행되는 온라인 교육훈련 프로그램의 효율성에 대한 피드백을 받기 위해 운영되었던 시범프로그램은 시행 과정에서 발생한 어려움으로 제 기능을 다하지 못했다. 2013년 3월 말부터 사이버범죄방지 가상포럼웹페이지 개편을 위해 온라인 교육훈련 프로그램은 일시 중단되었다.

---

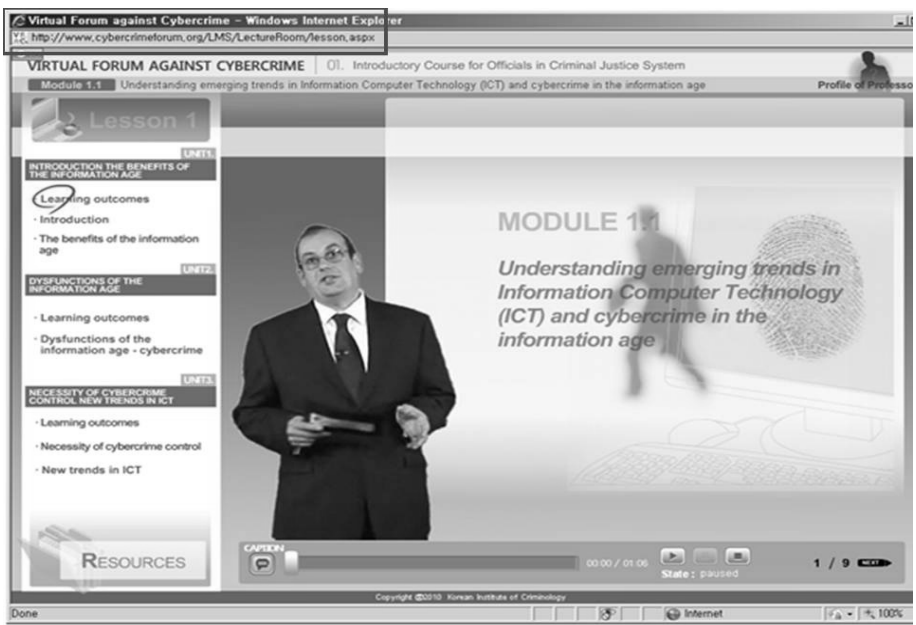
23) 장준오 외 8인, 2013UN·국제협력사업 성과보고서, 한국형사정책연구원, 2013, 114쪽.

2. 연구네트워크

연구네트워크의 기능은 사이버범죄의 최신 동향 및 통계, 사이버범죄 전문가 및 관련 저서, 사이버범죄 전문 연구기관, 사이버범죄 대응을 위한 주요 국가들의 법률안 및 관련 세미나에 대한 정보를 제공하는 클리어링 하우스(clearinghouse)와 전 세계의 학자, 법집행 형사사법 공무원 및 산업 전문가들을 연결하는 지식 네트워크(knowledge network)등 두 가지의 역할을 담당하는 것이다. 연구네트워크는 온라인 교육훈련 프로그램의 교육과정에서 제공하는 자료를 보완하기 위한 추가 자료를 제공한다.

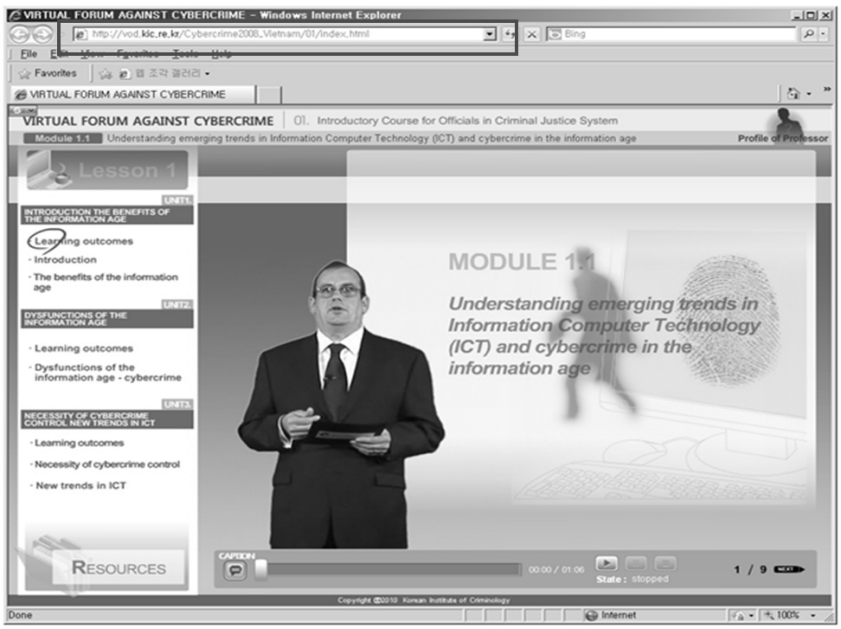
가. 2010년 연구네트워크 보안강화 및 업그레이드 작업

사이버범죄방지 가상포럼웹 사이트는 공식오픈 이후 최적화된 인터넷 환경과 콘텐츠 보안 등의 기술적인 보완점들이 나타났다. 따라서 웹 사이트의 안정 유지를 위해 보수작업이 시행되었다.



[그림 2-2] URL 노출

1) **동영상 페이지 URL 주소 노출 보완** : URL 주소의 노출은 보안상의 심각한 문제를 초래하기 때문에 웹 페이지상의 URL주소가 직접적으로 노출되는 문제를 보완하였다.



[그림 2-3] URL 노출보완

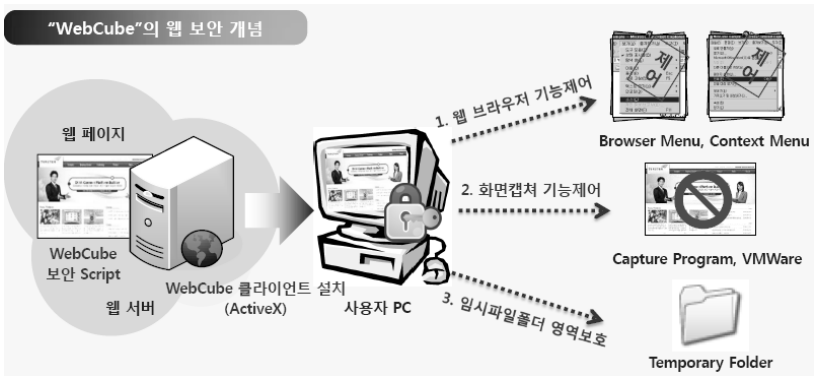
2) **사용자 계정 그룹화** : 사이버범죄방지 가상포럼 웹 사이트의 사용자 로그인 계정을 그룹화 하여 시스템 접근의 차별화 및 유지의 편리성을 향상시켰다. 사이버범죄방지 가상포럼 관계자 (Moderator 포함) 및 개발자 전용계정은 연구네트워크, 온라인 교육훈련프로그램 및 관리자 페이지 전체에 대한 접근을 가능하도록 하였다. LMS(온라인 교육훈련프로그램)관리자 계정은 관리자 계정은 관리자 화면 중 온라인 교육훈련 프로그램 관련 부분 접근만 허용하였다. 학생(Student) 전용 계정은 오직 온라인 교육훈련프로그램 페이지만 접근이 가능하도록 제한하였다. 전문가(Experts)계정은 연구네트워크 메뉴접근만 가능하였으나, 모든 메뉴에 '글쓰기'기능을 추가할 계획을 세웠다.

3) **다중 로그인 방지** : 초기 개발된 시스템에서는 같은 ID로 접속이 허용되었으나, 다중 로그인을 금지하였다. 하나의 ID로 중복 로그인이 되었을 때 시스템은

로그인 ID와 세션 ID를 동시에 체크하여 먼저 접속자를 강제 로그아웃 시켰다. 강제로그아웃 팝업 메시지를 통해 사용자에게 ID 도용에 대해 알려서 중복사용 방지를 예방하였다.

[그림 2-4] 팝업메세지

4) **동영상 보안 솔루션(캡쳐방지)설치** : 웹 브라우저의 동영상 강의는 강의 콘텐츠의 불법 복제, 정보의 유출 및 도용 등 정보보안에 대한 보호장치가 없는 심각한



[그림 2-5] "WebCube"의 웹 보안개념

무제가 야기되었다. 이러한 정보보안 문제 해결을 위해 디지털 콘텐츠 보안 전문업체인 ㈜ Teruten '테르텐'으로부터 웹 보안 솔루션인 "WebCube"를 구매하여 정보 유출을 차단하고자 하였다.

WebCube 프로그램이 설치된 상태에서 웹 페이지 화면을 캡쳐 했을 때는 다음과 같이 화면 캡쳐가 차단되었다.

[그림 2-6] 화면 캡쳐 차단 메시지

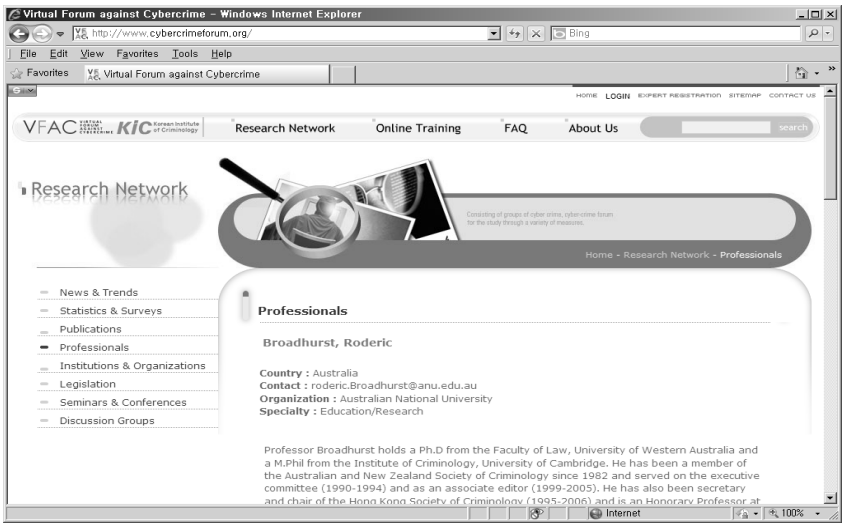
[그림 2-7] 로그인을 알리는 메세지

5) **웹 브라우저 호환성** : 사이버범죄방지 가상포럼 웹 사이트는 인터넷 익스플로러를 기반으로 개발되었다. 그러나 전 세계의 사용자들의 웹 브라우저 환경에 적합하지 않으며 시스템 사용 장애를 일으키는 문제점을 초래하였다. 각 사용자의 웹 브라우저 환경에 적합한 웹 사이트를 제공하기 위해 웹 브라우저 호환성 최적화 작업이 요구되었다. 프로그램 상에서 웹 브라우저 종류를 구분하여 각 웹 브라우저 별로 브라우저 특성에 맞는 프로그래밍 작업이 요구되었다.

6) **강의 목록 보안강화** : 초기에는 강의 수강 메뉴에서 비 로그인상태에서도 전체 강의 목록 정보 열람이 가능하였다. 그러나 강의 정보의 보안을 위해 로그인 한 경우에만 강의 목록을 오픈할 수 있도록 하였다.

7) **연구네트워크 Professionals 페이지 수정** : 기존의 전문가(Professionals)소개 페이지에 전문가들의 국가(Country), 연락처(Contact), 소속기관(Organization),

전문분야(Speciality)등을 추가하였다.



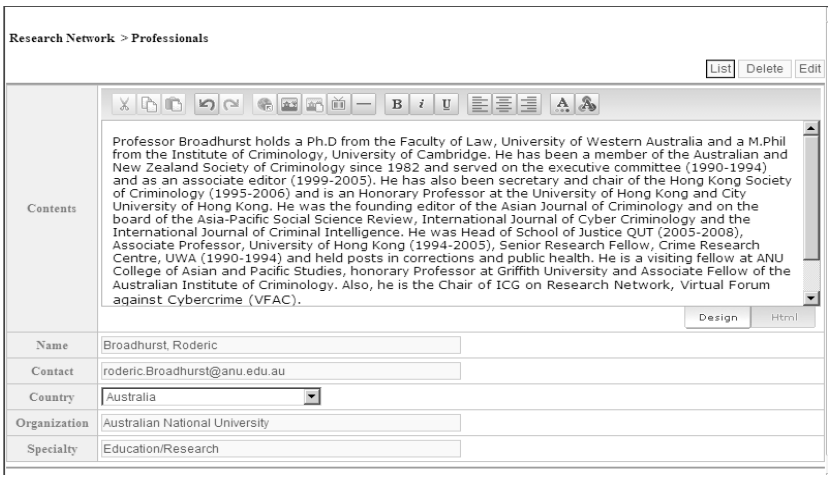
[그림 2-8] 전문가 소개 페이지

위 그림의 표에서 전문가들의 이름, 국가, 전문분야, 소속기관을 클릭했을 시 해당 칸에 대해 자동 정렬되었다.

No	Name	Country	Specialty	Organization
1	Bloss, William P.	United States	Education/Research	East Carolina University
2	Brenner, Susan W.	United States	Criminal Law, Cybercrimes	University of Dayton School of Law
3	Broadhurst, Roderic	Australia	Education/Research	Australian National University
4	Butterfield, Liz	New Zealand	Education	Hector's World Limited (HWL)

[그림 2-9] 수정된 "Professionals"페이지

또한, 관리자 페이지에서 전문가 등록 페이지에도 소속기관 및 전문분야를 추가하여 전문가들의 전문분야를 분류화 하였다.

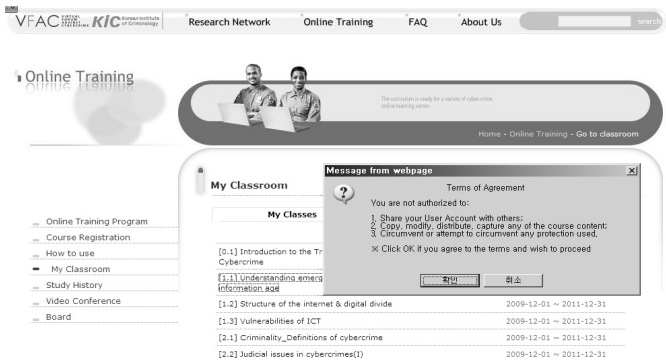


[그림 2-10] 전문가 전문분야 상세설명 페이지

8) **검색기능 오류 수정** : 연구네트워크 서브 메뉴에서 기존에는 제목으로만 검색이 가능하였으나 날짜, 본문, 제목과 본문, 제목과 날짜 등으로도 검색이 가능하도록 수정하였다.

[그림 2-11] 연구네트워크의 검색기능

9) **'Terms of Agreement' 메시지 추가** : ID도용 및 중복사용, 강의 콘텐츠의 보안 유지를 위한 'Terms of Agreement'를 강의실에 삽입하였다. 이는 한국형사정책연구원의 동영상 강의 및 강의정보 콘텐츠의 저작권 보호를 위한 동의이며, 동의를 해야만 온라인 강의 수강이 정상적으로 이루어지도록 하였다.



[그림 2-12] "Terms of Agreement" 메시지

10) **시스템 백업** : 사이버범죄방지 가상포럼시스템의 안정적인 운영을 위해 백업(Back-up) 서버를 동시에 운영하였다. 그러나 실 서버와 백업서버 간의 동기화(Syncronization)가 맞지 않아 실서버 장애 발생 시 자동서보의 복구가 불가능해지는 문제점이 발생되었다. 이 문제점을 해결하기 위하여 두 서버간의 동기화를 맞췄으며, 실시간 백업 및 로컬 백업을 추가하여 원하는 날짜로의 백업이 가능하도록 하였다.

나. 2011년 연구네트워크 추진 현황

1) 최신정보 업데이트[24]

사이버범죄방지 가상포럼 연구네트워크에 포함되어 있는 사이버범죄 관련 자료들은 다음과 같으며, 최신의 정보들이 매일 주기로 업데이트 되었다.

- 컴퓨터 범죄(무단 접근, 자료 수정 및 절도, 스팸, 피싱)
- 온라인 사기, 신용도용, 사이버 스토킹, 아동 대상 성적 접근(child grooming), 아동포르노, 자금 세탁 등 인터넷 관련범죄
- 온라인 범죄조직 및 국제범죄조직
- 보트넷, 트로이젠 바이러스(Trojans), 스파이웨어와 같은 멜웨어(Malware)
- 보안사고 및 보안정보 공개

24) 장준오, 이윤미, 유엔협력사업·국제교류협력사업, 한국형사정책연구원, 2011, 61-69쪽.

- 사이버범죄에 대한 사법기관의 대응
- 사이버범죄를 규제하기 위한 노력
- 정보기술 보안 산업 연구 및 행사

① **형사정책 연구기관**(Crime Research Institutes)

'형사정책연구기관' 섹션에서는 사이버범죄 관련 정보의 제공 및 사이버범죄 연구기관에 대한 자세한 정보를 포함하였다.

② **사이버범죄 법률자료**(Cybercrime Law Resources)

'사이버범죄 법률자료' 섹션에서는 사이버범죄 관련 법률의 연구 및 정보를 제공하는 연구기관에 대한 자세한 정보를 포함하였다.

③ **포렌식 자료**(Forensic Resources)

'포렌식 자료'섹션에서는 디지털 포렌식 관련 자료의 출처 및 기관에 대한 자세한 내용을 포함하였다.

④ **인터넷 보안기관**(Internet Security Agencies)

'인터넷 보안기관'섹션에서는 관련 기관의 세부사항 및 인터넷 보안 정보의 출처를 포함하였다. 자료의 출처가 되는 사이트들은 컴퓨터 사고 또는 비상 대응팀과 같은 기술전문 분야를 중점으로 하거나 사이버범죄에 대한 사회의 인식 제로를 목표로 하고 있다.

⑤ **법률 및 입법** (Law and Legislations)

'법률 제정'섹션에서는 국가별 사이버범죄 및 컴퓨터 범죄 관련법과 법률제정에 대한 자세한 내용을 포함하였다.

⑥ **뉴스와 최신 동향**(News and Trends)

'뉴스와 최신 동향'섹션에서는 사이버범죄 및 컴퓨터 범죄관련 뉴스와 최신 동향에 관한 자세한 내용을 포함하였다. 연구 네트워크에서 '뉴스와 최신 동향'의 업데이트는 사이버범죄방지 가상포럼 웹 사이트의 이미지 향상에 매우 중요한 역할을 담당하였다. 정기적인 업데이트가 웹사이트에 대한 관심도를 표현하기 때문이다. 2011년 3월 이후, 약 500여건의 뉴스기사가 업데이트 되었다.

⑦ **경찰 수사센터** (Police and Investigation Centers)

'경찰 수사센터'섹션에서는 감시활동 및 수사관련 기관의 정보출처에 대한 자세한 내용을 포함하였다. 2011년 3월 말 경부터 최신 정보를 업데이트하기 위한 집중적인 작업이 진행되었다.

⑧ **전문가**(Professionals)

'전문가'섹션에서는 사이버범죄분야의 전문가 및 학자들에 대한 자세한 정보를 포함하였다. 2011년부터 사이버범죄 전문가 그룹의 업데이트를 위한 집중적인 노력이 진행된 결과 1년 사이에 등록된 전문가의 수가 두 배로 증가하였다.

⑨ **출판물/ 서적**(Publications/Books)

'출판물/서적'섹션에서는 사이버범죄 분야의 도서들을 포함하였다. 2011년 4월 말 경부터 집중적으로 출판물 자료들이 업데이트 되었다.

⑩ **출판물/정기간행물**(Journals)

'출판물/정기간행물'섹션에서는 전문가 그룹에 포함되어 있는 전문가들의 학술지 및 정기간행물 위주의 자료들이 포함되었다.

⑪ **출판물/연구논문**(Research and Papers)

'출판물/연구논문'섹션에서는 전문가 그룹의 전문가들의 정기간행물을 위주로 사이버범죄 관련 연구논문이 포함되었다.

⑫ **세미나와 회의**(Seminars and Conferences)

'세미나와 회의'섹션에서는 사이버범죄와 관련된 행사정보를 포함하였다. 행사는 주기적으로 업데이트 되었다.

⑬ **통계** (Statistics)

'통계'섹션에서는 국가별 사이버범죄와 관련된 통계정보들을 포함하였다. 등록된 통계자료의 수는 각 구가별 통계 자료 발표에 따라 변동이 있었으며, 일부는 자동 업데이트되었다.

2) 지식 네트워크 (Knowledge Network)[25)]

사이버범죄방지 가상포럼 연구네트워크 내에서 지식 네트워크는 전문가(experts), 실무자(practitioners), 산업 회원(industry members), 외부 산업 관계자(external industry acquaintances)의 4개 그룹으로 구성되었다.

3) 자문단 권고안에 따른 조치[26)]

2011년 3월 4일 호주 국립대학교의 로데릭 브로드허스트 교수가 사이버범죄방지 가상포럼 연구 네트워크에 대한 자문 보고서를 제출하였다. 자문위원의 열 가지 권고안에 따라 조치가 진행 되었다.

① 메일링 리스트 작성
② 뉴스 및 최신동향 섹션의 정기적인 업데이트
③ 통계 및 조사섹션의 정기적인 업데이트
④ 사이버범죄 분야 전문가, 학자 및 실무자에게 사이버범죄방지 가상포럼 회원 가입을 위한 초대장 발송
⑤ 신간 및 법률제정의 정기적인 업데이트
⑥ 세미나 및 컨퍼런스 부문에 '논문 모집'섹션 추가
⑦ 토론 그룹 장려
⑧ 사이버범죄방지 가상포럼웹 사이트 등록 회원수 및 방문자 표시
⑨ 모든 하이퍼링크 점검
⑩ 사이버범죄방지 가상포럼 웹사이트 홍보를 위한 UNODC 및 유럽위원회 등의 국제기구와 연계

다. 2011년도 연구 네트워크 개선 현황[27)]

1) 세계적 사이버범죄 입법 검토

2011년도 3분기에는 연구네트워크 클리어링 하우스(Research Network Clearing

25) 장준오, 이윤미, 유엔협력사업·국제교류협력사업, 한국형사정책연구원, 2011, 70쪽.
26) 장준오, 이윤미, 유엔협력사업·국제교류협력사업, 한국형사정책연구원, 2011, 71쪽.
27) 장준오, 이윤미, 유엔협력사업·국제교류협력사업, 한국형사정책연구원, 2011, 73쪽.

house)의 법률제정 콘텐츠 수집을 위한 작업이 시행되었다. 전 세계의 사이버범죄 및 컴퓨터범죄 관련 법률제정 파악을 위해 244개 국가를 대상으로 연구조사를 실시하였다. 현지 법 집행기관과 접촉하여 사이버범죄방지 가상포럼을 소개하였으며 노력의 결과로 114개국의 145개 입법을 보유하였다.

2) 사이버범죄방지 가상포럼 뉴스레터

2011년 6월 사이버범죄방지 가상포럼의 최신 정보와 사이버범죄의 정보를 포함한 사이버범죄방지 가상포럼 뉴스레터가 발간되었다. 사이버범죄방지 가상포럼 뉴스레터는 매월 주기로 제작되어 이동식 문서파일(PDF)포맷으로 제작되어 이메일로 발송되었다. PDF로 제작한 이유는 다양한 운영체제들과 장치들에서 읽힘과 동시에 다양한 포맷 설정과 하이퍼링크 연결이 가능하기 때문이다.

3) 웹2.0 및 소셜 네트워크 서비스(SNS)활용

웹 2.0은 본질적으로 상호적인 인터넷과 콘텐츠 참조의 기능과 최종 사용자들 간의 교환의 트레드를 나타낸다. 소셜 네트워크는 이러한 형태의 서비스를 이용하기 위한 가장 기초적인 노력이었다. 소셜 네트워크는 또한 사이버범죄방지 가상포럼콘텐츠의 홍보를 위하여 외부 블로그와 커뮤니티를 이용하기도 하였다. 외부 블로그 및 커뮤니티에 콘텐츠가 제출되면 검색엔진의 크로울 인덱스(crawled indexes)에서 웹페이지의 색인과 평가가 링크, 사이트 관련 용어들과 함께 증가하여 사이버범죄방지 가상포럼웹사이트의 인지도가 향상되었다.

소셜 네트워크의 인터넷을 통한 사람들 간의 접촉 및 교류와 기관 간의 정보교환을 이용하여 사이버범죄방지 가상포럼 웹사이트를 활성화 하였다. 소셜 네트워크 사이트의 콘텐츠는 검색 엔진들에 의하여 색인되며, 검색을 통한 사용자들의 접속 가능성을 증가시켰다. 뿐만 아니라, 소셜 네트워크 서비스의 이용은 네트워크 산업과의 또 다른 연결고리를 제공하였다. 이를 바탕으로 연구네트워크가 사이버범죄 관련 산업의 최근 동향 및 우려 사항들을 효과적으로 파악할 수 있도록 하였다.

4) 페이스북 계정 개설

사이버범죄방지 가상포럼 페이스북 계정에 회원들을 등록하여 정기적으로 게시물을 올렸다. 또한 사이버범죄 분야의 회원들 간의 관계강화를 위한 교류를 진행하였다.

5) 트위터 계정 개설

트위터 계정을 통해 정기적으로 최신 뉴스 및 동향에 관한 정보와 사이버범죄 가상포럼 관련 뉴스를 배포하였다. 또한, 트위터는 사이버범죄의 전쟁과 관련된 최신 뉴스, 행사, 최근 동향 및 견해들의 정보를 제공하였다.

[그림 2-13] 사이버범죄방지 가상포럼 페이스북

[그림 2-14] 사이버범죄방지 가상포럼 트위터

6) 호주 국립대학교와 공동 설문조사 진행

국제적으로 사이버범죄 대응 및 방지를 위한 연구 기관 조사 지원을 위해 호주

국립대학교 자료들을 제공하였다. 이 프로젝트는 사이버범죄의 정확한 자료수집의 목적을 가지고 있었다.

7) 사이버범죄방지 가상포럼 웹사이트 업그레이드

2011년도에는 초기에 제작된 사이버범죄방지 가상포럼 웹 사이트의 디자인 교체작업을 진행하였다. 사이버범죄방지 가상포럼 온라인 교육·훈련 프로그램에서 교육 관리자 편의성(manager-friendly)을 유지하면서, 최소한의 관리 인원으로 다수의 사용자들을 효율적으로 관리할 수 있는 시스템을 유지 및 보수하는데 중점을 두었다.

① 웹사이트 개편

2008년도에 제작 개발된 사이버범죄방지 가상포럼 웹사이트 디자인의 노후화로 인하여 2010년 12월부터 2011년 2월까지 약 2개월 동안 디자인 교체작업을 진행하였다. 기존의 사이버범죄방지 가상포럼 웹디자인 프레임은 유지하면서 메인 페이지의 대표 이미지와 콘텐츠 배치 등을 변경하였다. 또한, 메인화면에 연구네트워크(Research Network)와 온라인 교육훈련 (Online Training)콘텐츠들을 전면 배치시켜서 사이버범죄방지 가상포럼 웹사이트의 성격을 명확히 표현하였다.

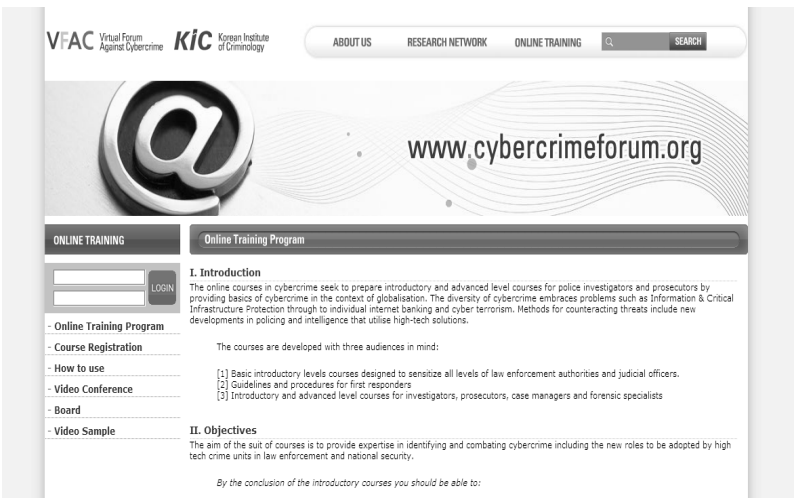
[그림 2-15] 변경 전 디자인

[그림 2-16] 변경 후 디자인

② 2011년도 유지보수 현황

ⅰ) 온라인 교육훈련 프로그램 화면의 로그인 기능 추가

온라인 강의 수강생들의 사용편의를 위하여 Online Training 섹션에 사용자들의 로그인 기능을 추가하였다.

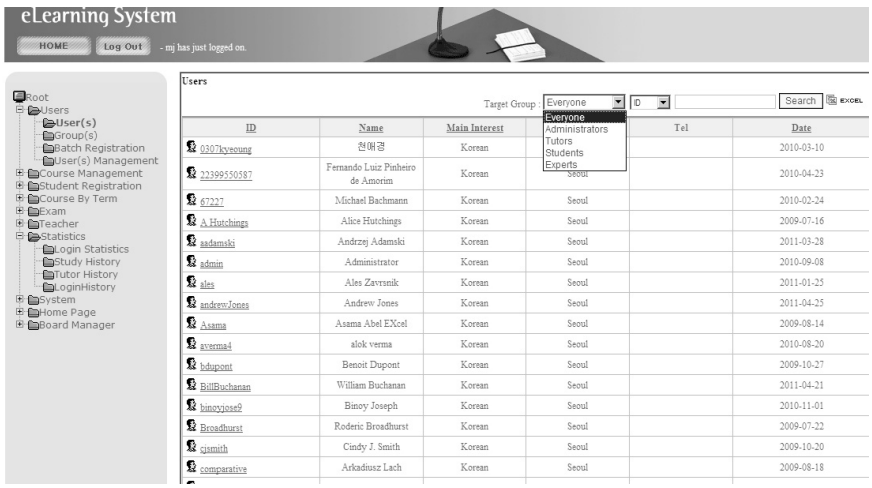


[그림 2-17] 온라인 강의 화면에 로그인 기능 추가

ii) 관리자 페이지 수정

사용자들의 로그인 기록을 아이디별 혹은 날짜별로 검색할 수 있는 사용자 검색 도구를 로그인 히스토리 메뉴에 보완하였다. 또한, 사용자 관리 메뉴에서 사용자 그룹별로 기본 정보를 검색할 수 있는 기능을 추가하여 시스템 관리자의 편의를 보완하였다.

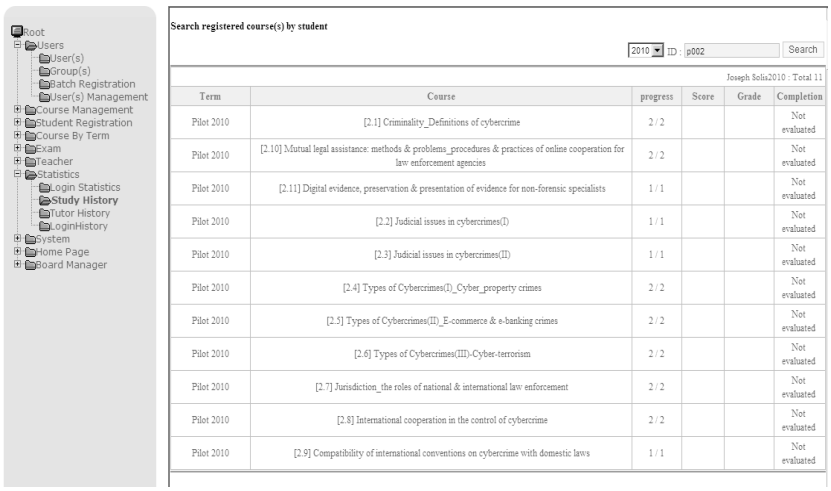
[그림 2-18] 로그인 통계메뉴-검색방법의 다양화



[그림 2-19] 사용자 관리 메뉴-사용자 그룹별 검색기능 추가

ⅲ) 교육 현황 통계 페이지 보완

수강생들의 교육 현황을 나타내는 Study History메뉴에서 학습 진척사항을 한눈에 볼 수 있도록 보완하여 프로그램 관리자에게 효율적인 수강생들의 학습 진행 현황을 제공하였다.



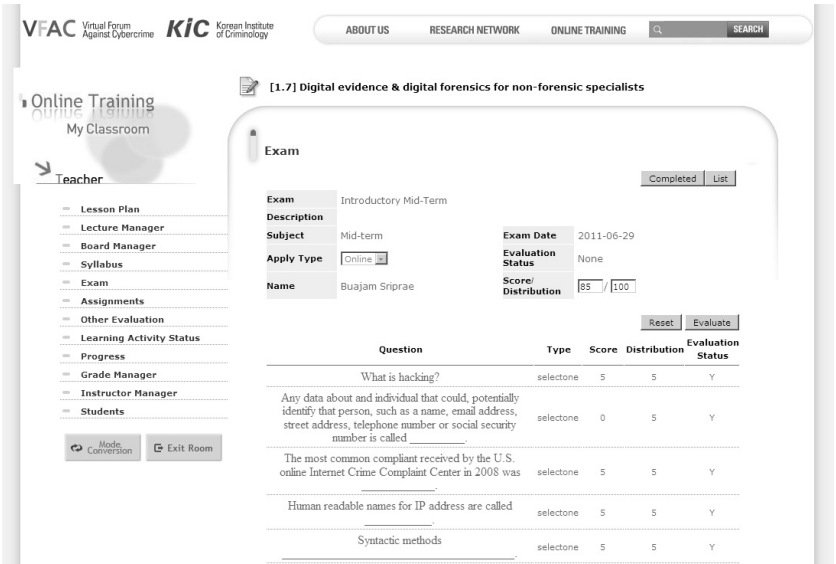
[그림 2-20] 교육현황 통계메뉴- 학습 진척 사항 Progress 항목이 반영

ⅳ) 검색기능 편의성 보완

사이버범죄방지 가상포럼 웹사이트에 있는 검색창에서 검색어 입력 후 검색 버튼 클릭까지 완료해야만 검색이 가능하고, 엔터키를 입력 시에는 메인 페이지나 검색 페이지로 이동되는 문제점을 수정하여 검색 편의성을 보완하였다.

ⅴ) 시험 점수기록 초기화 기능 추가

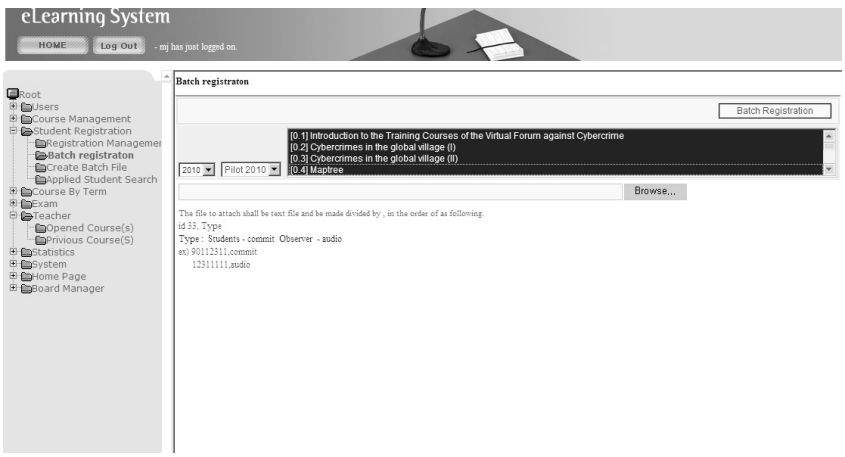
초기에는 수강생들의 중간 및 기말 시험 횟수를 1회씩으로 제한하였다. 그러나 수강생들의 낮은 학업 성취도와 성적이 좋지 않은 수강들의 요청 및 배려차원에서 시험 응시 기회를 무제한으로 제공하는 평가정책으로 변경하였다. 수강생들의 재시험을 위해 기존 점수기록을 관리자가 초기화 할 수 있는 시험점수 기록 삭제 리셋 기능을 추가하였다.



[그림 2-21] 수강생들의 시험 기록 초기화 기능 추가

vi) 다중강의 수강신청 방법 보완

기존에는 온라인 교육 프로그램 관리자가 특정 강의에 대하여 다수의 학생을 등록하는 수강신청 방법을 유지하였다. 그러나 이 방법은 많은 불편함을 야기 시켰다. 문제점의 보완을 위하여 Ctrl키를 누른 뒤 다수의 강의를 선택하면 동시에 다중 강의 수강신청이 가능하도록 일괄 다중강의 수강신청 기능을 보완하였다.



[그림 2-22] 일괄 다중강의 수강신청 기능 추가

vii) 검색 대상 콘텐츠 추가

기존의 사이버범죄방지 가상포럼 웹사이트 검색 시스템에서는 키워드 검색 시 News&Trends, Publications 그리고 Institution&Organizations 콘텐츠에서만 검색이 가능하였다. 그러나 Journals 및 Seminar&Conference에서도 검색이 가능하도록 검색 대상 콘텐츠를 추가하여 검색의 폭을 확대 시켰다.

viii) 관리자 페이지 정렬 및 편의 기능 추가

연구네트워크 관리자 페이지에서 관리자의 편을 위해 저자별, 주제별, 발행 연도별 정렬이 가능하도록 데이터 정렬 기능을 보완하였다. 또한 기존의 무질서한 콘텐츠를 테이블 칼럼으로 정리하여 관리자의 편의를 보완하였다.

Research Network > Publications > Research & Papers

No	Author	Subject	Year
1	Sameer HINDUJA, Justin W. PATCHIN	Offline Consequences of Online Victimization: School Violence and Delinquency	2007
2	Sameer HINDUJA, Justin W. PATCHIN	Cyberbullying: an exploratory analysis of factors related to offending and victimization	2008
3	Sameer HINDUJA	Neutralization theory and online software piracy: An empirical analysis	2007
4	Jason R. INGRAM, Sameer HINDUJA	Neutralizing music piracy: an empirical examination	2007
5	Sameer HINDUJA	Deindividuation and Internet Software Piracy	2008
6	Sameer HINDUJA, Jason R. INGRAM	Self-Control and Ethical Beliefs on the Social Learning of Intellectual Property Theft	2008
7	Sameer HINDUJA, Joseph A. SCHAFER	US cybercrime units on the world wide web	2009
8	Sameer HINDUJA, Jason R. INGRAM	Social learning theory and music piracy: the differential role of online and offline peer influences	2009
9	Janet J. Prichard and Laurie E. MacDonald	Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks	2004
10	T.J. McIntyre B.C.L., LL.M., B.L.,	Computer Crime in Ireland: A critical assessment of the substantive law	2005
11	Louise I. Shelley	Organized Crime, Terrorism and Cybercrime	2001
12	Rebecca GRANT	Victory in Cyberspace	2007
13	James A. LEWIS	Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats	2002
14	Amit YORAN	Virtual Threat, Real Terror: Cyberterrorism in the 21st Century	2004
15	Keith LOURDEAU	Virtual Threat, Real Terror: Cyberterrorism in the 21st Century	2004
16	Clay WILSON	Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress	2008
17	Clay WILSON	Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress	2003

[그림 2-23] 저자, 주제, 발행년도 별 정렬

ix) 파일 업로드 용량추가

연구네트워크 관리자 페이지에서의 자료 업로드는 용량크기 제한으로 대용량 자료의 업로드에 문제점이 발생하였다. 이러한 문제점의 해결을 위해 업로드 용량 제한을 무제한으로 상향 조정하였다.

x) 동영상보안 (캡쳐방지)솔루션 소프트웨어 업그레이드

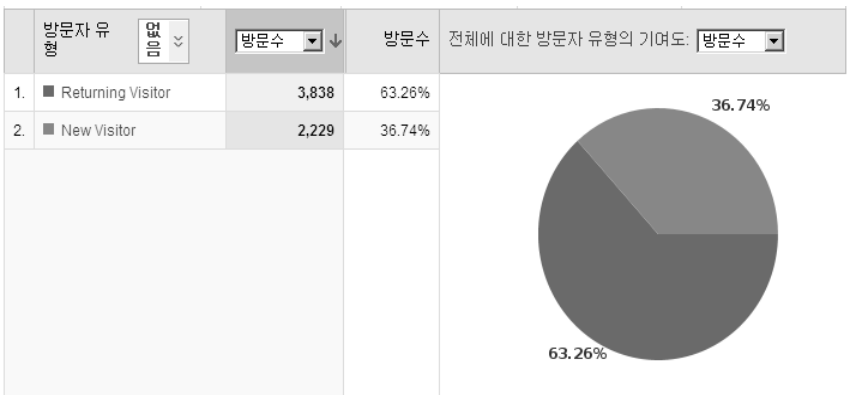
온라인강의 프로그램의 정보보안을 위해 설치하였던 'WebCube' 소프트웨어의 상위 버전 운영체제 및 웹 브라우저들이 출시됨에 따라 사용자들의 컴퓨터 사용환경 또한 상향되었다. 기존 사용자 컴퓨터 지원환경(Windows 2000, Windows XP,

Windows 2003)을 Windows Vista, Windows 7(32bit/64bit) 및 인터넷 익스플로러 9(Internet Explorer 9)버전 등으로 확대하기 위하여 보안 소프트웨어 WebCube 3.6.1.8버전에서 4.0.1.8버전으로 업그레드 하였다.

〈표 2-4〉 사용자컴퓨터 지원환경비교

	WebCube 3.6.1.8	WebCube 4.0.1.8
웹 브라우저(IE)	인터넷 익스플로러 8 이하	인터넷 익스플로러 9
운영체제	32bit 체제의 Windows 2000, Windows XP, Windows 2003	Windows 2000, Windows XP, Windows 2003, Windows Vista, Windows7(32bit/64bit)

xi) 방문자 분석: 2010년 10월부터 사이버범죄방지 가상포럼 웹사이트 접속자들을 분석하기 위하여 구글 웹로그 분석 솔루션을 통합하였다.



[그림 2-24] 사이버범죄방지 가상포럼 웹사이트 방문자의 신규방문과 재방문 비율

방문자 수, 방문자의 언어 및 분포, 신규 방문 및 재방문 비율, 페이지 뷰, 사이트에 머문 시간 등 방문자에 대한 데이터를 제공하였다. 또한, 방문자의 컴퓨터 환경(브라우저 및 운영체제)과 전체 트래픽 소스에 대한 분석 데이터를 제공하였다.

라. 2012년 연구네트워크 추진현황[28)]

2012년도에는 뉴스레터의 활성화를 위한 출판 소프트웨어 솔루션 교체와 디자인 개선 및 배포 확대를 위한 노력이 진행되었다.

1) 출판 소프트웨어 솔루션 교체

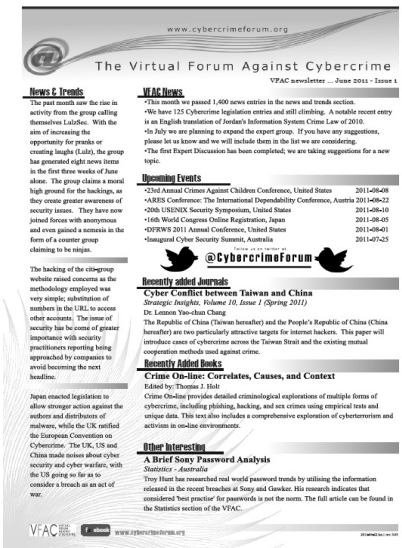
뉴스레터 제작을 위하여 기존에 사용되었던 Scribus를 마이크로 소프트 퍼블리셔로 교체하였다. Scribus는 윈도우 시스템에서 비효율적으로 작동하고 PDF로 변환할 경우 불일치 현상이 빈번하게 발생하였다. 마이크로소프트 솔루션은 뉴스레터를 위한 다양한 기능들을 갖추고 PDF변환 시에도 아무런 문제가 발생하지 않았다. 또한, 협동작업이 가능할 수 있는 기능을 제공함으로써 효율적인 뉴스레터 작성이 가능해지도록 하였다.

2) 디자인 개선

새로운 뉴스레터 디자인은 기존 사이버범죄방지 가상포럼로고의 4가지 색상인 빨강, 노랑, 파랑, 초록의 명암을 활용하여 선명함과 기능성을 강조 하였다. 뉴스레터 1면은 최근 현안 및 개최예정인 세미나에 대한 정보와 사이버범죄에 관한 다양한 정보를 소개하였다. 2면은 해당 월의 뉴스와 최신동향에 대한 소식을 담았다. 3면은 전문가들이 기고한 기사를 게재하였다. 각 섹션은 붉은색 경계선과 그래픽을 이용하여 뉴스와 동향으로 나누고, 나머지 기사는 초록, 파랑, 노랑으로 별도 표시하였다. 네 가지 색상을 사용한 뉴스레터의 디자인적 요소를 사이버범죄방지 가상포럼 웹 사이트와의 동일성, 전문성을 가미하기 위해 기타 미디어에도 사용하였다.

---

28) 김은경 외 9인, 2012유엔·국제협력사업 성과보고서, 한국형사정책연구원, 2012, 260쪽.


www.cybercrimeforum.org

The Virtual Forum Against Cybercrime

VFAC newsletter ... June 2011 - Issue 1

News & Trends

The past month saw the rise in activity from the group calling themselves LulzSec. With the aim of increasing the opportunity for pranks or creating laughs (Lulz), the group has generated eight news items in the first three weeks of June alone. The group claims a moral high ground for the hackings, as they create greater awareness of security issues. They have now joined forces with anonymous and even gained a nemesis in the form of a counter group claiming to be ninjas.

The hacking of the citi-group website raised concerns as the methodology employed was very simple; substitution of numbers in the URL to access other accounts. The issue of security has be come of greater importance with security practitioners reporting being approached by companies to avoid becoming the next headline.

Japan enacted legislation to allow stronger action against the authors and distributors of malware, while the UK ratified the European Convention on Cybercrime. The UK, US and China made noises about cyber security and cyber warfare, with the US going so far as to consider a breach as an act of war.

VFAC News

•This month we passed 1,400 news entries in the news and trends section.
•We have 125 Cybercrime legislation entries and still climbing. A notable recent entry is an English translation of Jordan's Information System Crime Law of 2010.
•In July we are planning to expand the expert group. If you have any suggestions, please let us know and we will include them in the list we are considering.
•The first Expert Discussion has been completed; we are taking suggestions for a new topic.

Upcoming Events

•23rd Annual Crimes Against Children Conference, United States 2011-08-08
•ARES Conference: The International Dependability Conference, Austria 2011-08-22
•20th USENIX Security Symposium, United States 2011-08-10
•16th World Congress Online Registration, Japan 2011-08-05
•DFRWS 2011 Annual Conference, United States 2011-08-01
•Inaugural Cyber Security Summit, Australia 2011-07-25

Follow us on twitter at @CybercrimeForum

Recently added Journals

Cyber Conflict between Taiwan and China
Strategic Insights, Volume 10, Issue 1 (Spring 2011)
Dr. Lennon Yao-chun Chang
The Republic of China (Taiwan hereafter) and the People's Republic of China (China hereafter) are two particularly attractive targets for internet hackers. This paper will introduce cases of cybercrime across the Taiwan Strait and the existing mutual cooperation methods used against crime.

Recently Added Books

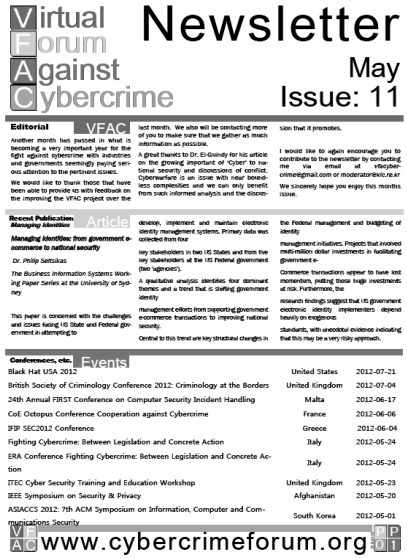
Crime On-line: Correlates, Causes, and Context
Edited by: Thomas J. Holt
Crime On-line provides detailed criminological explorations of multiple forms of cybercrime, including phishing, hacking, and sex crimes using empirical tests and unique data. This text also includes a comprehensive exploration of cyberterrorism and activism in on-line environments.

Other Interesting

A Brief Sony Password Analysis
Statistics - Australia
Troy Hunt has researched real world password trends by utilising the information released in the recent breaches at Sony and Gawker. His research indicates that considered 'best practise' for passwords is not the norm. The full article can be found in the Statistics section of the VFAC.

VFAC www.cybercrimeforum.org

〈2011 뉴스레터 레이아웃〉


Virtual Forum Against Cybercrime

Newsletter

May

Issue: 11

Editorial VFAC

Another month has passed in what is becoming a very important year for the fight against cybercrime with industries and governments seemingly paying serious attention to the pertinent issues.

We would like to thank those that have been able to provide us with feedback on the improving the VFAC project over the last month. We also will be contacting more of you to make sure that we gather as much information as possible.

A great thanks to Dr. El-Ghindy for his article on the growing important of 'Cyber' to national security and discussions of conflict. Cyberwarfare is an issue with near boundless complexities and we can only benefit from such informed analysis and the discussion that it promotes.

I would like to again encourage you to contribute to the newsletter by contacting me via email at vfacbercrime@gmail.com or moderator@vfac.re.kr

We sincerely hope you enjoy this months issue.

Recent Publication Article

Managing Identities: from government e-commerce to national security

Dr. Philip Sarlskas

The Business Information Systems Working Paper Series at the University of Sydney

This paper is concerned with the challenges and issues facing US State and Federal government in attempting to develop, implement and maintain electronic identity management systems. Primary data was collected from four key stakeholders in two US States and from five key stakeholders at the US Federal government (two agencies).

A qualitative analysis identifies four dominant themes and a trend that is shifting government identity management efforts from supporting government e-commerce transactions to improving national security.

Central to this trend are key structural changes in the Federal management and budgeting of identity management initiatives. Projects that involved multi-million dollar investments in facilitating government e-Commerce transactions appear to have lost momentum, putting those high investments at risk. Furthermore, the research findings suggest that US government electronic identity implementers depend heavily on exogenous standards, with anecdotal evidence indicating that this may be a very risky approach.

Conferences, etc. Events

Black Hat USA 2012	United States	2012-07-21
British Society of Criminology Conference 2012: Criminology at the Borders	United Kingdom	2012-07-04
24th Annual FIRST Conference on Computer Security Incident Handling	Malta	2012-06-17
CoE Octopus Conference Cooperation against Cybercrime	France	2012-06-06
IFIP SEC2012 Conference	Greece	2012-06-04
Fighting Cybercrime: Between Legislation and Concrete Action	Italy	2012-05-24
ERA Conference Fighting Cybercrime: Between Legislation and Concrete Action	Italy	2012-05-24
ITEC Cyber Security Training and Education Workshop	United Kingdom	2012-05-23
IEEE Symposium on Security & Privacy	Afghanistan	2012-05-20
ASIACCS 2012: 7th ACM Symposium on Information, Computer and Communications Security	South Korea	2012-05-01

VFAC www.cybercrimeforum.org

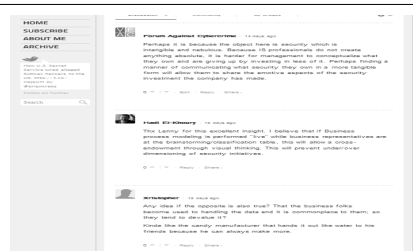
〈2012 뉴스레터 레이아웃〉

[그림 2-25] 사이버범죄방지 가상포럼 뉴스레터 레이아웃 변경 전후

〈트위터 페이지와 로고〉

〈페이스북 페이지와 로고〉

〈구글+페이지와 로고〉



〈써드 파티 사이트 아바타 로고〉

[그림 2-26] 사이버범죄방지 가상포럼관련 사이트

3) 뉴스레터 확대개편

2011년 발간당시 1-2페이지에 불과하였던 뉴스레터를 20페이지로 확대하였다. 2012년 구성된 CRU팀을 중심으로 뉴스레터를 통해 소개된 다양한 자료를 별도로 재편집하여 사이버범죄방지 가상포럼 Annual Report를 발간하였다.

마. 사이버범죄연구팀 (CRU)의 신설[29]

1) CRU 설치목적 및 역할

"Global Risks 2012"라는 주제로 개최된 2012년 세계경제포럼[30]에서 UNODC 사무총장은 사이버범죄의 심각한 문제점을 강조하고 사이버범죄 퇴치를 위한 국제협력을 촉구 하였다. 사이버범죄에 대한 국제적 흐름에 부합하기 위하여 한국형사정책연구원은 "Cybercrime Research Unit (이하 CRU)"를 공식 출범시켰다.

CRU는 국내외 사이버범죄에 대한 최신 동향파악, UNODC의 사이버범죄 연구 수행 및 형사정책연구원의 사이버범죄방지 가상포럼사업을 주관하는 역할이 주요임무였다. 또한, 국내 사이버범죄 연구를 선도적으로 수행하고 관련 정부기관 및 연구기관들과 적극적으로 협력하여 사이버범죄 형사정책에 대한 이론적 기틀을 마련하며, 사이버범죄 관련 정책 및 법제도 입원 지원을 목표로 삼았다.

2) CRU 구성

CRU 연구진은 한국형사정책연구원의 사이버범죄 관련 연구역량의 집대성을 위하여 사이버범죄 연구의 경험과 노하우를 갖춘 부연구위원급 연구원을 중심으로 구성되었다.

3) CRU 활동 및 역할

CRU의 활동은 크게 국내와 국외로 구분할 수 있다. 국내활동에서의 역할은 다시 사이버범죄 대응을 위한 유관기관의 카운터 파트너로서의 역할과 사이버범죄방지 가상포럼수행의 역할, 연구 역할로 구분 할 수 있다.

---

29) 김은경 외 9인, 2012유엔·국제협력사업 성과보고서, 한국형사정책연구원, 2012, 248-250쪽.

30) 세계경제포럼(WEF : World Economic Forum)은 전 세계의 저명한 기업인 · 경제학자 · 저널리스트 · 정치인 등이 모여 세계 경제에 대해 토론하고 연구하는 국제민간회의이다. 독립적 비영리재단 형태로 운영되며, 본부는 스위스 제네바에 위치한다. 세계경제포럼 공식홈페이지, http://www.weforum.org.

① 국내활동

ⅰ) 사이버범죄 대응을 위한 유관기관과의 협력

CRU는 사이버범죄 관련 실무기관들의 학문적인 지원 및 국제적 동향을 공급해주는 역할을 담당하였다. 대검찰청 사이버범죄 수사단, 경찰청 사이버테러 대응센터, 경찰대학 사이버범죄 연구센터 등과 구체적인 업무협조를 위한 실무자 회의를 개최하였다. 또한, 사이버범죄 수사단으로부터 사이버공간에서의 형사소송법에 대한 연구, 사이버테러 대응센터로부터 디지털 포렌식센터에 대한 연구프로젝트를 의뢰받기도 하였다.

ⅱ) 사이버범죄방지 가상포럼 사업수행

CRU는 사이버범죄방지 가상포럼을 주관하는 역할을 담당하였다. 사이버범죄방지 가상포럼의 효과적인 운영을 위하여 폐쇄적인 운영 시스템을 개방적으로 변환하고, 액티브X의 사용을 중지시켰다. 또한 일부 강의내용을 업데이트하여 실용적인 강의내용을 추가하였다. 사이버범죄방지 가상포럼 온라인 강의에 대한 전문가들의 의견을 수집하여 강의 커리큘럼을 개정하고 내용의 재편 작업을 수행하였다. 국내 사이버범죄 전문가들의 확충과 실질적인 연구가 가능할 수 있ㄷ록 경찰대학교 사이버범죄 연구센터와 정기적인 학술모임을 가졌다.

ⅲ) 연구활동

CRU의 연구활동은 크게 수탁과 수시연구 및 자체 스터디 모임으로 구분되었다. 특히, 수시연구로 진행된 한국의 사이버범죄에 대한 동향 및 정책, 논의내용 등을 소개하는 “Cybercrime in the Republic of Korea: Law and Policy on Cybercrime”은 2012년 4월 오스트리아 비엔나에서 개최된 제21차 CCPCJ 회의에서 해외 국가 및 연구기관에 배포되었다. 그밖에 사이버범죄방지 가상포럼 소개책자를 발간하고 사이버범죄방지 가상포럼 뉴스레터를 재편집하여 Annual Report를 출판하였다. CRU는 개인의 연구역량 강화, 해외의 사이버범죄 관련 법령 및 동향, 이론 등의 공유를 위하여 스터디 모임을 진행하였다.

② 국외활동

CRU의 국외활동은 주로 UN국제회의 참석 및 외국의 사이버범죄 대응지원으로 구분할 수 있다.

ⅰ) 제21차 범죄방지 및 형사사법 위원회 참석

UN국제회의에 참석하여 UN의 동향을 파악하고 우리나라 정부기관이 사이버범죄 관련 내용에 대하여 의견을 표명할 경우 이론적으로 지원해주는 역할을 하였다.

ⅱ) 필리핀 사이버범죄 관련 법률제정을 위한 워크숍 참석

테러리즘 및 관련 범죄 대응을 위한 효과적인 법적 구조 구축을 위한 국가적 노력의 일환으로, UNODC의 지원을 받아 필리핀 대테러 위원회(Philippine Anti-terrorism Council's Program Management Centre: ATC)가 주관한 전문가 워크숍에 참석하였다. CRU는 한국의 사이버테러 대응실태 및 형사사법적 대응 시스템에 대하여 발제를 하였다.

ⅲ) 제2회 국제 사이버범죄 연구세미나 참석

CRU팀은 경찰대학교 국제 사이버범죄 연구센터와 교류협력의 일환으로 2012년 11월 "Inside Online Child Exploitation (온라인 아동대상 범죄의 이해)"를 주제로 개최된 제2회 국제 사이버범죄 연구 세미나에 참석하였다. 동 세미나를 통해 아동음란물에 대응하는 선도국 최고의 전문가들의 강연을 듣고 온라인 아동 대상범죄의 심각성에 대한 공감대 형성 및 국제적 대응방안을 위한 논의를 하였다.

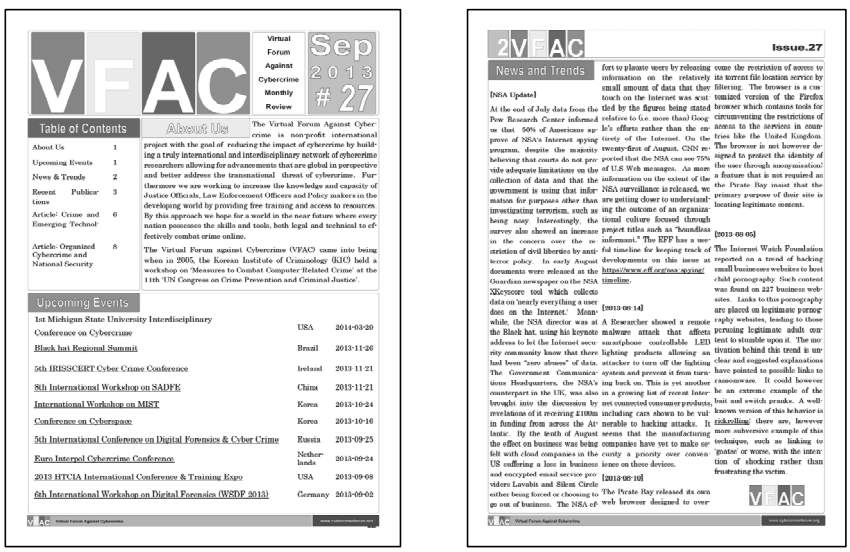
ⅳ) 사이버범죄 전문가 방문 및 세미나 개최

사이버범죄방지 가상포럼 프로젝트의 일환으로 영국 더햄 대학의 교수이자 사이버범죄방지 가상포럼 지식 네트워크 회원인 David Wall 교수가 한국형사정책연구원을 방문하여 강연을 하였으며 사이버범죄 관련 주제에 대한 세미나를 개최하였다. 동 세미나에는 CRU팀원들, 경찰대학교 사이버범죄 연구센터 회원 및 외부교수, 경찰청 사이버범죄 전문 수사관들이 참여하였다. 동 세미나를 통하여 한국형사정책연구원의 사이버범죄관련 연구에 대한 자문을 받을 수 있었다. 또한, 영국 더햄(Durham) 대학의 Wall 교수와 MOU체결을 논의하였다.

바. 2013년 연구네트워크 추진현황[31)]

1) 사이버범죄방지 가상포럼 리뷰

사이버범죄방지 가상포럼 리뷰 (이하 VFAC 리뷰)는 2011년 6월 '사이버범죄방지 가상포럼 뉴스레터'로 처음 제작되어 2013년 8월부터 리뷰 형식으로 제작되었다. 주요 내용은 사이버범죄의 동향 및 사이버범죄방지 가상포럼 웹사이트에 업데이트되는 정보들이며, 국내외 저명한 사이버범죄 전문가들의 글들이 매달 게재되었다. VFAC 리뷰는 지식 네트워크를 확대하고 사이버범죄방지 가상포럼에 대한 인지도를 향상시키는 역할을 수행하였다. 한국 형사정책연구원의 사이버범죄 관련 전문지식도 수록되었으며, 영문으로 제작되어 연구원의 국제적 홍보 및 연구역량 강화에 도움을 주었다. 리뷰는 매달 PDF문서의 형식으로 이메일 통해서 배포되었고, 9월부터는 두 달의 리뷰를 통합하여 'Bimonthly 리뷰'를 발행하였다.



[그림 2-27] VFAC리뷰 표지 및 내부 콘텐츠

31) 김지영 외 10인, UN·국제 교류협력 사업 보고서, 한국형사정책연구원, 2014, 184쪽.

2) 연구 네트워크 확대구축

지속적인 연구네트워크의 확대구축을 위하여 2013년 8월 캐나다 몬트리올대학교 국제범죄학센터 (International Center on Criminology)를 방문하였다. 방문을 통해 향후 한국형사정책연구원과의 공동연구 프로젝트와 국제협력 및 양해각서 체결을 위해 노력하기로 합의하였다. 또한, 2014년 1월 캐나다 정부 관리들과의 공동회의인 'SERENE 프로그램[32]'에서 형사정책연구원이 연구네트워크 구축을 위한 자문을 담당하고 VFAC리뷰를 매달 배포하기로 하였다.

제3절 지속 발전 단계 : 2014년-2015년

1. VFAC 리뷰[33]

2013년 9월부터 시작된 VFAC 리뷰는 격월로 제작되었다. 2개원 동안의 사이버범죄 관련 소식 및 동향을 정리하고 향후 개최될 사이버범죄 관련 컨퍼런스를 소개하였다. 또한 사이버범죄 관련 연구보고서 및 출판물을 발굴하여 수록하고자 노력하였다. 사이버범죄 전문가들과의 소통을 통해 그들의 연구보고서 및 논문을 채택하여 각 호에 게재하였다.

가. 2014년 VFAC 리뷰의 주요 내용

1) 2014년 VFAC 리뷰, 제3호 (1-2월)

① **일상활동이론[34]과 사이버범죄**(Routine Activity Theory and Cybercrime:

32) 캐나다의 사이버보안 위험에 관한 인식 제고 및 지식 공유를 통한 대응 능력을 강화하기 위한 스마트 사이버보안 네트워크.
〈http://www.serene-risc.ca/en/about-us/about-serene-risc〉

33) 김지영 외 10인, UN·국제 교류협력 사업 보고서, 한국형사정책연구원, 2014,187-195쪽.

34) 동기가 부여된 범법자, 적절한 표적, 보호 능력의 부재라는 조건이 동일한 시간과 공간에 주어질 때 범죄가 발생한다는 Lawrence Cohen과 Marcus Felson의 이론이다. 그리고 이와 같은 세 가지의 범죄유발요인이 동일한 시간과 공간에 나타나는 지의 여부는 개인의 일상적인 활동양상에 의존한다고 한다. 여기서 일상활동은 인간의 기본적인 욕구를 위하여 자주 행해지는 활동으로 정의되며, 생활 양식의 용어와 유사하게 일상활동은 공식적 작업, 여가, 의식주를 위한 행동, 사교적 욕구 및 성적 욕구 등을 위한 활동이 포함된다. 경찰학사전, 민수홍 외 공역, 2005, 73쪽.

What about Offender Resources)[35]에서는 범죄자가 범행에 활용한 자원(Offender Resources)에 따라 사이버범죄의 유형을 분류하였다. 범죄자가 범행에 활용한 자원이 일상활동이론 요소들과 독립적으로 작용하여 자원이 범죄자에게 내재된 경우, 해당 자원이 범죄 발생 전 과거의 행동으로 작용한 경우, 상호 작용하는 요소들이 서로 복잡한 체계를 이루어 작용하는 경우로 나누어 설명하였다. 또한 사회논리학적 갈등 모형 추가의 필요성도 제안하고 있다.

② **결점을 사이버안보정책에 포함시키지 않는 기업의 결점**(The Flaw of Not Including Flaws in Security Planning)[36]은 기업의 사이버안보정책 수립 시 유의해야 할 사항을 설명한다. 특히 안보 결점을 발견하였을 때 수용, 처리 및 대응할 수 있는 시스템을 마련해야 하고, 사이버 공격을 당한 경우 해당 공격에 대한 공식적인 입장 공개의 중요성을 강조하였다.

③ **지하드(Jihad)의 사이버 활동 및 범죄 형태에 관한 연구**(Middle East Dilemma from the Caliphate to Open-Source Jihad)[37]는 물리적 테러 활동 외에 온라인 상에서 범죄를 저지르는 사이버 지하드에 대해 소개하고 경고한다. 사이버 공간에서는 지하드의 전술이 변화되어 오픈소스[38] 지하드가 증가할 것이라 예측된다. 또한 활동 기금 마련을 위해 가상통화 범죄, 신용카드 정보 도용 등의 범죄가 발생할 수 있음을 경고한다.

2) 2014년 VFAC 리뷰, 제4호 (3-4월)

① **사이버범죄 피해자 통계 연구보고서**(Experiences with Online Deviant and Illegal Activities: Findings from a University Campus)[39]는 미국 사우스 플로리다 대학교(University of South Florida Sarasota-Manatee)를 포함한 동남부 지역 대학

35) VFAC 리뷰 제 3호, 20-22쪽.
36) VFAC 리뷰 제3호, 23-27쪽.
37) VFAC 리뷰 제3호, 28-32쪽.
38) 오픈소스 소프트웨어(OpenSource Software)를 일컫는다. 소프트웨어의 설계도에 해당하는 소스코드를 인터넷 등을 통하여 무상으로 공개하여 누구나 그 소프트웨어를 개량하고, 이것을 재배포할 수 있도록 하는 소스코드 또는 소프트웨어를 말한다. 두산백과, http://www.doopedia.co.kr/doopedia/master/master.do?_method=view&MAS_IDX=101013000799797
39) VFAC 리뷰 제4호, 23-29쪽.

생들을 대상으로한 사이버범죄 피해 통계를 제공한다. 성별, 연령, 인종에 따라 사이버범죄의 피해자가 될 가능성과 피해 실태를 수치화하였다.

② **사이버범죄 척결을 위한 국제협력 동향과 전망**(International Trends and the Prospect for Measures to Combat Cybercrime)[40]은 초국가적인 성격을 지니는 사이버범죄의 척결을 위해서는 국제협력을 통한 대응이 필수적임을 강조한다. 현존 부다페스트 협약(Budapest Convention on Cybercrime)[41]으로는 한계가 있음을 지적한다.

③ **하트블리드(Heartbleed)의 위험성과 대응방안**(Is This the Start of a Bleeding Hearts Club?)[42]에서는 하트블리드의 개념과 위험성, 대응방안을 설명한다. 하트블리드는 웹 서버와 클라이언트 사이의 신호 길이를 조작하여 개인 정보 등 필요 이상의 정보를 탈취하는 버그다. 이는 오픈소스에서 처음 발견되었다. 하트블리드의 대안으로 제시할 수 있는 방법은 오픈소스 개발 시 결점을 보완하고 지속적인 업데이트를 실시하는 것이다. 이 과정에서 보안전문가와 웹서버 관리자 간의 긴밀한 협력을 통한 문제 해결이 필수적임을 이야기하고 있다.

3) 2014년 VFAC 리뷰, 제5호 (5-6월)

① 망 중립성(Net Neutrality)과 망 프라이버시(Net Privacy)유지방안(Criminal Policy on Net Neutrality and Net Privacy)[43]에서는 인터넷 서비스 공급자(ISP)[44] 혹은 정부가 인터넷 상의 모든 컨텐츠를 동등하게 다루어야 한다는 원리인 망 중립성을 설명한다. 또한 망 중립성 유지를 통한 네트워크 상에서의 프라이버시를 의미하는 망 프라이버시 유지방안을 다룬다.

---

40) VFAC 리뷰 제4호, 33-36쪽.
41) 유럽연합 평의회의 사이버범죄 협약(Convention on Cybercrime of the Council of Europe, CETS No.185) 의 다른 이름이다. http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG
42) VFAC 리뷰 제4호, 36-40쪽.
43) VFAC 리뷰 제5호, 23-26쪽.
44) Internet Service Provider의 약자로 개인이나 기업에게 인터넷 접속 서비스, 웹사이트 구축 등을 제공하는 회사를 말한다. 두산백과, http://www.doopedia.co.kr/doopedia/master/master.do?_method=view&MAS_IDX=101013000870274

② 아동 성 음란물에 대한 법적 쟁점들과 정책제안(Responses to Online Child Exploitation Materials: Legal Issues and Policy Suggestions)[45]에서는 아동 성범죄는 꾸준히 증가하고 있는 반면 국내 관련범죄 처리 및 처벌에 대한 선례부족으로 처벌기준이 모호한 상황을 지적한다. 이와 관련 영국, 캐나다, 미국 등 선진국의 음란물 수위 처벌 단계를 바탕으로 국내 처벌기준 설정 필요성을 강조하고 경찰청 산하 사이버범죄 아동 전담팀 구성을 통한 선제적인 대응을 제안한다.

③ 딥웹(Deep Web)의 위험성(Inside the Deep Web)[46]에서는 검색 엔진으로 검색되지 않거나 유료 데이터 뱅크에 있는 컨텐츠의 인터넷 환경을 말하는 딥웹을 설명한다. 또한 토르(Tor)[47]는 인터넷 상에서 딥웹으로 들어갈 수 있는 게이트 역할을 수행하며 익명성을 띠고, 이러한 익명성으로 인해 사이버 범죄에 악용될 가능성이 크다는 점을 지적한다.

4) 2014년 VFAC 리뷰, 제6호 (7-8월)

① 대학생들의 사이버 왕따(Cyber bullying), 사이버 성희롱(Cyber Harrassment), 사이버 스토킹(Cyber Stalking)에 관한 조사(What our college kids are doing and what they know about cyber bullying, cyber harassment and cyber stalking)[48]에서는 사이버 공간에서 발생하는 범죄 피해자의 보호를 위한 법 체제가 미비함을 지적한다. 특히 사이버 왕따의 경우 파생되는 범죄로 사이버 성희롱, 사이버 스토킹이 있는데 이에 대한 법적 처벌기준 정립의 필요성이 강조된다.

② 청소년들의 섹스팅(Teen sexting)에 관한 법적 논란 및 대책(Teen Sexting: A Critical Analysis on the Criminalization Vis-A-Vis Victimization Conundrums)[49]에서는 10대들이 문자메시지를 통해 성적으로 음란한 내용을 주고받는 행위를 의미하는 섹스팅의 문제점을 설명한다. 또한 섹스팅에 대한 정의 및 법적분석, 친구

45) VFAC 리뷰 제5호, 26-30쪽.
46) VFAC 리뷰 제5호, 31-36쪽.
47) 토르 혹은 토르 네트워크(Tor Network)라고도 한다. 전 세계에서 자발적으로 제공되는 가상 컴퓨터와 네트워크를 여러 차례 경우하면서 사용자의 인터넷 접속 흔적을 추적할 수 없게 하는 서비스다. IT용어사전, 한국정보통신기술협회, http://word.tta.or.kr/terms/terms.jsp
48) VFAC 리뷰 제6호, 21-28쪽.
49) VFAC 리뷰 제6호, 29-36쪽.

및 부모의 역할 고찰과 현 법체제의 한계점을 지적하며 문제 해결을 위한 정책모델을 제시한다.

5) 2014년 VFAC 리뷰, 제7호 (9-10월)

① 합성 카티논(Cathinone)사용 관련 법적 문제와 다크넷(Darknet)의 활용도(Use of Synthetic Cathinones: Legal Issues and Availability fo Darknet)[50]에서는 인터넷 상의 숨어있는 웹사이트 다크넷[51]에서 마약성분인 합성 카티논이 대규모로 거래되는 점을 다룬다. 대표적인 거래사이트는 딥웹 내에 불법으로 운영되는 실크로드가 있으며, 지불 수단에는 가상화폐인 비트코인이 이용됨을 설명한다. 이러한 초국가적 범죄의 효과적인 대응을 위해 UNODC의 노력과 각국 법 집행 기관간의 공조가 강조되었다.

② 사이버범죄협약과 형사절차상 적법절차원칙: 저장된 데이터의 보존 및 일부공개를 중심으로(Convention on Cybercrime and Due Process of Law: On Preservation and Partial Disclosure of Stored Data)[52]에서는 유럽연합평의회의 사이버범죄협약(Convention on Cybercrime)과 관련된 저장된 데이터 보존과 일부공개를 논한다. 협약의 목적이 사이버범죄에 대한 효율적 대처임에도 불구하고 실체적 진실 발견에 중점을 두어 협약의 절차법적 규정들이 정보적 자기 결정권 등 인권에 위협이 될 수 있다는 비판이 있다. 이에 대해 적법절차 원칙을 준수하는 가운데 꼭 필요한 범위 내에서만 정보적 자기결정권을 제한하는 것을 주장한다.

---

50) VFAC 리뷰 제7호, 26-31쪽.

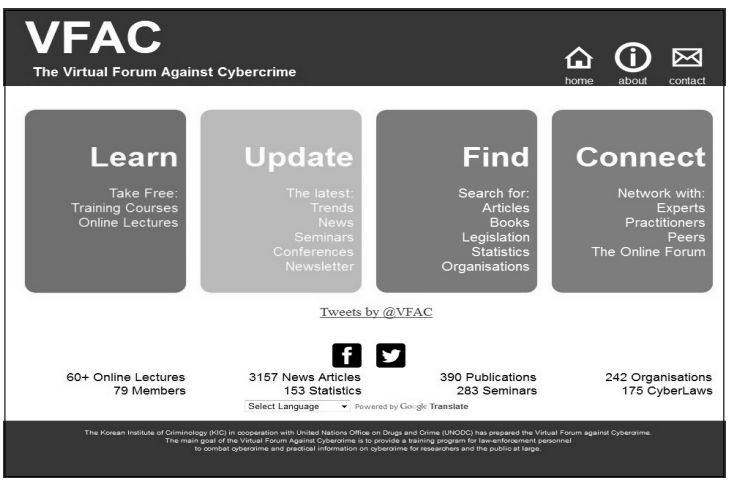
51) 다크넷(Darknet)은 서로 신뢰하는 피어들 간에 공유를 위한 폐쇄형 사설 분산 P@P 네트워크를 의미하며 F2F라고도 한다. 표준 프로토콜과 포트를 사용하지 않고 IP주소가 공적으로 공유가 안되는 익명이에서 기관이나 정부의 간섭을 쉽게 피할 수 있다는 점에서 다른 일반적인 P2P와 구별된다. 저작권기술용어사전, 한국저작권위원회, http://www.copyright.or.kr/information-materials/dictionary/view.do?glossaryNo=501&pageIndex=1&searchLangType=&searchkeyword=%EB%8B%A4%ED%81%AC%EB%84%B7&pageDisplaySize=10&searchIdx=&searchText=&clscode=01&searchTarget=

52) VFAC 리뷰 제7호, 32-36쪽.

2. 2014년 사이버범죄방지 가상포럼 2.0 개설[53)]

사이버범죄방지 가상포럼 웹사이트는 2014년 5월까지 매월 평균 약 200여명의 방문자들에게 서비스를 제공하였다. 2014년 3분기에 인력재편으로 인한 업데이트의 비활성화로 방문자수가 다소 감소하기도 하였다. 그러나 기존 연구네트워크와의 소통 활성화 및 새로운 정보 업데이트를 통해 10월에는 400여명의 방문자가 사이트에 접속하였다.

사이버범죄방지 가상포럼 웹사이트 접속자의 2/3이상이 인터넷 익스플로러가 아닌 다른 브라우저를 사용하는 것으로 나타났다. 이러한 한계점의 극복을 위해 2014년 2월 새로운 버전인 사이버범죄방지 가상포럼 2.0이 출시되었다. 사이버범죄방지 가상포럼 2.0 출시 이후 방문자들은 인터넷 익스플로러이외에 크롬(Chrome), 사파리(Safari), 파이어폭스(Firefox) 브라우저 등으로 사이트의 기능을 이용할 수 있게 되었다.



[그림 2-28] 사이버범죄방지 가상포럼 2.0

53) 장준오 외 8인, 2013UN·국제협력사업 성과보고서, 한국형사정책연구원, 2013, 124쪽.

〈표 2-5〉 브라우저별 사이버범죄방지 가상포럼 홈페이지 접속현황 (2014.10월 기준)

브라우저		방문자	새로운 방문자 %	새로운 방문자	바운스 비율	페이지/방문자수
1	Chrome	901	58.71%	529	49.39%	6.70
2	Internet Explorer	520	60.77%	316	45.38%	6.34
3	Safari	480	83.75%	402	80.62%	2.06
4	Firefox	404	51.49%	208	32.92%	6.05
5	Android Browser	29	68.97%	20	62.07%	3.31
6	Mozilla Comparable Agent	12	100.00%	12	100.00%	1.00
7	Opera Mini	7	100.00%	7	100.00%	1.00
8	Safari (in-app)	7	100.00%	7	57.14%	3.14
9	Opera	4	100.00%	4	50.00%	3.25
10	UC Browser	4	100.00%	4	75.00%	1.25
Total		2,371	63.77%	1,512	52.64%	5.46

3. 웹사이트 개편[54)]

사이버범죄방지 가상포럼 웹사이트는 주요 기능을 4가지로 뚜렷하게 인덱싱하여 인터넷 저개발 국가인 개발도상국 방문자들에게 콘텐츠 검색 및 전달을 용이하게 하였다. 그러나 콘텐츠의 가시성 부족으로 방문자의 친숙도가 낮다는 점이 지적되었다. 이를 보완하기 위하여 사용자 중심의 트렌드에 맞는 다양한 정보형 콘텐츠 및 소통형 콘텐츠를 배치하기로 하였다.

정보통신기술의 중심이 컴퓨터에서 모바일로 이동되면서 모바일의 접근이 용이한 형태의 웹사이트로 개편하였다. 2014년 11월 후반부터 개편작업이 시행되었다.

가. 모바일 버전 웹사이트 구축

스마트폰 사용자의 급격한 증가에 따라 사이버범죄방지 가상포럼 모바일 버전을 구축하여 방문자들과의 소통을 강화하기 위한 작업이 수행되었다. 사이버범죄방지

54) 김지영 외 10인, UN·국제 교류협력 사업 보고서, 한국형사정책연구원, 2014, 199쪽.

가상포럼 모바일 버전은 스마트폰의 다양한 운영체제 및 버전에서 작동 할 수 있도록 설계되었다. 스마트폰 및 테블릿 등의 접속 기기에서의 최적화된 화면을 제공하고 PC와 모바일 페이지의 관리자 기능을 일원화하여 업무 효율성을 증가시켰다. 또한, 일반 사용자 및 장애인들의 접근성 향상을 위하여 모바일 웹 표준 지침인 '모바일 OK'[55]를 준수하였다.

[그림 2-29] 사이버범죄방지 가상포럼 모바일 버전 접속화면

55) 모바일 기기에서 웹 사이트를 완벽하게 볼 수 있다는 것을 인증하는 마크이다. 휴대전화를 비롯하여 다양한 이동 단말기에서 기존 인터넷과 포털들의 콘텐츠 및 서비스를 이용이 가능할 수 있도록 웹 사이트 개발가이드를 중심으로 마크업 언어, 단발정보 규격 등을 표준화한다. 우리나라에서 모바일 웹 표준화는 2006년 3월 설립된 모바일 웹2.0 포럼이 주도하고 있다. 네이버 지식백과, http://terms.naver.com/entry.nhn?docId=865560&cid=42346&categoryId=42346

제3장

KOREAN INSTITUTE OF CRIMINOLOGY

사이버범죄방지 가상포럼 연구네트워크 발전방안

김한균·승재현·나주원

제3장

사이버범죄방지 가상포럼 연구네트워크 발전방안

제1절 사이버범죄방지 가상포럼의 사이버범죄 동향, 통계, 법률안 자료

1. 2015년 사이버범죄방지 가상포럼 웹사이트 관리 체제 재편

사이버범죄방지 가상포럼 웹사이트[56]는 개편작업을 거쳐 2015년 8월 6일부터 새로운 인터페이스로 콘텐츠를 제공하기 시작하였다. 특히 2015년부터는 인력재편에 따른 웹페이지 관리 및 업데이트 비활성화를 방지하기 위하여 새로운 관리 체제를 마련하였다.

웹페이지 관리는 크게 사이버범죄방지 가상포럼 웹사이트 기술 및 인터페이스 관리와 콘텐츠 업데이트 관리 두 부분으로 나뉜다. 그러나 웹사이트 콘텐츠가 영문 및 중문으로 관리됨에 따라 웹사이트 기술 관리자가 콘텐츠까지 전담으로 맡아서 관리하기에는 인력 충원의 어려움이 있었다.

따라서 올해부터는 담당자 변경 등에 상관없이 사이버범죄방지 가상포럼 웹사이트 서비스의 지속성을 유지하기 위하여 콘텐츠 관리를 시스템화 하였다. 특히 콘텐츠 관리는 연구계약을 맺은 고려대학교 사이버법센터[57]를 활용해 사이버범죄 전문가가 검토 및 수집하고, 국제협력센터에서 자료 가공 및 업데이트를 진행하는 방식을 처음으로 시도하였다.

---

56) http://www.cybercrimeforum.org/
57) http://www.kuclc.org/

가. 사이버범죄방지 가상포럼 웹사이트 관리 체제화 사전준비회의

4월 24일 전문가 자문 회의를 통해 기존의 사이버범죄방지 가상포럼 웹사이트의 개편 방향을 논의하였다. 사이버범죄방지 가상포럼 사업의 기본 취지는 사이버범죄의 방지와 관련하여 개도국의 사이버범죄 방지 및 통제를 위한 기술지원 및 훈련을 제공하는 역할과 자료축적 및 전문가들의 네트워크를 담당하는 허브 역할임을 제시하였다. 회의 참석자들은 발전적 재편이 필요함에 동의하며 온라인 프로그램의 오프라인 자료 전환 및 개도국이나 일반인 대상 교육교재의 활용 가능성을 논의하였다. 특히, 앞으로 웹사이트 콘텐츠 업데이트 부분은 동북아 지역을 포함하기로 하였다.

6월 8일 회의에서는 UNODC에서 2015년 신설한 Cybercrime Repository(사이버범죄 자료실)[58] 과 관련하여 사이버범죄방지 가상포럼 콘텐츠의 활용 방안이 논의되었다. 제안 사항으로는 기존의 자료 수집과 유사하게 하되, 기존 자료의 재분류를 통해 동북아 지역 및 개도국 사이버범죄 동향파악에 집중하기로 하였다.

7월 30일과 8월 12일 회의에서는 새롭게 개편된 사이버범죄방지 가상포럼 웹사이트를 함께 진단하고, 콘텐츠 업데이트에 있어서 고려대 사이버법센터와 형정원의 역할을 결정하였다. 또한 콘텐츠의 일관성을 갖추고 향후 재분류 작업에 활용하기 쉬운 방향을 모색하기 위하여 자료 수집 및 가공의 가이드라인을 마련하였다.

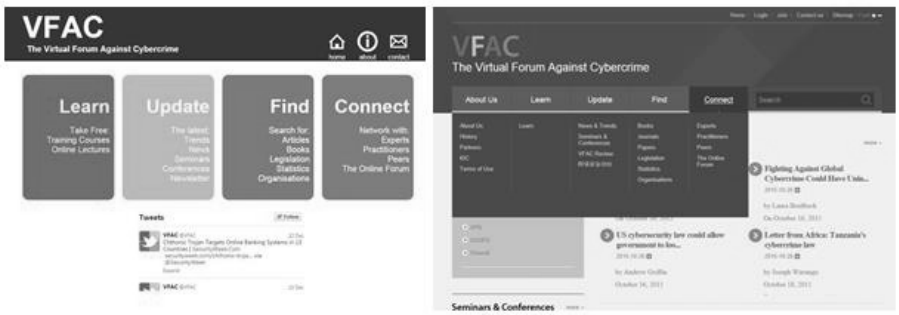
2. 사이버범죄방지 가상포럼 웹사이트 개편 내역 및 성과

가. 홈페이지 개편

사이버범죄방지 가상포럼 웹사이트에서 가장 눈에 띄는 변화는 레이아웃 변경이다. 기존에는 웹사이트 접속 시 웹사이트의 카테고리를 보여준 반면, 개편된 홈페이지는 각 카테고리별 콘텐츠의 미리보기가 제공된다. 따라서 웹사이트 사용자에 대한 콘텐츠의 노출도가 증가하였다.

---

58) 2013년 UN 범죄방지 및 형사사법 위원회 (CCPCJ) 논의 결과(Resolution 22/8)로 채택된 온라인 사이버범죄 자료실(https://www.unodc.org/cld/index-cybrepo.jspx)이다. 자세한 내용은 본 보고서의 제3장 제2절의 1에서 설명하였다.



[그림 3-1] 사이버범죄방지 가상포럼 웹사이트 개편 전·후 비교

예를 들어 개편된 웹사이트에서는 각 카테고리별 최신 게시글 1-5개가 홈페이지에 노출된다. 그 결과, 홈페이지에 노출된 글의 조회수는 노출되지 않은 글의 조회수보다 현저하게 높아졌다. 사이버범죄 및 보안 관련 국제회의와 세미나를 소개하는 Seminar&Conferences의 경우, 홈페이지에 노출된 글의 조회수가 15-25회인 반면, 노출되지 않은 글의 조회수는 5-10회로 나타났다.

또 다른 변화는 중문 서비스 시작이다. 중문 서비스는 현 단계에서는 시범사업 차원에서 진행하고 있다. 현재는 News&Trend 게시글 중 동북아지역 사이버범죄 및 보안과 관련된 내용을 번역하여 콘텐츠로 제공하고 있으며, 추가적으로 중국어 서적 및 논문 소개를 진행할 수 있을 것으로 기대된다.

나. 콘텐츠 업데이트 구성

콘텐츠의 내용은 사이버범죄 동향, 통계, 논문, 서적, 법률안 자료 등으로 구성되어 있다. 웹사이트에 개재된 콘텐츠를 바탕으로 VFAC Review를 발간하고, UNODC의 사이버범죄 자료실(Cybercrime Repository)에도 제공할 예정이므로, 양질의 콘텐츠가 필요하다.

고려대 사이버법센터에 요청한 자료 수집 및 가공 지침은 다음과 같다.

〈표 3-1〉 사이버범죄방지 가상포럼 콘텐츠 가공 지침

카테고리	세부	자료 수집 및 가공 지침
Update	Trends& News	매주 있었던 주요 사이버범죄 뉴스 혹은 사이버보안 관련 뉴스나 동향을 제공.
	Seminars& Conferences	사이버범죄 관련 세미나 및 국제회의를 중심으로 하되, 사이버 안보 혹은 최근 IT 기술 관련 교육 훈련 등도 함께 소개.
Find	Books	최근 발간된 사이버범죄 관련 서적을 소개하고 영문초록과 링크, ISBN을 함께 제공.
	Journals& Papers	최근 발간된 논문을 중심으로 사이버범죄 관련 논문을 소개하고 영문 초록과 링크를 함께 제공.
	Legislation	각 국가별 사이버범죄 관련 법률안을 검토하여 국가, 연도, 법조문 제목, 다운로드 가능한 링크를 제공.
	Statistics	각 국가별 통계청 및 민간 기업 발표 자료 등을 이용하여 사이버범죄 관련 통계 자료를 제공하되, 검색용 키워드와 다운로드 가능한 링크를 포함.

다. 주요 콘텐츠 업데이트 내용

고려대학교 사이버법센터에서는 8월 웹사이트 개편 시점부터 일주일에 1회 총 13주 간 약 300여건의 자료를 제공하였다. 대부분의 콘텐츠는 기존의 사이버범죄방지 가상포럼 웹사이트 콘텐츠 내용과 일관성을 유지하였다.

추가로 구성한 내용은 다음과 같다. Books의 경우 영문초록 외에 ISBN, 이미지를 함께 제공한다. Journals&Papers의 경우 기존 웹사이트에서 구분이 명확하지 않았던 점을 보완하였다. Journal에는 사이버범죄 관련 국제 저널에 실린 각종 소논문 및 논문을, Paper에는 저널 외에 각 국가별 사이버범죄 관련 웹사이트 혹은 기업 및 연구소의 논문 등을 소개하였다. 또한 주요 참고자료로 활용된 경우 해당 내용도 함께 표시하였다.

제2절 UNODC 사이버범죄 자료실 (Cybercrime Repository)

1. UNODC 사이버범죄 자료실 (Cybercrime Repository)

UNODC는 2015년 5월 18-22일 개최된 제24차 유엔 범죄방지 및 형사사법 위원회에서 사이버범죄 자료실(Cybercrime Repository)의 발족을 공식 발표하였다. 사이버

범죄 자료실이 개발된 배경과 사이버범죄 자료실의 역할은 다음과 같다.

가. 사전논의 및 배경

2013년 개최된 제 22차 유엔 범죄방지 및 형사사법 위원회의 결의안(Resolution 22/8)에서 '사이버범죄 퇴치를 위한 국가별 대응책과 국제협력강화를 위한 기술 원조 및 역량 강화 지원'을 근거로 마련되었다. 결의안 5문단에서 위원회는 다음과 같이 명시하였다.

○ E/CN.15/2013/27 Resolution 22/8 (제22차 유엔 범죄방지 및 형사사법 위원회 결의안 일부)[59]

필요성 및 형사사법 역량의 지속적인 평가 및 기술 원조의 전달 및 조정을 목적으로 추가적으로 UNODC가 사이버범죄 법률 및 사례의 중앙 자료 자료실 역할을 할 것을 요청한다.

사이버범죄 자료실의 필요성은 2015년 제13차 유엔 범죄방지 및 형사사법 총회에서도 강조되었다. UNODC는 홈페이지를 통해 사이버범죄의 중요성에 대하여 다음과 같이 제시하였다.

○ UNODC 홈페이지 뉴스 게시글[60]

2015년 범죄총회: 사이버범죄에 초점(2015년 3월 4일)

사이버범죄는 그 진화속도가 가장 빠른 초국가 범죄이자 이미 전세계 수 백 만 명에게 영향을 끼치고 있는 범죄다. 사이버범죄의 형태는 개인정보 관련 범죄, 저작권 및 지식재산권 침해, 아동 음란물 및 학대 등이 있다. 20억 명에 달하는 사용자가 의식적으로 혹은 무의식적으로 개인정보를 사이버공간에 저장하는 오늘날 가장 큰 위협으로 다가오고 있다.

59) 제22차 유엔 범죄방지 및 형사사법 위원회 결의안 참조. https://www.unodc.org/documents/data-and-analysis/statistics/crime/ICCS/7_CCPCJ_Report_22nd_session.pdf

올해 4월 제13차 UN범죄총회에서는 다양한 종류의 범죄를 검토하고, 개발에의 영향, 지속가능한 개발 성취에 범죄 퇴치의 중요성이 논의될 것이다. 중점은 사이버범죄로 범죄의 규모를 가늠하고 초국가적인 특성과 관련된 사례를 논의한다.

사이버범죄는 기술 발전에 따라 범행은 점점 더 쉬워진 반면 법집행 기관이 방지하기에는 어려워졌다. 특히 개발도상국은 사이버공격 퇴치역량 부족으로 높은 피해율을 보이고 있다. 세계시만을 사이버범죄로부터 구할 필요성이 더욱 커진 것이다.

사이버범죄는 도하에서 열리는 제13차 유엔 범죄방지 및 형사사법총회에서 논의되는 초국가 범죄중 하나다. 정부, 정책입안가, 전문가들은 4월 12일부터 19일에 걸쳐 초국가 범죄 위협에 대처하기 위한 경험을 공유하고 국제협력을 강화할 것이다. 국제사회가 포스트 2015 개발의제 논의를 지속하는 것처럼 범죄 총회도 안보, 정의, 법치, 더 나은 세상, 더 평등한 세계 만들기의 연결고리를 찾는데 집중할 것이다.

나. 사이버범죄 자료실 구성

UNODC는 사이버범죄 관련 법안, 판례 등을 집대성한 온라인 사이버범죄 자료실(https://www.unodc.org/cld/index-cybrepo.jspx)[61]를 만들어 공개하였다. 사이버범죄 자료실의 자료 구성, 사용법 그리고 활용방안은 다음과 같다.

1) 자료 구성

사이버범죄 자료실은 UNODC가 추진하고 있는 셜록(SHERLOC, SHaring Electronic Resources and Laws On Crime)[62] 프로젝트와 유사한 특성을 가진다.

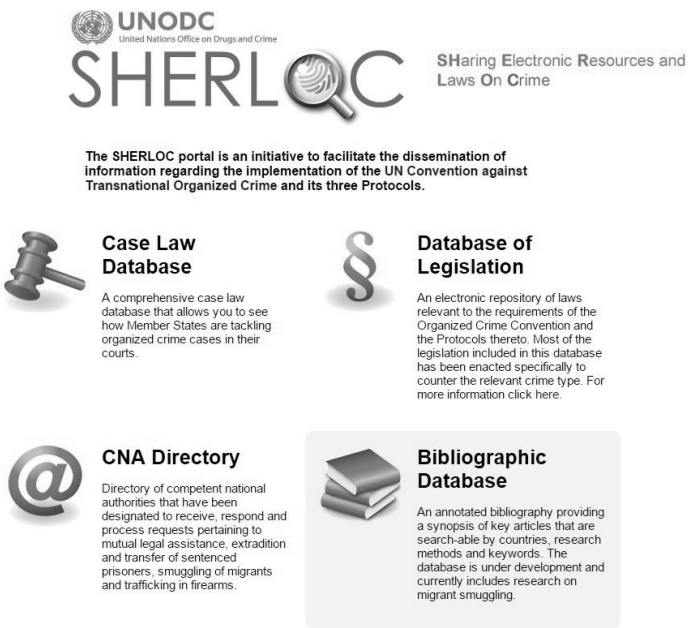
---

60) UNODC 홈페이지, http://www.unodc.org/unodc/en/frontpage/2015/March/focus_its-a-crime_-cybercrime.html?ref=fs2

61) 사이버범죄 자료실은 사이버범죄 법안과 모법사례를 제공하며, 그 목적은 형사사법 역량의 지속적인 평가 촉진, 그리고 기술 원조의 전달과 조정에 있다. https://www.unodc.org/cld/index-cybrepo.jspx

62) SHERLOC:SharingElectronicResourcesandLawsonCrime의 줄임말로 조직범죄 퇴치 정보 교환 온라인 플랫폼의 역할을 한다. 초국가 조직범죄는 지속적이고 진화하는 특성을 가지며 범행 수법이 점점 교묘해지고 복잡해지고 있다. 이러한 특성이 있는 초국가 조직범죄의 퇴치를 위해서는 정보 공유 및 국제 협력을 통한 국제사회 공동의 노력이 시급하다. 이러한 배경으로 UNODC는 유엔 국제조직범죄방지협약(United Nations Convention against Transnational Organized Crime)의 이행과 관련된 정보를 공유할 수 있는 포털사이트를 개설하였다. 웹사이트에 협약 이행 관련 사건이 게재되는 만큼 국가, 경찰 및 법 집행기관, 시민 사회 및 기타 기관의 정보 교류가 촉진될 것으로 기대된다. 2013년 개설된 이후 1,800여개의 개별 사건,

셜록은 유엔 국제조직범죄방지협약(UN Convention against Transnational Organized Crime)[63] 이행 관련 정보의 교류 확대를 위한 포털이다. 구성은 각국 범죄 관련 판례법, 입법 자료, 참고 자료, 유관 기관 디렉토리로 구성되어있다.



[그림 3-2] SHERLOC 홈페이지

반면 사이버범죄 자료실은 오픈소스[64] 연구, UNODC 사이버범죄에 관한 종합연구(UNODC Comprehensive Study on Cybercrime)[65], 국가별 사이버범죄 정보를 제

4,000여건의 국가별 법안 관련 정보가 데이터베이스로 구축되었다. 웹사이트는http://www.unodc.org/cld/index-sherloc.jspx로 접속 가능하며, 데이터베이스는 각국 범죄 관련 판례법, 입법 자료, 참고 자료, 유관 기관 디렉토리로 구성되어있다. 정부, 사법 기관, 법 집행 공무원, 법조인, 학자 등 다양한 사용자를 대상으로 구축되었고 사이버범죄, 인신매매, 돈세탁, 개인정보 침해, 야생동식물 및 산림 범죄 등 다양한 범죄 정보를 담고 있다.

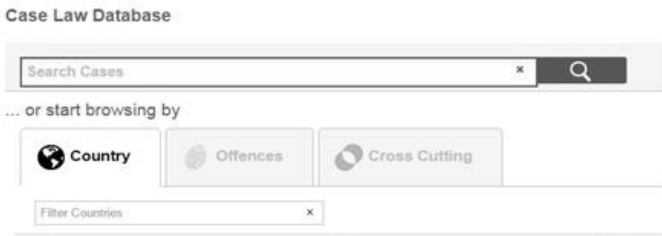
63) 2000년 11월 15일 유엔 총회 결의안 55/25로 채택된 초국가범죄 방지를 위한 국제 도구이다. UNODC 협약 홈페이지, https://www.unodc.org/unodc/treaties/CTOC/

64) 그 생산 혹은 개발 단계에서 무료 라이선스를 통해 모든 사람 및 사용자에게 접근 권한을 제공하는 자료 혹은 정보를 말한다. 주로 소프트웨어 개발에 사용된다. 자세한 내용은 다음을 참조. Gerber, Aurona, Onkgopotse Molefe, and Alta van der Merwe. "Documenting open source migration processes for re-use." Proceedings of the 2010 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists. ACM, 2010.

공한다. 이후 사이버범죄 자료실 관리자의 자료 검토를 거친 후 각 자료 유형에 따라 나누어서 개재된다.

데이터베이스는 사이버범죄와 관련된 판례법(case law), 입법 정보(legislation), 모범 사례(lessons learned)로 구성하였다. 검색 필터로 국가별, 범죄 유형별 분류를 제공하고, 사이버범죄 외에도 기타 범죄유형과 관련된 법안 등은 추가 검색기능이 제공된다. 다음은 각 데이터베이스별 구성 특성이다.

판례법 데이터베이스에서는 전자 증거 관련 사이버범죄에 관한 판례 및 법집행 운영의 성공 사례를 소개한다.



[그림 3-3] 판례법 데이터베이스

입법 데이터베이스에서는 법 전문 검색과 발췌가 가능하다.

[그림 3-4] 입법 데이터베이스

모범 사례 데이터베이스에서는 사이버범죄 방지 및 퇴치를 위한 국가별 전략과 정책의 모범사례를 소개한다.

65) UNODC 홈페이지, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[그림 3-5] 사례 데이터베이스

이를 통하여 사이버범죄 자료실은 국가의 사이버범죄 퇴치 역량 강화를 지원하고자 한다. 특히 법률안 마련, 사이버범죄 관련 정책 대응, 사이버범죄 수사·기소·예방 관련 모법 사례 및 교훈 공유, 제3자와 협력 강화, 공식적·비공식적 국제협력 확대에 기여할 것으로 기대된다.

2. 사이버범죄방지 가상포럼 웹사이트 콘텐츠 활용방안

가. 사이버범죄방지 가상포럼 웹사이트 - UNODC 사이버범죄 자료실 MOU 체결방안

1) 사이버범죄방지 가상포럼 웹사이트 활용 가능성 및 추진 배경

사이버범죄방지 가상포럼 웹사이트 콘텐츠와 사이버범죄 자료실에서 제공되는 콘텐츠는 유사성을 지닌다. 특히 사이버범죄방지 가상포럼 웹사이트에서 제공하는 입법, 사례 자료의 경우 규모면에서 사이버범죄 자료실을 능가한다. 현재 사이버범죄방지 가상포럼 웹사이트의 입법(Legislation) 데이터베이스에는 총 115개국, 175개의 사이버범죄 관련 법률안이 저장되어있고, 다운로드도 가능한 상태다. 사례 관련 자료도 현재 사이버범죄방지 가상포럼 웹사이트의 자료 4,000여건 중 2013-2014년 자료만으로도 13개국, 30여개의 사이버범죄 대응 모범 사례 관련 자료를 제공할 수 있다.[66]

또한 제24차 유엔 범죄방지 및 형사사법 위원회의 제1위원회 보고서: 워크숍3에서도 사이버범죄 방지를 위한 자료 수집이 다시 한 번 강조 되었다.

---

66) www.cybercrimeforum.org

○ 제24차 유엔 범죄방지 및 형사사법 위원회 제1위원회 보고서
(A/CONF.222/L.3/Add.1 para.23. (d))

(d) 사이버범죄와 문화재 밀매 등 진화하는 범죄 중 특히 조직 범죄 단체와 테러 단체과 연관된 범죄의 다양성을 이해하기 위한 회원국의 자료 수집 노력의 지속 및 추가 연구에의 기여 중요성이 강조되었다. 발표자들은 거듭하여 관련 분야에서 그리고 시민 사회와의 협력에서 유관 국제기구의 역할을 강조하였다.[67]

2) 사이버범죄방지 가상포럼 웹사이트 – UNODC 사이버범죄 자료실 MOU 체결 논의 진행사항

사이버범죄방지 가상포럼 웹사이트 콘텐츠의 활용도가 높으며, 사이버범죄방지 가상포럼 사업의 발전적 재구성을 위하여 제24차 범죄방지위원회 이후 UNODC 사이버범죄 자료실과의 협력협정을 추진해왔다. 1차 협의는 24차 범죄방지위원회 당시 UN 정책분석국 공보 및 정책지원과 과장 Gillian Murray와 진행되었다. 이후 6-8월간 이메일을 통한 MOU 제안 및 사업안 검토를 거친 두 9월 24일 UNODC 사이버범죄 사업담당자와 회의를 가졌다. 논의 내용은 다음과 같다.

먼저, 사이버범죄 자료실 협력 사업을 위한 MOU 체결방식은 2005년 사이버범죄방지 가상포럼 사업을 위한 MOU가 만료되었으므로, 새로운 MOU를 체결한다. 단, 사이버범죄 자료실과 지역범죄통계협력센터(CoE) 협력 사업을 포괄하는 MOU를 일차 체결하고, 각 사업별로 3개년에 걸친 공동연구 계약을 개별 체결하는 방식으로 추진하는 방안을 협의하였다. 이와 관련, 한국형사정책연구원은 UNODC 측에 프로젝트 제안서 및 공동연구 계약서 초안을 제시할 것을 요청하고, 이를 검토하여 추후 협의를 진행하기로 하였다.

또한 MOU에 포함될 구체적 사항으로는 저작권 공유문제, 한국형사정책연구원의 사이버범죄방지 가상포럼 웹사이트 및 간행물에 UNODC 로고 사용문제 등의 규정을 요청하였다.

---

67) 제24차 유엔 범죄방지 및 형사사법 위원회 홈페이지, https://www.unodc.org/documents/congress//Documentation/IN_SESSION/ACONF222_L3ADD1_e_V1502497.pdf

마지막으로 향후 사이버범죄 자료실과 사이버범죄방지 가상포럼 의 전략적 협력 및 상호정보 공유사업을 위한 협의 필요사항에는 ① 정보를 업데이트하고 점검하기 위한 양 기관 연락담당관(focal point)의 지정, ② 사이버범죄 자료실 운영을 위한 인력지원, ③ 사이버범죄 자료실 홍보를 위한 이벤트 개최 및 오프라인 정기간행물 공동발간, ④ 사이버범죄 자료실 정보수집 분석 및 평가를 위한 전문가 실무그룹 조직 및 운영, ⑤ 사이버범죄 자료실 성과정리를 위한 연례회의 개최가 포함되었다.

제3절 VFAC 리뷰의 지속적 간행

1. VFAC 리뷰 구성

VFAC 리뷰는 2014년 제7호(9/10월호) 발행이후 발행이 잠정 중단된 상태였다. 그러나 8월 사이버범죄방지 가상포럼 웹사이트 개편에 맞추어 그 콘텐츠를 토대로 다시 발간을 시작했다. 2015년은 하반기부터 격월로 매 짝수 달에 출간하며 제7호에 이어서 제8호부터 발간하였다.

콘텐츠 구성은 기존과 마찬가지로 사이버범죄 관련 주요 국제회의 및 세미나, 최신 뉴스 및 동향, 최신 논문 소개, 사이버범죄 전문가 기고문으로 구성하였다. 달라진 점은 기고문 구성방식이다. 기존 VFAC 리뷰에서는 사이버범죄분야 국내외 전문가의 글을 받아 개제하였다. 그러나 2015년에는 연구계약을 맺은 고려대 사이버법센터에서 전문가의 글을 국문 혹은 영문으로 받아 국문의 경우 한국형사정책연구원이 번역작업을 하였다. 그 결과 국내·외 학자뿐만 아니라 경찰 등 수사 일선에서 겪는 사이버범죄 관련 동향 및 형사사법 문제 등에 관한 의견을 수렴할 수 있었다.

2. VFAC 리뷰 주요 내용

가. 2015년 VFAC 리뷰 제8호

1) 진화하는 사이버범죄[68]

사이버범죄는 그 유형과 범행수법이 점차 진화하고 있다. 그에 따라 범죄 유형을

68) VFAC 리뷰 제8호, 20-22쪽.

파악하기 힘들고, 범죄의 원인 및 동기를 찾아내기 힘들며, 대처 방안을 고안하기 힘들다는 특성이 있다. 정책적 대응에 있어서도 용어 불일치, 범죄 분류의 모호성, 다양한 행위가 관여된 특성으로 인한 범죄의 복잡성, 초국가적 특성으로 인한 피해 정도의 차이, 동시다발적인 특성이 문제가 된다.

이처럼 진화하는 사이버범죄와 그 위협에 대응하기 위해서는 국가별 사이버범죄 퇴치역량 강화, 사이버범죄 방지 법률안 검토, 민관 협력을 통한 사이버범죄 대응, 사이버범죄 문제 대응을 위한 지역 및 국제 사회 협력 추진 및 정보 공유, 사이버범죄 대응 형사사법 역량 강화를 위한 기술 지원을 고려해야한다.

2) 뇌-컴퓨터 인터페이스: 새로운 트로이 보안[69]

뇌-컴퓨터 인터페이스(BCI)[70]는 우울증 치료부터 뇌졸중 치료까지 다양한 용도로 사용된다. 또한 사고가 가능한 기계의 통제를 위한 인터페이스 시스템으로도 사용된다. 이처럼 의료 및 컴퓨팅 등 다방면에 걸쳐 사용될 수 있는 기술인만큼, 악용 및 범죄의 위험도 늘어나고 있다.

BCI 기술과 관련된 첫 번째 법적 문제는 자유의지다. 예를 들어 BCI기술이 적용된 체내 삽입 기기가 해킹이 될 경우, 이를 사람의 자유의지로 볼 수 있을지의 문제가 생긴다. 두 번째는 타인의 의도에 의한 위협이다. 예를 들어 프로그래머의 의도를 타인이 왜곡한 경우 새로운 형태의 범죄가 발생할 수 있으며, 그에 따른 형사사법 문제가 뒤따른다.

3) 사이버범죄의 초국가적 특성에 대응하기 위한 국제협력[71]

초국가적인 사이버범죄에 효과적으로 대응하기 위해 국제협력의 중요성이 강조되고 있다. 현재 수사 기관이 마주하고 있는 국제협력의 어려움으로는 주권과 관할권 문제, 클라우드나 네트워크에 저장된 사이버 공간상의 증거 확보 문제 등이 있다.

---

69) VFAC 리뷰 제8호, 23-25쪽.

70) Stefano Silvoni, Ander Ramos-Murguialday, Marianna Cavinato, Chiara Volpato, Giulia Cisotto, Andrea Turolla, Francesco Piccione, and Niels Birbaumer. Brain-Computer Interface in Stroke: A Review of Progress. Clinical EEG and Neuroscience, 42(4):245-252, October 2011.

71) VFAC 리뷰 제8호, 25-26쪽.

해결책은 규제 완화 등을 통한 국제협력 및 합의이지만, 그와 동시에 그 방식이 인권 및 개인정보 침해 등 법익에 방해가 되지 않는 방향으로 진행되어야 한다.

나. 2015년 VFAC 리뷰 제9호

1) 사이버 범죄와 디지털 포렌식[72]

디지털 포렌식은 디지털 매체에 저장되어 있거나 네트워크에 있는 범죄와 관련된 데이터를 수집 및 분석하여 법정에 증거로 제출하고 제출된 증거가 사실인정의 자료로 채택되기까지의 과정을 일컫는다. 또 그 중요성이 증가함에 따라 다양한 법제들이 등장하고 있다. 디지털 증거는 물리적 공간에 존재하지 않는다. 따라서 그에 맞는 수사 기법의 활용을 위해서는 형사소송 절차에 많은 변화가 필요하다. 그러나 증거수집과 관련된 조항은 국민의 기본권을 침해하는 성격을 가질 수도 있다. 따라서 사이버범죄 처벌 규정의 신설 외에 범죄자 신속 검거를 위한 증거수집절차와 관련된 규정의 신설이 필요하며, 다만 헌법상 보장된 국민의 기본권이 침해되지 않도록 하여야한다.

2) 스파이앱(SpyApp)[73] 범죄 동향[74]

2015년 사이버범죄 동향은 모바일 환경 확대에 따른 스마트폰을 통한 개인정보 탈취와 이를 통한 경제적 이득이 특징이다. 특히 스마트폰에 허위 메시지를 보내 개인정보 탈취 어플리케이션을 설치하여 개인정보를 빼내는 스파이앱 범죄가 증가하였다. 스파이앱 범죄와 관련된 법률 쟁점으로는 먼저 스파이앱의 전달·유포하는 행위를 처벌할 수 없다는 점이 있다. 기존 법률에서는 기존의 사이버범죄의 형태를 규정하는 형식으로 처벌을 결정하기 때문이다. 유럽연합평의회의 사이버범죄 방지 협약(Convention on Cybercrime)[75] 내 조항은 사이버범죄 행위를 상술하기 보다는 '모든 형태의 공격 의도'를 가진 행위로 규정하고 있다. 향후 처벌 규정 신설에 참고할만

72) VFAC 리뷰 제9호, 38-39쪽.
73) 스마트폰 사용자의 통화 내용, 문자메세지, 음성 녹음을 통한 도청 및 감청 기능을 갖춘 어플리케이션을 일컫는다. 네이버 용어사전, http://terms.naver.com/entry.nhn?docId=2070345&cid=55570&categoryId=55570.
74) VFAC 리뷰 제9호, 45-48쪽.
75) 유럽연합평의회 협약 홈페이지, http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

한 국제 조항이다. 이러한 법제적 조치 외에 안티 스파이앱 개발[76], 민관 협력, 대국민 인식제고 등의 노력이 필요하다.

3) DDoS 공격에 있어서 장애의 의미와 봇넷구축 행위에 대한 예비·음모죄 신설 필요성[77]

DDoS 공격은 보안이 취약한 다수의 컴퓨터의 통제권을 불법적으로 획득하여 하나의 네트워크를 구축하여 특정 시스템에 접속하여, 해당 시스템의 처리기능에 장애를 일으키는 행위다. 장애의 의미 판단에 있어서는 처벌의 목적에 따라 정상적 사용자들의 행위가 불법으로 처벌되지 않게 현실적 사용 불능을 장애로 규정지을 필요가 있다. 또한 봇넷을 구축하는 행위가 DDoS 공격의 사전준비행위에 해당한다고 볼 수 있으므로 이에 대한 예비·음모죄를 신설할 필요가 있다.

---

76) 예를 들어 경찰청 사이버범죄대응과에서 개발한 폴-안티 스파이앱이 있다.
https://play.google.com/store/apps/details?id=com.cyber.dfc.polantispy

77) VFAC 리뷰 제9호, 45-48쪽.

제4장

KOREAN INSTITUTE OF CRIMINOLOGY

사이버범죄방지 가상포럼 교육훈련 프로그램의 성과 평가

김한균·승재현·조민정

제4장

사이버범죄방지 가상포럼 교육훈련 프로그램의 성과 평가

제1절 사이버범죄방지 가상포럼 온라인 교육 프로그램

1. 사이버범죄방지 가상포럼 온라인 교육 개발 현황

한국형사정책연구원은 2006년부터 2009년까지 UNODC와 함께 사이버범죄방지 가상포럼 온라인 교육·훈련 구축사업을 진행했다. 사이버범죄방지 가상포럼 웹사이트의 본격 지원이 제공된 2010년 이후, 2011년 번역 및 추가 강의 제작을 마친 사이버범죄방지 가상포럼 온라인 교육 프로그램의 현황은 다음과 같다.

가. 교육훈련 커리큘럼

현재 온라인 교육훈련 커리큘럼으로 제작된 과정은 총 137개다. 앞서 언급된 것과 같이 온라인 교육·훈련 과정: 입문과정과 온라인 교육·훈련 과정: 고급과정으로 나뉜다. 입문과정은 모듈0, 모듈1, 모듈2의 총 33강으로 이루어져 있고, 고급과정 및 세미나 과정은 모듈3, 모듈4, 모듈5의 총104강으로 구성된다. 과정별 강의 프로그램 구성은 다음과 같다.

〈표 4-1〉 온라인 교육·훈련 과정: 입문과정(Introductory Course)

Lesson	Course	Module	주요 사항
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	서비스 제공 중지
0-2-1		[0.2] Cybercrimes in the Global Village (Ⅰ)	서비스 제공 중
0-3-1		[0.3] Cybercrimes in the Global Village (Ⅱ)	

Lesson	Course	Module	주요 사항
1-1-1	[1] Understanding Information and Communication Technology	[1.1] Understanding Emerging Trends in ICT and Cybercrimes in the Information Age	서비스 제공 중
1-1-2			
1-1-3			
1-2-1		[1.2] Structure of the Internet and Digital Divide	
1-2-2			
1-3-1		[1.3] Vulnerabilities of ICT	
1-4-1		[1.4] ICT and Network Security	
1-5-1		[1.5] Forms of Intrusion and Hacking	
1-5-2			
1-6-1		[1.6] E-commerce and Forms of Electric Payment	
1-7-1		[1.7] Digital Evidence and Digital Forensics for Non=forensic Specialists	
1-7-2			
2-1-1	[2] Understanding Cybercrime Laws	[2.1] Criminality – Definitions of Cybercrime	서비스 제공 중
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 and 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 and 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 and Problems – Procedures and Practices of Online Cooperation for Law Enforcement Agencies	
2-10-2			
2-11-1		[2.11] Digital Evidence, Preservation and Presentation of Evidence for Non-forensic Specialists	

〈표 4-2〉 온라인 교육·훈련 과정: 고급과정(Advanced Course) 및 세미나 과정(Seminar)

Lesson	Course	Module	주요 사항
3-1-1	[3] Cybercrime Investigations – Procedure and Techniques	[3.1] Computer Investigation Techniques (Ⅰ)	서비스 제공 중
3-1-2			서비스 중단
3-1-3			서비스 제공 중
3-1-4			
3-2-1		[3.2] Computer Investigation Techniques (Ⅱ)	서비스 중단
3-2-2			
3-3-1		[3.3] Investigation System and Procedure of Developed Countries	서비스 제공 중
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 and Digital Evidence	
3-4-2			
3-5-1		[3.5] Modus Operandi of Cybercrime and Investigation Techniques (Ⅰ) – Computer Viruses, Hacking & Botnet	서비스 중단
3-5-2			
3-5-3			
3-5-4			
3-6-1		[3.6] Modus Operandi of Cybercrime and Invesigation Techniques (Ⅱ) – Cyber Stalking and Electronic System	서비스 중단
3-6-2			
3-6-3			
3-7-1		[3.7] Modus Operandi of Cybercrime and Investigation Techniques (Ⅲ) – Computer Fraud and Phishing	
3-7-2			
3-8-1		[3.8] Modus Operandi of Cybercrime and Investigation Techniques (Ⅳ) – Terrorist Use of the Internet	
3-8-2			
3-9-1		[3.9] Preservation and Presentation Threat of Anonymous Communication	
3-9-2			
3-10-1		[3.10] Assessment Potential Threat of Anonymous Communication	
3-10-2			

Lesson	Course	Module	주요 사항
3-11-1		[3.11] Network Security	
3-11-2			
3-11-3			
3-11-4			
3-11-5			
3-11-6			
3-12-1		[3.12] Incident Response Teams - Priorities and Team Buildings	서비스 제공
3-12-2			
3-13-1		[3.13] Investigative Beset Practices - Case Studies	
3-13-2			
3-14-1		[3.14] Practicum - Project Exercise	
4-1-1	[4] Cybercrime Investigations - Digital Forensics	[4.1] Understanding and Applying the Rules of Digital Evidence	
4-2-1		[4.2] Acquiring Forensic Images and 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 and Forensic Techniques (I) - Program Analysis	
4-4-2			
4-4-3			
4-4-4			
4-5-1		[4.5] Analytical Procedures and Forensic Techniques (II) - Network Analysis	서비스 중단
4-5-2			
4-5-3			
4-6-1		[4.6] Analytical Procedures and Forensic Techniques (III) - Database Analysis	
4-6-2			
4-6-3			
4-6-4			
4-6-5			
4-6-6			
4-7-1		[4.7] Analytical Procedures and 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	서비스 중단
4-8-2			
4-9-1		[4.9] Keyword Analysis	
4-9-2			
4-10-1		[4.10] Internet Activity Analysis	서비스 중단
4-10-2			

Lesson	Course	Module	주요 사항
4-11-1		[4.11] Encryption and Stenography	
4-11-2			
4-11-3			
4-11-4			
4-11-5			
4-12-1		[4.12] Computer Security Ristks and Remedies	
4-12-2			
4-12-3			
4-12-4			
5-1-1	[5] Special Online Seminars	[5.1] Privacy and Data Protection	
5-1-2			
5-1-3			
5-1-4			
5-2-1		[5.2] Obscenity and Offensive/Racist Materials	
5-2-2			
5-2-3			
5-2-4			
5-2-5			
5-3-1		[5.3] Online Game and 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 and 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	
5-7-2			

나. 온라인 교육·훈련 프로그램 모듈별 구성내용

사이버범죄방지 가상포럼의 온라인 교육·훈련 프로그램은 2007년 시범사업으로 10개의 강좌를 제작한 것이 시작이다. 본격적인 프로그램은 2008년부터 4개년에 걸쳐 개발되었다. 그리고 2011년에 사이버범죄방지 가상포럼 웹사이트를 통해 공개되었다. 그러나 정보통신기술의 발달에 따른 사이버범죄의 급격한 변화에 신속히 대처하기 위해서는 3-4년에 걸쳐 완성된 교육과정이 시대적 흐름에 부합하지 않을 수도 있다. 이에 따라 2011년 까지 제작이 완료된 118개의 강좌에 대해서는 재검토가 이루어졌다.

다음은 한국형사정책연구원에서 외부 전문가를 활용해 강의의 시의성과 의미를 살핀 〈사이버범죄 방지를 위한 가상포럼 교육·훈련 프로그램 검토 결과보고서(2011)〉의 내용이다.

1) 모듈 0: 사이버범죄방지 가상포럼 교육·훈련 프로그램

모듈 0은 사이버범죄방지 가상포럼 사업의 일환인 온라인 교육·훈련 프로그램에 대한 소개 강의 1개와 초국가적인 사이버범죄에 따른 도전과제들과 해결책을 수개하는 강의 2개로 구성되어 있는 강좌이다. 커리큘럼의 구성 상 필요한 위치에 있으며 주제, 콘텐츠, 활용도 등 모두 매우 높은 것으로 평가되고 있다.

또한 초국가적인 사이버범죄에 따른 도전들과 해결책에 대한 강의(예: [0.2] Cybercrime in the global village(Ⅰ) 및 [0.3] Cybercrime in the global village(Ⅱ))의 경우 사이버범죄 방지를 위한 강좌를 시작하는 강의로 매우 적합한 것으로 검토되었다. 다만 본 강의에서 다루고 있는 사례는 이미 과거의 사례이며, 소셜네트워크서비스(Social Network Service, 이하SNS), 스마트폰 및 클라우드 컴퓨팅(Cloud Computing)[78]의 사용이 증가하면서 발생하고 있는 새로운 사이버범죄에 대한 내용이 추가될 필요가 있을 것으로 사료된다. 특히 최근 들어 대두되고 있는 사이버 공간에서의 기본권 인정과 관련한 문제가 추가적으로 다루어질 필요가 있다.

강사가 직접 촬영에 협조하여 완성된 모듈0의 경우 강의의 내용을 수정하는 것이 어려울 수 있을 것으로 간주되어, 새로운 강의를 신설하는 것을 고려해 볼 수 있다. 예를 들어, SNS, 스마트폰 및 클라우드 컴퓨팅 등에 대한 내용을 다루는 새로운 강의와 사이버 공간에서의 기본권 인정에 대한 강의를 신설하도록 해야 한다.

2) 모듈 1: 정보통신기술의 이해

모듈1은 정보통신기술의 이해를 다루는 강좌로, 정보통신기술 및 사이버범죄에

78) 기본 기능을 갖춘 단말기로 인터넷을 통해 운영체제와 응용프로그램등의 소프트웨어가 탑재된 중앙 컴퓨터에 접속, 언제 어디서든 컴퓨터 작업을 할 수 있는 기술이다. 2006년 9월 구글의 엔지니어인 크리스토프 비시글리아가 제안했다. 복잡하고 번거로운 일들을 더 이상 지상(개인 PC)에서 하지 않고 구름 위(중앙 서버)로 올려보낸다는 의미에서 이름 붙여졌다. 구글이 상용화를 준비중인 온라인 오피스(문서작업 소프트웨어)가 초보적인 단계의 클라우드 컴퓨팅이다. 문서를 인터넷을 통해 저장해 놓으면 휴대폰이나 컴퓨터 등 어떤 기기를 활용하든지 그 파일에 대한 접근이 가능하며, 동시에 여러 사람이 문서 작업에 참여할 수 있다. 한경 경제용어사전, http://dic.hankyung.com/apps/economy.view?seq=7890.

대한 전반적인 소개와 인터넷의 구조, 정보 격차, 정보통신기술의 취약성, 네트워크 보안, 해킹, 전자증거 등으로 구성되어 있다.

모듈1에 대한 전반적인 검토의견은 다음과 같다. 우선, 사이버범죄의 진화, 사이버범죄의 추세, 정보통신기술의 이해, 그리고 네트워크 보안에 대한 강의는 역시나 최근 발생하고 있는 SNS, 스마트폰 및 클라우드 컴퓨팅과 관련된 문제점들을 다루고 있지 않은 점이 공통적인 지적 사항으로 나타났다. 둘째, 강의의 순서와 관련한 의견도 있었다. 강의의 순서를 고려하였을 때, '인터넷의 구조'와 '정보격차' 및 '전자상거래'에 대한 강의는 사이버범죄를 설명하기 이전에 언급되어야 할 내용이기 때문에 순서상 앞으로 갈 필요가 있다. 즉, 이 개념은 사이버범죄를 이해하기 위한 선개념인 것이다. 셋째, 해킹에 대한 강의와 관련해서는 해킹에 대한 명확한 정의 및 구분에 의해서 해킹에 대한 내용들이 더 추가되어야 한다. 마지막으로, 내용의 중복성이 문제점으로 나타났다.

본 강좌가 정보통신기술 및 사이버범죄 소개를 큰 주제로 다루고 있고 이를 담당하는 강사들이 여러 명으로 구성되어 있다 보니 강사마다 사이버범죄의 특징에 대한 내용을 포함시키고 있다. 뒤의 강의에서 중복된 내용이 나오는 경우 같은 내용을 수정해야 할 것이다. 모듈1외의 다른 모듈에서도 비슷한 지적사항이 언급된 만큼 향후 강의를 수정할 시 이 부분을 면밀히 검토해야 하겠다.

3) 모듈 2: 사이버범죄 관련 법률의 이해

모듈 2는 '사이버범죄 관련 법률의 이해'라는 주제로 사이버범죄의 정의, 사이버범죄와 관련된 사법적인 이슈, 다양한 사이버범죄 유형(재산범죄, 전자상거래 및 전자뱅킹, 사이버테러리즘), 국내외 관련 관할권, 사이버범죄 방지를 위한 국제공조 및 법적 지원, 그리고 전자증거, 보존 및 증거 제시 등 총 16개 강의로 구성되어 있다.

모듈2에 대한 검토 의견으로는 앞에서 이미 언급되어 있듯이, 사이버범죄의 개념에 대한 강의에 SNS, 스마트폰 및 클라우드 컴퓨팅 등에 대한 최신 내용이 추가되어야 하는 지적이 또다시 나왔다. 또한 여러 강사들로 인한 내용의 중복 또한 지적사항으로 언급되었다. 특히 사이버범죄의 종류에 대한 강의(예:[24] Types of cybercrime - Cyber-property crimes (Ⅰ) 및 (Ⅱ), [2.5] E-commerce and e-banking crimes

(Ⅰ) 및 (Ⅱ), 사이버범죄 관련 국제협약 및 국내법과의 관계에 대한 강의, 그리고 디지털 증거, 보존 및 증거 제시에 대한 강의에서 중복되는 내용이 발견되었다.

강의 순서의 변경에 대한 의견도 나왔다. 사이버범죄와 관련된 사법적 이슈를 다루고 있는 강의(예: [2.2] Judicial issues in cybercrime)는 모듈 2의 흐름 상 사이버범죄의 정의와 유형 이후에 나오는 것이 적절할 것으로 사료된다. 또한, 현재 두 개의 모듈, 즉, [2.2] 및 [2.3] 으로 나누어진 본 강의는 하나의 강의로 제작해도 무관하며, 사법적인 개념에서 영미법에만 국한시킬 것이 아니라 대륙법적인 관점에서도 비교할 필요가 있다.

마지막으로 모듈 2의 후반부에 나오는 관할권과 관련된 강의와 사이버범죄 관련 국제협약 및 국내법 대한 강의는 전반적으로 강의 내용을 재구성할 필요가 있다. 강의 제목과 내용을 비교하였을 때 일치하지 않는 부분이 있는가 하면, 일부 내용에만 지나치게 치중하고 있어 포괄적인 내용을 담고 있지 않는 경우도 있기 때문이다.

4) 모듈 3: 사이버범죄 수사 – 절차 및 기술

모듈 3은 사이버범죄 수사기법에 대한 과정으로 컴퓨터 수사기법, 선진국들의 사이버범죄 수사 시스템 및 절차, 디지털 증거의 원칙, 습득 및 보존, 사이버범죄 및 수사기법의 방법, 네트워크 보안, 사이버범죄에 대한 사건·사고 대응팀 등 총 34개 강의로 구성되어 있다. 모듈3에 대해서는 다음과 같은 의견이 제시되었다.

2009년에 제작된 모듈 3의 강의들은 대다수 2000년대 초부터 2008년까지의 통계자료와 관련 자료를 활용하였다. 그러하므로 강의 제작 후 2년이란 시간이 흘렀기 때문에 최신의 자료로 업데이트하여 수강생들에게 더욱 정확한 정보를 제공해줄 필요가 있겠다.

사이버범죄 수사기법의 방법에 관한 강의에서는 각 범죄분야에 대한 범죄유형과 대응방법을 제시하고 있다. 하지만 각 범죄유형에 대한 일반론, 종류 및 사례 소개 등의 내용에 치중하고 있어 오히려 형사사법 기관에서 실무에 적용하기에는 유용한 정보를 제공하고 있지 못하다. 네트워크 보안에 대한 강의 역시 개념적 이해와 구성의 종류 등에 대한 단면적 설명에 치중하고 있기 때문에 실무에서 적극 활용하기에는 충분한 정보를 제공해 주지 못하고 있다. 따라서 형사사법 기관에서 실무적으로 활용

가능한 방향으로 대응방법에 대한 내용을 추가 보완할 필요가 있다.

모듈 3의 기타 의견으로는 일부 강의, 특히 사이버범죄의 수사 기법(Modus Operandi of cybercrime and investigation technique) 강의와 관련해서 강의 주제에 부합하게 수사의 기술적·법적 대응방안 등에 대한 설명이 보완될 필요가 있겠다는 의견이 제시되었다. 또한 일부 강의에서 참고문헌을 그대로 인용하는 부분이 있는데, 출처를 밝혔어도 용인될 수 있는 적정 수준에서 인용을 하도록 내용을 정정할 필요가 있는 것으로 사료된다.

5) 모듈 4: 사이버범죄 수사 - 디지털 포렌식

모듈 4는 사이버범죄방지 가상포럼 온라인 교육·훈련 프로그램의 고급과정으로 본 프로그램에서 가장 복잡하고 어려운 강좌에 해당된다. 특히, 디지털 포렌직을 대주제로 다루고 있는 만큼 실무에서 실질적으로 활용되는 사이버범죄 수사기법을 제시하는 강좌이다. 모듈 4는 디지털 포렌식의 기본 개요부터 전자증거의 보관과 추출, 데이터베이스를 통한 정보 분석, SQL Injection 공격, 전자증거 분석, 이메일 수사, 키워드 분석, 암호학, 컴퓨터 보안 위험 및 대처 등 총 30개 강의로 구성되어 있다.

정보통신기술의 급속한 발전으로 인해 모듈 4 역시 최신 기술의 내용을 포함해야 한다는 의견이 제시되고 이쌀. 예를 들어, 전자증거와 이메일 수사 등과 관련한 강의(예: [4.1] Understanding and applying the rules of digital evidence 및 [4.8] Email investigation)의 경우 Twitter, Facebook, Myspace와 같은 SNS에 대한 연결 구조뿐만아니라 클라우드 서비스에 대한 내용도 포함시켜야 할 것이다.

모듈 4에서 두드러지게 나타난 의견은 웹브라우저를 이용한 수사기법에 대한 설명에서 유독 Internet Explorer(IE)에서의 사용만을 제시했다는 점이다. IE 외에도 해외에서 많이 사용되고 있는 Chrome, Firefox와 같은 웹브라우저에 대한 내용을 포함시켜야 수사하는데 있어서 그 활용도를 더욱 높일 수 있을 것으로 사료된다. 특히 디지털 증거, 이메일 수사, Internet Activity 분석에 대한 강의 (예: [4.1] Understanding and applying the rules of digital evidence, [4.7] Analytical procedure and forensic techniques(Ⅳ), [4.8] Email investigation 및 [4.10] Internet activity analysis)에서 이런 언급이 주로 나타났다.

그 외의 주요 의견으로는 다음과 같다. 네트워크 분석에 대한 강의(예: [4.5] Analytical procedure and forensic techniques(Ⅱ) - Network anaylsis)의 경우 기술적·실무적으로 사용하기에는 활용도가 떨어지게끔 제작되어 있다. 실무에서 활용할 수 있도록 절차적으로 해야 할 부분과 역할에 대해서 기술을 해야 할 것이다.

디지털 증거 분석과 관련된 강의(예: [4.7] Analytical procedure and forensic techniques (Ⅳ) - Digital evidence analysis) 중 EnCase[79]와 관련된 강의는 전반적으로 재구성해야 할 필요가 있다. 가장 기본적인 내용으로 왜 EnCase를 사용하는지부터 시작하여 형사사법 및 수사 실무에 있어서 실질적으로 활용할 수 있도록 분석기법을 설명해야 할 필요가 있으며, 시나리오 몇 가지에 대한 실제 분석과정을 보여주는 방법으로 본 강의를 재구성할 필요가 있다.

사이버 상에서 다루어지고 있는 암호학과 관련된 강의(예: [4.11] Encryption and stenography)에서는 단순히 암호학에 대한 이해와 설명에 비중을 두기 보다는 이것이 범죄에 어떻게 사용되고 활용되고 있는지를 보여주는 것이 더 바람직한 것으로 사료된다. 따라서 암호학에 대한 강의를 전반적으로 재구성하여 틀을 다시 잡을 필요가 있다.

6) 모듈 5: 온라인 세미나 – 이슈·주제

마지막 모듈인 모듈 5는 고급과정에 속해있는 강좌이며 사이버범죄와 관련한 특별주제에 대한 강의들로 구성되어 있다. 모듈 5는 주로 프라이버시 및 데이터 보호, 음란물 및 공격성/인종 차별 관련 자료, 온라인 게임 및 도박, 무선기술의 잠재적 위협의 평가, ID 절도 및 온라인 사기, 사이버범죄의 도전 등 총 21개의 강의로 구성되어 있다. 본 모듈에 대해서도 앞의 모듈들과 전반적으로 유사한 검토의견이 나타났다.

우선 일부 강의에서는 최근의 현상으로 다양한 SNS를 이용한 사이버범죄 현상에 대한 내용을 포함해야 한다는 의견이 나왔다. 오래된 통계자료를 사용한 강의에서는 최신의 자료로 업데이트를 해야 한다는 비슷한 의견들도 제시되었다. 또한 강의 내용이 형사사법 기관 등 수사 실무 측면에서 유용성을 제공하는 방향으로 내용을 개선해

79) 디지털 포렌식에서 사용되는 데이터 복구 등을 지원하는 제품. 디지털 포렌식 전문가에게 반드시 필요한 소프트 웨어. 관련 서적은 다음을 참조. Bunting, Steve, and William Wei. “EnCase Computer Forensics.” (2007).

야 한다는 의견과, 실무에 실질적인 도움을 줄 수 있는 구체적인 전략과 방안을 제시하여 교육·훈련 프로그램의 활용도를 높여야 한다는 지적도 나왔다.

프라이버시 및 데이터 보호와 ID절도 및 온라인 사기에 대한 일부 강의에서는 내용이 초급과정 수준이라는 지적도 나왔다. 모듈 5가 고급과정에 포함되어 있는 만큼, 해당 강의에 대한 내용도 단순한 개념 설명이나 기초적 사항에 머물 것이 아니라 사례 분석 등을 통한 실무에서의 활용을 고려하여 내용을 고급화할 필요가 있다. 음란물 및 공격성·인종 차별 관련 자료에 대한 강의와 ID절도 및 온라인 사기에 대한 강의에서는 전반적인 강의의 구성과 내용을 개선해야 한다는 의견이 나왔다. 현재 위 강의의 내용은 일반적인 내용에만 초점을 두어 내용이 부실한 상태이고 강의 내용이 강의명과 상이한 부분이 있어 강의를 재구성해야 할 필요가 있다.

다. 온라인 교육·훈련 프로그램 평가

위의 모듈별 구성 내용 소개 및 검토 결과에서 보듯 사이버범죄의 급속한 변화와 그 초국가적인 특성을 고려할 때 시의성과 실무에의 적용 등에 대한 재검토가 필요하다. 검토 결과 보고서(2011)에서 공통적으로 지적된 내용을 정리하면 다음과 같다.

첫째, 최근 스마트 폰의 보급 등으로 사용자가 급격히 증가한 SNS, 클라우드 컴퓨팅 등에 대한 기본적인 이해를 돕고, 이를 악용한 범죄 사례 소개 및 범죄 활용 가능성과 수시 기법에 대한 내용을 포함해야 한다.

둘째, 강의 순서의 변경이 필요하다. 현재 온라인 교육·훈련 프로그램의 커리큘럼은 국내외 사이버범죄 분야의 학자 및 실무가로 구성된 자문위원에 의해 완성되었음에도, 강의 구성 변경 혹은 순서 변경의 필요가 있다. 예를 들어 한 주제에 관한 여러 개의 강의는 내용의 재구성이 필요하다.

셋째, 강의의 중복성이 있다. 그러나 입문과정만 수강하는 경우 혹은 입문과정을 듣지 않고 고급과정부터 수강하는 경우가 있기 때문에 현재 단계에서는 강의를 수정할 필요는 없다.

넷째, 고급과정의 디지털 포렌식 수사 기법과 관련한 강의에서 활용 가능한 웹브라우저의 다양성이 필요하다.

마지막으로 기술적·실무적 활용도가 떨어진다. 디지털 포렌식을 다루는 강의는 법집행 공무원들이 사이버범죄를 수사하는데 있어서 배운 기술을 실무에서 바로 활용할 수 있도록 하는 것이 매우 중요하다.

2. 온라인 교육·훈련 프로그램 활용 사례 평가

온라인 교육·훈련 프로그램의 시범 사업은 2008년 6월 입문과정 모듈 1의 강의 내용에 대해 베트남 공안부의 경찰총국 실무자를 대상으로 시행되었다.[80] 또한 2010년 8월 온라인 교육·훈련 프로그램을 공식 오픈한 후, 2013년 3월까지 우선 시범사업 대상 국가인 아시아·아프리카·중남미의 국가를 대상으로 시범강의와 입문과정을 제공했다.[81]

그러나 2013 UN·국제협력사업 성과보고서와 2014년 UN·국제 교류협력 사업 보고서에서는 그 성과에 대해서는 부정적 평가를 내렸다. 먼저, 케냐에서 진행된 시범사업의 경우 시범 프로그램의 실용성에 부정적인 결론을 내렸다. 다음은 2013년 평가 내용이다.

시범 프로그램은 온라인 사이버범죄 교육·훈련 프로그램과 오프라인 프로그램이 혼합된 형식으로, 개도국의 역량 강화를 위한 프로그램의 효과성을 평가하기 위하여 케냐에서 시행되었다. 그러나 오프라인 워크숍과 병행되는 온라인 교육훈련 프로그램의 효율성에 대한 피드백을 얻기 위해 운영되었던 시범 프로그램은 안타깝게도 프로그램의 시행 과정에서 있었던 어려움으로 인해 제 기능을 다하지 못했다.[82]

2014년도 같은 평가를 하며 2013년 3월 태국 법무부 소속 6명의 온라인 교육·훈련 프로그램 이수 이후 프로그램을 일시 중단함을 밝혔다. 다만 사이버범죄방지 가상포럼 홈페이지를 통해 온라인 강의 입문과정은 수강할 수 있게 하였다.[83]

---

80) 연성진 외 4인, 유엔 및 국제협력백서, 한국형사정책연구원, 2009, 18쪽 요약.
81) 장준오, 이윤미, 유엔협력사업·국제교류협력사업, 한국형사정책연구원, 2011, 49쪽; 김은경 외 9인, 2012유엔·국제협력사업 성과보고서, 한국형사정책연구원, 2012, 255-256쪽; 장준오 외 8인, 2013UN·국제협력사업 성과보고서, 한국형사정책연구원, 2013, 114-115쪽; 김지영 외 10인, UN·국제 교류협력 사업 보고서, 한국형사정책연구원, 2014, 182쪽 요약.
82) 장준오 외 8인, 2013UN·국제협력사업 성과보고서, 한국형사정책연구원, 2013, 114쪽.
83) 김지영 외 10인, UN·국제 교류협력 사업 보고서, 한국형사정책연구원, 2014, 182쪽.

이에 따라 2015년 11월 현재, 위의 〈표 4-1〉과 〈표 4-2〉의 서비스 제공이라 별도 표시한 강의만이 접속 가능하다.

3. 온라인 교육·훈련 프로그램 활용 방안 제언

사이버범죄방지 가상포럼 웹사이트는 사이버범죄 관련 동향 제공, 사VFAC 리뷰 발행 등으로 다양하게 활용되고 있다. 시의성과 실효성 등에서 아쉬운 점이 있지만, 사이버범죄방지 가상포럼의 온라인 교육·훈련 프로그램도 발전적인 재편과 재활용이 가능할 수 있다.

그 첫 번째 방안은 앞서 언급된 온라인 강의 신규 제작과 추가 번역 등으로 문제점들을 보완하는 것이다. 2011년 사이버범죄 방지를 위한 가상포럼 교육·훈련 프로그램 검토결과보고서에 참여한 전문가들의 제언내용을 정리하면 다음과 같다.

커리큘럼을 수정·보완하는 작업을 시작으로 추가 강의제작을 위한 작업과 일부 강의의 수정 작업에 착수해야 할 것이다. 이를 위해 국내외 사이버범죄 전문가들에게 사이버범죄방지 가상포럼 온라인 강의 커리큘럼을 화정하는 작업을 우선적으로 진행해야 할 것이다. 그리고 확정된 커리큘럼을 토대로 강사로 참여할 전문가 풀을 구성하여 강사 섭외 및 계약진행, 강의 제작에 착수해야 한다.

그리고 두 번째 방안은 기존 온라인 교육·훈련 프로그램 중 시의성이 떨어지는 부분을 제외하고, 그 실효성을 높이는 방안을 찾는 것이다. 두 번째 방안에 대해서는 그 동안 온라인 강의를 제작하며 쌓은 네트워크, 경험, 인력 풀 등을 사용하여 오프라인 교재화가 제안되었다. 또한 해당 교재를 대학 강의 등에 사용함으로서 동북아 지역 내 사이버안전 협력체제 발전의 기초로 활용하는 방안이 논의 되었다.

제2절 온라인 교육·훈련 프로그램 교육 교재 활용방안

1. 오프라인 교육을 위한 교재화

가. 강의 교재화 배경 및 목적

앞서 다루어진 것처럼 사이버범죄방지 가상포럼 온라인 교육·훈련 프로그램의 발

전적 재편 방안으로 오프라인 강의 중 실용성이 있는 내용과 주제 강의를 선별하여 교재화 하는 작업이 이루어졌다.

이를 통해 사이버범죄와 관련된 교육의 교재로 활용할 예정이다. 강의교재는 온라인 교육·훈련 프로그램을 기본으로 하고, 추후에는 현재의 상황에서 발생하는 사례 등을 선별하여 추가로 포함할 예정이다.

이를 위해 현재 본 연구원 웹사이트에서 서비스를 제공하고 있지는 않지만 이미 국/영문 번역작업을 마친 강의 스크립트 전문을 사용하였다. 각 과정별 모든 모듈을 검토하였으며, 부족한 부분의 내용은 교재에 부가적인 설명을 통하여 설명하였다. 또한 교재 내에 워크북 및 강의 내용 정리를 포함하여 온라인 및 오프라인 강의를 동시에 진행할 수 있도록 구성하였다.

나. 온라인 교육·훈련 프로그램 활용

강의 교재는 총 10차시로 구성하였다. 전체 모듈 중 필요한 내용과 주제에 따라 강의 회차에 따른 교재 구성 내용도 달라졌다. 또한 강의 내용에 필요한 사이버범죄방지 가상포럼 강의는 순서에 맞게 녹화하여 수강할 수 있게 하였다.

올해 온·오프라인 강의를 위한 교재는 국/영문으로 제작하고 국내에서 파일럿 프로그램을 통해 적용한 후 평가를 통해 수정 및 개선 작업을 진행 할 예정이다. 이를 바탕으로 개발도상국의 대학 및 형사사법기관 등에서도 강의 교재로 쓰일 수 있는 교재로 활용할 것이다. 따라서 추후 해당 교재를 해당 나라에 적합한 언어로 바꾸는 작업이 필요할 것으로 기대된다.

다. 강의 교재 구성

강의 교재를 위한 작업은 고려대 사이버법센터에서 진행하였고, 본 연구원에서 감수를 진행했다. 현재 강의 교재에서 사용된 사이버범죄방지 가상포럼 온라인 교육·훈련 프로그램은 다음과 같다.

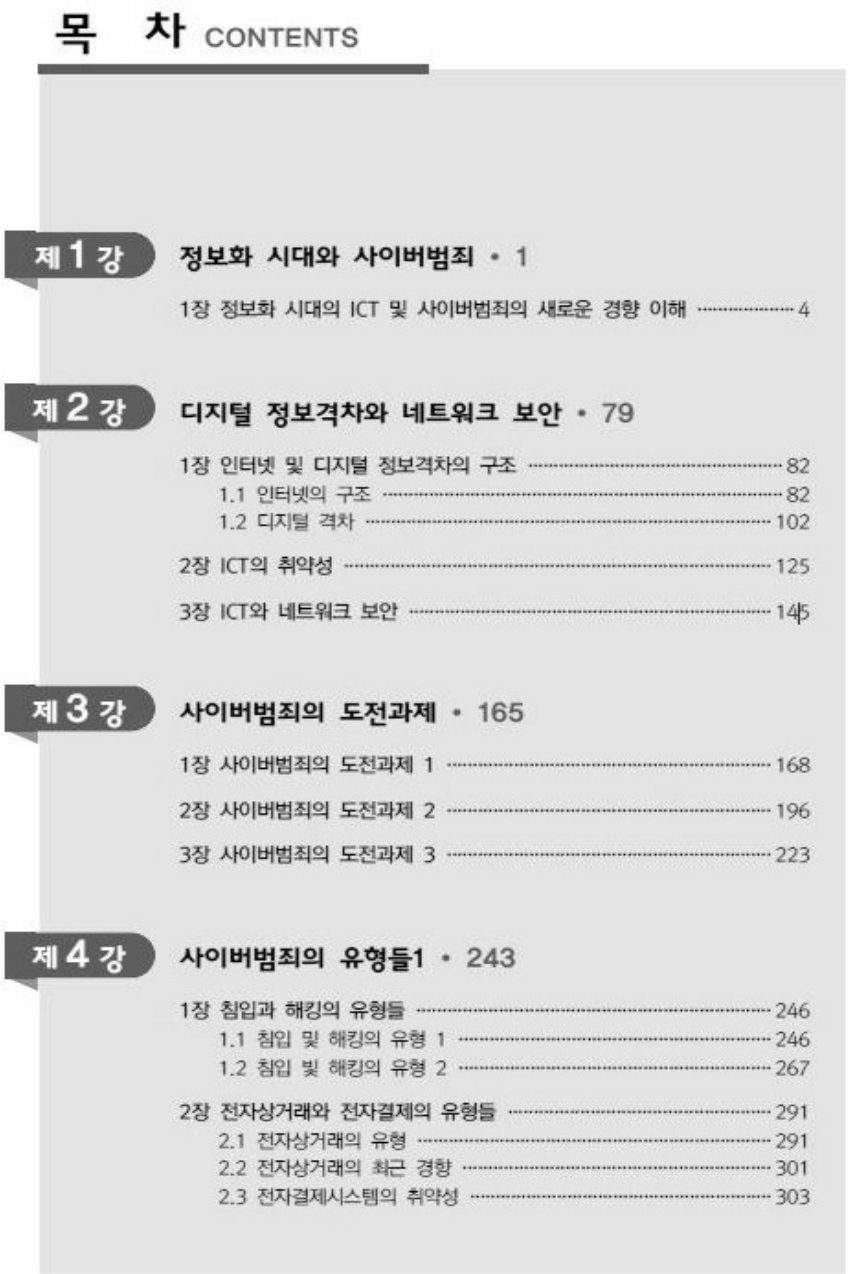
〈표 4-3〉 강의 교재에 사용되는 사이버범죄방지 가상포럼 온라인 교육·훈련 프로그램

강의 회차	해당 사이버범죄방지 가상포럼 온라인 교육·훈련 프로그램
제1강	1.1 Understanding emerging trends in ICT & cybercrime in the information age(총82분 33초)
제2강	1.2 Structure of the Internet & digital divide(총 45분 59초) 1.3 Vulnerabilities of ICT(총 24분 40초) 1.4 ICT & network security(총 21분 47초)
제3강	5-6-1 The Challenge of Cybercrime 1 5-6-2 The Challenge of Cybercrime 2 5-6-3 The Challenge of Cybercrime 3
제4강	1.5 Forms of intrusion & hacking(총 46분 28초) 1.6 E-commerce & forms of electronic payment(총 23분 51초)
제5강	3-6-1 Cyber Stalking: Criminal Patterns and Countermeasures(총 30분 29초) 3-6-2 Cyberbullying(총 33분 12초) 3-6-3 Electronic Vandalism Criminal Patterns and Countermeasures(총 22분 20초)
제6강	5-2-1 Online pornography&Criminal conspiracy in website 5-2-2 Suicide website&Bomb/weapons manufacturing website 5-2-3 Legal and institutional countermeasures& Technical countermeasures 2.2 Judicial issues in cybercrimes(I)(총 15분 50초) 2.3 Judicial issues in cybercrimes(II)(총 23분 53초)
제7강	2.6 Types of cybercrimes (III) – Cyber-terrorism(총 61분 15초) 5-7-1 Profiling Hackers
제8강	2.11 Digital evidence, preservation & presentation of evidence for non-forensic Specialists(총 34분 22초) 3.9 Preservation & presentation of digital evidence
제9강	2.7 Jurisdiction – the roles of national & international law enforcement(총 26분 44초) 2.8 International cooperation in the control of cybercrime(총 57분 38초)
제10강	2.9 Compatibility of international conventions on cybercrime with domestic laws(총 30분 05초) 2.10 Mutual legal assistance: methods & problems – Procedures & practices of online cooperation for law enforcement agencies(총 56분 7초)

표에서 보는 것과 같이 강의의 순서와 내용에 따라 현재 사이버범죄방지 가상포럼 온라인 교육·훈련 프로그램의 강의 모듈을 재편성하였다. 각 과정별로 적어도 1개에서 5개의 모듈을 포함해 총 25개의 모듈이 활용되었다.

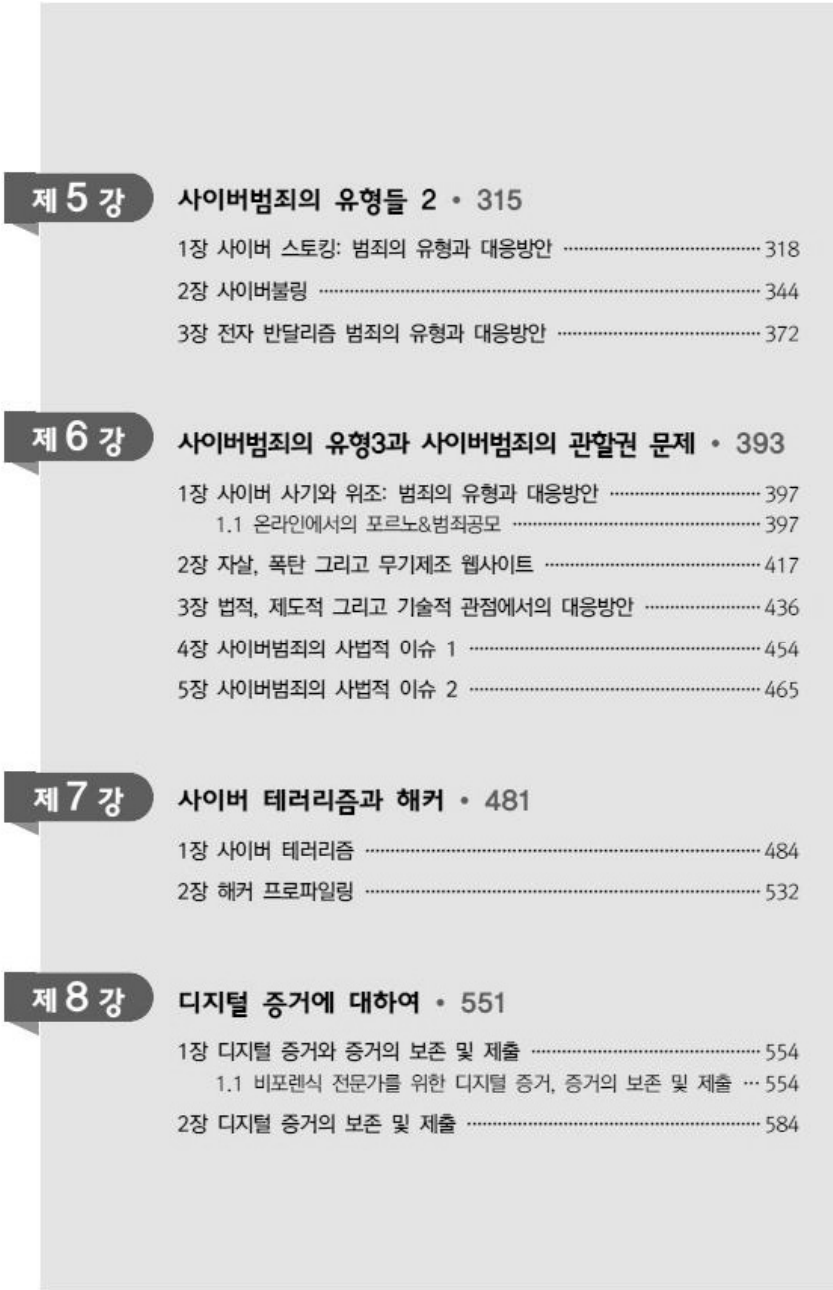
각 강의는 90분가량 진행 된다. 또한 필요성에 따라 대학 교재 등으로 활용할 예정이지만 시의성 및 기술 발달에 따른 범죄 동향의 변화로 고급 과정 및 세미나 과정에 포함된 모듈을 활용하기도 하였다.

이를 토대로 구성한 강의 교재의 목차는 다음과 같다.

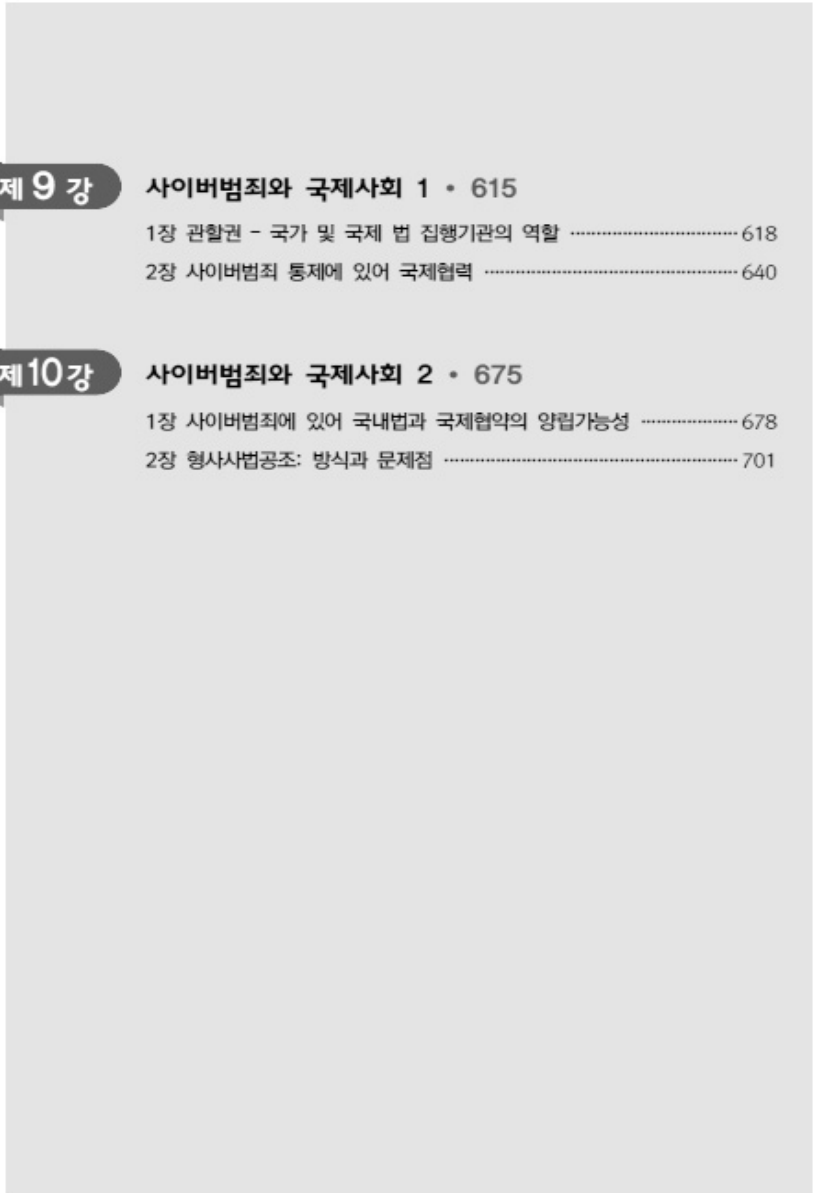


목 차 CONTENTS

[그림 4-1] 사이버 범죄의 이해- 목차 1



[그림 4-2] 사이버범죄의 이해- 목차 2



[그림 4-3] 사이버범죄의 이해- 목차 3

또한 교재 디자인 면에서는 향후 강의에 활용할 것을 감안하여 필기를 할 수 있도록 메모 공간을 따로 구성하고, 매 장이 끝나면 그 장을 정리하는 페이지를 삽입하였다.

MEMO

2 The Evolution of Cybercrime (사이버범죄의 발전) 요약

- 정보 격차(digital divide)는 국가 간 뿐 아니라 국내에서도 차이가 있음. 중국의 경우 단일 인구 집단으로는 인터넷 사용자 수가 최대이나 15%의 가정에서만 인터넷 이용이 가능. 정보 격차로 인하여 일부 국가들은 사이버 범죄 대응에 있어, 사법적인 대응책이 발전이 되지 않은 경우도 있음.
- 사이버 범죄의 공격유형(Cybercrime offences)은 다양함. 이동 통신 시스템을 통해 작동되는 각종 디지털 제품이나 이메일 및 통신 상품에 대한 침해 행위, 아시아 일부 지역에 있어서는 저작권 침해, 페이스북 등의 출현으로 인한 사이버 스토킹 및 사이버 불링(cyber bullying)과 같은 개인 간에 일어나는 위법행위, 전자적 반달리즘(electronic vandalism), 사이버 테러리즘, 대형 범죄 집단의 서비스 거부 공격, 선금사기(advance fee frauds), 신원도용, 어린이포르노그래피 등과 같은 콘텐츠 범죄(content crime)가 있음.
- 사이버 범죄는 많은 사법 관할권에 걸쳐 있기 때문에 기소가 어려움. 달리 말해 위법행위의 모든 요소가 같은 사법관할권에 있는 것은 아님. 위법행위를 성공적으로 수사, 기소하기 위해서는 경찰 기관과 사법기관 간에 상호협력 및 법적조력이 가능한 빠른 시간 내에 이루어져야 함. 이는 위법행위가 사공간을 넘나들며 순식간에 일어나기 때문.
- 미국 버라이즌(Verizon)의 연구에 따르면 데이터 파괴의 9%는 실제 컴퓨터 시스템에 대한 물리적 공격에 의한 것으로 확인됨. 그러나 사이버 범죄자의 2/3는 비물리적 공격인 해킹을 선호. 즉, 해킹은 컴퓨터에 접근하는 중요한 방법이며, 상업적 이익과 연결된다는 것. 상당한 데이버 위반은 기업에서 사회 공학적 기법으로 부르는 기술과 연관되어 있는데, 그 기술은 컴퓨터 침입이나 해킹을 할 필요 없이 비밀번호를 넘겨줄 수 있는 직원들을 유혹하는 것과 같은 방법이 있다는 것을 강조함.
- 증가하고 있는 위법 행위 중에는 신용사기 또는 사기 및 피싱(phishing)이 있음. 미국 인터넷 범죄 신고 센터(Internet Crime Compaint Center)에서는 신고 된 사건 중 1/4 이상의 사건이 사기와 관련되어 있었음. 주로 이베이(e-bay)와 같은 온라인 경매 사이트에서 발생하며, 흥미로운 것은 신고 된 전체 손실 금액이 신고 범죄에 따른 예상치 보다 낮은 수준의 금액이라는 것.

[그림 4-4] 메모 및 요약

강의 교재 1차 제작분은 파일럿 프로그램용이며, 2015-2016 겨울 계절학기 혹은 2016년 봄 정규학기에 사이버범죄 관련 강의에 사용할 수 있을 것으로 기대된다.

2. 월드뱅크 툴킷 프로그램 기여

가. 월드뱅크 툴킷 소개

월드뱅크(World Bank, 혹은 세계은행)는 극심한 가난 퇴치와 세계 번영을 추구를 사명으로 하는 국제개발기구[84]로서, 세계 각국 및 저개발국의 주요 인프라 건설을 위한 투자를 관리하는 수탁자의 의무(fiduciary obligation)[85]를 지닌다. 월드뱅크는 사이버범죄가 지속적이고 건전한 개발과 성장에 미치는 영향을 이해하며, 따라서 사이버범죄에 대한 위험 평가 및 적절한 대응의 중요성을 인식하고 있다.[86]

이러한 인식아래 월드뱅크가 한국 정부의 지원으로 새롭게 시작한 프로젝트가 월드뱅크 툴킷 프로젝트다. 영문 공식 명칭은 Toolkit on Best Practice in Policy/Legal Enabling Framework and Capacity Building in Combatting Cybercrime(툴킷 프로젝트)이다. 월드뱅크가 본 프로젝트를 추진하는 이유 중 하나는 부작위로 발생하는 위험(risk of doing nothing)을 방지하기 위함이다.

툴킷 프로젝트는 2014년 7월부터 2년간 진행 계획이며 사이버범죄와 관련된 지침서를 작성하는데 그 목표가 있다. 국제사회의 범죄 및 수사 관련 기관 등 다양한 조직이 참여하고 향후 정책 입안가, 국회의원, 검사, 수사관, 시민사회 등이 사이버범죄 퇴치에 있어 정책, 특히 법률적 및 형사정책적인 역량을 강화하는데 기여하고자 하는 목적을 갖고 있다. 그 방법으로 사이버범죄 대응과 관련된 모범사례를 정리하여

---

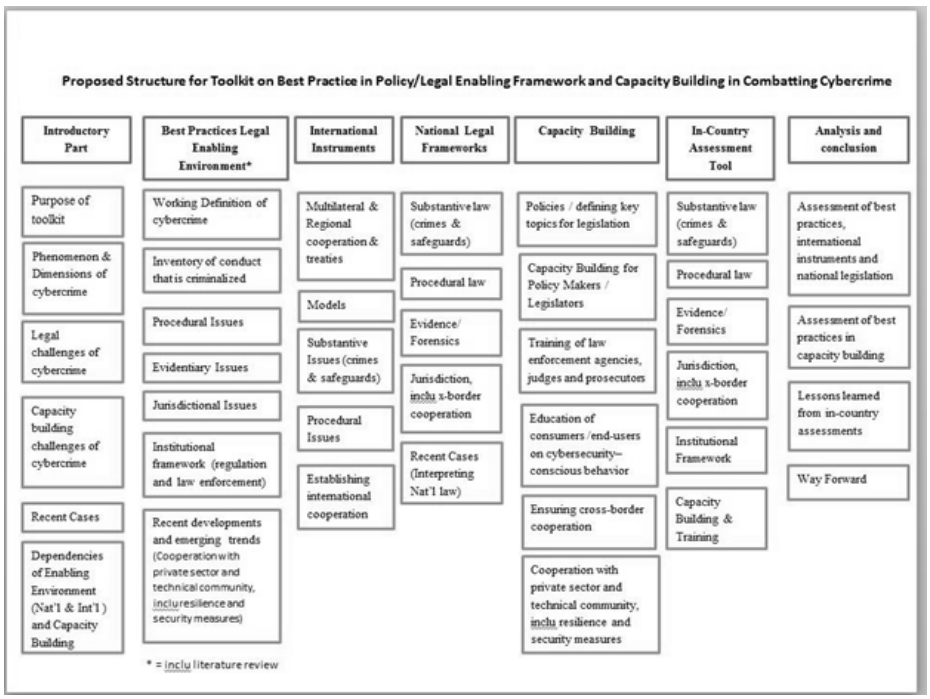
84) 월드뱅크 홈페이지, http://www.worldbank.org/en/news/feature/2013/04/17/ending_extreme_poverty_and_promoting_shared_prosperity

85) 월드뱅크 파견 정진용 검사는 제13차 유엔 범죄방지 및 형사사법 총회 워크숍3 발표문에서 수탁자의 의무에 대해 다음과 같이 설명했다. "경제 개발 사업에서 정보통신 및 기타 주요 인프라와 서비스를 담당하는 자본 보유기관으로서 회원국의 적절한 사이버 위협 대처능력 개발을 보장하는 의무를 말한다(Financier of essential communications and other critical infrastructure, services and applications in economic development projects; to ensure that our clients appropriately address cyber risks)", 정진용, 제13차 유엔 범죄방지 및 형사사법 총회 워크숍3 〈월드뱅크 프로젝트 – 사이버범죄 퇴치: 신흥 경제성장국가를 위한 도구와 역량 강화〉 발표자료.

86) 정진용, 제13차 유엔 범죄방지 및 형사사법 총회 워크숍3 〈월드뱅크 프로젝트 – 사이버범죄 퇴치: 신흥 경제성장국가를 위한 도구와 역량 강화〉 발표자료.

하나의 책으로 출판하고자 한다.

2015년 툴킷 프로젝트 진행상황은 다음과 같다. 각 협력 기관별 기여 가능 부분에 대한 조사를 마치고 역할 분담을 완료하였으며, 기존 사이버범죄 측정 및 평가 지침에 관한 비교분석과 국가별 사이버범죄 법률 파악도 완료하였다. 2015년 6월까지 지침서 초안 작성을 위한 서식을 마련하고, 일정 분야는 초안 작성을 시작하고 협력 기관에서 검토를 진행한다. 지침서 서식은 주요 개념, 현황 분석, 모범사례, 결론 및 권고의 틀을 따를 것이다. 2015년 9월까지는 지침서의 각 부문의 개발을 완료하고 초안을 토대로 편집을 시작한다. 이 작업이 끝나면 2016년 6월 시범국가에 적용하고 프로젝트를 마무리하게 된다.



[그림 4-5] 월드뱅크 툴킷 프로젝트 구성안

나. 형사정책연구원의 역할

본 연구원은 월드뱅크, 대검찰청, 유엔 지역간 범죄 및 사법 연구소(United Nations Interregional Crime and Justice Research Institute, UNICRI)와 공동으로 월드뱅크 툴킷 작성에 참여한다. 담당하고 있는 부분은 총 9개 부분으로 법제도를 뒷받침하는 환경에 관한 사례를 다루는 2장에서 4부분, 국가별 법체제를 다루는 4장에서 4부분, 역량강화를 다루는 5장에서 1부분이다. 상세 내용은 다음과 같다.

〈표 4-4〉 월드뱅크 툴킷 프로젝트 중 형사정책연구원의 역할

목차	
II 법제도를 뒷받침하는 환경	B. 범죄화 대상 행위
	C. 절차관련 문제
	D. 증거관련 문제
	F. 제도의 틀 (규제와 법 집행)
IV 국가별 법체제	A. 실체법(범죄와 범죄방지)
	B. 절차법
	C. 증거/포렌식
	D. 국경 간 협력을 포함한 관할권
V 역량 강화	C. 법집행기관, 판사 및 검사 교육·훈련

다. 사이버범죄방지 가상포럼 온라인 교육·훈련 프로그램 활용

월드뱅크 툴킷 프로젝트 작성과 관련하여 형사정책연구원은 참여를 제안받았다. 이에 기존의 사이버범죄방지 가상포럼 온라인 교육·훈련 프로그램을 활용해 참여하게 되었다.

그러나 이를 위해 관련 강의를 살펴본 결과 국가별 모범사례를 집대성한다는 취지의 월드뱅크 툴킷 프로젝트를 위한 초안 작성에 부족한 부분이 있을 수 있다고 판단했다. 사이버범죄방지 가상포럼의 강의 내용과 그 목적은 개도국 법 집행 및 수사 기관에 사이버범죄에 관한 교육·훈련 제공으로 그들의 수사 등 역량강화를 돕는 것이다. 따라서 모범사례를 다루기보다는 사이버범죄별 개념 설명 등을 다루고 있다. 이 때문에 툴킷 작성의 목적에 부합하지 않을 가능성이 있다고 보았다.

하지만 Ⅱ장 법제도를 뒷받침 하는 환경 F. 제도의 틀 (규제와 법 집행), Ⅳ장 국가별 법체제 D. 국경 간 협력을 포함한 관할권, Ⅴ장 역량강화 C. 법집행기관, 판사, 및 검사 교육·훈련에 관해서는 툴킷 초안 작성에 활용할 강의가 있는 것으로 판단했다. 따라서 이와 관련된 초안 작성에 참여하여 월드뱅크의 툴킷 프로젝트에 기여할 것으로 기대한다.

라. 월드뱅크 툴킷 초안

1) Ⅳ장 국가별 법체제 D. 국경 간 협력을 포함한 관할권

The Roles of National and International Law Enforcement

1. Statement of the Issue

Many area of illegal and harmful behaviors in the cyberspace are not being adequately addressed by the official criminal justice system including the police, courts, prisons, and probation and parole systems.

A. Concept and Types of Cybercrime and Computer Crimes

Most people are confused about the difference between cyber-crime and computer crime. In fact, some cybercrime authors do not appropriately separate the use of the terms.

Casey (2001) defines cybercrime as "any crime that involves computers and networks, including crimes that do not rely heavily on computers" (p. 8). Thomas and Loader (2000) also note that cybercrime is "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks" (p. 3). Basically, cybercrimes cover wide categories of crime in cyberspace or on the World Wide Web including, "computer-assisted crimes" and "computer-focused crimes" (Furnell, 2002, p. 22).

In general, special computer operating skills are not required to commit cybercrime. For example, a suspect and a victim may communicate via Web based chat-rooms, Microsoft Network messenger (MSN), or e-mail. Once the criminal gains the potential victim's trust, the criminal is in the position

to commit a crime against the victim. In this case, even though the Internet probably assisted the suspect in communicating with the victim, it does not mean that the technology or the Internet caused the crime (Casey, 2000). Indeed, in computer-assisted crimes, a computer does not have to play a major role in the crime.

It can merely be the tool that is used by the suspect that assists in facilitating the eventual offense such as in the case of fraud or in a confidence scam.

While, computer crime is a violation of law involving a computer, according to Casey (2000), the more general term cybercrime can be contrasted with computer crime or computer-focused crime, special types of cybercrime. Specifically, these refer to a limited set of crimes that are specially defined in laws, such as the US Computer Fraud and Abuse Act and the UK Computer Abuse Act. These crimes include theft of computer services; unauthorized access to protected computers; software piracy and the alteration or theft of electronically stored information; extortion committed with the assistance of computers; obtaining unauthorized access to records from banks, credit card issuers, or customer reporting agencies; traffic in stolen passwords and transmission of destructive viruses or commands. (pp. 9-10)

These computer crimes require more than a basic level of computer-operating skill for offenders to commit these crimes successfully against the victims. In fact, offenders who commit a cybercrime or a computer crime are both contacting this new place, cyber-space, which is a realm different from the physical world, and which has different jurisdictions and different laws that we can apply.

2. Statement of Constituents of Good Practices (cross references to other sections)

It is importanat to introduce the concept of routine activities theory, which may help you better understand the nature of cyber-space and jurisdiction issues.

In 1979, Cohen and Felson proposed their routine activities theory, which focused mainly on opportunities for criminal events. Cohen and Felson

posited that there are three major tenets that primarily affect criminal victimization. The main tenets are (a) motivated offenders, (b) suitable targets, and (c) the absence of capable guardians against a violation. The criminologists argued that crime is likely to occur via the convergence of the three tenets. In other words, lack of any of the suggested tenets will be sufficiently capable to prevent a crime occurrence.

Other criminologists, namely Akers (2004) and Osgood et al. (1996) noted that routine activities theory suggests that most crimes are associated with the nature of an individual's daily routines based on sociological interrelationships; thus, illustrating that crime is based on situational factors which enable the criminal opportunities.

Cohen and Felson (1979) emphasized the importance of "the spatial and temporal structure of routine legal activities" that facilitates an interpretation of how criminals take opportunities to transfer their criminal inclinations into criminal acts (p. 592). In other words, an individual's daily activities in a social situation produce certain conditions or opportunities for motivated offenders to commit criminal acts. Utilizing burglary as an example, frequent social activities away from home can facilitate increasing criminal opportunity, as the absence of a capable guardian at home is likely to make household property a suitable target (Garofalo, 1987).

Indeed, many studies support the likelihood of property crime victimization as being associated with frequent absences from the home (Corrado et al., 1980; Gottfredson, 1984; Sampson & Wooldredge, 1987; Smith, 1982). Routine activities theorists also argue that crime victimization can be determined by a "proximity to high concentrations of potential offenders" (p. 596; see Lynch 1987; Cohen et al., 1981; Miethe & Meier, 1990). However, the important question is how to link from these concepts in the physical world to cybercrime issues.

3. Examples of applying good practice

Cyberspace shares a common social environment with the physical world. Castells (2002) asserted that cyberspace is oriented from the social and international environment in our society and reflects the "real world" of socioeconomic and cultural dimensions (p. 203). In other words, cyberspace is "real space" that is closely correlated to the physical world. Internet users

can view diverse Web pages everyday as a part of their routine activities in relation to their different needs. Online users with different demographic backgrounds may visit different types of Web sites based on their different interests and, thus, the compilation of a cyber-community can be distinguished by its members' interests in cyberspace (Castells).

In addition, even though there are no limitations on physical distance in order to connect another place in cyberspace, Internet users usually find a popular Web site (i.e., Ebay, MSN, AOL, Myspace.com) that has a higher density of Internet connections than other domains via a search engine (i.e. Google, Yahoo). Therefore, a higher density of Internet connection may indicate the proximity of computer criminals and computer-crime victims (Yar, 2005). In fact, computer victimization occurrences can be seen in many social networking Web sites.

The significant difference between physical-space and cyberspace is that, unlike a physical location, cyberspace is not limited to distance, proximity, and physical separation (Yar, 2005). Mitchell (1995) referred to cyberspace and its environment as "antispatial" (p. 8). Stalder (1998) also asserted that the cyber environment is composed of a zero-distance dimension. Clicking a digital icon in cyberspace takes an online user everywhere and anywhere. Thus, the mobility of offenders in cyberspace far exceeds the mobility of offenders in the physical world. Although it has been proposed that the mobility rules of the physical world would not apply in the world of cyberspace (Dodge & Kichin, 2001; Yar), this would only necessarily apply in dealing with the weight or physical bulk of the target.

Routine activities theory assumes that a crime event occurs in a particular place at a particular time, which indicates the importance of a clear temporal sequence and order for a crime to occur. Cohen and Felson (1979) asserted that "the coordination of an offender's rhythms with those of a victim" facilitates a convergence of a potential offender and a target (p. 590).

4. Recommendations / Conclusions

In sum, the application of VIVA to cyberspace indicates that target suitability in cyberspace is a fully given situation. When an online user accesses the Internet, personal information in his or her computer naturally

carries valuable information into cyberspace that attracts computer criminals. In addition, if computer criminals have sufficiently capable computer systems, the inertia of the crime target becomes almost weightless in cyberspace. The nature of visibility and accessibility within the cyber-environment also allows the motivated cyber-offenders to detect crime targets and commit offenses from anywhere in the world.

In cyberspace, computer crime is likely to occur when online users have an absence of formal capable guardians. Law enforcement agencies contribute formal social control against criminals to protect prospective victims (Grabosky, 2000). Tiernan (2000) argued that primary difficulties in prosecuting computer criminals arise because much of the property involved is intangible and does not match well with traditional criminal statutes such as larceny or theft. This problem weakens the reliability of formal social control agents and is compounded by the increasing number of computer criminals who have been able to access both private and public computer systems, sometimes with disastrous results (Tieran, 2000).

제5장

KOREAN INSTITUTE OF CRIMINOLOGY

결 론

김 한 균

제5장

결 론

1. 사이버범죄방지 가상포럼의 성과와 한계

사이버범죄방지 가상포럼은 한국형사정책연구원 유엔범죄방지및형사사법프로그램 네트워크 기관으로서 활동을 시작하면서 유엔마약및범죄사무소을 비롯하여 연구교류협력협정을 체결한 국내외 형사사법기관 및 형사정책분야 연구기관과의 최초의 본격적 협력사업이자 최장기간 지속된 대표적 사업이다. 2005년 이래 2015년 현재까지 성과를 축적하며 지속적으로 발전하고 있다.

특히 사이버범죄방지 가상포럼사업은 국제사회의 사이버범죄를 비롯한 초국가적 조직범죄 대처역량 강화노력에 적극 기여하면서 주로 아시아, 아프리카 개발도상국가 형사사법공무원을 대상으로 한 사이버범죄 역량강화 교육훈련 프로그램, 전세계의 사이버범죄 전문가들의 토론장을 열어 주고 동 분야 최초로 사이버범죄 관련 정보를 축적하는 하나의 저장공간을 개설했다는데 상당한 의미가 있다고 자평할 수 있다.

또한 그 개발과 운영과정에서 본 연구원내 사이버범죄 연구역량도 강화되었으며, 본 연구원이 유엔 범죄방지형사사법총회와 부속 워크숍, 연례 유엔범죄방지형사사법위원회 관련 회의주관의 성과를 구체적 국제협력사업의 성과로 구체화하였다는 점에서도 실효성을 확보했다.

다만 이러한 대표적 국제협력사업으로서의 성과에 대한 높은 수준의 국제적 평가, 그리고 이를 위해 투입된 상당한 재정 및 인력자원을 고려해 보면 본 연구원 내에서의 객관적 평가와 역량지원에서는 미흡한 점이 있다. 본 VFAC 사업의 지속적 발전을 통한 결실을 맺으려면, 무엇보다도 내부적 이해와 협력이 절실하며, 이를 위해 본 사업의 성과에 대한 객관적 내용을 공유하여 이해도와 참여도를 높이고, 부정적인 오해와 불신의 장애요인을 극복해 나가야 할 것이다.

2. 사이버범죄방지 가상포럼의 발전 전략

현재 VFAC 사업은 개발과 운영단계를 넘어 중장기적인 지속적 발전전략을 모색하고 실천해 나가야 할 단계에 있다. 기존의 온라인 교육훈련프로그램은 그 교육대상과 보급방식을 혁신함으로써 확대발전되어야 한다. 급변하는 사이버범죄 환경과 사이버범죄 수사 및 대응의 전문성을 고려할 때 계속적인 온라인 교육훈련프로그램의 개발과 보완에는 엄연한 한계가 인정된다. 특히 애초 개도국 형사사법공무원을 대상으로 실시한 바, 개도국의 경우 온라인 교육훈련 과정을 충실하게 이행할 만한 인터넷 인프라가 먼저 갖추어져 있지 않은 점을 고려하지 못하였다. 또한 언어적 장벽 또한 보급확산에 장애요인이라는 점도 인식하게 되었다. 이에 온라인 교육훈련과정 중에서 오프라인 교재화, 현지어 번역이 가능한 내용을 선별하여 일반인 또는 기초교육용 교재로 재활용하는 방안을 추진해 나가야 할 것이다.

한편 온라인 연구네트워크를 통해 축적된 사이버범죄동향과 사이버범죄대책 및 대응법제 정보는 사이버범죄 대응정책 연구개발에 매우 유용한 자료가 된다. 이를 고립적으로 운영하기 보다는 국내외 유사 데이터베이스 개발사업과 연계하여 시너지 효과를 모색하는 효과적 방안이 모색되어야 한다. 한국형사정책연구원은 유엔마약및범죄사무소가 주도하고 있는 사이버범죄 저장소 데이터베이스의 초기 개발단계에 참여하여 공동개발자로서 기여할 수 있다. 이를 계기로 유엔마약및범죄사무소와의 사이버범죄 분야 협력관계를 한단계 높일 수 있다. 한국형사정책연구원이 사이버범죄 분야에서 국제적 연구기관으로서의 위상을 높일 수 있게 됨은 물론이다.

참고문헌

1. 국내문헌

김은경 외 9인(2012), 2012유엔·국제협력사업 성과보고서, 한국형사정책연구원
김지영 외 10인(2014), UN·국제 교류협력 사업 보고서, 한국형사정책연구원
신형기 외 8인(2012), 경찰학 사전, 법문사.
연성진 외 4인(2009), 유엔 및 국제협력백서, 한국형사정책연구원
장준오 외 8인(2013), 2013 UN·국제협력사업 성과보고서, 한국형사정책연구원
VFAC 리뷰 제3호(2014), 한국형사정책연구원
VFAC 리뷰 제4호(2014), 한국형사정책연구원
VFAC 리뷰 제5호(2014), 한국형사정책연구원
VFAC 리뷰 제6호(2014), 한국형사정책연구원
VFAC 리뷰 제7호(2014), 한국형사정책연구원
VFAC 리뷰 제8호(2015), 한국형사정책연구원
VFAC 리뷰 제9호(2015), 한국형사정책연구원

2. 국외문헌

Bunting, Steve, and William Wei(2007). "EnCase Computer Forensics."

Gerber, Aurona, Onkgopotse Molefe, and Alta van der Merwe(2010). "Documenting open source migration processes for re-use." Proceedings of the 2010 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists. ACM.

Stefano Silvoni, Ander Ramos-Murguialday, Marianna Cavinato, Chiara Volpato, Giulia Cisotto, Andrea Turolla, Francesco Piccione, and Niels Birbaumer(2011). Brain-Computer Interface in Stroke: A Review of Progress. Clinical EEG and Neuroscience.

3. 웹페이지

고려대학교 사이버 법센터 http://www.kuclc.org/

네이버지식백과

http://terms.naver.com/entry.nhn?docId=2070345&cid=55570&categoryId=55570

네이버지식백과

http://terms.naver.com/entry.nhn?docId=865560&cid=42346&categoryId=42346

두산백과사전

http://www.doopedia.co.kr/doopedia/master/master.do?_method=view&MAS_IDX=101013000870274

세계경제포럼 http://www.weforum.org

세계은행

http://www.worldbank.org/en/news/feature/2013/04/17/ending_extreme_poverty_and_promoting_shared_prosperity

유럽평의회

http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

한경닷컴 http://dic.hankyung.com/apps/economy.view?seq=7890

한국저작권위원회

http://www.copyright.or.kr/information-materials/dictionary/view.do?glossaryNo=501&pageIndex=1&searchLangType=&searchkeyword=%EB%8B%A4%ED%81%AC%EB%84%B7&pageDisplaySize=10&searchIdx=&searchText=&clscode=01&searchTarget=

한국정보통신기술협회http://word.tta.or.kr/terms/terms.jsp

ODS (Operational Data Store)

http://daccess-dds-ny.un.org/doc/UNDOC/GEN/V12/507/77/PDF/V1250777.pdf?OpenElement

SERENE RISC http://www.serene-risc.ca/en/about-us/about-serene-risc

UNODC

https://www.unodc.org/documents/congress//Documentation/IN_SESSION/ACONF222_L3ADD1_e_V1502497.pdf

http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

https://www.unodc.org/unodc/treaties/CTOC/

http://www.unodc.org/cld/index-sherloc.jspx

http://www.unodc.org/unodc/en/frontpage/2015/March/focus_its-a-crime_-cybercrime.html?ref=fs2

https://www.unodc.org/documents/data-and-analysis/statistics/crime/ICCS/7_CCPCJ_Report_22nd_session.pdf

https://www.unodc.org/documents/congress//Documentation/11Congress/ACONF203_18_e_V0584409.pdf

https://www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf

VFAC 공식홈페이지 http://www.cybercrimeforum.org

Abstract

UN·International Cooperation and Research for Crime Prevention (XI)

Report on The KIC Virtual Forum Against Cybercrime Program

Kim Han-kyun · Seung, Jae-hyun
Na, Joo-won · Cho Min-Jeong

This paper studies the Virtual Forum against Cybercrime(VFAC) project (2005-2015), categorizing the project into three stages: development, operation, and follow-up stage. For each stage, it analyzes how each sub-project was planned and carried out. Based on this, the paper aims to visualize a long-term strategy for a continuos development of the project.

The main subjects of the study are online training program on cybercrime for the law enforcement of developing countries; and the use of online expert network, a database on cybercrime trend and information for cybercrime experts and law practitioners.

In Chapter 2, this paper summarizes stages of development(2005-2009), operation(2010-2013) and follow-up(2014-2015). In the past 10 years, reviews were limited to a single-year outcome of the project. However, this paper

conducts a systematic review to find out a long-term plan.

In Chapter 3, it suggests a strategy for further development of the VFAC research network. A review on database of the VFAC website on the trend, statistics, and legislation on cybercrime is conducted, followed by suggestions on how to develop the VFAC in line with UNODC's Cybercrime Repository project.

In Chapter 4, this paper assesses the online training program. A review on the processes of development, application, outcome, and the limits of the program is conducted. Based on this assessment, the paper suggests ways to make the best use of *Understanding Cybercrime*, a textbook that accumulates materials of the online-training program.

연구총서 15-B-13

사이버범죄방지가상포럼(VFAC) 사업 정책성과 연구

발 행 | 2015년 12월
발 행 처 | 한국형사정책연구원
발 행 인 | 김 진 환
등 록 | 1990. 3. 20. 제21-143호
주 소 | 서울특별시 서초구 태봉로 114
전 화 | (02)575-5282
홈 페 이 지 | www.kic.re.kr
정 가 | 7,000원
인 쇄 | 삼신인쇄 (02)2285-6478
I S B N | 978-89-7366-940-0 93330