'14. 3.

사이버안전 확보 기본 계획

경 찰 청

(사이버안전국)

목 차

Ⅰ. 사이버안전 현황과 미래 전망

1. 사이버안전 현황

○ 우리나라는 ICT 인프라에 있어서 세계 최고 수준으로 평가되나, 사이버 안전에 대한 **국민 개인의 인식과 예방·대응 조치는 상대적으로 미흡**

※ '12년 UN 전자정부평가와 '13년 세계지적재산권기구(WIPO)·국제전기통신연합(ITU) 평가에서 1위

○ 더불어, '12년 美 MS의 'Security Intelligence Report'에 의하면 우리나라 악성코드 감염율이 **전세계 1위로 사이버침해에 매우 취약한 상태**

○ 모바일 환경의 확산으로 **악성코드 발견이** '13년 125만 1,586건으로 '12년 대비 **376% 증가**(AhnLab)하고 DDos 공격방식이 지능형으로 진화되면서 **국가기반시설까지 사이버테러가 확대**

○ 생활영역 전반이 사이버공간과 결합함으로써 사기·성매매·도박·명예훼손 등 **다수의 범죄가 사이버공간으로 전이되어 발생**

○ **사이버범죄 발생건수**는 '13년 155,366건으로 '12년 대비 **43.5% 증가**

2. 미래 전망

1) 사회적 측면

○ 아시아 인터넷 인구 증가와 글로벌화의 가속화로 **아시아 경제를 기반으로 하는 국가에서 국제적 사이버범죄의 위험성 증가**

○ 자립성·수익성을 갖춘 **조직화된 범죄 집단의 주요 범죄 수단화**

○ **네트워크 중심의 미래 사회**는 범죄조직에도 영향을 미쳐 **사이버 범죄의 네트워크화 현상 가속**

○ 세계 각국의 경쟁·분쟁 격화로 국가·공공기관, 금융·전기·항공·교통 등에 대한 **사이버테러·사이버전 위협 증대**

※ 이란·중국의 원자력시설 마비('10년), 미국 펜타곤 F-35 전투기 정보유출('09년), 에스토니아 국가망 3주 마비('07년), 한국 10개 국가기관의 기밀유출('04년)

2) 기술적 측면

○ 해킹, 바이러스, 스팸, 악성코드 등 **사이버 위협이** 금전 탈취 등을 위한 **수단으로 연계·결합 가속화**

○ 음성, 데이터, 방송망이 통합되는 추세의 미래 **IT인프라에 따라 개별망의 피해가 전체망 피해로 확산**

※ 인터넷전화(VoIP), IPTV, RFID/USN 등 새로운 기술, 서비스의 확산과 각종 단말기의 인터넷 접속이 보편화될 경우 **공격기법은 더욱 다양화되고 피해도 증가**될 것

○ **분산서비스거부(DDoS) 등 공격 기법을 넘어 사물인터넷**(Internet of things)에 기초한 신종 사이버범죄의 끊임없는 등장**

* 각종 전자기기가 네트워크를 통해 운영·통제되는 환경이 가속화되어 자동차 제동장치 해킹을 통한 사고 유발 등 새로운 피해발생 예상

○ **토르*(Tor) 등 수사기관의 추적을 회피할 수 있는 신종 통신체계의 지속적인 등장 및 통신기술 융합 가속화로 사이버범죄 종류 증가**

* 사생활 보호와 익명의 인터넷 통신을 위해서 이용자와 인터넷서버 사이에 다수의 프록시서버를 경유하도록 구성한 서비스로서 사실상 근원지 추적 불가능

ex) 전화에 의한 보이스피싱이 사이버공간을 이용하게 되면서 사이버범죄로 진화

3) 제도적 측면

○ 디지털증거의 휘발성, 위변조 용이성으로 인한 **증거능력 다툼 증대**

○ 특히, 공판중심주의, 배심제, 조사자 증언제도 등 **사법환경의 변화로 더욱 첨예하고, 집요한 법정 다툼 촉발 예상**

○ 관계기관, 통신·금융·보안업체 등 다양한 업무 영역이 결합되어 영역 다툼이 더욱 첨예화됨으로써 **사이버안전 확보를 위한 연구·제도 개선에 장기간 소요**

Ⅱ. 경찰의 현위치와 나아갈 방향

1. 경찰 사이버안전 활동의 현위치

1) 국민 측면 : 사이버범죄의 위협에 노출

○ 사이버공간에 대한 예방·안전활동보다 해킹 등 '범죄' 발생 이후 수사에 중점, **사이버범죄로부터 '선제적 국민 보호' 활동 미흡**

※ 해킹・도박・피싱・아동음란물 등 예방 측면에서 국민 기대에 부응하지 못함

○ **급변하는 IT환경, 해킹수법 등 정보수집 부족, 한발 늦은 기술공조로 스미싱 등 신종범죄 해결 능력 한계, 최근 검거율 하락 추세**

※ 검거율 '12년 78.5% → '13년 55.4%. 최근 비트코인(bitcoin)이 자금세탁 수단으로 등장, 전자화폐에 대한 압수수색・지급정지 방법이 수사기관의 새로운 고민거리로 등장

○ 불법 영역의 '범죄' 중심의 활동으로 인해 사이버불링*, 불안감조성, 음란성광고 등 사이버상 **위협과 무질서로부터 국민 안전 확보 미흡**

* SNS, 카카오톡 등 메신저, 메시지 등을 이용해 특정인을 지속적으로 괴롭히는 행위

○ **사이버 피해 신고 채널**이 일원화되어 있지 않고, **사이버 안전 정보**도 체계적으로 통합・정리되어 있지 않아 **국민에게 불편과 혼선 초래**

○ 사이버공간의 **범죄 환경 제거 활동** 및 피해 예방, 피해 최소화 방법 등에 대한 **대국민 홍보, 교육 미흡**

2) 기업 측면 : 일정 거리 둔 채 경찰과의 협조에 미온적

○ 대형포털, 보안・금융업체 등 **기업을 상호 협력의 대상으로 대우하기 보다 '조치의 대상'으로 대응**

※ 일정 거리를 두고 대응하면서 사건수사 등 필요한 경우에만 협조를 요청

○ 사이버범죄 정보는 시스템을 운영・관리하는 기업이 보유, **기업의 협조 없이는** 사건 해결, 유사피해 예방에 **한계가 있다는 점을 간과**

3) 유관기관 측면 : 부처간 실질적 협업 미흡

○ '해킹피해 신고 의무화'에 따라 국정원·방통위에 공공기관·민간업체의 피해신고가 이뤄지고 있으나, 수사주체인 **경찰과 협력은 미미**

○ 유관기관간 업무 중복 및 정보 공유 등 실질적 협업이 어려워 신종·테러형 범죄 등 **국가적 차원의 사이버상 위협 측정이 곤란한 상황**

○ 한편, **유관기관은 집중적으로 인력·예산 투입, 역할 확대로** 업무·권한을 강화하는 추세이나 **경찰의 역할은 오히려 정체·축소 위기**

< 유관기관 동향 >

- 대검 : 2개과(68명) 확대('07년), 포렌식센터(144억) 신축('08년)
- 국정원 : 사이버위기관리법 제정 추진 중 → 컨트롤 타워로서 위상확보 노력
- 안행부·방통위 : 해킹·DDOS·개인정보·스팸 등 다양한 예방정책 추진
  ※ 방통위 : '스팸'에 대한 특사경권 확보('08년)

4) 역량 측면 : 단기과제에 치중

○ **사이버공격**의 경우 초기대응, 복구 등을 주관하는 기관 및 외국과의 협조상 한계로 인해 **공격주체(개인, 단체, 국가)와 동기(해킹능력과시, 업무방해, 테러 등)를 신속·정확하게 밝혀내기 어려운 상황**

○ 연구개발기능(R&D) 침체와 비체계적 활동 등 **중·장기 전략 부재로 인해 첨단범죄에 대한 대응 역량 확보 지연**

※ 외국 경찰은 '협업·전문·연구조직' 구성, 사이버범죄의 첨단화에 대응 중

○ 범인 검거, 정보 공유, 공적개발원조 지원, 국제기구 파견 등 **국제사회의 한국 경찰에 대한 기대는 크나 기여는 미흡**

○ 디지털포렌식 과정·결과의 신뢰성을 의심하는 사례가 발생하고 있으나, **사람·절차·장비·랩실 등에 대한 전문·표준화**는 **이제 시작 단계**

2. 경찰 사이버안전 정책의 방향성

○ (신중) **사이버공간**은 프라이버시가 중시되고 개방적인 **특성이 인정되는 영역인 만큼 신중하게 경찰 활동 추진**

○ (참여) 유관기관 참여하에 **사이버범죄별 대응전략** 수립·공개·추진 등 **국가 사이버안전 관련 정책 중 경찰 부문 이행에 적극 참여**

○ (Two-Track) 수사 중심의 사후대응만으로는 한계, 범죄분석·예방·국제협력 등 **치안 인프라 강화** 및 **'발생감소+검거증대' 전략** 필요

○ (공개) 경찰이 보유하고 있는 사이버안전 정보를 **적극적으로 공개**하고, 국민·기업의 협조를 이끌어 내 **함께하는 사이버안전 추진**

○ (협업) **유관기관 및 민간기업과의 協業**을 통해 **실효성 있는 안전대책 추진** 및 **새로운 기술에 대처할 수 있는 기술력 확보**

○ (선제적) **각급 관서별 전문 수사체제 구축**하여 수사 효율성 제고, 최신 수사기법·제도 연구 개발을 통한 **선제적 사이버범죄 대응**

○ (R&D) 사법환경 변화에도 부합하고, 공격기법의 변화에 뒤쳐지지 않고 앞서나갈 수 있도록 **디지털포렌식 분야 등 R&D 부문 투자 확대**

Ⅲ. 비전 및 정책 방향

1 비전

< 사이버공간에서의 국민 안전 확보 >

사이버공간의 치안을 확보하여 국민이 안심하고 이용할 수 있고 기업이 활동하기에 안전한 환경 조성

2 사명

○ 민간·유관기관·외국과의 긴밀한 협력을 바탕으로 선제적 사이버범죄 예방 정책을 발굴·시행하여 국민·기업·국가의 피해 최소화

○ 지속적인 연구개발로 인적·물적 자원과 기술의 전문성을 높이고, 선택과 집중을 통해 효율적으로 주요 범죄를 제압하여 사이버치안 확보

3 지향 가치

가 치	내 용
존 중	사이버공간에서의 Privacy를 존중하여 정책 수행
봉 사	공공의 안녕과 질서를 유지하기 위한 서비스 활동 전개
투 명	안전 관련 정보와 정책을 국민·기업·유관기관에 개방하고 안전 정책 이행 여부 '대외 평가'로 feedback
협 력	예방, 안전활동, 수사 등 조치 時 국민·기업·유관기관 및 외국과의 협력 하에 진행
전 문	과학화, 표준화, 체계화 등을 통한 전문화 추구
효 율	경찰 조직내 역할 분담, 대외 기관간 중복 지양

Ⅳ. 전략적 정책 방향

1 예방 중심의 사이버안전 서비스 제공

1) 사이버공간에서의 경찰 안전활동을 위한 법제 정비

○ 사이버경찰의 임무를 명확히 하기 위해 **구체적 수권 조항 입법화 추진**

○ 사이버범죄 예방 및 대응에 관한 입법 지원 및 법률 제·개정 추진

2) 국민 · 학계 · 기업 등 민간과의 협력안전활동 강화

○ 누리캅스*의 활동 영역 확대, 자율방범대 수준의 조직체로 발전

* 누리꾼의 '누리'+'cops'(경찰)의 합성어, 불법·유해정보 모니터링과 사이버범죄 예방을 위해 IT업계 종사자 등 일반인으로 '07년 발족한 사이버명예경찰('13년 884명)

○ 민간 온라인 협회의 자체 범죄예방활동 유도

○ 안전활동에 있어 '국민의 적극적인 참여' 유도 정책 추진

○ 사이버 · 개인정보 전공대학 등과 官學연계 외연 확대

○ 금융(은행·증권) · 통신(이통사) · 보안(백신) 등 유관기업 · 기관과 협력 강화

3) 대국민 사이버범죄 피해 예방 강화 정책 추진

○ 사이버안전과 범죄예방 관련 교육 확대로 사회적 인식 제고

○ 사이버공간 이용 취약계층 대상, '찾아가는 사이버 보호 활동' 확대

○ 온라인 사업자와의 협업을 통해 범죄예방을 위한 조치 확대

4) 사이버범죄 피해 최소화 및 피해자 등 보호활동 전개

○ 단일화된 사이버범죄 신고 체계와 효율적인 처리 절차 마련

○ 해킹피해 時 '취약정보' 피해기업 · 기관에 제공, 유사피해 차단

○ 인터넷사기 등에 대한 계좌정지 · 피해금 환부 절차 간소화

○ 사이버범죄 피해자에 대한 경찰 주관 지원 가능 영역 개발, 추진

○ 가출자 등 발견을 위한 휴대폰 등 포렌식 서비스 확대

○ 자살기도자 긴급구호를 위한 온·오프라인 협력 체계 강화

2 범죄 정보 조기 분석을 통한 선제적 대응

1) 협업과 시스템을 통한 범죄 정보 조기 분석, 활용

○ 유관기관 및 업체와 인적교류 등 협력 강화로 사이버침해 정보·징후 조기 탐지

○ 경찰이 업무 처리 과정에서 축적한 DB를 활용한 '범죄 정보 분석 시스템' 등 구축, 징후 분석

2) 분석 결과 지속 관리 및 공유로 위협 대응 역량 강화

○ 사이버공간의 안전 확보를 위한 경찰 대응전략 이행 실태 공개

○ 사이버범죄통계·범죄분석 정보를 국민·학계·기업에 적극 제공

○ 사이버범죄 분석결과 정보를 공유함에 있어 허브 역할 수행

○ 사이버범죄 분류 체계 조정 등 사이버범죄 통계 체계 개선

3) 분석 결과에 따른 선제적 기획수사 및 제도 개선 추진

3 수사역량 강화를 통해 사이버범죄 강력 단속

1) 경찰청·지방청·경찰서간 사이버범죄 효율적 대응 체계 정비

○ 지방청 전담조직 대폭 확충, 핵심 사이버범죄에 대한 지휘체계 강화

○ 중요 미검 사이버범죄에 대한 별도 관리 절차와 국가안보위협 사건에 대한 비상대응 절차 마련

2) 사이버 불법행위 조성 환경에 대해 강력히 대응

○ 대규모 스팸·스미싱, 유언비어 등에 대한 유관기관 공동 즉응태세 강화

○ 국가·공공기관·기업에 대한 '해킹미수범죄' 단속, 피해발생 차단

○ 저작물·음란물 등 유통의 원천인 불법 P2P·웹하드업체 운영자 단속

3) 수사역량 강화를 위한 인프라 개선

○ e-CRM*과 KICS** 연계, 전자적인 업무처리 기반 구축

* 네탄 홈페이지에 구축되어 있는 사이버범죄 신고접수 코너 ** 형사사법정보시스템

○ 인터넷전화 회사, 금융계좌 개설지 등 확인 곤란한 문제점 해결

○ 수사관 개인의 수사기법을 DB로 구축, 수사정보 자원으로 승화

4 국내외 협력 강화를 통한 사이버 치안역량 제고

1) 민간 · 유관기관과의 실질적 협력체계 강화

○ '거버넌스 치안체계'를 위한 사이버치안자문 조직 발족

○ 유관기관 · 보안업체 · 포털 등에 적극적으로 자료 · 정보 제공

○ 민관 합동 '디지털포렌식연구회(협회)' 창설 유도

2) 국제 교류 협력 확대

○ 중국과의 교류 확대를 통한 동북아권 국가 경찰간 공조체제 선도

○ UN·ITU(국제전기통신연합), 개도국으로 국제협력 대상 확대

○ 네델란드 · 호주 등 선진국과의 디지털포렌식 국제 협력 강화

3) 기술 · 인력 교류 등 국제적 협업 내실화

○ 「24/7」* 대응체계 구축, 국제적 사이버범죄 수사활동에 적극 참여

* 24 hour, 7 day : 24시간 365일 무중단 업무 협력 체계

○ FBI와 MOU 수정 체결, 공조절차 간소화 및 정보공유 활성화

※ 기존 MOU는 내용이 추상적 · 포괄적이어서 절차 · 공유방식 등 구체화 필요

○ 국제사이버범죄 심포지엄 등 국제회의 및 국외위탁교육 확대

○ 인터폴 사이버수사관 양성 교육과정 국내 유치 및 강사 지원

5 전담요원과 업무시스템의 전문성 고도화

1) 사이버범죄 대응 요원의 전문성 강화

○ IT전공자 비율을 現 30%에서 '18년까지 50%로 확대

○ 전문경찰관 양성을 위한 연계교육체계 도입 등 교육과정 고도화

○ 한국경찰을 대표하는 국제 사이버범죄 전문가 지속 양성

○ 민간 디지털증거분석 전문가 특채 지속 추진, 전문성 강화

2) 전문시스템 구축을 통한 업무처리 효율화

○ '해킹·디도스·봇넷 프로파일링시스템' 마련, 용의자 추적 강화

○ '디지털포렌식 관리시스템', 지방청별 '해킹·악성코드 분석실' 구축

3) 디지털증거분석 절차 개선, 분석결과의 공정성·신뢰도 제고

○ 독립 분석기관 의뢰 및 교차분석을 통한 공정성 확보

○ 증거분석 결과의 신뢰도 확보 및 내실화

※ 수사/분석 겸직 제한 등 디지털증거분석관의 윤리 강령 수립, "디지털증거 취급 및 처리 규칙" 제정, 디지털증거분석요원 표준화된 피복 지급 등(과학수사요원과 유사)

○ '아동음란물 프로파일링 시스템' 구축, 아동음란물 단속 역량 강화

○ 국내외 악성코드 공조수사 시스템 구축, 투명한 형사절차 확보

6 조직 개편 및 연구 개발(R&D)로 변화에 능동적 대처

1) 사이버안전활동 대응 인력·조직 확충·정비

○ 경찰관 2만명 증원과 연계, 역할 확대에 따른 사이버요원 지속 증원

○ 지방청 사이버수사대 등 사이버안전과로 연차적 전환 추진

※ '14년은 1차적으로 서울·부산·경기·대구·인천청 '사이버안전과' 창설 추진

2) 발전적 조직 개편 연차 추진

○ 경찰에 대한 국민의 '사이버범죄신고 종합 접수·대응 센터' 추진

○ '사이버범죄 예방교육 총괄 전담기구' 추진

○ '사이버 위협 정보 공유 센터' 추진 ※ 정부민원포털인 '민원 24'와 유사

○ '디지털 증거 연구소' 설립 추진 ※ 국립과학수사연구원과 유사

※ 수사와 증거분석 활동을 분리함으로써 증거분석 결과의 신뢰도를 제고하고 연구개발 기능을 강화, 전국 거점별 디지털 증거 연구분소 구축, 국가기관이 공동 활용

3) 사이버안전 연구·개발(R&D) 전담조직 운영

○ 長期 정책·개발연구과제 전담관리기구로 경찰대학 '국제사이버범죄연구센터'를 확대 개편

※ 경찰청은 정책결정·예산확보·제도입법화, 전담관리기관은 연구과제 발굴·정책대안 제시

○ 사이버범죄/포렌식 분야 연구를 국가 R&D 과제로 격상 추진

4) 중장기 정책과제 체계적 연구·개발

○ 사이버공간에서의 '악성 무질서' 행위로부터 국민 안전 확보 방안 연구

○ 不罰 영역으로 남아 장래적 범죄요인이 되고 있는 '아이템 편취', '게임 ID 거래'에 대한 대응 방안 연구

○ 디지털프로파일링시스템* 구축, 수사 및 법적 증거로의 활용 방안 연구

* 디지털증거를 통합 DB화하여 상관관계 분석 후 범죄자 특징, 행동, 범행 타임라인 등 추출

○ 스마트모바일사이버수사포털* 구축, 수사의 신속·효율화 방안 연구

* 현장에서 실시간 접속하여 IP분석(PROXY, VPN 등), 웹서버피싱 모니터링, 원격지원서비스 등 활용

#부록. 정책 방향 실천 과제 [6대 분야 20개 과제]

1 예방 중심의 사이버 안전 서비스 제공

❑ 사이버공간에서의 경찰 안전활동을 위한 법제 정비

○ 경찰법, 경찰관직무집행법상 경찰의 임무·직무 범위 등 규정은 모두 오프라인 안전활동, 범죄진압 등에 맞추어져 있는 상태

○ 제4의 영토인 **'사이버공간의 치안 질서 유지'**라는 경찰의 임무를 명확히 하기 위해 **구체적 수권 조항 입법화 추진**

○ 사이버범죄 관련 실체법, 절차법에 대한 **입법 지원**, 사이버범죄 **예방 및 대응에 관한 법률 제·개정 추진**

❑ 국민 · 학계 · 기업 등 민간과의 협력안전활동 강화

○ **누리캅스* 역할과 규모 확대**

- 음란물 업로드 모니터링 수준에 머물러 있는 민간 사이버협력단체의 활동 영역을 **사이버공간의 제반 안전위협요소에 대한 모니터링 및** 대국민 사이버안전 교육, 교재 마련 활동 등으로 확대

* 누리캅스 : 누리꾼의 '누리' + 'cops'(경찰)의 합성어, 불법·유해정보 모니터링과 사이버범죄 예방을 위해 IT업계 종사자 등 일반인으로 '07년 발족한 사이버명예경찰('13년 884명)

- 사이버협력단체로서 **"자율방범대"와 유사한 성격의 조직체로 발전** 추진

○ **민간 온라인 협회의 자체 범죄예방활동 유도**

- **수익자 부담 원칙과 사적영역 자율 규제 원칙**에 따라 **민간 온라인 사업자의 연합체인 협회를 통해 자체적으로 사이버범죄 예방활동을 강화**하도록 정책적 지원 및 **사이버 NGO와 연계 추진**

- **(1안)**온라인게임협회, 인터넷PC방협회 등 **現存 협회의 활동영역에 범죄예방 추가, (2안)민간 사이버범죄예방협회 창설 유도, (3안)**경찰 주관 **사이버범죄예방협의회 창설** 추진

※ 예방홍보·피해최소화·법률검토 등 위해 필요시 경찰관 파견 등 지원

- 사이버 치안대상 규모 확대, **사이버 보안 분야 우수 벤처 기업 적극 발굴**·포상으로, 기업 인지도 상승 기회 제공 및 성장 동력 부여

○ **안전활동에 있어 '국민의 적극적인 참여' 유도 정책 추진**

- 사이버상 불법·유해정보 등 안전위협요소에 대한 신고대회 개최

※ '07年 ~ '14. 1月간 총 75,772건 신고 · 50,598건 폐쇄삭제요청 · 1,149건 수사착수

- **「사이버테러 신고보상금 제도」***도입, 신고·제보 채널 다양화

※「범죄신고등보호및보상에관한규칙(경찰청훈령)」개정 / 신고보상금 최대2천만원

○ **사이버 · 개인정보 전공대학 등과 官學연계 외연 확대**

- 사이버경찰학과, 해킹보안학과, 정보보호학과 등 **학계와 MOU체결, 연구용역의뢰, 인력 특별채용** 등을 통한 협력 확대

※ 國內 호서대 · 한국IT 사이버경찰학과, 세종사이버대학원 정보보호학과 등 다수 존재

○ 금융(은행·증권) · 통신(이통사) · 보안(백신) 등 **유관기업 · 기관과 협력 강화**

- 위해요인 탐지·긴급 경보체제 발령 및 피해 조기 차단
- 언론보도와 관련한 민간과 경찰간 협력·대응 절차 마련
- 사이버범죄 전문 분야별 민·관 전문가 인력풀 구성
- 신종범죄 발생 즉시 범죄유형·악성코드 등 분석 가능한 **Real time 협업대응체제 구축**

※ ┌ **조기 정보공유** : 금융감독원, 금융위원회, 은행연합회 등
├ **악성코드 유포 차단** : 한국인터넷진흥원, 보안업체, 각 이동통신사 등
├ **휴대전화 소액결제 제도개선** : 미래창조과학부, 이통사, 결제대행사, 게임사 등
├ **금융시스템 보안** : 금융감독원, 금융위원회, 각 금융기관 등
└ **스마트폰 보안** : 미래창조과학부, 단말기 제조사, 보안업체 등

❑ 대국민 사이버범죄 피해 예방 강화 정책 추진

○ 사이버안전과 범죄예방 관련 교육 확대로 **사회적 인식 제고**

- 드라마 · 광고 등 미디어를 활용한 **사이버범죄 예방 홍보 확대**
- **사이버범죄 피해예방 수칙 개발 및** 전문강사 · 교육컨텐츠 확충

※ 매년 전문강사 40명씩 확충 추진(현재 전문강사 1·2기 40명 활동 중)

- 초·중·고·노인대학, 정규 교육과정에 '사이버안전' 교육 편성 추진
- 국내 사이버안전 컨퍼런스 개최를 통해 예방지식 공유 및 경찰정책 홍보, 전문가 강연 내용은 동영상 콘텐츠로 제작, 국민들에게 지속 전파

  ※ 사이버센터 홈페이지內 '사이버범죄 예방' 카테고리 신설하여 서비스 제공 추진
- 사이버안전국 공식 SNS 개설, 온라인 홍보역량 강화

○ 사이버공간 이용 취약계층 대상, '**찾아가는 사이버 보호 활동**' 확대

- 노인정·학교·어린이집 등 방문하여 **사이버캅앱 설치, 악성코드 차단 기능 설정 또는 앱(App) 설치, 소액결제 차단** 등 스미싱·피싱 등 예방을 위한 **기술적 조치 및 사이버안전 교육 실시**

  ※ 사이버안전요원과 지역경찰관 등이 공동으로 대응, 현장 진출하여 조치 및 교육

○ **온라인 사업자와의 협업을 통해 범죄예방을 위한 조치 확대**

- **일정 규모 이상의 대형사이트에 '사이버범죄 신고하기' 배너 추진**
- 국민이 대형 상거래 홈페이지 이용時 경찰이 보유하고 있는 **범인의 'ID·금융계좌·휴대폰번호' 등을 조회할 수 있도록 서비스 제공**

  ※ (1안) 경찰이 개발, 서비스 중인 사이버범죄 예방정보 알림이 「넷두루미(Net-durumi)」 기능을 확대 적용(현재 네이버·G마켓 등 국내 20여개 회사 사이트에 배너 게시 중) (2안)대형포털社에 범인의 ID·금융계좌·휴대폰 등 정보 제공, 사업자 스스로 조회 기능 개발
- 아동포르노 DB를 P2P·웹하드업체에 제공, **자발적 필터링 유도**

❑ 사이버범죄 피해 최소화 및 피해자 등 보호활동 전개

○ **단일화된 사이버범죄 신고 체계와 효율적인 처리 절차 마련**

- **범죄신고 편의성 제고, 신고 활성화 및 실질적 범죄예방정보 제공을 위해** 범죄신고, 예방정보 확인 가능한 **앱(App) 개발·배포**

< 신규 앱 주요 기능 >

◈ (범죄신고) 본인 인증을 통한 사이버범죄 신고 * 신고방식 간소화

◈ (범죄이용자동확인) 전화·문자가 오면 범죄에 이용된 번호인지 자동 표시

※ 범죄 신고 접수된 번호와 이용자들이 직접 입력·저장한 번호 이용, 이중서비스

◈ (범죄이용여부조회) 범죄에 사용된 전화번호, 금융계좌 여부 임의 조회

◈ (경보령 등 자동알림) 신규 스미싱 수법 등 대국민 공지사항 Push '팝업' 제공

◈ (맞춤형 정보검색) 신종 범죄 취약계층(노인 등)의 눈높이에 맞춘 간편 정보검색 및 전화상담 연결

◈ (사이버안전정보 종합포털) 범죄예방법, 피해구제절차, 범죄동향 등 경찰 내·외 홈페이지 총망라, 사이버안전에 관한 정보 통합 서비스(Link)

- 암수범죄를 최소화시키기 위한 사이버범죄별 신고 활성화 대책 마련
- 국민이 e-CRM에 신고·기술한 내용이 진정서·진술서와 동일한 효력이 인정되도록 법원 등과 **전자서명 효력 관련 법률 개정 논의**

※ 현재는 피해자가 진술조서(진술서) 등을 작성하기 위해 경찰관서 방문이 불가피한 상황

○ 해킹피해 時 **'취약정보' 피해기업·기관에 제공, 유사피해 차단**

○ **인터넷사기 등에 대한 계좌정지·피해금 환부 절차 간소화**

※ 현재 전기통신금융사기피해금환급에관한특별법에 보이스피싱, 파밍 등으로 인한 피해는 계좌정지 등 법제화 상태 ; 명백한 인터넷사기 등이 포함되도록 재추진 필요

○ **사이버범죄 피해자에 대한 경찰 주관 지원 가능 영역 개발, 추진**

○ **가출자 등 발견을 위한 휴대폰 등 포렌식 지원 확대**

※ 추후, 디지털 포렌식 시장이 성숙될 경우, 민간에서 처리 유도

○ **자살기도자 긴급구호를 위한 온·오프라인 협력 체계** 강화

- 사이버공간에서 **자살 관련 징후가 포착된 국민**에 대하여 **긴급 구호 활동을 전개할 수 있는 온·오프라인 협력 체계** 정비

※ 사이버안전순찰요원과 112·지역경찰요원 및 소방, 보건복지부, 방통위, 한국자살예방협회 등 유관기관 협업(모니터링단 운영 / 자살글·독극물 관련정보 삭제 등) 체계 강화

- 자살글 게시자 추적을 위한 **'IP, 휴대폰, ID' 조회 법적근거 마련**

2 범죄 정보 조기 분석을 통한 선제적 대응

❑ 협업과 시스템을 통한 범죄 정보 조기 분석, 활용

○ 국정원·미래부 등 **유관기관간 인적교류를 통한 협업 체계와** 인터넷진흥원·보안관제센터·대형기업 등과 협력 체제를 통해 **사이버침해 정보·징후 조기 탐지**

○ **경찰이 업무 처리 과정에서 축적한 DB를 활용한 '범죄 정보 분석 시스템'***을 구축하여 범죄 징후 분석 역량 강화

* KICS정보·e-CRM정보·넷두루미정보·범죄첩보·경찰청홈페이지정보 등 활용

○ 분석 결과는 ▲**유사범죄 경향분석을 통한 경보 발령** ▲유사사건 수사정보를 활용한 **신속한 사건 해결** 등에 활용

❑ 분석 결과 지속 관리 및 공유로 위협 대응 역량 강화

○ 사이버공간의 안전 확보를 위한 **경찰 대응전략의 이행 실태**를 매년 평가하고 **'백서' 발간, 대국민 공개**

○ **사이버범죄통계·범죄분석 정보를 국민·학계·기업에 적극 제공**

- 범죄정보 공유, 활용에 관한 **가이드라인 제정**
- 정례적으로 범죄 동향 등 예측, "Report" 정기 발행, 공유

○ **사이버범죄 분석결과 정보를 공유함에 있어 허브 역할 수행**

- **유관기관간 위협 정보 공유를 위한 '플랫폼' 공동 구축**
- **기관간 협업** 목적에 부합되도록 인터넷진흥원(KISA), 국가보안기술연구소(NSRI) 등 **유관기관 상호 분석결과 등 정보를 공유할 수 있는 연계방식 기반의 시스템 공동 구축** 추진

※ 미래창조과학부, 국가정보원 등에서 구축 추진 중인 사이버안전정보 공유용 플렛폼과 협조

○ 사이버범죄 분류 체계 조정 등 **사이버범죄 통계 체계 개선**

- 국제적인 기준과 국내 특수성을 감안, **사이버범죄 재정의**
- **새롭게 정의된 사이버범죄 분류 체계에 따라 신규 통계체계 구축**

※ 죄종별 분류에 그치지 않고 범죄의 유형까지 반영한 통계 산출 추진

- 수기 취합 방식의 기존 사이버범죄 통계 산출 방식에서 탈피, KICS를 통한 **실시간 자동 산출 통계 체계로 전환**

❑ 분석 결과에 따른 선제적 기획수사 및 제도 개선 추진

○ 범죄 정보 분석시스템 활용, **국민이 최우선 척결 대상이라고 공감하는 사이버범죄**를 時宜適切하게 발굴

- 범죄유형별 위협의 정도를 측정하고 대응 우선순위 선정
- 발굴된 테마에 대하여 경찰의 **모든 역량을 총집중하여 기획안전·수사활동 전개**
- 단속 후 **수사기법·법제도 개선방안 발굴, 유관기관 통보제도화**

○ 유관기관의 법제도 개선 촉구 및 **이행여부 지속 관리**

【 특별단속 8단계 프로세스 】

① 여론·범죄통계 분석 → ② 단속테마 선정 → ③ 단속 → ④ 수사결과 분석 및 언론홍보 → ⑤ 수사기법 발굴 → ⑥ 법제도 개선방안 발굴 → ⑦ 유관기관 협조 → ⑧ 개선여부 이행관리

3 수사역량 강화를 통해 사이버범죄 강력 단속

❑ 경찰청·지방청·경찰서간 사이버범죄 효율적 대응 체계 정비

○ **각급 관서간 수사 역할 재정립 : 지방청 수사전담 조직 대폭 확충**

- **(경찰청)** 국가적 사이버테러 등 **고도의 기술과 중장기적, 집중적인 수사가 요구되는 범죄**에 대한 수사
- **(지방청) 도박·음란 등 조직형 사이버범죄**에 대한 인지 수사
- **(경찰서)** 사이버범죄 **신고민원**에 대한 신속한 조치 및 수사

○ **핵심 사이버범죄 수사지휘체계 강화**

- 핵심 사이버범죄에 대한 경찰청, 지방청 보고·지휘 기준 정립

- **본청·지방청에서 구체적 수사지휘를 통해 컨트롤타워 역할 담당**

○ **중요 미검 사이버범죄에 대한 별도 관리 절차 마련**

○ **국가안보위협 사건에 대한 경찰의 비상대응 절차 마련**

❑ 사이버 불법행위 조성 환경에 대해 강력히 대응

○ 국민에게 큰 불편을 끼치는 **대규모 스팸, 스미싱, 유언비어(괴담) 등**에 대하여 유관기관 공동대응, 전문수사팀 투입 등 현장 즉응태세 강화

※ 유관·민간과 함께 Virtual Taskforce팀 구성, 운영

○ 국가·공공기관·기업에 대한 **'해킹미수범죄' 단속, 피해발생 차단**

○ 저작물·음란물 등 유통의 원천인 **불법 P2P·웹하드업체 운영자 단속**

❑ 수사역량 강화를 위한 인프라 개선

○ 전자서명 관련 법률 개정을 전제로 **e-CRM과 KICS를 연계하여 전자적인 업무처리 기반 구축**

※ 현재 e-CRM 신고내용을 경찰관이 KICS에 재입력하고 있는 실정

○ 수사時 필요한 인터넷전화번호 가입회사 조회 서비스, 휴대전화 별정통신사업자 조회 서비스, 금융계좌개설지 확인 서비스 구축 추진

※ 경찰청과 통신사업자연합회간 네트워크 연결 및 "費用"문제 쟁점 해소, 금융위원회, 은행연합회 등 관련 기관과 협업 필요

○ 사건수사를 통한 **수사관 개인의 수사기법** 등을 향후 他사건 수사時 활용할 수 있도록 **DB로 구축, 수사정보 자원으로 승화**

※ 확보된 수사기법 정보는 KICS 또는 수사기법공유시스템(개발)을 통해 공유

4 국내외 협력 강화를 통한 사이버 치안역량 제고

❑ 민간 · 유관기관과의 실질적 협력체계 강화

○ 학계 · 민간 등 다양한 전문가가 참여하는 **'거버넌스 치안체계'를 위한 사이버치안자문 조직 발족, 운영**

- 사이버안전 관련 주요정책 추진時 법률적, 기술적, 학술적 자문을 통해 **정책의 완결성 보완 및 사이버경찰에 대한 지원 세력화**
- (1안) 포렌식·예방 등 여러 '분과'로 구성된 **'사이버치안자문위원회'**
  (2안) 사이버포렌식자문위원회 등 **'분야별 자문위원회'** 조직

○ **유관기관 · 보안업체 · 포털 등에 적극적으로 자료 또는 정보 제공**

※ 要보안사항은 제외, 정보공유협의체(가칭)와 같은 협력조직 구성

○ **민간 합동 '디지털포렌식연구회(협회)' 창설 유도**

- 최신 디지털 기기에 대한 신속한 동향 파악 및 학계 · 기업 · 기관간 협력을 통한 디지털증거 분석역량 강화

※ 구성(안) : 민간위원장 산하에 모바일 · 디스크 · 악성코드 · 네트워크 · DB분과위원회로 구성

❑ 국제 교류 협력 확대

○ **중국과의 교류 확대를 통한 동북아권 국가 경찰간 공조체제 선도**

- **중국과의 사이버수사 공조기반 마련**을 위한 사이버책임자 초청, 사이버 주재관 파견 등 추진
- 장기적으로 동북아권 국가 경찰기관 **사이버협의회(summit) 주도적 추진**

○ 네델란드 · 호주 등 선진국과의 디지털포렌식 국제 협력 강화

- 서유럽 법과학계 의장기관인 NFI(네덜란드 법과학연구소) 등과의 포렌식 공동연구 확대 등 활성화 추진
- 각종 디지털 증거분석에 대한 외국의 협조 요청 적극 지원, 외연 확대

ex) '12. 2. 호주에서 발생한 특수강도사건 관련, 호주 대사관 요청으로 CCTV 데이터 분석, 회신

○ **UN · ITU(국제전기통신연합) 및 개도국으로 국제협력 대상 확대**

- 사이버범죄 예방 및 수사에 필요한 **국제규범 가입, 추진**
- 인터폴→UN · ITU 등 국제협력 채널 다각화, 경찰위상 강화
- 개도국 대상 사이버치안체계 전수, **한국경찰에 대한 긍정 · 우호적 이미지 제고**를 통해 협력기반 구축, 재외국민보호 역량 강화

  ※ 국내 조직·인사·교육·기법 등을 개도국에 전수, 사이버치안 선진화 지원

- 해외 수사기관에 국내 사이버 대응시스템 및 전수모델 구축 추진

  ※ 나이지리아(인터넷 사용인구 4천만명) 등 인터넷인프라가 확대중인 개도국에 대하여 사이버 수사조직 역량 강화 지원

❑ 기술 · 인력 교류 등 국제적 협업 내실화

○ **「24/7」 대응체계 구축, 국제적 사이버범죄 수사**활동에 **적극 참여**

* 24 hour, 7 day : 24시간 365일 무중단 업무 협력 체계

○ **FBI와 MOU 수정 체결**, 공조절차 간소화 및 정보공유 활성화

- 기존 MOU는 내용이 추상적 · 포괄적이어서 구체화 조치 필요

※ 한국 수사관 FBI 교차 파견, 국내 수사관 FBI 사이버 교육(3주과정) 병행 추진

○ **국제사이버범죄 심포지엄 등 국제회의 및 국외위탁교육 확대**

- 인터폴·FBI 등이 참석하는 국제 심포지엄 지속 개최, 사이버치안 대책 관련 지식 공유를 토대로 **사이버안전 선도국으로 도약**
- 선언적 구호가 아닌 **실질적 공조수사 및 협력의 장으로 운용, 역량 있는 전담요원에 기반한 인적 네트워크 공고화**
- 인터폴 주재 **국제회의 적극 유치·참가를 통해 국제사회에서의 발언권 지속 확장**

※ '14년부터 인터폴 아시아 회의 및 교육이 유라시아로 확장

○ **인터폴 사이버수사관 양성 교육과정 국내 유치 및 강사 지원**

- 인터폴 주최 사이버관련 교관양성 프로그램을 정기적으로 유치함으로써 사이버범죄 관련 최신 동향 및 대응기법 습득
- 인터폴 회원국과의 교류 협력을 통해 정보 교환, 인적 네트워크 형성을 통한 수사공조 역량 강화

例) 인터폴 아동음란물전담수사관 양성 과정 유치('13. 3.), 인터폴 컴퓨터포렌식 교관양성과정(TTF) ('13. 10.)

5 전담요원과 업무시스템의 전문성 고도화

❑ 사이버범죄 대응 요원의 전문성 강화

○ **IT전공자 비율**을 現 30%에서 **'18년까지 50%로 확대**

- 경찰청·지방청에서 서버해킹·디도스·봇넷 사건 수사 직장

※ '13년末 현재 사이버수사요원 1,038명 중 IT전공자 310명으로 30%

< 연도별 IT전공자 특채 현황 및 '14년 이후 특채 계획(안) >

총 계	소계	'00~'10년	'11년	'12년	'13년	'14년	'15년	'16년	'17년	'18년
773	310	224	18	17	61	63	100	100	100	50

○ 전문경찰관 양성을 위한 **연계교육체계 도입 등 교육과정 고도화**

- 국제 사이버범죄 대응, 디지털 포렌식, 해킹·악성코드 분석 교육 등 분야별 전략적인 교육으로 전문인력 양성 추진
- 사이버요원 특기별 인력풀 구성, 매뉴얼화 교육을 통한 전문화 및 **필요한 전문 지식을 능동적으로 활용할 수 있는 교육 체계 마련**
- **초·중·고급수사관, 분석관 과정별로 이수해야 할 연계프로그램 구성,** 컨텐츠 제작을 통한 전문화 교육으로 교육 효과 극대화

○ **민간 디지털증거분석 전문가 특채 지속 추진**, 전문성 강화

- 디지털포렌식센터 '팀장'을 단계적으로 경찰관→연구관으로 변경
- 학위·자격증 취득지원과 민간위탁 교육으로 전문가 양성

○ 한국경찰을 대표하는 **국제 사이버범죄 전문가 지속 양성**

- 고위급 사이버범죄 국제전문가 육성
- 국제 사이버범죄 수사관 양성을 위해 美·中 **위탁교육 추진 등** 외국 국가별 담당 사이버범죄 대응 전문가 양성
- 경위~경정급 선발, 국제 커뮤니티 지속 참석으로 식견·안목 함양

❑ 전문시스템 구축을 통한 업무처리 효율

○ **'해킹·디도스·봇넷 프로파일링 시스템' 마련**, 공격패턴·여죄관리 등 범죄분석을 통한 **용의자 무한 추적체제 구축**

○ **'디지털포렌식 관리시스템'** 및 **지방청별 '해킹·악성코드 분석실' 구축**

- 지방청·경찰서에서 본청에 의뢰하는 매체별 디지털증거에 대하여 바코드 이용, 온라인상에서 의뢰→이첩→승인 절차에 따라 처리
- 지방청별 해킹·악성코드 분석으로 **증거 분석의 신속·효율성 강화**

○ **'아동음란물 프로파일링 시스템'*** 구축, 아동음란물 유통상황 분석을 통한 **아동음란물 단속 역량 강화**

* 아동음란물 해쉬값 DB화로 자동검색 기능 구현, 인터넷상 아동음란물 실시간 유통 현황 및 헤비 업로더 IP주소 추적을 통해 자동으로 자료 수집·분석

○ 국내외 **'악성코드 공조수사 시스템'** 구축, 민관 합동으로 공정하고 신빙성 있게 악성프로그램을 분석하여 투명한 형사절차 확보

- 백신소프트웨어 제작사에서 입수·제작한 악성프로그램과 분석 보고서 필요시 DB에서 조회하여 수사에 활용

※ 수사상 확보한 악성프로그램을 민간 백신업체에 제공, 민간 분석 기능 활성화

❑ 디지털증거분석 절차 개선, 분석결과의 공정성·신뢰도 제고

○ **독립 분석기관 의뢰 및 교차분석 등**을 통한 공정성 확보

※ 고위공직자, 경찰관 연루사건 등 사회 이목 집중 사건, 공정성 의혹 사건

- 디지털증거분석관 국가 자격화 방안 추진
- LAB실 국내 인증제 마련 및 국제 표준화 추진

○ **디지털증거 분석 결과의 신뢰도 확보 및 내실화**

- 수사/분석 겸직 제한 등 **디지털증거분석관의 윤리 강령 수립**
- **"디지털증거 취급 및 처리 규칙" 제정**(경찰청훈령) 추진

※ 디지털증거 수집, 운반, 보관, 분석 등 과정 전반에 대한 상세한 절차 규정

- 현장에 임장하여 디지털증거분석을 지원함에 있어 전문요원으로서의 이미지 제고를 위해 **과학수사요원과 같은 피복 지급 추진**

6 조직 개편 및 연구 개발(R&D)로 변화에 능동적 대처

❑ 사이버안전활동 대응 인력·조직 확충·정비

○ 경찰관 2만명 증원과 연계, **역할 확대에 따라 사이버요원 지속 증원**

- 관서간 역할 재조정에 따라 본청, 지방청 역할은 증가, 경찰서는 상대적 감소 예상 → **업무부담에 따라 관서간 증원 인력 배분**
- 수사·형사·외사·여성청소년·지역경찰 등 **기능간 업무부담 격차가 완화될 수 있도록 증원 인력 조정·분배 추진**

○ **지방청 사이버수사대 등 사이버안전과로 연차적 전환 추진**

- 1차적으로 **서울·부산·경기·대구·인천청 '사이버안전과' 창설 추진**
- **기타 지방청과 대규모 경찰서**도 연차적으로 '사이버안전과' 추진
- 署사이버수사팀은 **사이버안전팀으로 명칭·역할 변경 및 독립 직제화**

❑ 발전적 조직 개편 연차 추진

○ 경찰에 대한 국민의 **'사이버범죄신고 종합 접수·대응 센터'** 추진

※ 경찰 '182·112센터', KISA '인터넷침해대응센터'와 유사

- 182·112센터, 인터넷침해대응센터, 경찰서 사이버안전팀과 사이버신고종합센터 사이에 전화 또는 홈페이지를 통한 국민의 신고를 Non-stop으로 인수인계할 수 있는 체계 필요

○ **'사이버범죄 예방교육 총괄 전담기구'** 추진

- 교육 정책·시스템 개발 및 강사 양성 등을 통해 대국민 사이버범죄 예방 홍보·교육을 체계적으로 추진

○ **'사이버 위협 정보 공유 센터'** 추진 ※ 정부민원포털인 '민원 24'와 유사

- 사이버범죄 관련 정보들을 유관기관·관련기업·국민에게 배포하고 공유할 수 있도록 '정보공유 플랫폼' 등 시스템 구축 선행 필요

○ **'디지털 증거 연구소'** 설립 추진 ※ 국립과학수사연구원과 유사

- 수사와 증거분석 활동을 분리함으로써 증거분석 결과의 **신뢰도를 제고하고 연구개발 기능을 강화**

【 전용시설 구축(안) 】

① 디스크분석실	② 모바일분석실	③ 증거복구실	④ 해킹악성코드 분석실
⑤ 암호분석실	⑥ 네트워크분석실	⑦ 기법개발실	⑧ 데이터분석실

- 분석관에 대한 인증, 분석 보고서에 대한 품질 보증 및 관리절차 마련 및 교육훈련 프로그램 개발 추진
- 법과학적 증거의 정확성, 신뢰성, 타당성 발전을 위한 연구 추진
- 정부 출연기관과 연계, 디지털 포렌식 도구개발 사업 추진
  ※ 전국 연계 '지능형 포렌식시스템' 개발
- **전국 거점별 디지털 증거 연구분소 구축, 국가기관이 공동 활용**

❑ 사이버안전 연구·개발(R&D) 전담조직 운영

○ 長期 '사이버안전정책·제도개선, 시스템·기법개발' 등 정책·개발연구 과제 전담관리기구로 **경찰대학 '국제사이버범죄 연구센터'** 확대 개편
※ 경찰청은 정책결정, 예산확보, 제도·입법화 담당, 전담관리기관은 연구과제 발굴, 정책대안 제시

○ 사이버범죄/포렌식 분야 연구를 국가 R&D 과제로 격상 추진

- 사이버범죄/포렌식 분야 R&D 예산 별도 확보
- 사이버범죄/포렌식 분야에 대한 중장기 R&D 전략 별도 수립
- 일반대학내 사이버범죄/포렌식 연구센터 신설 지원(유도)

❑ 중장기 정책과제 체계적 연구 · 개발

○ 사이버공간에서의 **'악성 무질서' 행위로부터 국민 안전 확보 방안 연구**

- 사이버불링*, 음란성광고(과다노출과 유사), 불안감조성, 호객행위 등 **국민 누구나 공감하는 악성 무질서 행위로부터 국민 안전 확보 필요**

  * 인터넷상에서 SNS, 카카오톡 등 메신저, 메시지 등을 이용해 특정인을 지속적으로 괴롭히는 행위

- '개방성' 등 사이버공간의 특성에 반하지 않도록 신중하게 **악성 무질서 행위 분류 기준, 질서벌** 등 **실효성 있는 방안** 연구 필요

  ※ 공청회, 경범죄처벌법 개정·신규 입법 방안 등 폭넓은 검토 필요

○ 不罰 영역으로 남아 장래적 범죄요인이 되고 있는 **'아이템 편취', '게임 ID 거래'에 대한 대응 방안 연구**

  ※ 형사처벌時 '청소년 전과자 양산'이 우려되므로 질서벌化 검토·추진 필요

○ **디지털프로파일링시스템 구축**, 수사 및 법적 증거로의 활용 방안 연구

- 디지털증거 통합, DB화하여 증거간 상관관계 분석 후 범죄자 특징, 행동, 범행 타임라인 등을 시각화하여 제공하는 방안

○ **스마트모바일사이버수사포털 구축**, 수사의 신속·효율화 방안 연구

- 현장에서 사이버요원이 실시간 접속하여 IP분석(PROXY, VPN 등), 웹서버 피싱 모니터링, 원격지원서비스 등 기능을 활용하는 방안