군 사이버침해 범죄 실태와 대응 방안

Countermeasures of Problems about Cyber Attacks for Military System

김 호*·이 주 호**

차 례

국문요약

갈수록 첨단화되는 환경 속에서 증가하는 사이버 침해사고에 대하여 군 역시 자유로울 수 없는 것이 현실이다. 실제로 민간 기업, 공공기관 등에 사이버 침해사고 증가경향에 따라 국방망에 대한 침해시도 역시 적지 않은 영향을 받고 있다. 더구나 과거와 달리 군을 상대로 한 사이버 침해 공격이 단순하게 군사기밀이나 정보탈취가 목적이 아니라 개인 호기심, 능력 과시, 영리적 이익 등과 같이 다양해지고 있으며 공격자 역시 특정 국가나 단체에 그치지 않고 군과 관계없는 개별 인원 등과 같이 다차원적으로 변해가고 있는 실정이다. 그럼에도 불구하고 국방부는 아직도 군을 대상으로 한 사이버 침해에 대하여 작전적인 측면에 국한하여 대응함으로써 차단, 피해보전 등 방어적인 수단으로 일관하고 있어 정확한 피해현황 진단 제한, 공격자의 목적 파악 불가로 동일한 피해가 지속될 우려가 존재한다. 더구나 일부 침해사건에 대한 수사를 진행하는 과정에서도 수사관할 한계로 인하여 관련 법령 미비 등에 따라 증거수집 및 범인 검거가 지연되거나 실패할 여지가 다분하다. 이에 국방부를 비롯한 유관기관들의 군 대상 사이버 침해 사고에 대한 범죄수사의 필요성 등 인식의 전환과 실효성 있는 수사권 확보를 위한 관련 법령, 제도 개선 등을 제시하였다.

◈ **주제어 : 사이버침해, 특별사법경찰, 국방부 조사본부, 헌병**

* 동국대학교 일반대학원 법학과 박사과정(제1저자)
** 국방부 조사본부 수사단 사이버수사대장(교신저자)

Ⅰ. 서론

최근 들어서 IoT(Internet of Things, 사물인터넷), 비트코인(Bitcoin, 사이버공간에서의 가상화폐로 디지털 정보량 기본 단위인 비트(bit)와 동전을 뜻하는 코인(coin)이 혼합되어서 탄생한 용어) 등 사이버상의 가상 세계 현실화에 대한 일반 국민들의 접근성 증대가 일반화되어 그 대중성이 날로 커져 가면서 이에 상응하는 사이버 위협 역시 점차 증가하는 추세이다.

실제로 한국인터넷 진흥원이 발표한 2018년 1분기 사이버 위협 동향 보고서[1]에 따르면 가상통화 거래소와 개인정보 유출, 피싱(Phishing, 피싱은 개인정보를 뜻하는 'Private Data'와 낚시를 의미하는 'Fishing'의 합성 용어로 사회공학적인 방법이나 기술적인 은닉 수법을 활용하여 민감한 개인정보 및 금융계정 등을 절취하는 신종 금융사기 수법) 메일 유포, 스피어 피싱(Spear-phishing, 스피어피싱은 불특정 다수인의 개인정보를 탈취하는 피싱(phishing)과 달리 특정 개인의 정보를 불법으로 취득하기 위한 공격기법을 지칭한다. 어원은 열대지방 어민이 하는 작살낚시(spearfishing)에 빗댄 표현으로 알려져 있다.) 공격을 위한 악성메일 유포, 국가 행사 관련 홈페이지 접속 장애 등 사이버침해 사고가 지속적으로 발생하고 있고 특히 주요한 사회적 관심사("올림픽", "주요 사건", "유명인 등")에 따라 공격 횟수, 유형, 대상이 영향을 받을 뿐 아니라 그 파급효과 역시 적지 않은 것으로 파악되고 있다.

1) '2018년 1분기 사이버 위협 동향 보고서', 한국인터넷 진흥원, 2018. 4월, 2-3쪽.

더구나 이러한 경향은 군을 대상으로 하여서도 유사하게 나타나는 것으로 판단된다. 실제로 국방부에서 지난 2017년 3월경, 대변인을 통해 발표한 '軍 인터넷 사이트에 대한 사이버 공격 실태' 발표에 따르면[2] 국방부와 롯데가 성주 골프장 부지 맞교환 계약을 맺었던 2017년 2월 27일~28일을 기점으로 70여개의 軍 사이트에 대한 사이버 공격이 증가하였고 사드 발사대 등 일부 장비가 반입된 2017년 3월 7일 이 후에는 침해 시도가 더욱 심해진 것으로 알려져 있다.

문제는 위와 같은 침해시도가 지속적으로 발생하고 있음에도 불구하고 침해에 따른 피해복구, 피해수준 파악에 따른 예방대책 강구 위주의 대응으로 인하여 실제 침해자에 대한 검거 등 원점 추적의 중요성을 간과해 온 측면이 없지 않다는 점이다.

사실, 정부를 비롯한 민간 기업체에서도 사이버 침해사고를 당하고 나서 침해인원에 대한 추적, 검거보다 피해 현황을 파악하여 이를 차단하는 데에만 대부분의 역량을 집중해왔으며 결국 침해사고 대응의 목적이 조직에 대한 신뢰성 저하 최소화, 조속한 추가 피해 발생 방지대책 마련 등 사회적 비판 여론 대응에 중점이 맞추어져 왔다고 볼 수 있다.

그러나 위와 같은 방식의 대응은 문제의 핵심을 건드리지 않은 채 표면만 겉도는 임시방편적 조치에 불과한 것으로 이러한 방식의 조치 등에 관한 KISA 침해대응단 책임연구원[3]의 칼럼에 따르면 사이버 공격 침해의 원격 취약점이 알려지지 않고 계속 악용되도록 방치될 경우 공

2) 이데일리, "군 대상 사이버 공격 증가세...중국발 사드보복 추정", 2017. 3. 21, http://www.edaily.co.kr/news/read?newsId=03253766615865616&mediaCodeNo=257&OutLnkChk=Y(2018. 10. 12. 검색).

3) 한승원, "공격자 분석 관점의 대응방안", KISA 침해대응 사이버보안정책기획, 2018. 4월.

격자는 오랫동안 이런 취약점을 통해서 여러 서버를 공격하게 됨에도 불구하고 실제 피해자는 이를 인지하지 못하고 있을 수 있을 뿐 아니라, 특히 운영 중인 시스템이 외부로부터의 접근이 가능하거나 해커가 내부망 침입에 성공했다면 피해는 매우 심각한 수준으로 커질 수 있다고 경고하고 있다.

물론, 경찰 등 수사기관에서 침해사고에 따른 추적 등이 이루어져오긴 했으나 이러한 수치는 실제 발생한 침해사고 대비 현저히 적은 정도로 원점 근절이 미약한 만큼 후속 침해 우려는 여전히 존재하고 있고 특히 군의 경우 사이버 침해사고를 범죄수사 측면보다 사고대응이나 작전의 일환으로 인식하는 경향이 강하다 보니 그 동안 범죄수사를 통한 침해자 검거보다 공격자 신원 파악 및 침해피해 후속조치에 집중하여 제도적으로 수사부분 발전이 미흡한 측면이 없지 않은 것이 사실이다.

이에 본 글에서는 그 동안 군을 대상으로 발생한 사이버 침해의 경향 변화와 범죄수사를 통한 문제해결의 중요성 및 법령의 미비로 인한 사이버 침해사고에 대한 수사의 현실적 문제를 진단하여 그 대안을 제시하고자 한다.

Ⅱ. 사건개요 및 분석

그 동안 군을 대상으로 한 사이버 공격의 경우 대부분 군사기밀 탈취, 주요 인사 정보 취득과 같이 국가안보에 심대한 영향을 미칠 목적을 가진 사고로 정확한 침해 시도인원에 대한 특정없이 북한 추정 소행이라는 결론을 내는데 그쳐왔다.

실제로 2018년 5월 남북정상회담에 앞서 한국소비자원 등에 해킹 공격사례에 대하여 정확한 범인을 검거하지는 못하였지만 정부에서는 북한 해커 조직으로 알려진 '히든 코브라(Hidden Cobra)'의 해킹시도로 판단한 바 있으며[4] 남북이산가족찾기 전수조사를 사칭한 이메일을 이용한 APT 공격 및 2018년 6월의 북미정상회담 기간에 '미북 정상회담 전망 및 대비'라는 악성코드 공격에 대해서도 북한 해커 조직 '금성121(Geumseong121)'의 범행이라고 판단하였지만 명확한 증거가 있다고 보기는 어려운 실정이다. 더구나 국내 가상화폐거래소 중 하나인 유빗이 해킹피해로 파산절차에 들어간 사례 관련해서도 북한이 해킹의 배후세력일 가능성이 높다고 알려지는 등 음모론만 제기되어 국제적인 논란이 야기된 적이 있다.[5]

특히, 일본에서 계속하여 제기되는 북한 해커부대 세력 소개는 이러한 논란을 더욱 가중시켰는데, 이에 관하여 김흥광 NK지식인연대 대표는 "라자루스는 북한의 정보기관 정찰총국의 180 부대에 속하는 조직"이라고 니혼게이자이에 밝혔으며 해당 내용에 따르면 180부대는 김정은이 지시해 설립된 조직으로, 핵무기와 장거리미사일 개발에 필요한 외화획득을 주 임무로 하고 있으며 2013년에 설치된 180부대는 전부터 활동했던 라자루스를 흡수한 것으로 추정될 뿐 아니라 니혼게이자이에서는 해당 180부대가 2018년 1월말 일본에서 발생한 가상화폐 거래사이트 코인체크의 580억엔 해킹사건도 저지른 것으로 판단하고 있다고

4) 아주경제, "남북정상회담·추석연휴" 韓 사이버 위협 고조, 2018. 9. 19, https://www.ajunews.com/view/20180919142230946(2018. 10. 13. 검색).

5) 브리짓경제, "가상화폐거래소 유빗 파산, 배후는 비트코인 노린 북한?", 2017. 12. 22, http://www.viva100.com/main/view.php?key=20171221010007545(2018. 10. 15. 검색).

지적한 바 있다.

더구나 180부대는 외화획득을 위한 사이버 공격 외에 일본과 중국에서 소프트웨어 개발에도 손을 대고 있다고 알려져 있다. 또한 니혼게이자이는 180부대 이외에도 121부대, 91호실, 랩 110 등 북한의 사이버 전 부대가 활동하고 있다고 밝혔는데 121부대는 1998년 김정일이 설립한 것으로 외국 통신 전력, 교통 등의 인프라에 대한 사이버 공격을 주요 임무로 하며 인원도 수천명으로 정찰총국 내 최대 조직이고 91호실은 과학기술 정보 획득을 전담으로 한 조직으로, 인원은 500여명으로 추정되며 랩 110은 사이버공격 전술 개발을 목적으로 한다고 전해진다.[6)]

즉, 위와 같이 판단하게 된 이유 역시 과거 공격유형과 동일하거나 침해 경로 및 지역의 유사성 등을 들고 있으나 실제 범인 검거까지 이루어지지 않아 실체가 검증되지 않다 보니 공격자의 정확한 의도나 실제 침해시도를 통한 피해 수준을 파악하기 어려운 것이 사실이었다.

그러나 니처러 군이 운영하ㅓ나 군 관련 사이트를 대상으로 한 침해시도는 일반 기업체들의 그것과 달리 반드시 원점을 추적하여 공격자를 검거함으로써 범죄 목적과 피해 수준을 정확하게 파악하는 것이 중요하다. 이는 추정에 근거한 안보 불안 가중을 해소하고 자칫 증거가 없는 상태에서 특정 국가, 단체를 공격자로 지목할 경우 발생할 수 있는 외교적 마찰 등을 불식시키기 위해서이다.

실제로 2014년경, 육군 훈련소 홈페이지 해킹 시도 사례에서도 알 수 있듯이 당시 침해사고 발생 당시에만 해도 언론에서는 육군 훈련소라는 부대의 상징성을 감안하여 군사훈련 관련 비밀 탈취 등을 의심하

6) 뉴시스, "니혼게이자이 '北 정예 해커부대 수천명 조직적 활동 중'", 2018. 2. 25, http://www.newsis.com/view/?id=NISX20180225_0000236724&cID=10101&pID=10100(2018. 10. 16. 검색).

며 각종 추정 의혹이 불거졌으나 실제로 원점 추적을 통해 범인 검거까지 이루어진 결과 일반 대학생의 단순한 호기심에 의한 해킹 시도로 밝혀져 논란을 불식시킨 바 있다.

당시 수사결과에 따르면, 2014년 11월 1일 여대생이 육군 훈련소에 입대한 전 남자친구의 소식을 알아보기 위해 훈련소 홈페이지를 확인하던 중 게시판에 전 남자친구에게 다른 여성이 인터넷 편지를 보낸 것을 알고 해당 내용을 열람할 목적으로 훈련소 홈페이지 관리자 계정에 대한 해킹을 시도한 것으로 밝혀졌다.[7]

이 뿐만 아니다. 2017년에도 국방 산하 국방연구기관을 비롯한 육군 예하 부대 홈페이지에 대한 사이버 침해 공격 사건이 발생하자 당시 국방부는 공격자에 대한 검거 등의 조치보다는 "홈페이지는 국민들을 위한 대외 공개용 자료만 담고 있으며 망분리를 통해 군 내부 자료와는 별도로 관리하고 있다, 軍 홈페이지를 총괄하는 국방부 데이터센터 확인결과 외부 접근이나 공격정황은 발견되지 않았다"라고 입장을 밝힌 바 있다.

그러나 국제 해커 조직 어나니머스("Anonymous") 소속이라고 자신의 신원을 밝힌 미니언 고스트("SNS 아이디명")는 본인의 페이스북, 트위터를 통해 前 국회의장과 육군훈련소 홈페이지를 해킹하였고 심지어 2017년 8월 7일과 8월 17일에 해킹사실을 대외 공표하면서 '한국군 정보가 필요하면 무료로 제공할테니 연락하라'며 자신의 트위터 주소를 남김으로써 당시 국방부가 밝힌 자체 진상 조사 결과와 상반된 내용을 주장하여 논란이 불거지기도 하였다.(하단 첨부사진 참조)

---

7) 서울경제, "헤어진 남친소식 궁금..여대생 훈련소 홈피 해킹시도", 2015. 1. 28, https://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=102&oid=011&aid=0002633000(2018. 10. 14. 검색).

〈그림 1〉 공격침해 사례(육군훈련소)

▲ 미니언 고스트가 공개한 육군훈련소 공격 정황[자료=SNS 캡처]

더구나 2015년 4월경, 발생한 대한민국 공군 전우회, 한국방위산업학회 등 군 관련 4개 사이트에 동일한 악성링크 유포 등 사이버침해사고 발생의 경우 전현직 군인 개인정보 및 주요 방위산업 내용에 대한 탈취 시도가 있었음에도 불구하고 피해에 따른 복구조치 외에 제대로 된 수사가 진행되지 않아 침해 원점조차 파악되지 않아 동일 침해 우려를 낳기도 하였다.[8)]

8) 보안뉴스, "군 관련 홈피 4곳 타깃 공격? 동일 악성링크 포착", 2015. 4. 14, https://www.boannews.com/media/view.asp?idx=45945&kind=1(2018. 10. 17. 검색).

Ⅲ. 사이버 침해범죄에 대한 군 인식

더구나 이러한 실태 파악의 허점은 사드배치에 대한 불만으로 중국발 해킹의혹에 대한 국방부의 '피해 없음' 발표와 상반된 언론의 기사를 통해서도 알 수 있다.(하단 첨부 사진참조)

〈그림 2〉 중국발 해킹의혹

CNN 갈무리

이처럼 군을 대상으로 한 사이버 침해공격은 과거와 달리 공격 주체가 어떤 특정 단체나 국가에 국한되지 않고 반드시 군사적인 목적으로만 한정되지 않은 것이 현실이다. 앞서 본 사례와 같이 단순한 개인 욕구 해소, 영리적 이익 취득 차원이거나 아니면 특정 해커 조직의 능력 과시처럼 전투나 전쟁행위가 아닌 사이버 범죄 차원의 침해 사례가 적지 않은 것으로 보인다.

앞서 살펴본 바와 같이 군을 대상으로 한 사이버 침해범죄는 더 이상 안보적 차원의 공격작전 행위로만 간주해서는 안 될 것으로 보인다. 그럼에도 불구하고 최근 국방부를 비롯한 육해공군의 사이버 침해 대응 방안을 보면 아직도 사이버 침해를 범죄가 아닌 작전의 일환으로 판단하고 있는 것으로 추정된다.

실제 지난 2017년 9월 5일 '3군 합동 사이버안보 워크숍'[9]에서 다루어진 사이버 침해 관련 토의주제들을 보면 '사이버전 최근 동향 및 한국군 발전방향, 무기체계 사이버방호대책 강화방안, 함정 탑재 체계에 대한 사이버 위협 대응방안, IoT 기반 무기체계 사이버방호 방안, 지상작전과 연계한 사이버전 수행방안 등'으로 범죄수사 분야는 전혀 다루어지지 않았다.

군의 인식이 이렇다 보니 사이버 침해 피해를 입고도 수사를 통해 해당 범인을 검거하겠다는 등 실제 근본적인 문제에 대한 대응방안 검토는 제대로 이뤄지지 못하고 있다.

이는 지난 2017년 사드 관련 중국발 해커들의 軍 주요 사이트 공격 시도에 대한 국방부 대변인의 '최근 사이버 침해 시도는 다소 늘어난 수준이지만 이로 인한 해킹 피해 사례는 없는 것으로 확인되고 있다', '군 내부 전산망인 인트라넷과 인터넷 서버의 연결은 정확하게 분리돼 있다.', '인포콘(정보작전방호태세)을 격상했다.'와 같은 입장발표문을 통해서도 충분히 짐작할 수 있다.

그러나 위와 같은 인식은 軍 전력 저하 차원에서도 매우 위험한 발상이라 할 수 있다. 실제로 지난 2017년 언론에 보도[10]되어 사회적으로

9) 보안뉴스, "대한민국 육해공군, 사이버전 대응 위해 머리 맞댄다", 2017. 8. 23, https://www.boannews.com/media/view.asp?idx=56549&kind=2(2018. 10. 9. 검색).

물의를 일으킨 적이 있었던 '軍 전세객차 예약시스템 조작사건'의 경우만 해도 최근 댓글사건 등에서 논란이 되고있는 매크로 프로그램(특정 명령 자동 수행 기능)을 이용하여 국방망을 대상으로 사이버 침해 범죄를 자행하였을 뿐 아니라 당시 보도내용에 따르면 2015년 6월경 최초 해당 시스템에 불법 프로그램을 이용하여 사이버 침해범죄를 저지르고도 적발되지 않다가 업무 인수인계 과정에서 이를 인수받은 후임자가 2016년 1월부터 2017년초까지 1년여간 50여 차례에 걸쳐 불법적으로 침해행위를 한 사실이 국방부 조사본부(사이버범죄수사대)의 수사를 통해 밝혀지기까지 지속적으로 이루어졌다는 사실은 사이버 침해사고에 대한 범죄수사를 통하여 범인 검거 등 원점에 대한 근본적 해결이 얼마나 중요한지를 보여주는 사례라 할 수 있다고 하겠다.

만약 당시 수사가 제대로 이루어지지 않은 채 다른 침해사례와 같이 방어조치에 그쳤다면 지금도 해당 침해 행위는 진행되고 있었을 것이고 앞으로도 계속하여 이어졌을 가능성을 감안할 때 이로 인한 피해규모가 어느 정도일지 가히 상상하기 어려울 정도이다.

Ⅳ. 軍 대상 사이버침해범죄 수사한계

위와 같이 군을 대상으로 한 사이버 공격행위는 명백한 범죄로 이에 대해서는 적극적인 수사절차가 이루어져야 한다. 그러나 실제 수사가 이루어진다고 해도 현재의 법률적인 한계로 인해 그 실효성은 크지 않

10) 동아일보, "군 무료열차 타려고...예약시스템 뚫은 공군 중위", 2017. 4. 25, http://news.donga.com/3/all/20170425/84050765/1(2018. 10. 8. 검색).

을 것으로 보인다.

실제로 앞서 언급한 육군 훈련소 해킹 범죄의 경우처럼 최초 피해사실을 인지한 육군에서는 군사법경찰 조직인 육군 중앙수사단을 통해 범죄피해 발생사실을 인지하였으나 경찰에 수사의뢰를 하는 등 직접적인 수사를 하지 못한 것으로 보도된 바 있다.

또한 국방부 조사본부(사이버범죄수사대)에[11] 따르면 '16.2월 ~ 3월 어간, 인적불상자에 의한 현역 군인들에 대한 메일 계정 탈취 등 사이버 침해범죄 발생에 대하여서도 당시 국방부 조사본부(사이버범죄수사대)가 범인검거를 위해 추적 수사 과정에서 중국 거주 민간인 1명 등 총 6명을 식별하여 이들에 대한 혐의를 입증하고자 영장을 신청하였으나 신분이 민간인이란 이유로 기각되어 부득이하게 경찰로 사건을 이첩하는 상황이 발생하는 등 수사관할의 한계로 인하여 조사를 중단해야만 했던 사례가 있었다고 한다.

문제는 위와 같이 수사관할 한계에 따라 추적수사를 중단하고 경찰에 이첩하게 될 경우 최초 수사를 담당 했던 군사법경찰이 배제되어 수사의 연속성이 단절되고 이첩받은 경찰에 사건배경부터 최종 추적지점까지의 일련의 과정을 이해시키는 과정에서 사이버상 주요 증거인멸, 범인 잠적 등 수사의 실효성이 저하되어 결국 검거에 실패할 가능성이 높아진다는 점이다.

실제로 법리적으로도 現 형사소송법과 군사법원법상 군사법경찰의 경우 신분적 재판관할[12]이 현역 군인, 군무원 등으로 한정되어 있어서 군

11) 국방부 조사본부 사이버범죄수사대 국방 정보통신망 침해범죄 수사현황, 2018. 5. 1.

12) 「군사법원법」(법률 제15165호, 2017. 12. 12., 일부개정) 제2조에 따라 군사법원은 군형법 제1조 제1항에서 제4항까지 규정된 사람에게 적용하고 해당

사기밀 등이 탈취되었다는 명확한 피해사실이 입증되지 않은 이상 민간인을 대상으로 한 강제적 수사가 제한되어 인적불상자의 침해 공격에 대하여 사이버상의 추적 수사를 위한 각종 영장신청시 군검찰에서 기각되거나 군검찰에서 청구가 된다고 해도 군사법원에서 해당 청구에 대한 검토 자체를 배제하는 것이 현실이다.

물론 경찰에 수사의뢰를 하는 방식으로도 수사절차 진행은 가능하지만 앞서 살펴본 실제 주요 사례들을 통해서 알 수 있듯이 사이버 침해 범죄의 특성상 공격자는 공격 전후 증거인멸을 위해 경로 삭제, 개인 사용 PC 폐기, 공격지 이탈 후 잠적 등을 한다는 점을 감안할 때, 최초 인지 기관에서 조속한 초기 증거 확보 및 경로 추적이 무엇보다 중요한데도 경찰에 수사의뢰를 위한 내부 보고, 수사의뢰 후 경찰에 의한 현장방문, 군 내부 망에 대한 접속 허가 등의 부가적인 절차를 거치다 보면 이미 증거는 증발되고 범인은 잠적하여 수사의 실효성이 없는 경우가 부지기수이다.

물론, 임의수사의 일환으로 해당 인터넷 서버 관리 업체에게 접속 추적 경로 협조요청을 하거나 한국인터넷진흥원 등에 수사 협조 차원에서 사이버 침해 사고에 대한 초기 대응조치 일환으로 공격루트, 접속 원점 등의 정보를 요청해볼 수는 있겠으나 강제수사가 아니다보니 협조에 불

인원이 신분을 취득하기 전에 저지른 범죄도 재판권을 보유하되, 군에서 운용하는 공장이나 전투용으로 이용되는 시설 등에 물건을 저장하는 곳에 대해 군용시설물을 손괴하는 죄를 저지른 내외국인 등에 대하여는 적용을 제외한다. 또한 군사법원은 기소된 사건에 관해 군사법원이 재판권을 상실하게 되면 결정으로 해당 사건을 재판권 있는 동일 심급 민간법원에 이송하도록 하되 고등군사법원에 계류된 사건 중에 단독판사의 담당 사건에 대한 항소는 이에 대응하는 지방법원 항소부에 이송해야 한다. 그리고 이러한 경우에 이송을 하기 전에 이루어진 행위는 그 후에도 효력상 영향은 유지된다. 또한, 계엄법 및 군사기밀보호법 제13조의 죄에 대해서도 재판권을 가진다.

응할 경우 요구할 방법이 부재하고 한국인터넷진흥원에서 군의 요청을 받아들여 대리 요청을 수용함으로써 자료 확보를 한다고 해도 관련 법률상 제공받은 자료를 재이송할 수 있는 근거가 명확하지 않아 차후 이를 빌미삼아 범인 입장에서 증거능력 유무 여부를 따지게 되면 문제가 불거질 수 있다.[13)]

실제로 해당 법률은 과기부장관으로부터 침해사고 대응을 위한 권한을 위임받은 한국인터넷진흥원으로 하여금 침해사고 관련 정보수집과 전파, 예보와 경보, 사고발생시 긴급조치 등을 취하도록 하고 있으며 정보통신업체들로부터 위 관련 침해사고 유형 통계, 통신망 소통량에 관한 통계, 접속을 하는 경로별 이용량과 같이 침해사고와 관한 각종 정보를 제공받을 수 있고 침해사고에 관한 사항을 발견하거나 범죄혐의를 인지한 경우, 자체 신고나 민원을 접수받거나 이용고객들의 정보 안전 및 신뢰확보를 저해하는 침해사건이 발생한 경우 관계 물품이나 서류 등을 제출받을 수 있음에도 이를 다시 다른 기관에 제공할 수 있도록 하는 규정은 부재하다.

문제는 또 있다. 만약 위와 같이 임의수사의 일환으로 적극적인 협조가 이루어져서 군사법경찰에 의한 사이버 침해 사고 관련 범죄수사가 이루어진다고 해도 軍 자체 대응의 실효성을 위한 법령 근거가 미흡하다면 제대로 된 내부 진행이 이루어지기 어렵기 때문이다.

실제로 軍 관련 사이버 침해사고 발생 시 사이버 영역의 특성상 국방부, 육해공군 등의 구분이 있을 수 없어 일원화된 수사가 필요한 점을 고려함에 따라 관계 규정인 국방사이버안보 훈령에서는 사이버 침해에 따른 범죄수사 분야와 관련하여서는 국방부 조사본부에 '국방 사이버

13) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(법률 제14839호, 2017. 7. 26, 타법개정) 제48조의2.

영역에 대한 침해시도 및 사고에 대한 민간조사 협조업무'를 규정으로 명문화하고 있는 등 국방부를 포함한 전군 헌병(군사법경찰조직)에 대한 수사지휘권의 필요성을 명시하고 있음에도 불구하고 정작 국방부조사본부령에서는 이러한 법적 근거가 부재한 실정이다.[14]

실제로 해당 법령에서는 국방부 조사본부의 임무에 관하여 국방부나 예하 직할 부대나 기관, 청 등에 소속되어있는 군인과 군무원에 관한 범죄수사와 예방 및 범죄정보 관련 업무, 전군 헌병의 업무 중에 국방부장관으로부터 하명받은 사항, 2개 이상 타군이 연관된 범죄사안에 관한 수사, 민원제기 건 중에 군내 사망사건에 관한 조사, 군에 관한 중요사건이나 사고 관련 속보접수 및 처리와 분석대책 수립, 사망사건 발생시 현장감식과 지원업무, 과학수사와 범죄의 예방 등을 위한 연구, 軍 관련 범죄수사와 예방 등을 위한 유관기관 등과 협조, 부정 군수품에 관한 계몽 및 단속활동, 군교도소와 군미결수용실의 운영에 관한 업무를 규정하고 있다.

즉, 국방부 차원에서 전군을 포함한 국방망에 대한 사이버 침해 범죄 수사에 대하여서는 국방부 조사본부에 수사책임을 부여하고도 정작 국방부 조사본부령에 주어진 권한에는 각군 헌병에 대한 수사지휘권이 부재하여 각군 헌병의 사이버수사 조직을 활용할 수 없는 아이러니한 상황이 발생하고 있는 것이다.

14) 「국방부조사본부령」(대통령령 제28266호, 2017. 9. 5. 타법개정) 제1조.

〈그림 3〉 국방부 사이버침해 대응체계

Ⅴ. 수사실효성 확보를 위한 방안

이미 주지하다시피 군 대상 사이버 침해 공격의 경우 대상자가 누구인지 여부는 해당 인원을 검거하기 전까지는 신분확인이 제한됨에 따라 군사기밀 탈취가 아닌 이상 군사법경찰관으로서 수사의 한계가 존재한다. 그렇다고 하여 군사법원법과 형사소송법상 재판관할이 다른 사건에 대하여 상호 엄격한 분리주의를 천명한 대법원의 판례[15]를 감안할 때 사이버 침해 범죄에 대해서만 예외적으로 군사법원법에 민간인에 대한 수사관할을 추가할 수도 없는 노릇이다.

실제로 본 판결 관련 사건의 경우 현역 신분이던 대령이 재직 중 자신의 직위를 이용하여 탄약 등 군용물을 취득한 뒤, 방위사업체와의 방탄사업 관련 실험을 진행해오던 중 업체로부터 전역 후 특정 직위 등을 약속받는 등 뇌물을 수수하고 이에 대한 대가로 업체에서의 실험목적 대상인 실탄을 별도로 획득하기 위해 이미 개인이 확보하여 보유하던

15) 대법원 2016. 6. 16. 자 2016초기318 전원합의체 결정.

해당 실탄 등을 전역하면서 반출하였고 이 후에 실제로 업체에 취업하여 이를 이용하여 실험을 진행하였다가 적발되었으며 본 사건에 관하여 군사법원은 군용물의 절도혐의를 적용하여 비록 민간인 신분이지만 군사법원법 적용대상이라 점에 착안해서 예비역 대령에 관한 재판을 하였으나 재판 과정에서 군용물 범죄 외에 뇌물수수 등 일반 형법 적용 범죄까지도 함께 직권으로 유죄로 판결하였다가 피고인 신분이던 예비역 대령측이 재판권 문제를 제기하였다. 그리고 이에 관하여 대법원은 군사법원 및 민간 법원 사이의 재판권 관련 쟁의사건이 발생해서 피고인의 재판권 재정신청이 된 사안에 대하여 군사법원은 비록 군인 등의 신분인 자가 범죄 후 전역 등의 사유로 신분변경 시 재판권이 상실된다고 판결하였다.

바로 이러한 점을 고려할 때, 군사법경찰관으로 하여금 軍 대상 사이버 침해 범죄에 한하여 특별사법경찰권을 추가로 부여하는 방안이 검토되어야 한다.

현재는 법률[16]상 군사법경찰에 대하여 군용물 등 범죄에 관한 특별조치법이나 군사기밀보호법에 규정된 범죄에 관하여서만 민간 검사의 지휘를 받아서 사법경찰관리의 직무를 수행토록 하고 있어서 한계가 존재한다.

이에 따라 해당 조항을 개정하여 헌병 등으로 하여금 정보통신망 이용촉진 및 정보보호 등에 관한 법률상 국방망에 대한 침해범죄 부분 등에 한정하여 특별사법경찰권을 부여토록 하여 민간 검사지휘 아래 일반법원으로부터 영장발부를 받는 등 효과적인 수사를 통한 조속한 범인 검거 및 초기 인멸이 우려되는 주요 증거를 확보하여 공소유지의 내실

16) 「사법경찰관리의 직무를 수행할 자와 그 직무범위에 관한 법률」(법률 제15253호, 2017. 12. 19, 일부개정) 제9조.

을 기할 수 있다고 판단된다.

만약 위와 같은 법률 개정이 군사법경찰의 과도한 민간 개입 우려로 어렵다고 판단된다면 차선책으로 임의수사의 실효성을 확보하기 위한 방안의 하나로 정보통신망 이용촉진 및 정보보호 등에 관한 법률[17]상 방송통신위원회의 인터넷 서비스업체 대상 필요 자료제출권을 군사법경찰이 정당하게 이용할 수 있는 법적 근거를 마련해보는 것도 검토해볼 만한 사안으로 판단된다.

즉, 해당 조항 하단에 새로운 조항을 신설("예> 법률 제64조의2[자료활용 등] '제1항 수사기관은 범죄수사에 필요한 경우 방송통신위원회에 제64조 각호에 규정된 자료제출권 행사를 촉구할 수 있다. 제2항 방송통신위원회는 제64조에 의하여 제출받은 자료를 범죄수사를 위한 필요에 의하여 수사기관으로부터 요청받은 경우 이를 제공할 수 있다'")하여 군사법경찰과 같은 수사기관이 침해인원에 대한 추적 수사를 위해 인터넷 관리자, 사업자 등을 통해 획득해야할 자료를 긴급하게 방송통신위원회를 통해 요청하여 이를 획득할 수 있도록 할 수 있을 것이다.

만약 이와 같이 자료 확보 요청권을 부여한다면 임의수사의 일환으로 획득한 자료를 방송통신위원회를 거쳐 재차 임의제출 받음으로써 차후 증거능력에도 문제가 없을 것으로 보인다.

본안에서 검토된 사항 중 현재 군을 대상으로 한 사이버 침해범죄의 경우에 국방부 조사본부로 하여금 범죄수사를 하도록 책임을 지우고 있음에도 불구하고 각군에서 운용 중인 헌병 소속 사이버 범죄수사 조직에 대하여서는 일체의 통제, 지휘권을 부여하지 않음으로 인하여 수사의 효과 저하 및 대응이 어려운 것이 현실이다. 이에 따라 훈령상 부여

17) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(법률 제14839호, 2017. 7. 26, 타법개정) 제64조.

한 국방부 조사본부의 사이버 침해범죄 수사에 대한 책임 이행의 실효성 확보를 위하여 적어도 現 국방부 조사본부령 개정이 필요할 것으로 보인다.

즉, 국방부 사이버 안보훈령상 국방 사이버 영역의 침해시도 및 사고에 대한 민간조사 협조 업무를 담당하도록 규정한 국방부 조사본부에 대한 임무수행을 위해 現 국방부조사본부령의 임무규정에 '국방 사이버 침해 범죄에 대한 수사업무 관련 각군 헌병에 대한 수사지휘, 통제' 규정을 신설하여 전군에서 발생하는 사이버 침해 범죄에 대한 현황을 일괄적으로 파악하고 유사한 수법 및 경로, 각 군에서 진행 중인 수사진행 경과를 공유함으로써 범인의 특징, 활동 영역을 특정하고 가장 효율적으로 대응가능한 사이버 수사인력과 조직을 통합하여 활용하게 함으로써 수사의 내실을 기할 수 있을 것으로 판단된다.

Ⅵ. 결론

지금까지 軍 대상 사이버 침해범죄의 변화하는 경향과 現 대응체계의 한계 및 범죄수사의 실효성을 제고하기 위한 각종 법령 개정에 관하여 살펴보았다.

분명한 것은 갈수록 증가하는 사이버 환경의 특성과 더 이상 사이버 침해의 목적이 군사기밀 탈취 등에 한정되거나 특정한 단체나 국가로 국한되지 않으며 개인적인 분노 표출이나 능력 과시 등을 이유로도 침해범죄를 저지를 가능성이 높아지고 있다는 점이다.

특히, 해당 범죄에 대한 범인 검거 등 근본원인을 해결하지 않고 지

금처럼 방어적인 조치에 머물 경우 공격 시도 증가와 더불어 실제 피해를 입은 정도에 대한 파악조차 어려워질 수 있을 것으로 예상된다.

더불어 군과 민간의 구분이 어려워지는 사이버 침해 범죄의 성질, 경찰에 수사의뢰 등 지연 조치에 따른 증거인멸과 범인 잠적 등이 수시로 이루어지는 사이버 침해범죄 경향을 고려할 때, 군내 사이버 침해시도를 최초 인지한 군사법경찰에서 조속하게 증거확보, 범인 추적과 검거가 이루어질 수 있도록 현재의 미비한 각종 법령의 개정이 필요하다는 점에 대한 상황인식과 이를 개선 시 핵심적으로 검토되어야할 사항들에 관하여 대안을 제시하였다.

명심할 점은 시간이 흐를수록 침해 세력은 점차 커져갈 뿐만 아니라 그 피해는 군이 기존에 짐작한 것 이상으로 불어날 수 있다는 점이다.

그러므로 위와 같은 현실적인 문제점들을 깊이 있게 검토하여 신속히 개선이 이루어질 수 있도록 국방부, 각 군을 비롯한 관계기관들의 노력이 촉구되어야 할 것이다.

〈논문접수 : 2018. 10. 8, 심사개시 : 2018. 11. 19, 게재확정 : 2018. 12. 11.〉

참 고 문 헌

Ⅰ. 국내문헌

1. 단행본

한국인터넷진흥원, 사이버침해사고 신고 안내서, 2018.

2. 보고서

한국인터넷진흥원, 2018년 1분기 사이버위협 동향 보고서, 2018.

국방부 조사본부, 사이버범죄수사대 국방망 침해사고 수사 일반 현황, 2018.

3. 기타

대법원 2016. 6. 16. 2016초기318 전원합의체 결정

뉴시스, “니혼게이자이 ‘北 정예 해커부대 수천명 조직적 활동 중’”, 2018. 2. 25.

동아일보, “군 무료열차 타려고...예약시스템 뚫은 공군 중위”, 2017. 4. 25.

데일리시큐, “한국군, 안보, 대북 연구기관 타깃 APT 공격수행 포착”, 2018. 6. 9.

보안뉴스, “군 관련 홈피 4곳 티깃 공격? 동일 악성링크 포착”, 2015. 4. 14.

보안뉴스, “대한민국 육해공군, 사이버전 대응 위해 머리 맞댄다”, 2017. 8. 23.

보안뉴스미디어, “전 국회의장, 육군훈련소 홈피해킹 주장...팩트 체크해보니”, 2017. 8. 18.

브리짓경제, ‘가상화폐거래소 유빗 파산, 배후는 비트코인 노린 북한?’, 2017. 12. 22.

서울경제, “헤어진 남친소식 궁금..여대생 훈련소 홈피 해킹시도”, 2015. 1. 28.

아주경제, "'남북정상회담·추석연휴' 韓 사이버 위협 고조", 2018. 9. 19.
연합뉴스, "군 인터넷 홈페이지 해킹시도 증가", 2017. 3. 21.
이데일리, "군 대상 사이버 공격 증가세...중국발 사드보복 추정", 2017. 3. 21.

< ABSTRACT >

Countermeasure of Problem about Cyber Attacks for Military System

Kim, Ho · Lee, Ju-Ho

The reality is that the Ministry of National Defense can not be free from the growing number of cyber attacks in the increasingly sophisticated environment. In fact, attempts to violate the national network are also affected greatly due to the increase in cyber infringement incidents among private companies and public institutions. Moreover, since cyber attack on the Ministry of National Defense is not simply intended for military secrecy or information theft, it is not a matter of individual curiosity, show of ability, or profit, nor is the attacker in a particular country or group. Nevertheless, the Ministry of National Defense is still responding to cyber bullying in a way that is limited to operational aspects, limiting the diagnosis of the damages with the same purpose, as it can not be identified by defensive measures such as blocking and preserving the damage. Moreover, there is a high possibility that the collection of evidence and arrest of criminals will be delayed or failed in the course of an investigation on some of the violation cases due to insufficient jurisdiction of the investigation. Thus, the Ministry of National Defense and other related agencies presented the need for criminal investigations on cyber violation cases, related laws and systems for changing their perceptions, securing effective investigative rights, etc.

◈ Key words : Cyber attack, Military police, Ministry of National Defense