사이버범죄 정보분석 (Intelligence) 발전 방안

김기범 경찰대학 국제사이버범죄연구센터장

1. 머리말

지난 3월 22일 미래창조과학부와 한국인터넷진흥원은 '어나니머스 해킹조직'이 4월 14일에 한국정부를 공격할 예정이라고 발표했다. 경찰청도 어나니머스가 어떠한 조직인지, 실제로 공격을 예고했는지 확인할 필요가 있다고 밝혔다[1]. 당시 신용카드사의 개인정보 유출사고로 대표이사들이 사임했던 때라 부처와 민간 모두 긴장하면서 비상대응에 들어갔다. 비록 범죄자들이 며칠 후에 공격철회를 선언했지만, 경찰이 학생들이 장난삼아 범행한 것이라고 수사결과를 발표[2]할 때까지 경계를 늦출 수 없었을 것이다.

여기에서 몇 가지 질문을 할 수 있다. 왜 장난이라는 것을 즉시 알지 못했을까? 최소한 국내의 어나니머스 해킹조직은 파악하고 있어야 하는 것 아닌가? 좀 더 일찍 검거할 수는 없었을까? 이 순간에도 예고 없이 일어나고 있는 사이버범죄는 제대로 대응하고 있는 것인가?

위의 질문은 사건발생 이후 추적하는 사후적 방법에서 벗어나서 사전에 탐지하여 위험을 제거할 수 없는지에 대해 묻고 있다. 전통적 범죄와 달리 사이버범죄는 범죄자들이 익명성의 장막 뒤에 숨어 있고, 회피와 은닉기술 발달로 추적도 어려우며 피해가 크기 때문에 선제적 대응이 요구된다. 이를 위해서 사이버범죄에 대한 정보를 수집하고 분석하는 체계가 필요하다. 즉, 해킹조직의 인지와 정보수집, 공격의 규모와 위험 식별, 수사대상의 타겟팅과 우선순위 결정, 추적단서와 증거확보 등의 작업이 지속적으로 이루어진다면 가능할 것이다. 본 글에서는 사이버범죄 문제를 선제적으로 대응하기 위해 필요한 정보분석(Intelligence) 제도의 개념을 소개하고, 문제점을 살펴본 뒤 발전방안을 제시하고자 한다.

2. 이론적 고찰

2.1 정의

사이버범죄를 정의하는 것은 어렵기 때문에 실제 사용할 때 세분화하는 작업이 필요하다[3]. 여기에서는 유럽평의회(Council of Europe)의 사이버범죄협약(Convention on Cybercrime)에서 제시하고 있는 4개의 유형 중 '컴퓨터 데이터와 시스템의 기밀성, 무결성, 가용성에 대한 범죄'로 국한하여 정의하고자 한다. 경찰청에서 분류하여 왔던 '사이버테러형 범죄'의 개념과 비슷하다.

정보분석은 전략적 혹은 전술적 판단이 필요한 의사결정자를 위해 정보를 수집, 분석, 배포하는 조직적 활동을 의미한다. 정보분석에는 범죄와 무질서 데이터를 다루는 범죄분석(Crime analysis)[4], 범죄자 특히, 조직범죄자와 공모자들에 대한 정보를 다루는 범죄정보분석(Crime intelligence)[5], 범죄 특성에 기반한 범법자들의 물리적, 행동적, 심리적 프로파일링을 다루는 범죄수사분석(Criminal investigation analysis) 등 다양한 개념들이 존재한다. 본 글에서는 최근 통합추세를 보이고 있는 범죄분석과 범죄정보분석의 개념을 포괄하는 의미로 정보분석을 사용하고자 한다.

2.2 정보분석 필요성

국제범죄분석협회에 의하자면 정보분석은 ① 범죄의 해결 ② 미래 범죄를 예방하기 위한 효과적인 전략과 전술의 개발 ③ 범법자의 발견과 검거 ④ 안전과 삶의 질 향상 ⑤ 내부적 운용(Operation)의 최적화 ⑥ 순찰과 범죄수사의 우선순위 결정 ⑦ 고질적 문제의 발견과 해결 ⑧ 자원할당 ⑨ 장래 필요 자원에 대한 계획수립 ⑩ 효과적인 정책의 입안 ⑪ 공중에 대한 교육 등을 위해 필요하다[6]. 이는 사이버범죄에도 똑같이 적용될 수 있을 것이다.

특히 사이버범죄에서 정보분석이 필요한 이유는 대표적인 조직범죄로 범죄자들이 국제적으로 연결되어 있어서 중장기적으로 정보를 수집하고 분석하지 않을 경우 주범을 검거하기가 어렵기 때문이다. 무엇보다도 사이버범죄의 심각성에 따라 단속대상을 특정하고, 우선순위를 설정하여 제거하기 위해 필요하다. 국가의 인적, 물적 자원이 한정되어 있기 때문이다.

2.3 정보분석 가능성

사이버범죄는 전통적인 범죄와 달리 정보분석을 할 수 있는 데이터 확보가 용이하다. 충동적인 범죄가 아니라 일정한 수법을 가지고 있다. 대표적인 조직범죄로 다수의 공범자가 있고 이들은 휴대폰, SNS, 이메일, 온라인 포럼을 통해서 지속적으로 통신을 한다. 주로 경제적 이익을 목적으로 범행을 하고 있어 자금거래가 수반된다. 온라인상 활동은 대부분 디지털 증거로 분석이 용이하다. 비록 정보가 피해자별, 서비스 제공 기업별로 분산되어 있다하더라도 전통적인 범죄에 비해 분석할 여지가 많은 것은 사실이다.

비공개 정보는 관련 당사자의 협조로 확보할 수 있고, 제공이 법적으로 금지되어 있다면 수사기관의 압수수색으로 확보가 가능할 것이다. 이를 통해서 해킹도구, 공격기법, 악성코드, 공격대상 취약점, 공격대상 운영체제, C&C 서버위치, 좀비PC 현황, SNS 계정과 게시글, 사진, 동영상, 이메일, IP, MAC 주소, 계좌번호, 전화번호, 활동포럼 등 다양한 정보를 수집할 수 있고, 분석을 통해서 유의미한 결과를 도출해 낼 수 있을 것이다.

2.4 정보분석 순환모델

<표 1> 사이버시큐리티 전략 중 정보분석 관련 내용(발췌)

연도	구분	정보분석 내용
2009년	사이버위기 종합대책[10]	국가 사이버위기 발생 시 민·관 합동 범정부 대책기구 구성, 위협분석 및 경보발령 등 위기관리 체계 정비, 사이버공격 탐지 사각지대 해소
2011년	사이버안보 마스터플랜[11]	조직적인 해커공격에 대해 외부전문가가 참여하는 '민·관 합동 대응반' 운영
2013년	사이버안보 종합대책[12]	유관기관 간 스마트 협력체계를 구축하기 위해 국가 차원의 '사이버위협정보 공유시스템' 구축, 민간부분과의 정보제공·협력도 강화

정보분석 모델은 다양하지만, 여기에서는 CIA 모델, FBI 모델, 국제범죄분석협회 모델을 서술하고자 한다. 먼저 CIA 모델은 요구 → 수집 → 가공과 개발 → 분석과 생산 → 배포 → 환류를 거쳐 다시 요구 단계로 순환하는 모델이다. FBI 모델도 이와 유사하게 계획과 지시 → 수집 → 처리 → 분석 → 배포의 구조를 가지고 있다. 국제범죄분석가협회 모델은 데이터 → 정보(Information) → 지식(Knowledge)의 단계로 순환하고, 각각의 사이에 분석(Analysis)과 의사소통(Communication)이 수단으로 존재한다[7].

3. 정보분석 현황 및 문제점

3.1 사이버범죄 측정의 어려움

사이버범죄 측정은 정보분석의 출발점이다. 하지만 개념과 분류체계의 미확립, 분석단위에 대한 기준설정 부재, 해외공격의 포함문제, 낮은 범죄 신고율 등으로 측정에 한계가 있다[8].

먼저 전통적 범죄의 위협측정을 살펴보자. 다리가 무너지고 사람이 죽는 사고가 발생하였을 때, 경찰은 순찰 중에 확인하거나 목격자의 신고로 알게 된다. 사망신고라는 제도를 통해서도 알 수 있다. 특히, 시각적으로 확인이 가능하여 피해 규모를 측정하고, 심각성을 판단할 수도 있다. 그러나 해커조직이 수많은 기업의 전산망을 공격했을 경우 범죄자는 보이지 않고, 목격자도 찾기 어렵다. 피해기업은 다른 기업의 시스템을 볼 수 없어 피해를 알 수 없거나 무관심하기 쉽다. 그래서 전체적인 사이버범죄 피해규모를 파악하는 것이 어렵다.

3.2 사이버시큐리티 전략의 불완전성

사이버범죄 근절은 사이버시큐리티 전략과 주요 정보통신기반시설 보호전략에 있어서 필수적인 요소에 해당한다[9]. 실제 위에서 언급된 '어나니머스 해커조직'의 사례를 보더라도 사이버범죄 문제가 사이버시큐리티와 밀접한 관계가 있다는 것을 알 수 있다. 우리나라 사이버시큐리티 전략은 〈표1〉과 같이 정보분석 정책을 일부 시행하고 있다. 그러나 정보분석의 기반이 되는 사이버시큐리티 전략에서 사이버범죄 문제가 사실상 제외되어 있어서 사이버범죄에 대한 전체적인 정보수집, 공유 및 분석에는 한계가 있다. 이는 국가자원의 중복, 정보분석 역량 저하, 법집행력의 약화 등을 초래할 수밖에 없다.

우리나라와 달리 미국은 '사이버공간에 대한 국제전략(International Strategy for Cyberspace)[13]', 독일은 '사이버안보전략(Cyber Security Strategy for Germany)[14]', 영국은 '사이버안보전략(The UK Cyber Security Strategy)[15]'에서 각각 사이버범죄를 중요한 요소로 다루고 있다. 특히 영국은 사이버시큐리티 전략의 4개 과제 중에서 첫 번째로 사이버범죄를 언급할 만큼 큰 비중을 두고 있어서 우리나라와 대조를 보이고 있다.

3.3 정보공유의 내재적 한계

정보공유의 주체는 정보기관, 수사기관, 정책부처(미래부), 정보보안업체, 기업, 시민 등으로 볼 수 있다. 그간 정보기관은 국가안보라는 이유로, 수사기관은 수사비밀이라는 이유로 정보공유에 소극적이었다. 정책부처(미래부)는 피해정보는 충분히 확보할 수 있었으나, 범죄자 정보는 부족했다. 정보보안업체는 고객의 피해 사실을 공유할 수 없었을 것이고, 피해기업은 경제적 손실, 법적 책임추궁, 브랜드가치 하락 등을 이유로 정보공유에 방어적으로 대응하였다.

국정원, 미래부, 국방부가 국가·공공, 민간, 국방 등을 각각 전담하면서 신고를 개별적으로 접수하고 있으나 사이버범죄 정보가 수사기관에도 제대로 전달되지 않고 있다. 설령 신고하더라도 수사기관에서는 인력부족을 이유로 난색을 표하고 있어 악순환이 계속되고 있다. 이처럼 관련 주체들이 관련 정보를 조각조각 보유하고 있고 각자의 여건 때문에 정보공유에 소극적이어서 전체적인 대응을 어렵게 하고 있다.

3.4. 사후적(reactive) 대응의 한계

수사기관은 전통적으로 사건이 발생하면 추적하고 증거를 수집하는 사건기반의 접근(case-based approach)을 하고 있다. 그간 정보분석 제도가 활성화되지 않았기 때문이기도 하다. 이러한 맥락에서 볼 때 정부가 2004년 중국으로 추정되는 해커조직에 의한 국가기관 해킹사건, 북한에 의한 2009년 7.7 디도스 공격, 2011년 3.4 디도스 공격과 농협 전산망 침입사건 그리고 2013년 3.20 전산망 해킹과 6.25 사이버공격을 사전에 탐지하지 못한 것은 당연한 귀결일지도 모른다. 사후적 대응은 범죄자의 검거가 어렵고, 증거확보도 곤란하며 무엇보다도 피해를 사전 예방하지 못하는 한계점을 가지고 있다.

4. 정보분석 역량 강화방안

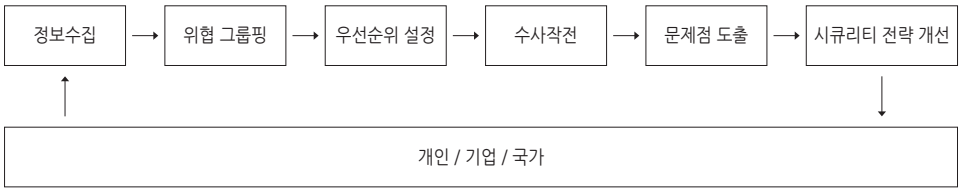
4.1 사이버범죄 측정 기반 구축

사이버범죄를 측정하기 위해서는 ① 측정 방법론 개발 ② 신고 활성화 ③ 부처 간 협력 등이 필요하다. 먼저, 사이버범죄가 어린이, 기업, 국가에 미치는 위협이 무엇인지, 스마트폰, 사물인터넷(IoT) 등 새로운 환경은 어떠한 위협을 초래하는지, 중국, 러시아, 동남아시아 등 국제적 위협은 무엇인지 등을 측정할 수 있는 방법론이 있어야 한다. 사이버범죄의 피해를 당한 개인, 기업 그리고 국가가 수사기관에 신고할 수 있도록 제도를 마련하고 인식을 제고해야 한다. 암수범죄가 많으면 사이버범죄의 전체 규모를 측정할 수 없고 인지되지 않은 범죄는 계속하여 사이버시큐리티의 위협요인이 될 것이다. 기업의 신고를 주저하게 하는 만드는 정보통신망이용촉진및정보보호등에관한법률(제28조, 제73조) 상 기술적·관리적 보호조치 위반죄도 반드시 재검토되어야 한다. 피해기업은 해킹 피해자에서 기술적·관리적 보호조치 위반의 피의자로 전락하게 된다. 수사협조에 소극적으로 대응하게 만든다. 기업에 강한 책임을 부여하는 정책이 결국 해킹 용의자 검거를 어렵게 만들고 있다.

4.2 사이버시큐리티 전략과 사이버범죄 문제 연계

사이버범죄 문제는 사이버시큐리티 전략 안에서 해결책을 모색해야 한다. 우리나라에서는 사이버시큐리티와 사이버범죄 대응이 분리된 것처럼 인식되고 있으나 양자는 분리될 수 없다. 즉, 정보분석과 범죄수사를 통한 사이버범죄 대응활동은 법위반자를 처벌하는 규제자로서의 기능뿐만 아니라 사이버

<표 2> 사이버범죄 대응체계 개선방안



시큐리티를 지키는데도 중요한 역할을 수행한다. 특히, 정보분석은 바른 전략과 전술을 구사하기 위한 필요조건인 동시에 그 자체가 위협에 대응하는 수단이기도 하다. 불법행위자가 정보분석으로 발각될 수 있다고 생각하게 된다면 스스로 위축될 것이기 때문이다. 따라서 사이버시큐리티 전략에서 사이버범죄 대응전략이 도출되어야 하고, 그 전략의 핵심은 정보분석이 되어야 하며 이는 다시 사이버시큐리티에 기여하는 선순환 체계가 되어야 한다.

4.3 정보공유분석 제도 및 기술 개발

기업은 정보자산을 지키기 위해서는 유사 업종 간 협의체를 구성하여 정보공유를 활성화할 필요가 있다. 우리나라는 현재 금융정보공유분석센터(ISAC)와 통신정보공유분석센터(ISAC)를 운영 중에 있으나 보다 개방적이고 다원화된 협의체가 필요하다. 기업의 정보공유는 익명성이 보장되면서도 자신에게 들어온 공격이 얼마나 심각한지를 측정할 수 있는 시스템에서 이루어져야 한다. 즉, 자신과 같은 피해를 입은 기업이 어디인지는 몰라도 얼마나 많은지 확인할 수 있는 시스템이 필요하다. 피해의 심각성과 긴급성을 판단할 수 있기 때문이다. 미국의 국가사이버포렌식및훈련연합(NCFTA)의 사례처럼 정부부처와 수사기관, 국제기구까지 포함하는 협의체라면 더욱 좋을 것이다.

미국 법무부는 백서를 발간하면서 합법적으로 공유되어야 할 자원이 무엇이고, 공유되어서는 안 되는 자원이 무엇인지에 대해서 가이드라인을 마련하였다[16]. 유럽평의회(Council of Europe)에서는 '인터넷서비스 제공자와 수사기관간의 협력에 관한 가이드라인'을 발표하였고[17], 유럽네트워크정보보안기구(ENISA)에서는 '사이버범죄 근절을 위한 법집행기관과 침해사고 대응기관 간의 협력방안에 대한 가이드라인'을 제시하였다[18]. 이처럼 우리나라도 공유되어야 할 정보와 공유될 수 없는 정보에 대한 법률적, 실무적 지침이 필요하다.

4.4 정보분석 기반의 사이버범죄 대응체계 확립

전통적인 범죄와 달리 사이버범죄는 자동화된 공격으로 규모가 상상을 초월하고, 국내외를 불문하여 이루어지며 그 피해의 확산속도는 매우 빠르다. 선제적으로 대응하지 않으면 검거하기 어렵다. 이러한 문제를 해결하기 위해서는 〈표2〉와 같은 사이버범죄 대응체계가 도입되어야 한다. 즉, 다양한 채널을 통해 정보를 수집한 후에 위협이 되는 요소들을 특정하여 그룹핑하고, 피해의 심각성·긴급성 등을 고려하여 단속 우선순위(priorities)를 설정한다. 우선순위에 따라서 수사작전을 전개하고 수사과정에서 도출된 문제점은 사이버시큐리티 전략의 개선을 위해 부처에 환류하여 법제도 개선에 기여한다. 이는 사이버범죄 근절과 더불어 사이버시큐리티 역량 강화에도 기여할 것이다.

5. 맺음말

우리나라에서 범죄 대응에 있어서 정보분석 제도는 다소 낯설다. 그간 대부분 발생 이후 추적 수사하는 방식을 취했기 때문이다. 사이버시큐리티 전략에서도 마찬가지다. 2009년 이후 3차례에 걸쳐서 사이버 시큐리티 전략을 만들어오면서 많은 법제도를 도입했지만 정부, 기업, 개인 간의 정보 수집, 분석, 공유, 환류에 대해서는 다소 미흡했다. 사이버시큐리티와 사이버범죄 문제가 분리되어 논의되고 있는 것이 그 반증이기도 한다. 사이버범죄는 갈수록 검거가 어려워지고, 따라서 사이버 시큐리티의 위협이 커지고 있다. 이에 대응하기 위해서 정보분석 제도의 도입은 필연적이다. 조속한 도입을 촉구하며 이를 뒷받침하기 위해 정보수집 및 공유 주체 간의 공감대 확보, 법제도 정비, 시스템 개발 등이 필요하다. 무엇보다도 정보분석 결과가 정부부처, 정보기관, 기업, 시민 등과 공유될 때 사이버시큐리티도 크게 강화할 것이라는 확신을 심어 주어야 할 것이다.

[참고문헌]

[1] 연합뉴스 인터넷 보도(2014. 3. 22.), '해커조직 어나니머스 4월 한국정부 해킹 예고(종합).

[2] 경향신문 인터넷 보도(2014. 4. 16), '정부 심판하겠다던 어나니머스, 잡고 보니 중고생'.

[3] Fafinski, S., Dutton, W.H. & Margetts, H., Mapping and Measure Cybercrime, OII Forum Discussion Paper No. 18, 2010.

[4] 범죄의 패턴, 추세, 문제를 발견하고 분석하며 해결하고, 감소시키며 예방하는 데 도움이 되는 정보를 생산하여 배포한다.(이웅혁, 장윤식, 송영진 등, 선진국의 사이버범죄 정보분석 제도 도입 방안, 경찰대학 치안정책연구소, 2013)

[5] 범죄조직과 위계 구조를 밝혀주는 자료, 자금과 상품의 흐름, 그들의 관계, 현재의 활동과 계획, 가담자의 개인정보 등에 대한 통상 가담된 자들의 체포와 기소를 위한 분석을 한다.(이웅혁, 장윤식, 송영진 등, 앞의 연구보고서)

[6] IACA(The International Association of Crime Analysts), 2008.

[7] 이웅혁, 장윤식, 송영진 등, 앞의 연구보고서.

[8] 이웅혁, 장윤식, 송영진 등, 앞의 연구보고서.

[9] ITU, 'Understanding Cybercrime: A Guide for Developing Countries', Draft April, 2009.

[10] 방송통신위원회 보도자료(2009. 9. 11.), '정부, 「국가 사이버위기 종합대책 발표」 확정 발표'.

[11] 방송통신위원회 보도자료(2011. 8. 8.), '정부, 「국가 사이버안보 마스터플랜」 수립'.

[12] 미래창조과학부 보도자료(2013. 7. 4.), '정부, 「국가 사이버안보 종합대책」 수립'.

[13] US White House, 'International Strategy for Cyberspace', 2011.

[14] Federal Ministry of the Interior, 'Cyber Security Strategy for Germany', 2011. 2.

[15] Cabinet Office, 'The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world', 2011. 11.

[16] US DOJ, 'Department of Justice White Paper – Sharing Cyberthreat Information Under I8 USC §2702(A)(3)'

[17] Council of Europe, 'Guidelines for the cooperation between law enforcement and internet service providers against cybercrime', 2008.

[18] ENISA(European Network and Information Security Agency), 'The fight against cybercrime - Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime', 2012. 2.