한국경호경비학회 – 제34호(2013): 259–278
투고일 2013. 1. 31, 심사일 2013. 2. 13, 게재확정일 2013. 3. 11

인터넷 시대의 정보활동: OSINT의 이해와 적용사례분석

이완희 · 윤민우 · 박준석

인터넷 시대의 정보활동: OSINT의 이해와 적용사례분석

이완희* · 윤민우** · 박준석***

〈요 약〉

21세기 정보통신기술의 발달과 급격한 인터넷의 확산으로 비밀 출처정보에서만 수집이 가능했던 정보(Information)가 인터넷을 통해 쉽게 검색이 가능하게 되었다. 공개정보(Open Source)가 폭발적으로 증가하면서 정보수집활동에 큰 변화가 일어나고 있으며, 이러한 변화는 국가정보기관에서의 정보수집활동에도 영향을 미치고 있다. 공개출처정보(Open Source Intelligence: OSINT)는 이렇게 넘쳐나는 정보를 효과적으로 처리하고 분석하기위해 등장하였다. OSINT는 주로 9.11테러 이후에 빠르게 적용되었으며, 국가정보기관에서는 이와 관련된 연구와 기술개발에도 적극 참여하고 있다. 이렇게 서구국가에서는 OSINT의 중요성을 인지하고 공개정보(Open Source)를 분석하는 일이 최우선 순위로 떠오르고 있다. 하지만 국내에서는 공개정보(Open Source)의 중요성에 대한 인식이 미흡한 실정이다. 본 연구에서는 OSINT를 소개하고 중요성을 제고하는 것을 목적으로 하였다. 감당하기 힘들 정도로 늘어나는 많은 양의 공개정보(Open Source)를 효과적으로 이용하기위하여 OSINT의 운용사례와 방법을 소개하고 중요성을 논의하였다. 이는 국가안보를 위협하는 테러뿐만 아니라 각종 범죄를 효과적으로 대응하기위한 방안이기도 하다.

주제어 : 공개출처정보(Open Source Intelligence: OSINT), 정보활동, 정보(Information), 정보(Intelligence), 테러리즘, 인터넷

* 가천대학교 경찰안보학과 교수 (제1저자)
** 가천대학교 경찰안보학과 교수 (교신저자)
*** 용인대학교 경호학과 교수 (제2저자)

목 차

I. 서 론

인터넷은 인류가 개발한 정보매체 중 가장 많은 사람들이 방대한 양의 정보를 가장 빠르고 편리하게 접촉할 수 있는 매체로 발전해왔다. 이러한 변화는 인류가 필요로 하는 모든 정보를 인터넷상에서 빠르고 편리가게 수집 할 수 있게 만들었다. 국가정보기관의 입장에서 인터넷은 다원적 공개출처 정보의 보고이며, 과거 수집 관에 의존해야 했던 상당부분 정보들은 이제 인터넷을 통해 실시간으로 수집이 가능해졌다(조병철, 2003). 최근 들어 전개되는 정보화 기술의 급속한 발전과 인터넷을 통한 방대한 양의 공개정보(Open Source)의 빠른 확산은 기술발전의 한 결과로 국가정보기관의 정보수집활동에도 큰 변화가 나타나고 있다.

이란이 2003년 이후 핵무기 프로그램을 개발하고 있지 않다고 미 정보기관들이 백악관에 보고한 것도 인터넷에서 공개정보(Open Source)를 통하여 수집한 최고급 정보의 대표적인 사례이다(이동훈, 2008). 이러한 공개정보의 중요성을 인지하여 현재 미국 대통령은 국가안보 사항 등 최고 비밀이 담긴 일일 브리핑을 받는 것을 하루 일과로 시작한다고 한다. 그런데 이 정보들이 특수공작이나 비밀 첩보위성 등을 통해 수집한 정보보다는 인터넷으로 누구나 접근할 수 있는 공개정보(Open Source)를 이용한 정보들이 큰 비중을 차지하고 있다(이동훈, 2008). 이는 미국 국가기관들이

필요로 하는 정보의 약 90%가 공개정보(Open Source)를 통하여 수집된 것이다(이동훈, 2008). CIA(Central Intelligence Agency)의 경우 인터넷 공개정보(Open Source)의 중요성을 인지하고 2005년부터 워싱턴 외곽에 공개정보센터(Open Source Center)를 만들어 공개정보의 집중분석을 담당하도록 하고 있다. 이는 주로 9.11테러 이후에 빠르게 발전해 온 분야이며(Bean, 2011), 이러한 정보수집활동의 변화는 미국 등 서구국가들에서 OSINT의 중요성을 인지하여 개념들이 소개되고 발전되어온 결과라고 할 수 있다(Appel, 2011).

최근 대한민국 국가정보기관이 김정일 사망을 파악하지 못하는 일이 발생하였고, 국가정보기관마저 누구나 쉽게 접근할 수 있는 공개정보(Open Source)를 통하여 알게 되어 비난을 받는 일이 발생하였다. 이것은 공개정보(Open Source)의 중요성에 대한 인식이 부족하였기 때문이다. 최근 들어 서구국가에서 주목받는 OSINT는 감당하기 힘들 정도로 넘쳐나는 공개정보(Open Source)의 효과적인 수집방안을 모색하기위해 개발된 방법이다. 따라서 본 연구는 국민의 사회 안전과 직접적으로 연관성이 있는 국가정보기관의 정보활동에서 OSINT의 중요성을 제고하며 OSINT의 개념과 특성을 이해하고 운용사례와 방법 등을 국내에 소개하여 효과적인 공개정보(Open Source)의 활용을 목적으로 하였다.

Ⅱ. OSINT의 정의와 개념

1. OSINT의 정의

일반적으로 공공에서 접근이 가능한 공개 정보(Open Source)를 이용하여 정보활동(Intelligence)을 하는 것을 OSINT라고 정의 한다(Tekir, 2009). 여기서 공공에서 접근이 가능한 공개정보(Open Source)란 신문, 방송, 간행물, 민간 및 공공부문의 보고서, 연구논문, 단행본, 회의록, 기자회견 및 연설문 등 전통적 매체와, 인터넷, 데이터베이스, On-line 상용정보 등 디지털 매체를 총 망라한 다원적 공개출처 매체(All kinds of open source media)를 통하여 수집된 정보(information)를 말한다(조병철, 2003). 또한 미 육군(U.S. Army)에서는 “정보(Information)가 공공으로 노출되는 것에 제약이 없는 공개정보(Open Source)를 통하여 이루어지는 정보활동”을 OSINT라고

정의한다(Department of the Army, 2006).

2. OSINT의 개념

정보의 개념은 “Information” 과 “Intelligence”로 구분하지 않고 사용하는 경우가 대부분이지만 사실상 이것은 서로 다른 의미로 구분이 된다. 공개정보를 대상으로 내용 및 출처에 관한 사실 확인 단계를 거쳐 획득된 정보를 “Intelligence”로 정의하며, 정보기관(Intelligence Agency)에서는 분석과 평가가 이루어진 정보만을 “Intelligence”라 한다(조병철, 2003). 반대로 분석과 평과가 이루어지기 전 단계에서 공개정보(Open Source)를 이용하여 수집된 자료(Data)를“Information"이라고 정의 한다(조병철, 2003). 다시 말해 OSINT는 정보수집의 한 방법으로, 수집단계에서의 정보(Information)가 분석과 평가를 통하여 유용하게 사용 가능한 정보(Intelligence)가 되기까지의 정보수집활동을 말한다.

정보기관에서 이루어지는 정보수집방법은 크게 공개정보수집(Overt Collection)과 비밀정보수집(Covert Collection)으로 나뉜다. OSINT가 공개정보수집에 해당하며, 비밀정보수집방법은 크게 HUMINT(Human Intelligence), TECHINT(Technical Intelligence)로 나뉜다. HUMINT(Human Intelligence)는 스파이 등 사람과의 접촉을 통해 정보를 수집하는 방법을 말하며, TECHINT(Technical Intelligence)는 기술이나 장비를 통해 정보를 수집하는 방법을 말한다(문정인, 2002). 일반적으로 비밀정보수집은 전통적인 정보기관의 정보활동에 해당되는 것으로 정보(Information)의 출처가 공공이 접근하기 어려운 비밀정보를 이용하여 이루어진 정보활동이다. 하지만, OSINT는 공공에서 접근할 수 있는 정보(Information)를 이용하여 정보활동을 한다는 점에서 비밀정보수집과 구별이 된다(Tekir, 2009).

Ⅲ. OSINT의 사용목적과 진화

최초의 사용된 OSINT는 자유롭게 취득 가능한 정보들을 창의적으로 조합하여 사용가능한 형태로 합성시켜 만들어진 것이었다(Glassman & Kang, 2012). 이것은 정보의 최종 소비자의 식견과 의미를 이끌어 내어 고유한 문제들을 풀 수 있는 특정

해결책을 제시하기 위하여 정보들 간의 연계를 하나의 도면으로 만드는 것이었다(Glassman & Kang, 2012). 이러한 OSINT는 제 2차 세계대전 당시에 최초 사용되었으며, 그 당시 개발된 OSINT는 공개정보(Open Source)의 접근방식과 매우 유사한 두 가지 중요한 요소들을 가지고 있다(Schaurer & Jorger, 2010). 첫째, 최종 정보가 소비자에게 전달되는 정보의 투명성이다. 정보의 출처(Reference)가 최종 분석을 읽는 모두에게 반드시 공개적이고 명확하며 용이하게 연결되어 있어야 한다는 것이다. 정보의 투명성은 모든 사용자들이 제한적인 정보의 전문성과 신뢰에 의존하기 보다는 스스로 정보를 직접 조사하고 분석하여 본인 고유의 결론도출을 가능하게 해준다. 이는 바로 공개정보(Open Source)의 가장 핵심적인 원리인 것이다. 정보 출처의 근원과 그 역사를 알지 않고서는 그 정보가 적용된 프로그램을 정말로 신뢰할 수는 없는 것이다(Burke, 2007). 또한, 정보의 투명성은 관심이 있는 다른 단체들이 그 정보와 관련된 중요 결정사항들을 보다 쉽고 빠르게 전달 할 수 있게 해주기 때문에 그와 유사한 상황이나 문제 발생 시 관련 정보들이 변형되어 사용되어 질 수 있게 해준다(Schaurer & Jorger, 2010).

둘째로, 정보활동의 목적에 따라 수집된 정보(Information)는 중요도순으로 노드정보(Information Nodes)로 배열되어지는데 이것은 문서를 구성하는 작은 크기의 의미 있는 정보 단위를 말한다. 최종 사용자는 자신이 희망하는 정보를 필요에 따라 즉각적으로 찾아낼 수 있어야 하고, 또한 이러한 정보들이 서로 어떻게 그리고 왜 연결되어 있는지를 다시 역추적 할 수도 있어야 한다(Schaurer & Jorger, 2010). 이는 모든 정보들이 지정된 특정 영역에 단순히 보관되어지는 것이 아니고 자체적으로 구축된 시스템 내에서 역동적(Dynamic)이 될 수 있게 한다(Glassman & Kang, 2012). 예를 들어 만약 한 정보사용자가 특정 지역의 상수원을 찾고 싶을 경우, 상수원에 대한 정보를 쉽고 빠르게 찾을 수 있으며, 그 상수원과 관련된 기후 변화, 상수원 관리자, 곡식 생산량, 곡식 가격, 곡식 공급에 다른 불만족 등 다양한 정보를 역추적하고 그 관계를 이해할 수 있다(Glassman & Kang, 2012).

일반적으로 OSINT는 이러한 두 개의 목적을 병행하는데 이것은 창의적으로 정보를 모으고, 선별적으로 정보를 인식하여, 투명한 정보들을 조합하고 새로운 문제의 해결책을 개발하는데 목적이 있으며, 이 과정에서의 자연스럽게 생성되는 정보의 투명성이 관련 정보수집가들에게 높은 신뢰를 제공한다. OSINT는 제 3자의 문제를 해결하고, 단체의 결론을 정당화하기 위하여 사용되고, 다른 커뮤니티와 공유하는

정보를 더욱 확장하기위해 사용되기도 하며, 이것은 부족한 신뢰를 조절하는데 큰 역할을 한다(Burke, 2007). OSINT는 특정 집단이나 개인들의 현상 유지를 위해 사용되는 수직적 구조이기 보다는 조직 전체에 퍼져나갈 수 있는 평행적인 구조이다(Glassman & Kang, 2012).

미군은 지난 200여 년 동안 다른 국가의 영토와 군을 이해하기위해서 공개정보(Open Source)를 통하여 데이터를 수집하고 자체적으로 개발한 OSINT 매뉴얼에 따라 분석해왔다(Department of the Army, 2006). 이것은 오랫동안 있어 왔던 정보활동인 OSINT의 일환으로 시스템적 추구방식(Systematic Approach)에 의하여 수집되고 분석이 되어왔다. 특히, 컴퓨터기술과 정보통신기술의 발달로 과거의 어떤 시점보다 OSINT의 중요성과 활용성에 주목을 받고 있다(Department of the Army, 2006). OSINT는 주로 9.11테러 이후에 빠르게 적용되고 발전되어왔으며, 최근에는 감당하기 힘들 정도로 넘쳐나는 정보를 효과적으로 처리하고 분석하기위한 방법론적 접근방법에 관심이 집중되고 있다. OSINT는 이러한 시대적인 정보환경의 변화에 적절히 대응하기 위해 사용되고 발전되어온 정보수집방법의 한 방법이다(Bean, 2011). 이러한 변화는 누구나 어디서든 쉽게 접촉하고 이용 가능한 공개정보(Open Source)가 폭발적으로 증가했기 때문이다(Appel, 2011).

Ⅳ. OSINT와 공개정보(Open Source)의 활용방안

1. 공개정보(Open Source)를 통한 정보(Information) 수집

OSINT의 가장 기본적이고 중요한 단계 중에 하나는 공개정보(Open Source)의 검색과 수집이다. 공개정보(Open Source)의 수집은 주로 관련 전문 자료의 검색과 확보와 관련이 있으며, 오늘날 폭발적으로 증가한 막대한 양의 정보를 어떻게 찾아내고 활용할 것인가에 대한 방안의 모색이다. 즉 인터넷에 유용한 정보가 있다고 해서 원하는 정보를 필요할 때 찾아내어 활용할 수 없다면 마치 해당 정보가 존재하지 않는 것과 마찬가지의 상황이 발생한다. OSINT는 이러한 상황에 대한 문제인식에서 출발한 것으로 특정 정보를 찾아내고 인터넷에 떠돌고 있는 정보를 보다 효율적으로 활용할 수 있게 체계적으로 데이터를 관리하는 것을 말한다(ISVG 참여관찰).

이렇게 감당할 수 없을 정도의 많은 양의 정보 중에 필요한 정보를 찾아내기란 쉬운 일이 아니다. 누구나 쉽게 접근할 수 있는 공개정보(Open Source)라고 하여도, 보이지 않는 웹(Invisible web)과 딥웹(Deep web)은 필요한 정보를 찾아내는데 방해 역할을 한다. 보이지 않는 웹(Invisible web)은 구글(Google)이나 네이버(Naver)와 같은 일반 검색엔진으로 검색이 되지 않는 웹사이트를 말한다. 반대로 딥웹(Deep web)은 일반적인 검색엔진으로 검색이 가능 하지만 검색의 우선순위에 밀려 잘 파악되지 않는 웹사이트를 말한다. 이러한 이유 때문에 대부분의 온라인상의 정보들은 검색엔진을 통해 검색되지 않거나 검색되어도 찾아내는 것이 어렵다. 대체로 사이버 공간에서 이 보이지 않는 웹(Invisible Web)에 해당되는 부분이 약 80% 정도에 해당하며 일반적인 검색엔진으로 검색되는 것은 대략 20% 정도에 불과한 것으로 평가되고 있다(Sherman et al., 2001).

대부분의 웹이 검색이 되지 않는 이유는 검색엔진의 검색방식으로부터 알 수 있다. 대부분의 검색엔진은 스파이더(Spider)라는 검색도구를 통해 여러 관련 웹사이트를 주기적으로 돌아다니며 정보 기록해 두었다가 재방문하는 방식으로 검색을 하는 방식이다(Sherman et al., 2001). 이것은 검색 키워드(Keyword)나 단어(Text)등을 통해 관련 웹사이트를 찾아내는 방식이나 반드시 하이퍼텍스트 마크업 언어(Hypertext Markup Language: HTML)와 같은 특정 형식의 단어(Text)를 포함하고 있어야만 검색이 가능하다(Sherman et al., 2001). 하지만 웹사이트가 이러한 단어(Text)가 아닌 다른 형태(이미지나 음성)로 구성되어있다면 검색의 대상에서 제외되어 검색이 안 된다. 하지만 딥웹(Deep web)의 경우 검색결과로부터 나타나는 현상으로 검색우선순위에서 밀려나 원하는 정보(Information)를 찾기 어려운 상황을 말한다. 대부분의 검색엔진은 검색이 자주 되거나 방문자 수가 많거나 아니면 광고료를 지불한 웹사이트를 검색 결과의 우선순위에 두기 때문에 검색결과의 검색순위에 영향을 받아 원하는 자료가 검색은 되지만 우선순위에서 뒤로 밀려 검색자로 하여금 쉽게 눈에 띄지 않게 된다. OSINT는 이렇게 보이지 않는 웹(Invisible web)과 딥웹(Deep web)으로 방해받는 부분을 극복하기위한 하나의 방법으로 수많은 자료로부터 유용한 정보(Information)를 효과적으로 검색하고 수집할 수 있게 사용되는 주요한 부분이다(Open Source Center, 2009; Sherman & Price, 2001; Tekir, 2009).

온라인상에서의 효과적인 공개정보(Open Source)의 수집을 위해서는 주로 보이지 않는 웹(Invisible web)이나 딥웹(Deep web)등에 해당하는 관련 웹 사이트들에 대한

파악과 이러한 웹 사이트들에 대한 목록확보와 정리가 중요한 역할을 한다. 일반적인 방법으로 검색되지 않는 보이지 않는 웹(Invisible web)이나 딥웹(Deep web)의 경우 도서관 검색이나 관련 서적의 참고문헌, 전문가의 제보 등의 오프라인 출처를 통해 웹 주소를 확보할 수 있다. 이를 단서로 연구방법론에서 제시하는 눈덩이 추출법(Snow balling sampling)과 유사하게 각종 링크를 통해 다른 관련 웹사이트에 관한 정보들을 확보해 나간다. 이렇게 수집된 유용한 웹사이트나 온라인 정보들을 따로 목록으로 만들어 관리한다(ISVG 관찰자 참여). 따라서 OSINT의 정보수집단계에서 관련 전문가와의 인터뷰, 대학의 전공 교수나 도서관의 정보검색사로부터의 도움이나 관련 연구 보고서, 논문, 도서의 검토 등은 중요하다(Appel, 2011; Sherman & Price, 2001). 다시 말해 능숙한 OSINT 사용자 혹은 사서를 찾아 도움을 받는 것이 효과적일 수 있다. 도서관 사서는 그들의 직업 특성에서 비롯된 공개정보(Open source)를 제공하는 몇 안 되는 전문가 중에 하나이기 때문이다. 또한 문화적 이해와 외국어 실력을 늘리는 것도 하나의 방법이 될 수 있다. 마지막으로 정기적인 OSINT 트레이닝 프로그램에 참가하는 방법이 있으며, 공개자료(Open source)에서 쉽게 구할 수 있는 OSINT 매뉴얼들을 통해 개별적으로 OSINT 능력을 개발시킬 수 도 있다. 전 미군 장교 Ben Benavides가 제공하는 “Online Quick Reference Handbook"과 Robyn Winder에 작성한 ”Untangling the Web, 2007"등이 대표적인 OSINT 매뉴얼이다(Draeger, 2009). 이 자료들은 정보를 능숙하게 다루고 처리 할 수 있는 기술에 대한 효율적인 정보를 제공하고 있다(Draeger, 2009).

검색우선순위에서 밀려 검색자로 하여금 눈에 잘 뛰지 않는 딥웹(Deep web)의 경우 각각의 검색엔진이 제공하는 “상세검색“ (예를 들어 언어 번역 기능과 시간과 지역, 주제 등을 제한하여 보다 제한되고 집중적인 방식으로 검색하는 것 등)을 적극 활용해야한다. 보이지 않는 웹(Invisible web)으로부터 유용한 정보를 효과적으로 수집하기 위해서는 서로 다른 다양한 검색엔진의 특징과 장, 단전을 파악하는 것 이 중요하다. 일반적으로 대부분의 검색엔진들은 각각 고유의 알고리즘을 갖고 있기 때문에, 검색창에 나타나는 결과들은 서로 다르게 나타난다. 그러므로 최소 두 개 이상의 검색엔진을 이용하여 정보활동에 필요한 신뢰할만한 정보(Information)를 수집 하는 것이 중요하다(Draeger, 2009). 예를 들어 검색엔진은 야후에서 사용하는 디렉터리 검색방식과 구글에서 사용하는 키워드 검색방식이 있으며 그 장·단점과 특성들이 서로 다르다. 최근에는 디렉터리 검색방식과 키워드 검색방식이 함께 운영되는 사례

가 늘고 있다. 검색엔진의 종류는 잘 알려진 Google과 Yahoo 이외에도 Hotbot, Lycos, Bing, Alltheweb 등 여러 검색엔진들이 있으며, 영어 이외의 특정 국가에서 해당 국가언어로 운용되는 검색엔진 등이 있어 특정국가나 지역의 정보(Information) 검색에 유용한 검색엔진들이 있다. 우리나라의 경우 네이버나 다음 검색엔진이 대표적이다. 이밖에 LexisNexis 등과 같이 특정 주제의 검색에 유용한 특정 주제만을 다루는 검색엔진 등도 있다.

이 밖에도 Ixquick 등과 같은 Meta-Search 엔진 등이 있다. 이 Meta-Search 엔진은 특정 검색어를 Google이나 Hotbot, Lycos 등 여러 검색엔진을 동시에 복수로 검색하도록 하는 통합검색 서비스이다. 이러한 통합검색 서비스는 여러 검색엔진은 동시에 검색할 수 있다는 장점이 있지만 하나의 검색엔진에 비해 검색의 깊이가 깊지 않다는 단점이 있다. 여러 종류의 검색엔진들의 서로 다른 검색방식의 특성과 장·단점을 이해하고 정보활동의 목적에 맞는 유용한 정보(Information) 수집을 위해 복수의 검색엔진들을 이용하는 것은 중요하다(Appel, 2011; Department of the Army, 2006; NATO, 2002; Open Source Center, 2009). 또한, 구글과 같은 경우 일반적인 검색창 이외에 이미지검색으로부터 그래픽 자료를 통해 보이지 않는 웹(Invisible web)의 주소를 파악하여 해당 웹사이트를 직접 찾아갈 수 있다. 이러한 방법을 사용하면 여러 불법적인 성격의 웹사이트를 찾아낼 수 있다(ISVG 참여관찰).

정보수집단계에서 OSINT는 정보수집목적에 맞게 유용한 웹사이트들과 목록을 설정하여 이를 토대로 정보(Information)를 검색 하는 것이 중요한 부분이다. 그리고 그러한 일련의 검색과정을 일관되고 체계적으로 설계하여 정형화된 OSINT 검색과정을 구축하는 것이 필요하다. 이러한 체계적 관리는 검색주체의 역량과 검색 시기에 따라 다르게 검색되는 웹사이트의 종류 때문에 정보수집이 일관되지 못하고 신뢰성을 확보할 수 없는 문제들로부터 효과적인 대처를 할 수 있게 해준다(NATO, 2002). 온라인상에서 정보수집과 관련하여 주요한 이슈로 다루어지는 부분은 원하는 정보를 어떻게 검색을 할 것인가에 대한 방법이며 이것은 보이지 않는 웹(Invisible web)이나 딥웹(Deep web)으로부터 방해받는 요소를 극복하기위한 가장 중요한 방법이다. 이러한 구체적인 인터넷 검색기법은 온라인상에서 공개자료(Open source)를 통해 습득할 수 있으며 또한 다양한 노력과 경험을 통해 노하우를 축적해 나가야 한다(Appel, 2011; Department of the Army, 2006; NATO, 2002; Open Source Center, 2009).

2. 수집된 정보(Information)의 분석과 평가

공개정보(Open Source)를 통하여 수집한 정보를 데이터베이스화하여 분석 또는 평가를 수행하는 것이 또 하나의 중요한 OSINT의 역할이다. 다시 말해, 일차적으로 수집된 정보(Information)들과 관련성이 있는 정보(Information)들을 찾아내고 그 정보들을 포괄적으로 의미가 있는 정보들과 조합하고 분석하여 필요한 정보(Intelligence)로 변형시킬 수 있는 방법을 말한다(Glassman & Kang, 2012). 이러한 단계는 막대한 양의 공개정보(Open Source)의 활용도를 높이고 그러한 공개정보의 이차분석을 통해 단순히 정보(Information) 상태로 있던 자료들 속에 숨어있는 중요한 의미를 찾아내고 그러한 의미들을 서로 연결함으로서 정보활동 목적에 맞게 유용하게 활용된다. 이러한 분석을 위해서는 주로 데이터 마이닝(Data Mining)이나 회귀분석(Regression), 지리정보분석(GIS), 네트워크 분석(Network Analysis), 시계열 패턴분석(Time-series Analysis) 등의 각종 통계분석을 통해 양적분석이 이루어지며 경우에 따라서는 내용의 교차분석을 통한 질적 분석이 이루어지기도 한다(ISVG 참여관찰). 이렇게 온라인 또는 오프라인 상에 존재하던 수많은 정보(Information)는 데이터베이스 구축과 분석이라는 가공과정을 거치면서 활용가치가 높은 정보(Intelligence)로 바뀐다(Appel, 2011).

OSINT의 최종단계에서는 구축된 데이터베이스를 활용하여 각종 질적, 계량적 분석이 이루어진다. 질적 분석은 관련 지역이나 특정 분야에 전문성을 갖춘 분석전문가가 내용을 분석하여 논문(monograph , manuscript), 또는 보고서나 서적 형태로 나타난다. 또한 데일리 리포트 형식으로 짧은 정세보고 형식으로 이루어지기도 하며 FDD(Foundation for Defense of Democracy)의 경우처럼 보름에 한 번씩 정세분석 보고서의 형태로 나오기도 한다(ISVG 참여관찰). 한편, 계량적 분석은 구축된 데이터베이스를 이용하여 데이터마이닝이나 각종 고급, 중급 통계분석, 지리정보분석, 네트워크 분석 등이 이루어지며 이러한 분석결과가 보고서 형태로 생산된다(ISVG 참여관찰). 이처럼 공개정보(Open source)를 통하여 수집된 정보(Information)와 분석단계를 거쳐 구축한 정보(Intelligence)는 상당한 활용가치를 지니고 있다.

V. OSINT의 적용

1. OSINT의 적용분야

OSINT의 정보활동으로 가공되어진 정보(Intelligence)는 국가안보위협이나 테러, 또는 범죄 활동과 관련된 숨겨진 사실들을 파악하기 위해서 여러 분야에서 사용된다. OSINT는 정보활동(Intelligence) 이외에 인터넷 베팅(Internet vetting), 범죄수사(Crime investigation)등 여러 가지 활동에 적용이 가능하다(Appel, 2011). 인터넷 베팅은 특정 개인이나 집단에 대한 뒷조사와 이를 통한 프로파일과 관련된 제반 활동을 의미한다. 전통적으로 이러한 활동은 오프라인 상에서 특정 개인이나 집단의 구성원들이 위치한 주거지나 근무지, 또는 다녔던 학교나 살았던 지역, 근무했던 직장, 또는 여타 다른 교회나 클럽 등의 단체 등의 해당 인물에 대해 잘 아는 주변 사람들을 인터뷰함으로서 이루어졌다. 하지만 오늘날에는 사이버 공간이 또 다른 의미 있는 공간으로 추가되었다. 대부분의 사람들이 이 사이버 공간에서 주요한 개인적 활동들을 하게 된다. 따라서 오히려 오프라인 공간보다 온라인 공간에서 더욱 풍부하고 자세한 특정 개인이나 집단의 구성원들에 대한 특성이나 이력 또는 경력, 성향들에 관한 정보를 취득할 가능성이 높아졌다. 인터넷 배팅(Internet vetting)은 이러한 상황 변화에 대응하여 온라인 공간상에서 특정 개인이나 집단의 구성원들에 대한 정보를 파악하고 수집하는 것과 관련된 제반활동과 그와 관련된 여러 기법들을 의미한다(Appel, 2011).

범죄수사는 온라인상에서의 범죄 증거확보와 관련된 활동이다. 하지만 OSINT에서의 범죄수사는 단지 디지털 포렌식(Digital Forensic)과 관련된 기술적 영역만을 다루지는 않는다. 탐문 수사와 행적 수사를 포함하며, 온라인상에서의 증인 및 목격자 인터뷰 까지도 포함한다(Appel, 2011). 또한 온라인상에서 테러리스트나 범죄자의 웹 포럼 등에 신분을 가장하고 참여하여 구성원으로 활동하면서 정보를 수집하는 등의 온라인상에서의 HUMINT활동을 포함하는 개념이며, 각종 테러 및 범죄관련 웹사이트들이나 SNS(Social Network Service) 등을 서핑하거나 침투하여 수동적으로 동향관찰을 하거나 능동적으로 참여하여 활동하면서 정보를 확보한다(Appel, 2011).

2. OSINT의 적용사례

공개정보를 통한 테러리즘 데이터베이스 구축의 대표적인 사례로서 미국의 ISVG(Institute for the Study of Violent Groups) 프로그램과 START(National Consortium For The Study of Terrorism and Responses to Terrorism) 프로그램을 들 수 있다. 이 두 프로그램 모두 미국 연방정부의 연구 자금을 지원받아 테러리즘과 관련된 데이터베이스를 구축한 연구프로젝트이다. ISVG는 샘 휴스턴 주립대학(Sam Houston State University)에서 주도하여 정보활동이 이루어졌으며 현재는 뉴해븐 대학(University of New Haven)으로 옮겨서 활발하게 활동이 이루어지고 있다. START 프로그램은 메릴랜드 대학(University of Maryland)에서 주도한 사업이다.

ISVG(Institute for the Study of Violent Groups) 프로그램은 온라인상에 이용 가능한 공개정보를 활용하여 전 세계에서 일어나는 테러사건과 테러조직, 그리고 주요 테러리스트에 관한 정보를 데이터베이스화 하는 작업이다. 2004년부터 OSINT와 관계 데이터(Relational Database)의 개념에 기초해 테러리즘 데이터베이스를 구축하였고, 인터넷과 FBIS(Foreign Broadcasting Information Service), 그리고 미디어 보도 등 공개 자료(Open Source)를 활용하여 테러사건, 테러리스트 및 테러조직에 대한 데이터베이스를 구축했다. 이것은 OSINT의 일차적인 정보(Information) 수집 단계이며, 2004년에 시작하여 2012년 현재 약 15만 건 이상의 테러사건에 관한 데이터베이스를 구축해오고 있다. 이렇게 수집된 가공되지 않은 정보(Information)는 관계 데이터(Relational Data) 원칙에 기초하여 동일한 사건과 인물, 또는 테러조직에 관한 여러 서로 다른 출처의 공개정보를 동일한 사건으로 연결하고 관련성이 있는 다른 정보(Information)들을 찾아내어 포괄적으로 의미가 있는 정보들과 조합하고 분석하여 사용가능한 정보(Intelligence)로 변형시키는 단계이다.

특정 사건이나 인물 또는 조직에 관한 내용이 서로 연결되어 검색을 통해 통합적인 정보를 확인할 수 있게 데이터베이스를 구축하였다. 일차적으로 수집된 정보(Information)는 각 지역별로 데이터베이스가 구축된다. 서로 다른 언어권의 정보(Information)를 활용하여 다양한 정보들을 구축하여 정보의 활용성을 높였다(ISVG 참여관찰). 이러한 OSINT의 정보활동은 대체로 온라인상에서의 공개정보를 활용한 데이터 수집과 데이터베이스 구축은 이와 유사한 방식으로 이루어지며 현재 수많은 정보활동이 이루어지고 있다.

START(National Consortium For The Study of Terrorism and Responses to Terrorism) 프로그램은 2005년에 메릴랜드 대학교(University of Maryland)에서 시행중이며 주도로 미국 국토안보부(Department of Homeland Security)의 지원을 받아 설립되었다. 이 프로그램은 효과적인 대테러 활동을 위해 필수적인 테러리즘과 테러리스트와 관련된 행동패턴과 심리적 영향 등 다양한 분야에 관한 사회과학적, 행동과학적인 이해를 목표로 정보활동이 이루어진다. 현재 메릴랜드 대학의 START 프로그램과 샘 휴스턴 대학의 ISVG 프로그램은 서로 독자적으로 발전하였지만 2008년에는 각자의 장점을 살려 시너지 효과를 내기위해 통합하게 되었다. 일차적인 정보(Information) 수집이 강점이 있었던 ISVG는 데이터베이스 구축에 집중하고 연구와 분석으로부터 활용 가능한 정보(Intelligence)로 변형시키는 것에 강점이 있었던 START는 연구 및 분석을 담당 하였다. 이후 통합된 START 프로그램은 미국의 테러리즘 연구에서 가장 중심적인 연구기관의 하나로 자리 잡게 되었고 2009년에 START는 미국 국토안보부로부터 미국 안보에 기여한 공헌을 인정받았다(START 웹사이트 참조).

현재 START 프로그램에서는 테러리즘 연구자들을 위해 전 세계에서 일어나는 테러리즘 사건들을 데이터베이스로 구축하여 서비스하고 있다. 이는 Global Terrorism Database(GTD)로 불리며 1970년부터 2007년까지 전 세계에서 일어났던 테러사건들을 공개정보(Open source)에 기초하여 구축한 데이터베이스이다. 이와 함께 START 프로그램은 테러 조직에 대한 프로파일도 구축하여 이에 대한 데이터베이스를 서비스하고 있다. 한편 START와 통합되어 협력관계에 있으나 ISVG도 역시 여전히 독자적으로 테러리즘에 관한 데이터베이스를 구축하여 서비스하고 있다. ISVG에서 구축된 데이터베이스 역시 공개정보에 기초하여 수집되었으며 테러조직에 관한 정보뿐만 아니라 테러리스트 인물정보에 관한 데이터베이스도 서비스하고 있다(ISVG 웹사이트 참조; START 웹사이트 참조).

Ⅵ. 결 론

현재 대한민국 국가정보기관들은 정보활동에 있어서 공개정보(Open source)보다는 HUMINT(Human Intelligence)와 TECHINT(Technical Intelligence)같은 비공개정

보에 많은 비중을 두고 있다. 이렇게 스파이, 비밀정찰 위성, 통신감청 등 수집에 고비용이 소요되는 비공개정보에 많은 비중을 두고 있는 이유는 누구나 쉽게 접근할 수 있는 비밀성을 보장받지 못하기 때문이다(조병철, 2003). 하지만 이러한 비공개 정보의 의존은 객관성의 결여를 초래할 수 있으며, 상황의 오판을 불러올 수 있다. 2차 대전 전황을 뒤집었던 연합군의 노르망디 상륙작전 성공은 독일 정보기관의 HUMINT에 대한 지나친 신뢰가 원인이었다(조병철, 2003). 최근 우리 국가정보기구가 김정일 사망을 파악하지 못한 사건은 OSINT의 중요성을 수면위로 떠오르게 한 중요한 계기가 되었다.

정보통신기술이 빠르게 발전하면서 엄청난 양의 정보들이 무작위한 형태로 인터넷 공간에 떠돌고 있다. 하지만 인터넷에 유용한 정보가 있다고 해서 원하는 정보를 필요할 때 찾아내어 활용할 수 없다면 마치 해당 정보가 존재하지 않는 것과 마찬가지의 상황이 발생한다. 즉, 감당할 수 없을 정도의 많은 정보의 양으로 인해 정보 활용과 처리가 문제가 되는 상황이 발생하게 된다. OSINT는 이러한 상황에 대한 문제인식에서 출발한 것으로 어떻게 유용한 정보를 찾아낼 것인지의 문제와 인터넷에 떠도는 유용한 정보를 보다 효율적으로 활용할 수 있게 하며, 광범위한 분야에 적용이 가능하다. OSINT의 정보(Information) 수집단계는 인터넷 검색방법과 노하우축적, 교육, 훈련 등 주요한 이슈로 다루어진다(NATO, 2002). 하지만 OSINT는 온라인상의 정보활동만을 의미하지는 않는다. 따라서 도서관 검색, 대학과의 협력, 오프라인 상에서의 전문가와의 인터뷰 등 두 가지가 활동이 통합적으로 수행이 되어야 한다(Appel, 2011).

서구국가에서는 오래전부터 OSINT에 대한 중요성이 인식되어져 왔고 이러한 활동과 관련한 전략적 패러다임과 시스템 구축, 기법 및 기술 개발, 그리고 이와 관련된 연구와 매뉴얼 및 보고서 작성 등이 이루어져 왔다. 하지만 국내에서는 아직까지 이러한 분야에 대한 인식이 미흡한 실정이다. 여전히 공개정보(Open source)는 누구나 쉽게 접근할 수 있는 비밀성을 보장받지 못하는 정보(Information)로 간주되어 중요성을 인식하지 못하는 실정이다. 따라서 본 연구는 국내에 OSINT를 소개하고 이 분야의 개념과 특성, 그리고 활용사례 등에 대해 논의함으로서 국내에서 OSINT 분야에 대한 중요성을 인식시키는 것에 목적을 가진다. 효과적인 공개정보(Open Source)의 활용을 위해 OSINT는 충분한 잠재적 가치를 가지며 이는 국내에서도 필요한 분야이다. 특히 정보통신기술의 발달과 급격한 인터넷의 확산으로 폭발적으로

늘어나는 정보(Information)를 보다 가치 있는 정보(Intelligence)로 변형시키고 확보해 나가는 것은 사회안전망 구축을 위해서도 필요할 것이다. 그리고 국가안보와 직접적으로 관련되어있는 북한의 군사적 안보위협과 테러리즘에 대한 대응뿐만 아니라 각종 범죄에 대응하는 효과적인 방안이기도 하다.

참고문헌

1. 국내문헌

문정인 (2002). *국가정보론*. 서울: 박영사.

조병철 (2003). 인터넷의 多元的 公開出處情報(OSINT)에 基盤을 둔 國家情報活動 體系. *정보보증 논문지. 제 3권 2호*: 41-55.

이동훈 (2008). 요즘 美대통령 일일브리핑 정보소스는 인터넷, 중앙일보. http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=104&oid=005&aid=0000309735

장호근 (2012). 내곡동 잔혹사의 교훈, 중앙일보. http://sunday.joins.com/article/view.asp?aid=24409

2. 외국문헌

Appel, E. J. (2011). *Internet Searches for Vetting, Investigations, and Open-source Intelligence*. Boca Raton, FL: CRC Press.

Bean, H. (2011). *No More Secrets: Open Source Information and the Reshaping of U.S. Intelligence*. Santa Barbara: Praeger.

Burke, C. (2007). Freeing knowledge, telling secrets: open source intelligence and development. Bond University: CEWCES Research Papers.

Classman, M. & Kang, M. (2012). Intelligence in the internet age: the emergence and evolution of Open Source Intellignce(OSINT). *Computes in Human Behavior,* 28. 673-682

Davind, A. (2005). Diving the Digital Dumpster: the impact of the internet on collecting open source intelligence. Air & Space Power Journal, 82-91.

Department of the Army. (2006). *Open Source Intelligence*. FMI 2-22.9

Drager, W. (2009) Take advantage of OSINT. Military Intelligence, 39-44.

NATO. (2002). Intelligence exploitation of the internet. *NATO OSINT Manual.*

Open Source Center. (2009). *Advanced Googling for Senior Executives*. Open Source Academy Internet Science Faculty.

Schedure, S. & Jorger. J. (2010). The evolution of open source intelligence. OSINT research reports, Switzerland: Zurich.

Sherman, C. & Price, G. (2001). The Invisible Web: Uncovering Information Sources Search Engines Can't See. Medford, NJ: CyberAge Books.

Tekir, S. (2009). *Open Source Intelligence Analysis: A Methodological Approach*. Saarbrucken, Germany: VDM.

3. 참여관찰

글쓴이는 2004년부터 2007년까지 ISVG(Institute for the Study of Violence Groups)에서 OSINT(Open Source Intelligence)에 기초한 테러리즘 데이터베이스 구축 프로젝트에 수석 연구원으로 참여하였다. 이 사업은 주로 온라인상에서 공개정보(Open Source)를 바탕으로 테러리즘 데이터베이스를 구축한 작업으로 미국 법무부의 연구자금 지원으로 시작하여 미국 국방부의 자금지원으로 현재까지 계속되고 있는 사업이다. 현재는 미국의 테러리즘 관련 주요 데이터베이스의 하나로 성장하였으며 현재 15만 건 이상의 테러리즘 관련 데이터베이스를 구축하는 성과를 거두었으며 이를 바탕으로 여러 다양한 테러리즘 관련 연구 및 분석을 수행해오고 있다.

4. 웹사이트

FDD(Foundation for the Defense of Democracies) 웹사이트

ISVG(Institute for the Study of Violent Groups) 웹사이트 www.isvg.rog

START(National Consortium For the Study of Terrorism and Responses to Terrorism) 웹사이트 www.start.umd.edu

【Abstract】

Intelligence in the Internet Era: Understanding OSINT and Case Analysis

Lee, Wan-Hee
Yun, Min-Woo
Park, Jun-Seok

With advances of information technology (IT) and the Internet, it became much easier to search and collect information through many different types of web search engine. Such information only restricted to the intelligence services became available to the public, and the increased open source changed the intelligence collection activities of governments. Open Source Intelligence (OSINT) was introduced to organize and analyze the large volumes of information. OSINT is actively used after the 9/11 terrorist attack, and the United States government invest a huge amount of budget to conduct research and develope technology about OSINT. Although many Western countries recognize the importance of OSINT and deal with open source as priority, South Korea has not fully understand the important role of OSINT. Therefore, this study introduces the fundamental principles of OSINT and provides practical examples of OSINT usage. OSINT is an effective source to prevent terrorist attacks as well as a variety of crimes. Extensive discussion and suggestions for future usages are provided.

Key words : Open source intelligence; OSINT, Information, Intelligence, Terrorism, Internet