스마트미디어 시대의 테러네트워크에 관한 고찰

임유석* · 김상진**

요 약

오늘날 테러조직의 구조는 복잡 다양한 네트워크 형태로 진화하고 있지만, 이는 무작위로 결합하여 생성된 네트워크가 아니라 선호도 결합 형태를 띠는 네트워크 현상으로 나타나고 있다. 이에 법집행기관의 효과적인 대테러 대책을 위해서는 테러네트워크의 특성과 유형에 대한 이해와 연구가 선행되어야 하며, 스마트미디어 시대에 적합한 기술 정보적 전략들을 수립해야 한다. 특히, 자생테러리즘은 전통적인 테러리즘과는 달리 국가와 지역의 경계 없이 불특정 다수를 대상으로 한 정치·이념·종교 등 다양한 목적의 폭력행위를 일삼는 새로운 형태의 위험성을 상징적으로 나타낸다. 스마트미디어 시대에서 극단적인 자생테러네트워크의 구성원들은 특유한 형태의 급진화 과정을 겪으면서 성장하고 있으며 활동영역 또한 추상적이고 광범위하기 때문에 국가적 차원의 법집행기관들이 치밀하게 테러네트워크를 파악해야만 한다. 아울러 온라인 공간에서 은밀하게 형성되고 진화되는 급진적이고 자생적인 테러조직 네트워크 형성에 접근할 수 있는 다양한 스마트미디어 매체들의 부정적인 측면을 고려하여 테러네트워크에 대한 추적과 차단에 정보공동체들이 활용해야만 한다.

Review on the Terror Network in Smart Media Era

Lim You Seok* · Kim Sang Jin**

ABSTRACT

Today, the structure of terrorist organizations in the form of a variety of network complexity are evolving. However, terrorist organization not combining randomly generated network but preferential attachment a network. So, it's research should be preceded a better understanding about the characteristics and type of terror network for a effective counter-terrorism policy of law enforcement. In addition, the appropriate response strategy have to technique establish in an era of smart media. In particular, homegrown terrorist attacks on unspecified people without boundaries of countries and regions unlike the traditional terrorism. Also, homegrown terrorism are violence and criminal activity by new various of religion, politics, philosophy. Besides the extreme members of homegrown terror networks went grow up through the evolutionary process in the age of smart media. Law enforcement agencies must identify the terrorist network at the national level. Therefore, terror networks evolving in the online space, forming a radical homegrown terror organizations have access to the network. Intelligence community track terrorist networks and to block the negative aspects of the smart media outlets should be considered.

Key words : Terror Network, Counter-Terrorism, Homegrown Terrorism, Radicalization, Smart Media

접수일(2013년 5월 13일), 수정일(1차: 2013년 5월 19일), 게재확정일(2013년 5월 20일)

* 선문대학교 경찰행정법학과
** 백석문화대학교 경찰경호학부

1. 서 론

최근 스마트미디어 시장은 다양한 첨단기술 도입을 바탕으로 급속히 발전하고 있다. 이로 인해 스마트미디어의 모든 사용자 상호간에 시간과 공간을 초월하여 온라인에 접속하여 소통할 수 있는 스마트 인터넷 시대가 열려 있으며, 사회 전반에 걸쳐 스마트미디어 기술이 활용되는 스마트사이어티(Smartciety) 시대라는 패러다임의 변화 속에서 일상생활을 유지하고 있다.

이러한 스마트사이어트 시대에 핵심적인 역할과 지위를 차지하고 있는 소셜네트워크 서비스(Social Network Service, 이하 'SNS'라 칭함)에 대한 연구들은 테러집단에 의해 실질적으로 활용되고 있는 경우가 상당하다. 그러나 이와 관련된 이론적인 논의와 법집행기관 업무수행 사이에 일정한 괴리와 한계가 있음을 보여주는 사례가 많이 나타나기도 한다. 이에 테러리즘에 대응하는 국가의 법집행기관은 지식관리형 경찰활동(KMP: Knowledge-Managed Policing)을 적극 활용하기도 한다.[14]

스마트미디어 시대에서 발생하는 전 세계 테러리스트들의 공격유형은 복잡 다양한 네트워크 형태로 진화하고 있지만, 이는 테러집단 구성원들이 무작위로 결합하여 생성된 네트워크 형태가 아닌 네트워크 선호도 결합(preferential attachment) 형태를 띠는 현상으로 나타나고 있다. 이에 대해 법집행기관의 대테러 전략은 테러네트워크의 특성과 유형에 대한 이해와 연구가 선행되어야 하며, 스마트미디어 시대에 적절한 기술적 전략들이 요구되고 있다.[2] 더구나 스마트미디어 시대의 테러리스트는 디지털 지하드(digital jihad)나 자생테러 네트워크(homegrown terror network)와 같이 활동영역과 성장단계가 전통적인 테러조직에서 나타나는 행태가 아니므로 이에 전문적이고 치밀한 대응전략들이 요구되기도 한다.

일반적으로 온라인 공간에서 형성된 테러집단들의 역할관계는 주로 암호화된 스테가노그래피 (steganography) 형식의 스팸메일(spam mail), 벌크메일(bulk mail), 정크메일(junk mail)을 사용하여 메시지를 전달하는 등 수사와 정보기관의 추적과 통제를 어렵게 하기 때문에 법집행기관이 업무수행을 하는데 어려움을 겪고 있다. 다양하게 발신·수신하는 메일은 보통 중요한 내용의 일부분을 첨가하거나 분리(chaffing and winnowing)하는 기술을 이용하여 전달하는 경우가 많고, 모자이크를 통해 패스워드를 전달하는 형식으로 이루어진다.[6]

실제 2001년 10월 뉴욕타임즈(New York Times)는 알 카에다(Al-Qaeda)가 스테가노그래피 파일을 이용하여 특정 이미지 메시지를 전달한 후에 이메일과 유즈넷(usenet)을 통해 2001년 9.11테러공격을 지시하였다고 보도하였다. 또한 2006년 4월 미국 사이버 안전 및 정보보안 연구개발을 위한 연방기획(The Federal Plan for Cyber Security and Information Assurance Research and Development)에서는 사이버공간에서 테러리스트들은 외국의 비밀정보 취득과 관련된 스파이 행위들을 한다고 밝혔다. 보통 초기에는 상업적인 거래 목적으로 접근하였다가 해커나 조직범죄 집단에 의해 금융 사기나 개인 신원정보 도용 등 다양한 유형으로 은밀하게 범죄행위를 일삼는다. 그 중의 한 가지 방법이 스테가노그래피 기술사용인데 단순한 범죄로 시작하여 국가안보에 심각한 위협을 줄 정도에 이르기까지 다양하게 전개된다. 그리고 스테가노그래피는 특정 집단에서 수많은 형태의 정보보고서로 활용이 되고, 아울러 테러리스트들의 훈련 매뉴얼이 되기도 하며, 심지어 알 카에다는 숨겨진 메시지를 포르노그래피에 숨겨두고 활용한 것으로 나타나기도 하였다.[19] 그러므로 시민들의 일상생활에 암묵적으로 자리잡고 있는 테러리즘의 구성요소를 파악하기 위해서라도 전문적이고 은밀한 수사와 정보기관의 역할이 반드시 필요하다.

이 연구에서는 오늘날 세계인들의 일상생활이 되어버린 SNS의 사용현황과 이면의 부정적 측면과 관련된 문제점에 대해 알아보고, SNS를 이용하여 발생할 수 있는 테러네트워크를 중심으로 테러리즘의 발생 가능성을 진단하고자 한다. 아울러 온라인 공간에서 진행될 수 있는 테러리즘의 단계와 특징 그리고 구조에 대해 살펴본 후에 법집행기관의 대응전략에 대해 논의하고자 한다.

2. 스마트미디어 시대의 네트워크

2.1 스마트미디어 시대의 의미

스마트미디어(smart media)란 “공동체 사회 구성원들 간의 소통 도구로 스마트기기 사용자 간의 상호작용이 가능하며, 시간적・공간적 제약 없이 융합콘텐츠를 제공하는 똑똑한 매체(네트워크컴퓨터, 스마트폰, 태블릿PC 등)”로 정의할 수가 있다.[3]

2012년 KT 경제경영연구소의 조사에 의하면 한국의 TV 보급률은 97.5%에 달하며, 두 대 이상 보유한 가구도 42.6%에 달한다. 그러나 TV를 보유하고 있음에도 PC, 스마트폰, 태블릿PC 등의 스마트 기기를 주 시청 기기로 이용하는 비율이 35.5%에 이르는 것으로 나타났다. TV수상기를 통한 시청형태가 스마트 기기 쪽으로 변화됨에 따라서 기존 영상콘텐츠에 대한 시청 방식도 실시간 채널에서 스트리밍 VOD로 바뀌고 있다. 이러한 시청 방식의 변화는 방송국에서 송출되는 채널을 일방적으로 시청하는 수동적인 시청에서, 본인이 원하는 콘텐츠를 선택하는 능동적 시청으로 그 방식이 바뀐다는 것을 의미한다. VOD 등 다운로드 콘텐츠의 사용률이 늘어나면서 TV 대신에 스마트 기기를 사용하는 비율 또한 증가하고 있다. 스마트미디어의 보급률 증가와 더불어 TV시청 행태에 나타나는 현상은 TV시청을 하면서 멀티태스킹을 하는 비중이 높아지고 있다는 것이다. TV를 시청하는 동안 과반수 이상이 다른 행동을 하며 가장 많은 행동이 웹서핑이라는 것이다. 이러한 현상은 다양한 기기에서 TV시청이 가능해지면서 기존의 “lean back” 개념의 휴식을 위한 TV의 전통적인 개념이 변화되기 시작하였다는 것을 의미한다.[3]

2.2 스마트미디어 시대 정보검색 및 환경 변화

스마트미디어 시대라는 환경에서 새로운 정보의 검색 기술과 환경변화는 다음과 같은 특징을 지니고 있다.[4]

첫째, 스마트폰 등의 이동형 스마트 기기의 보편화와 무선 인터넷 확산에 따라 사용자의 인터넷 접근이 용이해졌다. 이는 사용자가 의식하지 못하는 사이 인터넷 접속 환경이 장소와 시간의 구애 없이 개인 사용자에게 쉽게 제공되고 노출될 수가 있는 것이다.

둘째, 다양한 형태의 소셜네트워킹 플랫폼의 등장과 소셜네트워크를 기반으로 한 정보 및 콘텐츠의 폭발적인 증가에 따라 정보검색 시스템은 보다 우수한 검색 성능을 요구 받고 있다.

셋째, 최근 스마트미디어 환경과 사용자 수가 급격히 확산됨에 따라 다양한 모바일 애플리케이션이 등장하고 있는데 이는 기본적 개인정보에서부터 일상생활 전반에 걸쳐 제공되는 다양한 정보들은 사용자의 선호와 상황에 맞는 검색결과를 제공할 수가 있다.

넷째, 온라인 정보의 폭발적인 증가는 기하급수적으로 증가하는 검색 시스템에 새로운 도전 과제와 기회를 동시에 주고 있다. 이러한 검색 시스템은 방대한 정보를 빠르게 처리할 수 있어야 하며, 이른바 빅데이터 분석(big data analysis) 기술은 방대한 데이터의 상호 연결과 의미를 분석하여 숨겨져 있는 정보를 발견함으로써 궁극적으로 사용자의 올바른 의사결정과 문제 해결을 도울 수가 있다.

다섯째, 스마트미디어 시대는 새로운 기술의 도래, 새로운 미디어 환경의 확산, 다양한 정보와 콘텐츠 형태를 등장시켰고, 정보검색 시스템에 대한 사용자의 기대를 변화시키며 그 수준을 높이고 있다. 사용자는 확장된 맞춤화, 개인화, 지능화 등 자신들의 검색 경험과 검색 결과의 유용성을 획기적으로 증대시킬 수 있는 새로운 특성들을 검색 시스템에 기대하고 있다.

한편, 일반적으로 사회적 관계는 주로 실제공간에서의 면대면(face-to-face) 형식으로 선택적・한정적으로 이루어지고 발전해 나간다. 그러나 인터넷 공간에서의 사회적 관계는 비대면(non- facing) 형식으로 이루어지고, 지리적인 한계 역시 초월하여 비선택적으로 이루어진다는 점을 살펴보아야 한다. 이에 범죄의 예방지역과 발생하는 공간을 오프라인에 한정시켜 놓은 전통적인 범죄학과 경찰학은 공간의 이동에 따라 법집행기관의 범죄예방과 진압 및 수사를 위한 견지에서 재해석될 필요성이 있다.[5]

2.3 SNS 서비스 현황

소셜네트워크 서비스(SNS: Social Networking Service)란 사회구성원의 사회적 관계 형성 개념을 실제 공간이 아닌 인터넷 공간으로 가져온 것으로서 온라

인상에서 불특정 다수의 타인 및 개인이나 친구와 특정한 관계를 맺고, 정보를 공유하여 지속적으로 의사소통(communication)을 확대해 나가는 일련의 공동체(community) 구성활동을 지칭하는 말이다.[11]

SNS 공동체 사회의 연결을 담당해주는 전 세계 인터넷 사용자들의 현황을 <표 1>에서 살펴보면, 인터넷 사용자의 44.8%는 아시아 지역에서 사용하는 것으로 나타났다. 이어서 유럽(22.1%), 북미지역(12.0%), 남미지역 및 카리브해 지역(10.4%), 아프리카(6.2%), 중동지역(3.4%), 오세아니아(1.1%) 순으로 나타났다. 그리고 인구수에 따른 인터넷 사용자 점용률은 북미지역이 가장 많이 나타났고, 이어서 유럽과 아시아 지역에서의 사용자가 많은 것으로 나타났다.

<표 1> 세계 인터넷 사용자 현황

	인구	사용자	비율(%)
Africa	1,037,524,058	139,875,242	6.2
Asia	3,879,740,877	1,016,799,076	44.8
Europe	816,426,346	500,723,686	22.1
Middle East	216,258,843	77,020,995	3.4
North America	347,394,870	273,067,546	12.0
Lat Am/Carib.	597,283,165	235,819,740	10.4
Oceania	35,426,995	23,927,457	1.1
World Total	6,930,055,154	2,267,233,742	100.0

출처: 세계 인터넷통계(www.internetworldstats.com)

이어서 SNS 스마트시대에서 가장 빈번하게 사용되고 있는 네트워크의 유형을 <표 2>에서 살펴보면, 온라인 공간에서 형성되는 커뮤니티와 미니홈페이지, 블로그, 마이크로 블로그, 프로필 기반 제공서비스를 볼 수가 있다.

<표 2> SNS 유형분류

구분	정의	예시
커뮤니티 (카페, 클럽)	인터넷 상 취미, 관심분야가 유사한 사람 간의 정보교류 및 친목도모 모임	다음 카페 네이버 클럽
미니홈피	네티즌들이 직접 제작하여 상대방을 초대하는 공간으로 인맥 형성하는 1인 미디어	싸이월드, 세이클럽, 드림위즈, 버디홈피 등
블로그	개인 관심사 일기, 칼럼, 전문자료, 사진 등을 게시하여 타인과 공유하는 1인 미디어	다음 및 네이버 블로그, 티스토리, 이글루스 등
마이크로 블로그	140-150k 이내 단문 메시지로 생각과 감정 공유하는 미니블로그	트위터, 미투데이, 플레이톡, 토씨
프로필 기반서비스	개인정보 관련 사진, 동영상 등 프로필 페이지 제공하여 네티즌 인맥형서, 교류	페이스북, 마이스페이스, 링크나우, 링크드인 등

출처: 한국인터넷진흥원, 2010.[8]

미국의 대표적인 시장조사기관인 이마케터(eMarketer Inc.)가 제시한 전 세계 소셜네트워크 서비스(SNS) 사용인구 추세를 살펴보면 아래 <표 3>과 같다. 2011년에는 약 1,202,200,000명이 사용하였고, 2012년 약 1,433,500,000명, 2013년 약 1,662,400,000명, 2014년 1,854,700,000명이 사용할 것으로 나타났다.

특히, 아시아·태평양 지역에서는 중국이 가장 많이 사용하는 것으로 나타났고, 이어서 인도와 일본 그리고 한국, 호주 순으로 많이 사용하는 것으로 나타났으며, 남미 지역에서는 브라질에서 사용인구가 월등히 많은 것으로 나타났다. 동유럽 지역에서는 폐쇄적인 사회체제상 사용인구가 비교적 적게 나타났고, 독일과 영국을 비롯해 서유럽 지역 대부분의 국가에서는 전반적으로 소셜네트워크 서비스(SNS)를 사용하는 인구가 많은 것으로 나타났다.

<표 3> 세계 SNS 사용인구 추세

(단위: 백만명)

구분	2011	2012	2013	2014
아시아	439.5	615.9	745.6	853.7
남미	164.9	191.8	215.9	236.9
북미	163.9	174.7	181.9	189.2
동유럽	139.0	157.4	176.5	192.7
러시아	52.1	57.9	64.2	69.3
중동/아프리카	111.1	148.5	183.0	211.6
서유럽	129.8	145.3	159.4	170.8
합 계	1,202.2	1,433.5	1,662.4	1,854.7

출처: 이마케터(www.eMarketer.com)

3. 스마트미디어와 테러네트워크

3.1 테러리스트의 네트워크

다양한 정치·경제·사회·역사·종교 문제를 기반으로 형성된 테러집단과 이러한 테러리스트에 의해 사용되는 인터넷의 용도는 광범위하고 은밀하게 나타나고 있다.

Conway(2006)에 의하면, 테러리스트들이 주로 사용하는 인터넷의 종류는 테러조직운영을 위한 기금조성, 정보전달, 보안이 담보된 의사소통, 정치적 행동, 사이버공포 수집 및 확산, 테러조직 구성원 모집과 동기부여 등을 위해 테러리스트들이 암묵적으로 인터넷을 사용하는 것으로 설명하고 있다.

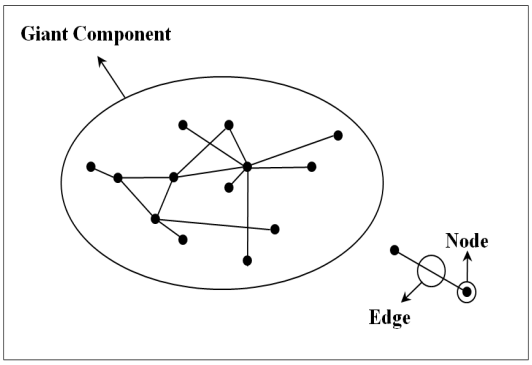
<표 4> 테러리스트 인터넷 사용

Author(s)	Uses
Furnell & Warren	Propaganda & Publicity / Fundraising Information Dissemination Secure Communications
Cohen	Planning / Finance Coordination & Operations Political Action / Propaganda
Thomas	Profiling / Propaganda Anonymous / Covert Communication Generating “Cyberfear” / Finance Command & Control Mobilisation & Recruitment Information Gathering Mitigation of Risk Theft / Manipulation of Data Offensive Use / Misinformation
Weimann	Psychological Warfare Publicity & Propaganda Data Mining / Fundraising Recruitment & Mobilisation Networking Share Information Planning & Coordination

출처: Conway(2006: 11).[13]

3.2 네트워크의 구성요소

소셜네트워크 공간에서의 네트워크 관계를 형성하는 구성요소와 구조들을 이해하기 위해서는 <그림 1>과 같이 노드-에지(node-edge) 구조의 개념을 파악해야 한다. 네트워크 공간 내의 노드-에지(node- edge) 구성요소들의 역동성과 파급성은 실제 공간에서의 급진화(radicalization)보다 그 속도가 월등히 빠르게 진행된다. 이러한 소셜네트워크에서 노드(node)는 보통 소셜네트워크 구성원들을 나타내고, 노드(node) 사이를 연결시켜 주는 역할을 에지(edge)가 담당한다. 에지(edge)는 네트워크 공간에서의 사회적 유대 또는 연결고리로서의 역할을 하고 그들 사이에서도 특성들을 나타내며 활동할 수도 있다. Giant Component는 다량의 노드(node)들이 결합된 또 하나의 거대한 집단이며, 소셜네트워크상에서 사회적인 역동성과 영향력을 집단적으로 표출하는 역할을 하기도 한다. 그러나 소셜네트워크 구성원들의 개인적·집단적인 영향력의 가시성은 쉽게 노출되지 않고 강한 유대관계를 형성할 수가 있기 때문에 구성원들이 공유하는 가치와 공감대를 파악하기에는 상당히 어려운 측면이 있다.[17]



<그림 1> Social Network 구성요소

출처: Scott(2012: 38).[17]

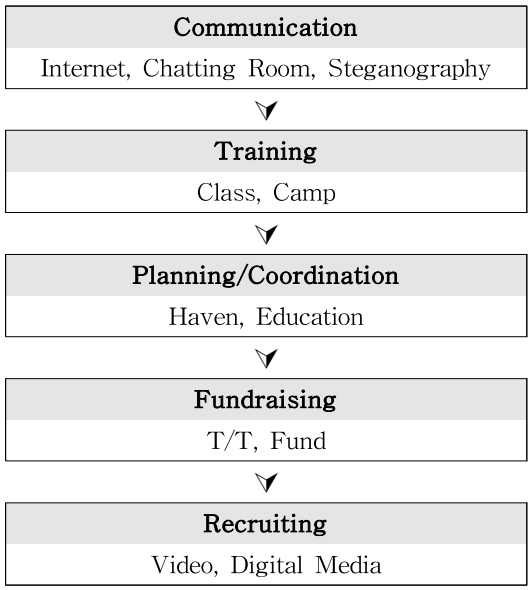
3.3 테러네트워크의 진행단계

오프라인 공간이 아닌 실제 공간에서 전통적인 테러리즘의 파급성과 급진화(radicalization)는 지리적으로 안정된 캠프에서 폐쇄적이고 은밀한 교육과 훈련 그리고 모집활동으로 이루어져 왔다. 이를테면, 알 카에다(al-Queda)의 전통적인 캠프훈련 활동영역은 주로 수단(Sudan)이나 아프가니스탄(Afghanistan)의 비공개 특정지역에서 이루어졌고, 콜롬비아 무장혁명군(The Revolutionary Armed Forces of Columbia: FARC)은 깊은 산속이나 정글에서 활동하였으며, 모로 이슬람해방전선(The Moro Islamic Liberation Front: MILF)은 필리핀 남서부 슬루(Sulu) 지역을 기반으로 활동해 왔다.[17]

그러나 인터넷 공간은 이러한 지리적인 환경에서 활동하는 것보다 훨씬 많은 부분의 기능과 업무를 전 세계에서 수행하는데 도움을 줄 수가 있어 지리적인 구역이나 환경들이 무색해지는 특징을 가지고 있다. 아울러 이러한 테러집단 구성원들의 조직적 성향은 개인적으로 은밀하게 전파가 되기 때문에 일정한 진행단계를 걸쳐 자생적 테러리즘(homegrown terrorism)으로 발전해 나갈 수가 있다.

또한, 전 세계 어디에서 누구든지 익명으로 테러조직에 접근할 수가 있고, 정보를 제공해 주는 주체(host)도 테러집단과 무관한 형태로 홈페이지를 만들어 은밀하게 운영하고, 사이버 은신처(cyber haven)로서의 기능을 유지할 수가 있다. 이러한 테러리즘의 단계는 오프라인 공간과는 달리 보다 은밀하고 조직적으로 움직이며, 실체 역시 지속적·영구적이지 않아 관련 범죄를 통제하려는 기관의 접근을 어렵게 만들고 있다. 그리고 오프라인 공간에서의 테러리즘 급진화과정과는 달리 의사소통단계에서부터 구성원들의 모집까지 추적을 어렵게 만들기도 한다. 인터넷공간에서의 테러리즘 진행단계를 살펴보면 <그림 2>와 같다.

인터넷 공간에서의 테러리즘의 진행단계는 의도적·기능적으로 접근한 특정인과의 인터넷 공간에서의 조우와 일방적 이메일 수신을 통한 의사소통으로부터 시작이 된다. 이후 사이버 은신처에서 기본적인 훈련과 교육 내용이 전달이 되고, 기금을 마련한 후에 테러집단 구성원들을 적극적으로 모집하게 된다.



<그림 2> 인터넷상 테러리즘 진행단계

3.4 자생테러리즘의 진행과 네트워크

2007년 10월 23일 시행된 미국 「폭력적 급진화와 자생테러방지법」(The Violent Radicalization and Homegrown Terrorism Prevention Act of 2007)의 정의에 따르면, 자생테러리즘(Homegrown Terrorism)이라 함은 "정치적·사회적 목적을 촉진시키기 위해 미국 정부와 시민 또는 이와 관련된 부분을 협박하거나 억압하기 위해 주로 미국 또는 미국의 속령 내에서 태어나서 자라거나 기반을 두고 활동하는 집단 또는

개인에 의한 완력 또는 폭력을 계획적·위협적으로 사용하는 행위"라고 정의하고 있다. 이러한 자생테러리즘의 급진화 단계는 온라인 공간에서 은밀하고 급속하게 진행될 수가 있으며, 급진화의 속도를 촉발시키는 결정적인 역할을 제공하고 있는 것이 바로 스마트미디어라고 볼 수가 있다.

한편, 인터넷이라는 가상공간은 지리적으로 다양한 위치에 있는 사람들을 한 마음으로 만드는데 상당히 쉬운 역할을 제공해 주기 때문에 증오집단들은 자신들의 태도와 행동에 대한 정당성을 부여하고 이러한 메시지를 널리 알릴 수 있는 더 없이 좋은 공간으로 작용할 수가 있다.[10] 이에 테러리스트들은 젊은 세대의 집단에게 테러조직의 이념과 사상을 전달하여 쉽게 동조하게 만든다. 특히, 사춘기 소년들과 같은 불안한 정체성을 가진 대상들에게는 테러리스트들의 메시지를 전달하는데 비교적 용이하다.[18]

그리고 Precht(2007)는 자생테러리즘의 급진화 과정에 대해서 테러공격에 이르기까지 그 수단의 유일한 기폭제나 원인은 존재하지 않고 다양하게 작용한다고 역설하였다. 특정 이념에 치우친 극단주의자들의 급진화 과정은 역시 다양한 동기와 요인에 의해 영향을 받고 자생테러리즘으로 나아간다. 이러한 요인으로는 배경요인과 촉발요인 그리고 기회요인으로 설명하고 있다.[1][15]

첫째, 배경요인(background factors)으로는 서구사회에서 무슬림으로서의 정체성 위기와 개인적인 고통과 차별의 경험과 상대적 박탈요인(사회적 불만족, 빈곤 등), 살아가는 환경과 동년배(분리와 평행사회)로부터의 소외와 정의롭지 못하다는 지각 그리고 이슬람 테러에 대한 무슬림들 간의 비판적인 토론의 상대적 부재를 들 수가 있다.

둘째, 촉발요인(trigger factors)으로는 서구사회의 대외정책이 낳은 유발적인 사건, 지하드의 신화와 행동에 대한 욕구, 카리스마 있는 지도자나 정신적인 조언자의 존재를 들 수가 있다.

셋째, 기회요인(opportunity factors)으로는 이슬람 사원, 인터넷과 위성방송채널, 학교, 대학, 청소년클럽, 작업장, 교도소, 놀이 활동, 카페, 서점을 통하여 급진적인 과정으로 진행한다.

특히, 이슬람교라는 종교의 특정 급진주의자들은 급진화 전단계(pre-radicalization), 종교 개종과 정체성(conversion and identification), 이슬람교의 교의(敎義) 신념과 주입(conviction and indoctrination) 및 교육, 행동(action) 등의 단계를 거쳐 자생적인 테러리즘으로 발달하게 된다.

4. 논의 및 결론

스마트미디어 시대에서 극단적인 자생테러 네트워크의 구성원들은 특유한 형태의 급진화 과정을 겪으면서 성장 발전하고, 활동영역 또한 추상적이고 광범위하기 때문에 국가적 차원의 정보공동체 기관들이 치밀하게 대응해야만 한다.

스마트미디어 시대인 오늘날 전 세계를 하나의 연결고리로 이어주는 역할을 하는 소셜네트워크 서비스(SNS)는 실제 공간이 아닌 온라인 공간에서 제공되고 있다. 그래서 소셜네트워크 내에서 이루어지는 테러리즘의 역학관계를 파악하기 위한 공식적인 형사사법기관의 역할은 그 한계가 본질적으로 내재할 수밖에 없다. 이는 인터넷을 기본으로 하여 SNS 사용자들은 지금 이 순간에도 지리적인 영역을 초월하여 기하급수적으로 늘어나고 있으며, 이러한 소셜네트워크 구조는 테러집단들이 은밀하게 활동하고 구성원들을 확보하기에 잠재적인 은신처로서 더 없이 좋은 환경이 될 수밖에 없다.

아울러, 스마트미디어 시대에서 테러네트워크의 중요한 구성요소인 테러리스트 개인에 해당하는 노드, 테러리스트 개인들 간의 연결 관계와 결합을 나타내는 에지 구조에서의 연결고리는 주요한 영향력을 행사하는 테러집단의 리더 또는 중간 간부 등을 의미하지만,[2] 자생적으로 성장하는 테러리스트의 테러네트워크 연결 관계는 일정한 선호도에 의해 형성되므로 이러한 부분을 주의 깊게 관찰하면서 접근하여야 한다.

오늘날 테러집단 중에서도 특히 알 카에다 또는 탈레반 종류의 이슬람 극단주의 테러집단들이 네트워크 형태로 진화했다는 사실은 많은 전문가들에 의해 지적되어 왔다. 하지만 이러한 테러네트워크집단들이 어떠한 종류의 네트워크로 이루어져 있는지에 대한 구

체적인 진단은 아직까지 충분히 이루어지지 않고 있다. 그리고 테러네트워크에 대한 부족한 이해는 대테러정책 슬로건이 테러리스트 개인에 대한 무작위 공격의 성격을 띰으로서 수많은 테러리스트를 제거했음에도 불구하고 이슬람 극단주의 테러네트워크의 작동 자체를 무력화시키는 데는 실패하게 되는 결과로 이어졌다.[2][10][16]

결국, 소셜네트워크 서비스(SNS)를 통한 테러리즘의 확산과 전이 그리고 급진화 현상에 대한 사전 가능성을 진단하는 것이 중요하다. 그러므로 전통적인 범죄학 영역에서도 온라인 공간에서 이루어지는 새로운 현상을 파악하고 대응하기 위해 사회통제와 해체요인 그리고 비대면 상황에서의 급진적 테러리즘 발전원인에 대해 재해석해야 한다. 아울러 형사사법기관에서도 테러리스트들의 활동 루트를 파악하기 위한 적극적인 수사와 정보활동으로 온라인 공간에서의 잠재적이고 극단적인 테러공격으로 나아갈 수 있는 테러네트워크를 파악하고 그 가능성을 진단해야 한다.

참고문헌

[1] 박철현, “국내 자생테러 발생가능성에 대한 연구: 이슬람 자생테러를 중심으로,” 형사정책연구, 제21권, 제4호, pp. 61-89, 2010.

[2] 윤민우, “소셜 네트워크 접근을 통한 테러네트워크 이해와 분석 및 전략적 접근방안: 탈레반, 알카에다 등의 이슬람 극단주의 테러를 중심으로,” 형사정책연구, 제22권, 제1호, pp. 201-230, 2011.

[3] 윤장우, "스마트미디어 시대의 도래 및 발전방향," 방송공학회지, 제18권, 제1호, pp. 10-22, 2013.

[4] 조준면, 김명은, 홍진우, “스마트미디어 검색기술 동향 및 전망,” 한국통신학회논문지, 제29권, 제10호, pp. 37-43, 2012.

[5] 최응렬, “자생테러리즘의 발생가능성과 지역사회에서의 대응방안,” 대테러연구, 제34집, pp. 215-242, 2012.

[6] 최응렬, “소셜네트워크 서비스(SNS)의 사용현황 및 테러발생 가능성 진단,” 대테러연구, 제35집, 2013.

[7] 최진혁, “SNS(Social Network Service)의 위험성 및 Policing(경찰활동)에 미칠 영향에 대한 시론적 연구,” 한국경호경비학회지, 제29호, pp. 301-336, 2011.

[8] 한국인터넷진흥원, “소셜네트워크 서비스(SNS) 현황,” 2010.

[9] Bakier, A. H., “The New Issue of Technical Mujahid, a Training Manual for Jihadis,” Terrorism Monitor, Vol. 5, No. 6, The Jamestown Foundation. 2007.

[10] Berkowitz, B., ‘The new face of war: how war will be fought in the 21st century,’ New York: The Free Press. 2003.

[11] Boyd, D. M. and Ellison, N. B., “Social Network Sites: Definition, History and Scholarship,” Journal of Computer-Mediated Communication, Vol. 13. 2007.

[12] Citron, D. K. and Norton, H., “Intermediaries and hate speech: Fostering digital citizenship for our information age,” Boston University Law Review, Vol. 91, p. 1438-39, 2011.

[13] Conway, M., "Terrorist use of the Internet and Fighting Back," Information & Security: An International Journal, Vol. 19, p. 11, 2006.

[14] Geoff, D., Peter, B. and Newman, J., “The Dark Side of Social Media: Review of Online Terrorism,” Pakistan Journal of Criminology, Vol. 3, No. 3, pp. 103-122, 2012.

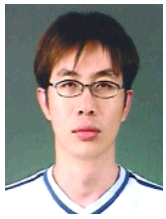
[15] Precht, T., ‘Homegrown Terrorism and Islamist Radicalization in Europe’, Research Report, Danish Ministry of Justice. 2007.

[16] Sageman, Marc,‘ Understanding terror networks,’ Philadelphia, PA: University of Pennsylvania Press, 2004.

[17] Scott, H., ‘Edges of Radicalization: Individuals, Networks and Ideas in Violent Extremism,’ The Combating Terrorism Center at West Point, 2012.

[18] Weimann, G., “Terror on Facebook, Twitter, and Youtube,” The Brown Journal of World Affairs, Vol. 16, No. 2, pp. 45-54, 2010.

[저 자 소 개]



임 유 석(You-seok Lim)

2005년 2월 학사
2008년 2월 석사
2013년 2월 박사

email : camus200@nate.com

김 상 진(Kim-Sang Jin)

2001년 2월 용인대학교 경호학과
체육학사
2003년 2월 용인대학교 경호학 석사
2008년 12월 경기대학교
경호안전 박사

email : ksj8004@naver.com