형사정책연구 Korean Criminological Review
제22권 제1호(통권 제85호, 2011 · 봄호)

소셜 네트워크 접근를 통한 테러네트워크 이해와 분석 및 전략적 접근방안 : 탈레반, 알카에다 등의 이슬람 극단주의 테러를 중심으로*

윤 민 우**

국 | 문 | 요 | 약

오늘날 테러조직은 네트워크 형태로 진화했다. 그리고 이 테러네트워크는 무작위로 결합하여 생성된 무작위(random) 네트워크가 아니라 선호도 결합 (preferential attachment) 형태를 띠는 scale-free 네트워크 이다. 때문에 대테러 전략은 이 scale-free 네트워크의 독특한 특성에 기초해서 디자인 되어야 하며 이를 위해서는 이러한 유형의 네트워크의 특성에 대한 이해가 선행되어야 한다. 이 논문은 scale-free 형태인 테러네트워크가 hub에 대한 선택적 공격에 취약함에 착안하여 전체 테러네트워크의 파괴나 무력화를 위해서는 우선 네트워크상에서 hub을 파악할 필요가 있으며 또 파악된 hub의 파괴에 대테러 기관 또는 법 집행 기관의 역량을 집중할 필요가 있음을 제시하고 있다. 궁극적으로 이 논문은 테러네트워크의 특성에 대한 이해를 통해 대테러 활동의 새로운 전략적 접근방안을 제시한다.

❖ 주제어 : 테러네트워크, Scale-Free 네트워크, 대테러 전략, 사회적 네트워크

Ⅰ. 머리말

1990년 냉전의 종결이후 지난 20년간 국제사회는 새로운 유형의 안보의 위협을 경험해오고 있다. 이러한 새로운 종류의 위협은 각종 지역분쟁과 테러리즘, 그리고 해적행위, 마약거래, 인신매매등의 각종 초국가범죄에 의해 대체되고 있는 것처럼 보인다. 지난 20년간의 변화는 놀랄만한 것이었으며 이러한 변화의 중심에는 세계

* 이 논문은 2010학년도 한세대학교 교내학술연구비 지원에 의하여 연구되었음.
** 한세대학교 경찰행정학과 조교수

화와 정보화라는 거대한 흐름이 있어 왔다. 하지만 불행하게도 세계화된 사회와 정보화된 세상의 편리함과 기회는 긍정적인 결과들 뿐 만아니라 글로벌테러와 지역분쟁, 그리고 각종 초국가범죄등의 간과할 수 없는 안보의 위협도 동시에 가져다주었다.

새로운 안보의 위협은 냉전시대처럼 하나의 강력한 국가로부터 오는 것은 아니다. 오히려 새로운 안보의 위협은 단일하지도 않으며 또 전통적 의미로 볼 때 결코 강력하다고도 볼 수 없는 여러 다양한 작은 비국가 행위자들의 총합이라고 볼 수 있다. 이들 가운데 이슬람 극단주의 테러리즘이 가장 주요한 안보위협으로 지목될 수 있으며 이 밖에도 분리주의 테러리즘, 민족주의 테러리즘, 사이버 테러리즘, 국가테러리즘, 환경테러리즘 등의 각종 테러리즘 위협들, 그리고 이라크, 아프가니스탄, 소말리아 등 각종 분쟁지역의 무장투쟁조직(Insurgents), 부족(Tribes), 그리고 혈족(Clans)등의 비국가 무장집단, 그리고 각종 조직범죄 집단들과 해적집단등의 다양한 비국가 폭력집단들이 세계화되고 정보화된 국제사회의 안보를 위협하고 있다(Shultz & Dew, 2009).

이러한 안보패러다임의 변화를 단적으로 보여주는 것이 전통적인 적대세력이었던 나토와 러시아가 함께 협력하고자 하는 시도일 것이다. 양측은 서로가 적대적인 안보위협이라는 것이 더 이상 현실적이지 않음을 인식하고 있다. 지난 달 리스본에서 열렸던 나토-러시아 정상회의에 2002년 이후 처음으로 러시아 대통령 메드베데프가 참석했던 사실은 이러한 인식의 전환을 간접적으로 보여주는 사건일 것이다. 양측은 적대적인 국가나 국가집단의 전통적인 군사침략은 더 이상 현실적으로 임박한 위협이 아니며 오히려 핵무기등의 대량파괴 무기의 불법집단이나 불량국가로의 확산, 테러리즘, 해상해적, 불법 마약거래와 확산등이 임박하고 현실적인 공통의 안보 위협이라는 사실에 인식을 같이 하고 있는 것 같다(Fewer dragons, more snakes, 2010).

새로운 형태의 안보위협의 대두와 함께 이러한 새로운 현상을 이해하고자 하는 여러 시도들 역시 있어왔다. 가장 이르게는 이미 1990년 초반에 엘빈 토플러에 의해 시도 되었다. 그는 생산의 양식이 파괴의 양식을 결정하는 경향이 있으며 따라서 정보화 시대의 도래는 새로운 전쟁 또는 갈등의 양식을 낳을 것이라고 예견했다. 그리고 그는 이러한 전쟁의 주요 행위자는 Ad-hoc으로 형성되고 수평적인 네트워

크 형태로 결합된 비국가 행위자들이 될 것이라고 지적했다(Toffler & Toffler, 1993). 한편 미국의 국제안보 및 전략 전문가인 Bruce Berkowitz(2003)는 오늘날의 전쟁은 과거의 전쟁과는 질적으로 다른 전쟁으로 변모하였으며 이 전쟁은 전면적인 군사적 공격을 통한 대량파괴가 아니라 특정 목표물에 최적의 폭력을 사용하여 정치적, 전략적 목적을 극대화하는 보다 복잡하고 미묘한 양식의 전쟁으로 진화했다고 주장한다. 한편, Reed(2008)의 경우는 보다 직접적으로 오늘날의 안보위협을 5세대 전쟁이라는 새로운 개념을 사용하여 정의하고 있다. Reed의 5세대 전쟁의 개념은 앞서 예기한 토플러와 버코비츠의 주장을 포함하면서 오늘날의 안보위협을 개념적으로 명확히 한다. 그에 따르면 5세대 전쟁은 기존의 전통적인 전쟁에 정치와 경제, 사회문화적인 요소, 그리고 사이버 공간 등이 추가된 통합적인 갈등을 지칭하며 이러한 새로운 전쟁양식의 대표적인 특징으로 나타나는 것이 전쟁과 범죄가 함께 융합하여 일어나는 안보위협이다. 따라서 오늘날의 테러리즘과 초국가범죄등의 현상을 이러한 5세대 전쟁에서의 안보의 위협으로 이해하여야 한다.

5세대 전쟁이라고 정의될 수 있는 오늘날의 안보위협은 전쟁과 범죄의 융합현상을 가져왔고 이는 바꾸어 말하면 국가안보와 치안활동간의 전통적인 경계가 더 이상 유효하지 않을 수도 있다는 사실을 말하고 있다. 실제로 세계화의 진행과 국경의 해체, 그리고 교통, 통신의 발달과 세계적인 산업 및 금융망의 구축 그리고 사이버 시대의 도래는 전통적인 의미의 국경의 실효성을 해체시키고 있다. 빈부의 차이와 문화와 종교의 차이 그리고 국적과 민족, 인종 및 정치적 신념의 차이에 따른 사람들간의 갈등을 기존의 국경으로 뚜렷이 구분 지을 수 없는 혼란스런 형태의 갈등 또는 소규모 전쟁들이 범람하는 현상이 나타나고 있다(Reed, 2008).

새로운 안보위협의 주체는 비국가 행위자들이다. 이 비국가 행위자들은 테러조직들, 무장집단들(insurgents), 부족 및 씨족들(tribes & clans), 마피아나 마약카르텔 등의 범죄조직들, 해상해적들등으로 이루어져 있는 무리들을 포함한다. 이 비국가 행위자들은 오늘날 각종 테러공격과 소규모 전쟁행위, 그리고 다양한 초국가범죄등을 실행하면서 민족-국가 체제의 약한 고리라 할 수 있는 허약한 국가들을 통제력을 상실한 실패한 국가들로 만들며 자신들의 정치적, 종교적, 경제적 이익을 극대화 하고 있다. 물론 이러한 행위자들이 국제사회에서 주요한 주체인 한국, 미국, 영국, 독

일등의 강력한 국가들과 직접적인 군사충돌 능력이 있지는 않지만 다양한 형태로 오늘날 국제질서의 기본축이라 할 수 있는 세계 경제, 법질서, 민주주의, 정치적 안정, 사회적 통합, 국민의 건강 및 안녕등을 위협함으로서 중대한 의미의 안보 위협이 되고 있다. 또한 비 국가행위자들은 서로의 필요에 의해 특정한 사업단위 별로 전략적인 동맹을 형성하고 서로 협조한다. 테러조직은 범죄집단이나 부족, 또는 무장투쟁집단과 전략적으로 협력하며 해적이나 범죄집단 역시 그들의 필요에 의해 테러조직이나 부족 또는 무장투쟁집단과 협업한다. 물론 이 비국가 행위자들이 어떤 거대한 음모아래에서 통합되어 있지는 않다. 그리고 그러한 협업역시 영구적인 기반에 의해 지속되지도 않는다. 오히려 이러한 전략적 동맹은 일시적이며 그때그때 필요에 따라 늘 변화하는 관계이다. 하지만 이러한 일시적이고 끊임없이 변화하는 비국가 행위자들의 전략적 동맹의 전일적 총합은 하나의 거대한 안보 위협이 되고 있다(Naim, 2005; Shultz & Dew, 2009).

네트워크개념은 오늘날 새로운 안보의 위협을 이해하는 키워드이다. 비국가 행위자들은 전통적인 의미의 관료적인 또는 군사적인 수직적 명령체계로 결합된 조직이라기보다는 여러 다양한 참여자들이 수평적으로 필요에 의해 결합된 하나의 네트워크이다. 그리고 이러한 네트워크의 결합 형태는 ad-hoc으로 그때그때 필요에 따라 그 결합구조가 지속적으로 변동한다. 네트워크상에서의 지휘통제체계는 누가 그 네트워크상에서 영향력을 보다 더 크게 행사하는 가에 따라 결정 되고 있다. 이러한 네트워크 형태의 조직구조는 오늘날의 해적, 조직범죄집단, 부족 및 무장세력등의 결합특성으로 이해되고 있으며 특히 이슬람 극단주의 테러집단을 포함한 테러 조직들의 결합특성으로 받아들여지고 있다(Sageman, 2004).

새로운 안보위협의 주체가 네트워크 형태로 결합된 것처럼 이들이 주도하는 새로운 안보위협 역시 네트워크상에서의 영향력확장이라는 네트워크형태의 전쟁으로 진화했다. 그리고 이 네트워크전쟁의 핵심은 오늘날 이슬람 극단주의 세력이 주도하고 있는 세계적 규모의 테러공격들이다. 이미 1996년에 미국의 저명한 안보 think-tank인 RAND는 “The Advent of Net War"라는 보고서에서 네트워크전쟁 형태의 안보패러다임을 지적했으며(Arquilla & Ronfeldt, 1996), 앞서 언급한 Reed(2008)의 5세대 전쟁개념역시도 알카에다등의 이슬람 극단주의 세력이 수행하

는 네트워크전쟁을 의미하며 이 극단주의 테러집단은 네트워크상에서의 영향력 확장을 통해 국가 행위자의 능력을 무력화시키는 전략을 채택하고 있다고 지적했다. 이러한 오늘날의 안보위협의 변화는 궁극적으로 윤민우(2010)가 지적했다시피 기존의 특정목표대상을 파괴하거나 무력화시키는 체스 형태의 전쟁에서 네트워크상에서의 공간의 점유를 통해 영향력을 행사하는 바둑 형태의 새로운 게임의 형태로 진화했음을 의미한다. 오늘날 테러공격의 특징인 system disruption과 권역장악을 통한 영향력 확산은 이러한 새로운 형태의 안보갈등 양상을 보여주는 증거들이다.

Ⅱ. 연구주제, 목적 및 방법

1. 연구주제 및 목적

새로운 안보위협의 주체가 네트워크형태로 결합되어있고 이들이 주도하는 안보위협 역시 네트워크전쟁의 양상을 띤다는 주장이 여러 차례 제기되어 왔음에도 이러한 실체에 대해 정확히 이해하고 전략적으로 가장 효과적인 방안을 찾으려는 노력은 미흡한 듯하다. 이는 9.11테러 이후 지난 10년간 계속되어온 대테러전쟁경험의 축적을 통해 최근 들어서야 그러한 주장의 중요성에 대해 인식하게 되었으며 여전히 이러한 네트워크개념에 대한 인식이 초기단계에 머물고 있다는 사실 때문인 것 같다. 그럼에도 불구하고, 새로운 위협으로서의 네트워크 개념을 제대로 파악하는 것은 이러한 새로운 안보위협에 대응하기위한 가장 핵심적이 사안일 것이다. 새로운 위협의 실체가 무엇이며 이 위협의 실체에 대응하기 위한 가장 효과적인 전략적 접근방안은 무엇인가에 대해 고민해 보는 것은 의미가 크다고 할 것이다. 이 논문은 이러한 목적을 가지고 있으며 이를 위해 여러 비국가 행위자들에 의한 안보위협 가운데 테러리즘(특히 그 중에서도 이슬람 극단주의 테러리즘)을 그 논의의 대상으로 선택했다. 보다 구체적으로 이 논문은 다음의 두 질문에 대한 해답을 구하고자 할 것이며 이를통해 테러리즘으로부터 오는 안보위협에 보다 효과적으로 대응 할 수 있는 전략적 방안을 제시하고자 한다.

가) 테러 네트워크를 어떻게 이해할 것인가? (What is your enemy?)
나) 테러 네트워크에 대한 바람직한 전략적 접근방안은 무엇인가? (How to destroy your enemy?)

2. 연구방법

이 연구는 기본적으로 문헌연구에 의한 meta분석의 방법을 사용했다. 우선 테러 네트워크와 관련된 이전의 여러 연구 보고 및 결과들을 중심으로 정리하였으며 이를위해 테러리즘 연구분야에서 가장 권위를 인정받고 있는 학술지인“Studies in Conflict & Terrorism”에 실린 논문들 가운데 테러리즘의 네트워크를 분석한 논문들을 선별하여 그 연구 결과들을 정리했다. 또한 여기에 덧붙여 미국의 저명한 연구기관인 RAND연구소의 보고서와 테러리즘 분야의 권위자로 인정받고 있는 Marc Sageman(2004)과 Bruce Berkowitz(2003), 그리고 Miller, Stone, 그리고 Mitchell(2002)의 저서 및 John P. Williams(2009)와의 인터뷰 내용을 논의 전개의 증거자료로 덧붙였다.

테러네트워크와 관련된 연구가 아직도 그다지 많지 않은 실정이어서 많은 증거자료들을 활용할 수 없음에도 불구하고 위에 열거한 다양하고 권위있는 정보의 원천들은 이 연구의 논의를 전개하는데 설득력 있는 근거를 제시할 수 있을 것이라고 기대된다.

Ⅲ. 이론적 틀

테러네트워크의 실체를 이해하기 위해서는 우선 네트워크란 무엇이며 이것의 실체는 무엇인가를 정확이 파악하는 일이다. 그리고 이러한 네트워크의 실체를 제대로 이해하기 위해서는 네트워크형태가 동일하지 않으며 서로 다른 종류들로 이루어져 있음을 이해해야 한다. 이를통해 테러네트워크는 어떠한 형태 또는 종류의 네트워크에 해당되는 지를 파악해야 하며 그리고 특정 유형의 또는 종류의 네트워크특

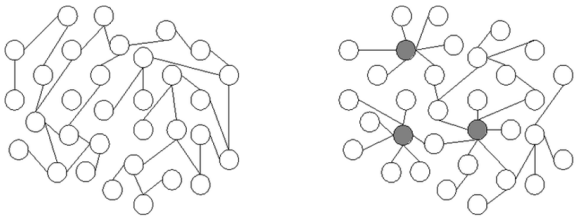
성을 정확히 이해하는 일이 우선되어야 한다.

1. 네트워크의 개념과 종류

네트워크는 어떤 행위자 또는 행위단위가 다른 행위자 또는 행위단위와 서로 연결되거나 관계를 맺는 연결 또는 관계망의 총합이라고 할 수 있다. 개념적으로는 이 행위자 또는 행위단위를 node 또는 vertex(복수로 vertices)라고 부르며 이 node 또는 vertex의 다른 node 또는 vertex와의 관계망을 edge 또는 degree라고 부른다. 보통 어떤 한 네트워크를 이루는 최소한의 node는 3개이며 하나의 네트워크는 3개 이상 n개의 node들로 형성된다. 또한 이 node들은 다른 node 또는 node들과 서로 1 또는 그 이상의 n개의 edge 또는 degree로 연결되거나 관계를 맺으면서 네트워크에 참여하게 된다. 한편, 네트워크상에서 예외적으로 많은 edge들을 가지고 있어 다수의 다른 node들과 관계를 맺고 있는 예외적인 node를 hub이라고 부르며 이 hub은 높은 값의 edge때문에 전체 네트워크상에서 다른 node들 보다 예외적으로 큰 영향력을 전체 네트워크에 행사할 수 있다. 이는 이 hub이 많은 관계들이 지나치는 교통망의 교차점에 위치하여 예외적으로 큰 영향력을 네트워크상에서 행사할 수 있기 때문이다(Newman, Barabasi, & Watts, 2006; Wasserman & Faust, 1994).

네트워크의 종류에는 무작위(Random)네트워크와 Scale-free네트워크등이 있다. 다음의 그림 1. 은 이 두 종류의 네트워크가 어떻게 서로 다르게 이루어져있는 지를 보여준다. 아래의 그림에서 동그라미는 각각의 node를 나타내며 이 동그라미를 연결하는 직선은 edge를 의미한다. 그리고 동그라미 가운데 회색으로 색칠된 부분은 네트워크상에서의 hub을 나타낸다(Barabasi, 2003; Bollobas, 2001).

〈그림 1.〉 네트워크의 모습



(a) Random network (b) Scale-free network

(출처 : Barabasi, 2003; Bollobas, 2001)

Random네트워크는 Random Graph라고도 불리며 위의 그림에서 보듯 node들 간의 어떤 무작위(random) 접촉과정에 의해 만들어 지는 그래프를 말한다. 따라서 각각의 node가 edge를 통해 이 네트워크에 연결될 때 어떤 특정한 패턴을 띠지 않으며 그래프 상에서 무작위의 확률분포(probability distribution)를 나타낸다. 이 때문에 위의 그림에서 보듯 네트워크의 모양이 어떤 특정한 모습이나 패턴을 띄지 않게된다(Porekar, 2002).

한편, Scale-free네트워크의 경우는 power law의 법칙에 따라 형성되기 때문에 power law분포라고도 불린다. 이 power law법칙은 관계 분포(degree distribution)가 power law를 따르는 네트워크를 의미하는데 이는 관계의 값이 증가할수록 그러한 높은 관계의 값을 가진 node의 수는 감소하게 되며 반대로 관계의 값이 감소할수록 그러한 작은 관계 값을 가지는 node의 수는 증가하게 되는 역방향으로 관계 분포가 형성된다는 것을 의미한다. 이러한 분포가 형성되는 것은 각각의 node가 다른 node와 연결되는 것을 통해 네트워크에 참여하게 될 때 선호도가 있는 애착(preferential attachment)의 체계(mechanism)로 네트워크가 만들어지기 때문이다. 따라서 이러한 네트워크의 경우에는 위의 그림에서 보듯 네트워크상에서 보다 선호되는 node에 더 많은 수의 다른 node들과의 관계가 형성되어 특정한 패턴을 나타내는 방식으로 네트워크가 이루어지는 모양을 나타낸다. 따라서 이러한 관계망의 중심에는 높은 관계 값을 가진 node인 hub이 형성되게 된다(Barabasi, 2003).

이 두 개의 서로 다른 네트워크의 형태 가운데 이 연구에서는 테러네트워크가

Scale-free네트워크의 형태로 이루어져 있다고 가정하기 때문에 이 scale-free 네트워크에 관해 다음 장에서 보다 자세하게 논의하고자 한다.

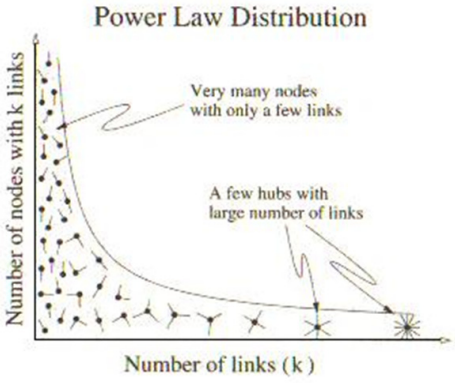
2. Scale-free네트워크

Scale-free네트워크는 네트워크상에서 하나의 node가 다른 node들과 k connection(edge 또는 degree)들을 가진 node들의 fraction P(k)는 k의 값이 증가하면 다음의 식에 가까워지게 된다는 법칙을 따른다(Barabasi, 2003).

$$P(k) \sim k^{-\gamma}$$

위 식에서 ϒ은 때때로 범위를 벗어나기는 하지만 일반적으로 범위가 2<ϒ<3의 값을 가지는 상수이다. Scale-free네트워크는 이러한 수학적 공식을 따르기 때문에 node의 관계값과 특정 관계값 k를 가진 node의 수와의 관계를 나타내는 그래프가 power law분포를 보여주며 다음과 같이 그려지게 된다(Barabasi, 2003).

〈그림 2.〉 Power Law Distribution

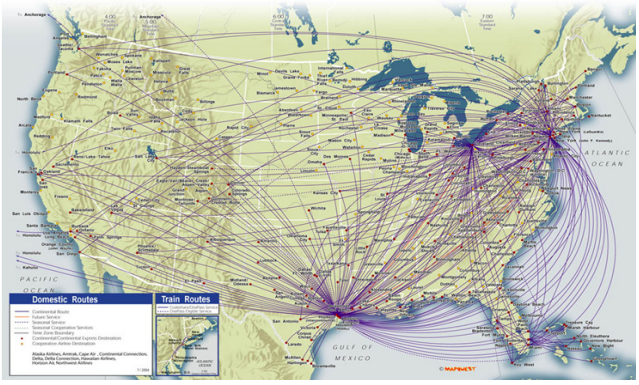


(출처 : Barabasi, 2003)

위의 그림 2에서 보이듯 scale-free네트워크에서는 작은 관계 값 k(edge, degree, 또는 link)를 가진 다수의 node 또는 vertex와 큰 관계 값을 가진 소수의 node로 이루어지며 이의 관계는 k값이 증가할수록 node의 수는 위 그래프의 우 하향 곡선을 따라 P(k)에 가까운 형태로 급격히 감소하다가 일정 분기점을 지나게 되면 완만한 형태로 지속적으로 감소하는 분포를 나타내게 된다. 이 때 대체로 이 분기점을 지나면서 기울기가 완만하게 감소하는 영역에 주로 네트워크상에서 차별적으로 큰 영향력을 행사하는 hub들이 분포하게 된다.

우리가 인식하고 있지는 못하지만 사실상 이 Scale-free네트워크는 우리의 일상생활에서 흔하게 발견된다. 다음의 그림 3.은 미국의 한 항공사인 콘티넨탈 항공사의 미국 내 항공노선 망을 나타낸 지도이다.

〈그림 3.〉 콘티넨탈 항공사 항공노선도(Continental Airlines Air Route)

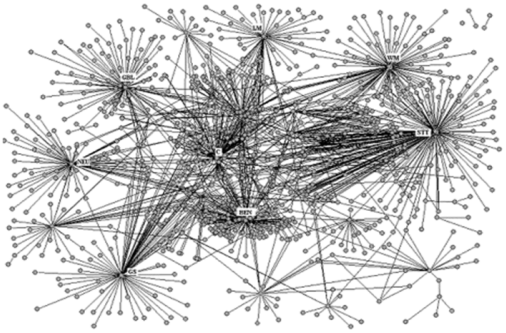


(출처 : 컨티넨탈항공사 공식 웹페이지, 2010)

위의 그림에서 보듯 이 항공사의 항공운항망은 scale-free네트워크의 구조를 띠는데 동그라미로 표시된 많은 수의 개별 도시들인 node들은 하나 또는 소수의 선(link 또는 edge)으로 이 네트워크에 결합되어 있는데 비해 많은 선들이 집중 된 3개의 hub 들이 나타난다. 참고로 이 3개의 hub 들은 각각 휴스턴, 시카고, 뉴욕이다.

또한 다음의 그림 4.는 현실에서 더욱 복잡하게 형성된 scale-free 네트워크의 한 사례를 보여준다.

〈그림 4.〉 2001년 뉴욕 주식 시장에서 거래 된 주식의 소유주들의 관계 그래프 (The graph of ownership for stocks traded in 2001 on the New York Stock Exchange)



(출처 : Caldarelli, 2004)

위의 그림은 전형적인 scale-free네트워크의 구조를 보여준다. 이 그림에서는 3개 정도의 핵심 hub들과 이와 연결된 5-7 정도의 중간 수준의 hub들로 네트워크가 이루어져 있음을 알 수 있으며 오른쪽 윗부분에 보이는 5개 정도의 node들은 이 전체 네트워크에 결합되어 있지 않고 고립되어 있음을 알 수 있다. 한편 위의 그림에서 보듯 이러한 형태의 scale-free네트워크를 형성하는 실제 사례들로는 인터넷에서의 twitter나 facebook등을 통한 연결망 World Wide Web 상에서의 웹 브라우저들 간의 연결망등을 들 수 있으며 학자들 간의 서로의 연구 업적을 참조하거나 인용하는 관계망, 실제 사회생활에서 친구를간의 관계가 형성되어 있는 친구관계도, 전기나 수도등을 공급하는 공급 시스템망, 에이즈나 성병등이 확산되는 확산 경로망, 영화배우들간에 서로가 함께 같은 영화에 출연을 결정하게 되는 영화배우들간의 협업관계등 여러 다양한 종류의 실제 사례들에서 scale-free네트워크 형태의 관계망이 발견된다(Barabasi, 2003; Newman, Barabasi, & Watts, 2006; Wasserman & Faust, 1994).

Scale-free네트워크는 power law분포를 따른다는 그 특성 때문에 뚜렷한 강점과 약점을 동시에 가진다. 우선 강점으로는 fault tolerant behavior라는 특징을 가지고 있는데 이는 무작위(random)공격이나 에러에 대한 저항성(robustness)이 크다는 의미이다. 많은 수의 작은 값의 degree를 가진 node와 소수의 큰 값의 degree를 가진

hub이 공존하므로 확률적으로 무작위 공격이나 에러가 발생할 경우에는 이 소수의 hub이 파괴될 가능성은 낮으므로 이 hub이 파괴되지 않는 한 네트워크상에서의 연결성(connectedness)이 생존할 가능성은 크며 따라서 네트워크 자체의 생존성은 커지게 된다. 이러한 성질 때문에 scale-free네트워크는 네트워크의 95%정도가 파괴되어도 hub이 생존해 있다면 네트워크가 생존할 수 있으며 시간이 지남에 따라 손쉽게 원래의 네트워크 규모로 복구될 수 있다. 이러한 강점 때문에 전기나 수도 공급망 또는 정보통신망등은 자연재해등의 무작위 파괴에서 생존성을 높이기 위해 인위적으로 이러한 형태의 네트워크망을 구성한다(Barabasi, 2003; Newman, Barabasi, & Watts, 2006; Wasserman & Faust, 1994).

반면 이 scale-free네트워크에는 그 자신의 특성 때문에 아킬레스의 뒤꿈치로 불리는 약점이 동시에 존재한다. 소수의 hub의 영향력이 상대적으로 크기 때문에 이 소수의 주요 hub에 대한 선택적 공격에는 취약하다. 소수의 hub의 파괴로 인해 네트워크 전체가 파괴되어 많은 수의 고립된 node들의 집합으로 변할 수 있으며 이 경우 5%정도의 주요한 hub의 선택적 파괴에도 전체 네트워크가 무력화되는 결과를 초래하게 된다. 이 경우 네트워크 전체의 본래의 성격은 잃어버리게 되며 고립된 node들은 주요한 능력을 잃거나 의미 있는 역할을 잃어버리게 되는 무능력한 고립된 개체들로 남게 된다(Barabasi, 2003; Newman, Barabasi, & Watts, 2006; Wasserman & Faust, 1994).

Ⅳ. 테러네트워크의 이해: What is your enemy?

오늘날의 테러집단들, 특히 그 중에서도 알카에다 혹은 탈레반류의 이슬람 극단주의 테러집단들이 네트워크형태로 진화했다는 사실은 많은 전문가들에 의해 지적되어 왔다(Berkowitz, 2003; Sageman, 2004; Williams, 2009). 하지만 이 테러네트워크집단들이 어떠한 종류의 네트워크로 이루어져 있는지에 대한 구체적인 진단은 아직까지 충분히 이루어지지 않은 것 같다. 그리고 이러한 부족한 이해는 테러네트워크에 대한 대테러대응이 테러리스트 개인에 대한 무작위 공격의 성격을 띰으로서

많은 수의 테러리스트를 제거했음에도 불구하고 이슬람 극단주의 테러네트워크의 작동 자체를 무력화시키는 데는 실패하게 되는 결과로 이어졌다(Williams, 2009). 이러한 맥락에서 여기서는 이슬람 극단주의 테러집단이 네트워크로 진화했을 뿐만 아니라 이 네트워크가 구체적으로 scale-free네트워크의 형태를 띠고 있다는 사실을 보여주고자 한다. 또한 이러한 입증을 통해서 이러한 형태의 네트워크가 무작위 공격에는 강한 저항성을 가지는 반면 소수의 hub에 대한 선택적 공격에는 취약한 특성을 드러냄으로 선택적 공격 전략을 대테러 대응의 기본전략으로 삼아야 한다는 사실을 제시하고자 한다. 테러 네트워크에서 node는 테러리스트 각 개인을 말하며, edge 또는 link는 이 테러리스트 개인들 간의 연결, 관계, 또는 결합을 나타내며, 여기에서 hub은 오사마 빈 라덴이나 아이만 알 자와히리, 물라 오마르, 안와르 알 왈리키등의 주요한 영향력 행사자이자 테러집단의 리더, 또는 중간 간부등을 의미한다.

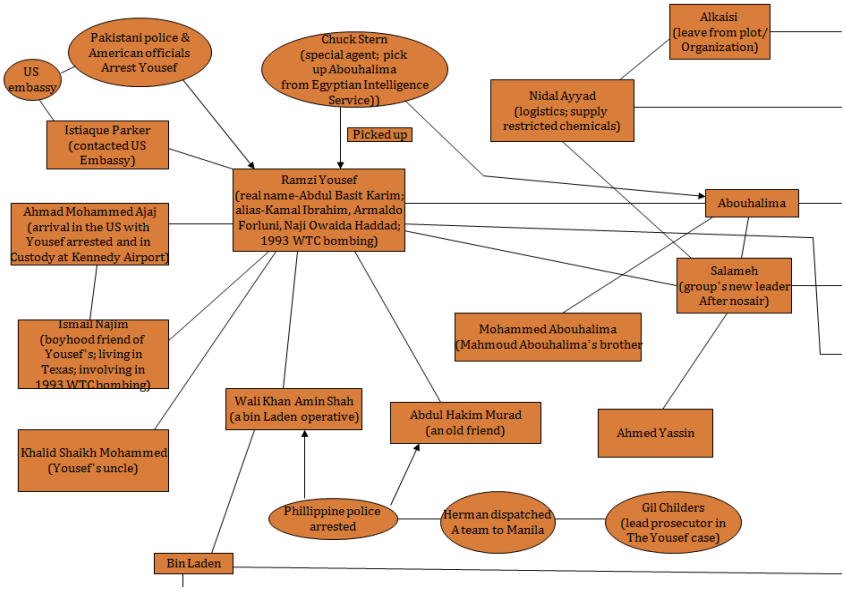
테러집단이 scale-free네트워크 구조를 형성하게 되는 것은 그들 나름대로의 전략적 이유가 있다. 우선 군사적 공세나 법집행기관에 의한 체포등 외부의 공격이나 내부 배신자에 의한 조직와해와 같은 내부적 에러로부터 테러집단 전체의 생존성을 강화할 필연적 이유가 존재한다. 이 때문에 이러한 조직요구를 충족하기 위해서는 예상되는 무작위 공격에 대응한 생존성과 영속성을 높이기 위해 scale-free네트워크 형태로 디자인 할 필요성이 있다. 또한, random네트워크와는 달리 scale-free네트워크는 hub에게 네트워크 전체를 지휘통제하고 네트워크 전체를 이 소수의 hub이 의도하는 방향으로 작동하도록 하게하는 능력을 허락한다. 반면에 random네트워크의 경우에는 hub자체가 존재하지 않으며 각각의 node가 네트워크상에서 거의 비슷한 정도의 영향력을 행사함으로 어떤 특정한 node가 전체 네트워크를 장악하고 지휘통제할 가능성이 없다. 때문에 전략적인 입장에서 테러의 지휘부는 필연적으로 scale-free네트워크를 선호할 가능성이 크다. 마지막으로, 새로이 테러네트워크에 결합하고자 하는 새로운 node의 경우는 (테러리스트 지원자 또는 희망자) 보다 잘 알려지고 유명한 hub에 접촉하고자 시도할 것이다. 이는 이 새로운 테러리스트 후보자의 네트워크에 대한 진입이 무작위로 이루어지지 않으며 보다 유명하거나 영향력 있는 네트워크상의 hub에게로 선택적으로 몰릴 가능성이 크다는 것을 암시한다. 이

러한 여러 가지 이유로 테러네트워크는 scale-free네트워크로 형성될 가능성이 크며 다음에 보여 줄 몇 가지 선택된 사례들은 이러한 형태의 네트워크구성을 입증하고 있다(Sageman, 2004; Williams, 2009).

1. 9.11 테러네트워크 사례

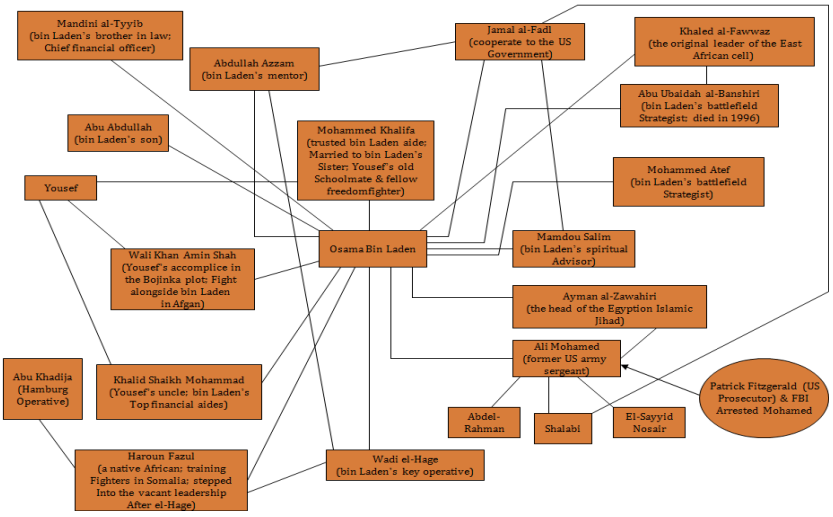
먼저 9.11테러공격과 관련된 알카에다 조직의 사례를 분석해 보면 이 공격에 참여한 주요 행위자들이 scale-free네트워크의 형태로 서로 결합되어 있었다는 사실을 발견할 수 있다. Miller, Stone, 그리고 Mitchell(2002)이 9.11관련 테러 사건의 자세한 내용을 기록한 “The Cell"의 내용을 분석하여 관련된 주요 행위자들간의 관계를 정리한 결과 다음과 같은 관계도를 도출할 수 있었다.

〈그림 5.〉 Ramzi Yousef를 중심으로 한 네트워크 결합도



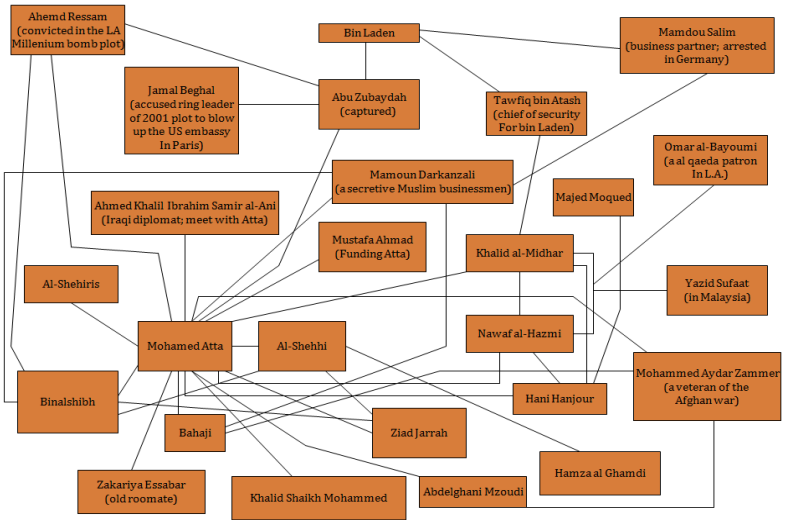
(출처 : 윤민우, 2010)

〈그림 6.〉 Osama bin Laden을 중심으로 한 네트워크 결합도



(출처 : 윤민우, 2010)

〈그림 7.〉 Mohamed Atta를 중심으로 한 네트워크 결합도



(출처 : 윤민우, 2010)

그림 5. 6. 7.은 “The Cell"에 등장하는 주요 행위자들의 관계를 그림으로 나타낸 것이다. 여기에서 네모모양으로 나타낸 행위자는 테러리스트를 의미하며 동그라미 모양으로 나타낸 행위자는 FBI 수사관등의 법 집행 공무원이나 CIA 요원 등의 대테러 요원등을 나타낸다. 그림 5.는 9.11 테러 이전 1993년에 있었던 1차 세계무역센터 폭탄테러의 주도자이었던 람지 유수프(Ramzi Yousef)를 중심으로 한 결합 관계의 그림이며, 그림 6.은 9.11 테러를 주도했던 오사마 빈 라덴을 중심으로 한 주요 알카에다 행위자들의 결합관계이며, 마지막으로 그림 7.은 9.11 공격을 현장에서 직접 수행했던 테러 공격조의 현장 지휘관이었던 모하마드 아타를 중심으로한 테러 행위 참여자들의 관계망이다. 위의 그림들에서 공통적으로 알 수 있는 것처럼 이 1993년 1차 폭탄테러 및 2001년 9.11테러에 참여하였던 알 카에다 참여자들의 네트워크는 hub이라고 볼 수 있는 람지 유세프, 오사마 빈 라덴, 모하마드 아타등에게 집중적으로 결합되어 있는 scale-free형태의 네트워크를 띠고 있음을 발견할 수 있다.

2. 2002년 발리 폭탄테러 사례

〈그림 8.〉 2002 발리 폭탄테러 네트워크

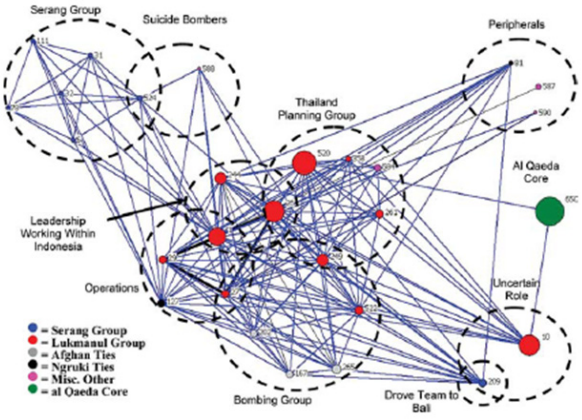


Figure 4. 2002 Bali bombing network.

(출처 : Magouirk, Atran, & Sageman, 2008)

2002년 인도네시아 발리 폭탄테러는 일반적으로 제마 이슬라미야라는 테러 조직이 감행한 것으로 알려져 있지만 사실상 여기에 참여한 행위자들의 결합관계를 세밀하게 분석해보면 해당 테러조직의 직접적인 의사결정과 집행의 결과가 아니라 여러 행위자 개인 및 그룹들이 scale-free네트워크 형태로 결합되었으며 이 네트워크상에서의 일부 행위자가 이러한 네트워크망에서의 그들의 역량과 인프라를 활용하여 테러공격을 감행한 사실을 파악할 수 있다(Magouirk, Atran, & Sageman, 2008).

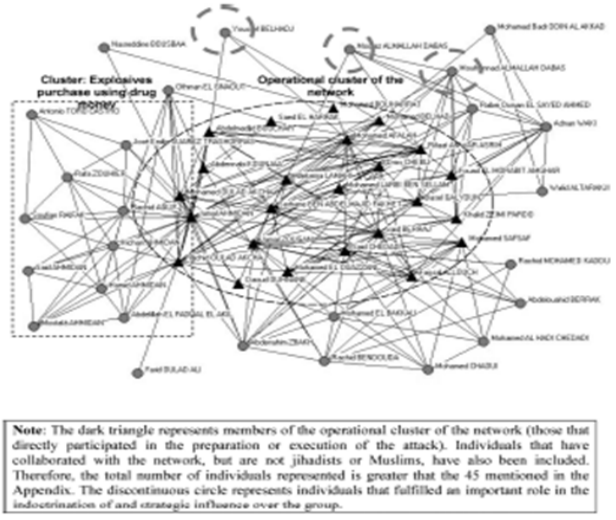
그림 8. 은 그러한 scale-free네트워크의 특성을 보여주고 있다. 이 발리테러는 제마 이슬라미야 지도부의 지휘통제없이 Lukmanul Hakiem Circle(Lukmanul Group)이라는 주도 세력에 의해 실행되었다. 위의 그림을 보면 이들 Lukmanul 써클에 결합된 행위자들이 네트워크상에서 주요한 hub의 기능을 담당하고 있음을 알 수 있으며 이 때문에 이들이 이 테러 네트워크의 관계망의 정보 흐름을 통제함으로서 이 네트워크를 발리 테러공격에 효과적으로 활용할 수 있었다는 사실을 발견할 수 있다. 또한 이 Lukmanul써클 중 에서도 Hambali라는 이름의 행위자가 가장 주도적인 역할을 한 것을 알 수 있다. 이 Hambali는 위 그림의 Thailand Planning Group 내에 있는 동그라미로 표시되어 있으며 520으로 나타나는 수치는 그의 네트워크상에서의 link, 즉 관계망의 크기를 나타낸다. 위의 네트워크를 살펴볼 때 이 Hambali가 발리 테러 네트워크의 중심에 있으며 상당히 큰 link값을 가지고 있음을 알 수 있다. 사실 상 Magouirk et al.의 연구결과에 따르면 발리테러는 이 Hambali의 사회네트워크의 주도적 활동과 핵심 알카에다(Al Qaeda Core)의 장기간에 걸친 지원의 결실이었다(Magouirk, Atran, & Sageman, 2008).

3. 2004년 마드리드 폭탄테러 사례

마드리드 폭탄테러사건 역시 네트워크형태로 서로 연결된 테러참여자들에 의해 저질러진 테러공격이었다. 알카에다가 직접 연계되지는 않았으며 배후조종세력도 존재하지 않았다. 이 사건은 순수하게 자발적으로 사건을 주도한 이슬람 극단주의 성향의 테러범과 이슬람 극단주의와는 전혀 상관이 없음에도 돈을 목적으로 이들에

게 폭발물을 판매함으로서 사건과정에 참여한 스페인 광부들의 인적 네트워크로 구성된 행위자에 의해 저질러진 결과물이었다(Jordan, Manas, & Horsburgh, 2008).

〈그림 9.〉 마드리드 사건을 주도한 Global Jihad Network



Note: The dark triangle represents members of the operational cluster of the network (those that directly participated in the preparation or execution of the attack). Individuals that have collaborated with the network, but are not jihadists or Muslims, have also been included. Therefore, the total number of individuals represented is greater that the 45 mentioned in the Appendix. The discontinuous circle represents individuals that fulfilled an important role in the indoctrination of and strategic influence over the group.

출처 : Jordan, Manas, & Horsburgh, 2008

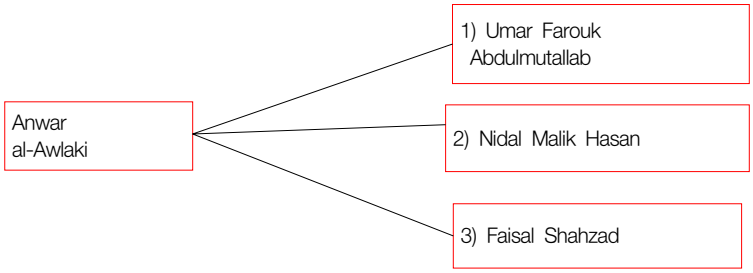
위 그림 9.에서 짙은 삼각형으로 표시된 node는 테러공격에 직접 참여하여 공격을 준비하거나 실제로 공격을 실행한 테러범들을 나타낸다. 반면, 옅은 색 동그라미로 표시된 행위자들은 이슬람 극단주의와는 관련이 없지만 돈을 목적으로 폭탄을 제공하는등의 여타의 동기로 간접적으로 테러공격에 참여한 행위자들이다. 위 점선의 네모 칸 안에 들어가 있는 node들은 스페인 광부들로서 마약을 사기위한 돈이 필요해 폭발물을 몰래 빼돌려 이슬람 극단주의자들에게 판매한 node들의 무리이다. 그리고 점선 동그라미로 표시된 부분은 테러공격주체들의 네트워크를 나타낸다. 이 그림에는 나오지 않았지만 Jordan, Manas, 그리고 Horsburgh(2008)의 연구는 관계도의 점수를 매겼는데 Jamal Ahmidan과 Serhane Ben Abdelmajid Fakhet이 함께 52.000의 가장 높은 관계도 점수를 획득했다. 이는 위의 그림에서 확인할 수 있는바 네트워크상에서 중심에 위치하며 많은 실선(관계 또는 link를 나타내는)들이 이 두

행위자에게 집중되어 있어 이들이 hub의 역할을 하고 있었음을 알 수 있다. 실제로 이 둘은 마드리드 테러 작전을 주도했던 리더였다. 이처럼 마드리드 테러의 네트워크도 몇몇의 hub에 집중되어 전체 네트워크가 구성된 scale-free네트워크의 모습을 보여주고 있다 (Jordan, Manas, & Horsburgh, 2008).

4. Anwar al-Maliki 사례

Anwar al-Maliki의 사례도 아직 구체적으로 밝힐 수는 없지만 그를 둘러싼 scale-free네트워크의 존재를 어느 정도나마 추리할 수 있게 만든다. Al-Maliki 는 이슬람 극단주의 이론가이자 전략가로 인터넷상에서의 빈 라덴이라 불릴만큼 많은 이슬람 극단주의자들에게 전략적, 정신적 영향력이 큰 인물이다. 이 al-Maliki는 적어도 3차례의 테러 사건에서 중요한 가이드이자 배후에서 영향력을 행사한 인물로 밝혀졌다.

〈그림 10.〉 Anwar al-Maliki 와 테러범들 간의 관계그림



(출처 : 윤민우, 2010)

위 그림 10.에서 Umar Farouk Abdulmutallab은 속옷폭탄테러범(the underpants bomber)으로 알려진 테러범이다. Abdulmutallab은 2009년 12월 25일 암스테르담에서 디트로이트로 향하던 미국 국적의 비행기에서 폭탄테러를 시도하다가 폭탄이 폭발하지 않는 바람에 체포되었다. 그는 PETN을 그의 속옷 안에 숨겨 기내에 탑승함으로서 속옷폭탄테러범이라는 별명을 얻게 되었다. Nidal Malik Hasan은 미군 소령으로 2009년 11월 5일 텍사스주 포트후드의 미군부대 내에서 자신의 권총으로

다수의 인명을 살해한 뒤 체포된 자이다. 마지막으로 Faisal Shahzad는 2010년 5월 1일 뉴욕시 맨해튼에 있는 타임스퀘어에서 차량을 이용한 폭탄테러를 시도했다가 체포된 자이다. 이들 모두는 테러 공격을 결심하게 된 주요한 동기가 인터넷을 통한 al-Awlaki와 그의 종교적, 전략적 가르침에 대한 접촉 때문이었으며 이러한 al-Awlaki의 종교적 메시지와 전략적 가이드가 그들의 테러감행에 주요한 영향력을 미쳤다고 진술했다. 이러한 사실을 바탕으로 추론해 볼 때 인터넷 상에서의 여러 이슬람 극단주의 테러리스트들과 극단주의에 대한 호기심을 갖고 이를 희망하는 지원자들의 네트워크상에서 al-Maliki가 주요한 hub 가운데 하나이며 이러한 네트워크상에서의 지위를 활용해 그의 영향력을 행사하고 있음을 알 수 있다. 따라서 이 al-Maliki를 중심으로 한 scale-free네트워크의 형성을 추론해 볼 수 있을 것이다.

Ⅴ. 전략적 접근방안 : How to destroy your enemy?

테러네트워크가 scale-free네트워크의 형태를 띠고 있다면 이러한 사실은 대테러 정책의 전략적 접근방안에 중요한 하나의 힌트를 준다. 이는 앞서 언급한 scale-free 네트워크의 강점과 약점에서 논의된 사항인데 궁극적으로 네트워크상에서 hub의 위치에 있는 주요한 소수의 행위자들을 선택적으로 파괴하고자하는 전략적 접근을 채택할 것을 알려주고 있다. 이러한 선택적 접근을 통한다면 5%정도의 hub의 파괴만으로 전체네트워크를 무력화 시킬 수 있을지도 모른다.

따라서, 선택적파괴라는 이러한 전략적 기본패러다임을 바탕으로 다음의 4가지 보다 구체적인 전략적 접근방안을 생각해 볼 수 있을 것이다.

1. 전략적 접근 방안 1: 데이터베이스 구축 및 분석

테러네트워크의 특성파악을 위해 테러네트워크에 참여하는 테러리스트 개인들에 관한 데이터베이스구축과 이 구축된 데이터를 바탕으로한 분석이 가장 먼저 고려되어야 할 것이다. 테러네트워크를 파악하여 이것이 scale-free네트워크에 해당하는지

를 살펴본 후 이 네트워크의 hub을 파악하고 이러한 파악된 hub을 선택적으로 공격함으로서 전체네트워크를 무력화시키는데 대테러 또는 법집행 역량을 집중할 필요가 있다. 그리고 이러한 전략채택의 전제조건으로 데이터베이스의 구축이 반드시 실행되어야 하며 이렇게 마련된 데이터를 사용하여 테러네트워크 특성을 밝히는 실질적 분석이 따라야 할 것이다. 데이터베이스는 open-source를 활용하는 방식으로 효과적으로 구축될 수 있다. 그리고 이러한 공개자료를 통해 구축된 데이터베이스에 필요하다면 정부기관이 획득한 첩보를 덧붙임으로서 신뢰도와 타당성을 높일 수 있다. 이러한 데이터베이스 구축시 유념해야할 점은 인적네트워크 또는 결합관계에 관한 정보가 반드시 들어가야 한다는 점이다. 또한 이렇게 구축된 데이터베이스를 제대로 활용하기 위해서는 데이터마이닝(또는 보다 구체적으로 text mining)이나 social network analysis등의 고급분석기법을 사용하여 테러네트워크의 관계도를 작성하고 이러한 결합도(link)를 수치화해서 나타내어야 할 것이다. 이렇게 함으로서 테러네트워크의 전체특성과 취약점을 파악할 수 있을 것이다. 한편 데이터베이스구축과 분석을 위해서는 이러한 작업에 사회과학자들의 참여가 반드시 있어야 할 것이다.

2. 전략적 접근방안 2: 테러내부네트워크의 탐지 및 감시

이 방안은 보다 전술적인 방안을 제시한다. 파악된 테러네트워크 전체에 관한 개략적 그림이 그려지고 그 구조적 특성이 파악되면 그 중에서 누가 또는 어떤 행위자들의 서클이 실제 테러공격을 감행하고자 하는 가를 사전에 탐지하거나 실제 테러공격을 주도했는지를 사후에 수사할 필요성이 생긴다. 이처럼 구체적 테러공격에 참여하거나 기도하는 행위자의 무리를 테러내부네트워크로 부를 수 있으며 이 테러내부네트워크는 전체테러네트워크의 일부에 해당한다. 테러내부네트워크의 탐지와 감시목적을 위한 전략적 접근은 두 가지 단계로 이루어지는데 첫 번째 단계는 전체네트워크상에서 의심가는 테러내부네트워크를 탐지하는 것이며 다음은 이 파악된 테러내부네트워크를 집중감시하는 단계이다.

먼저 구체적인 테러공격을 기도하거나 실행한 테러내부네트워크의 탐지를 위해

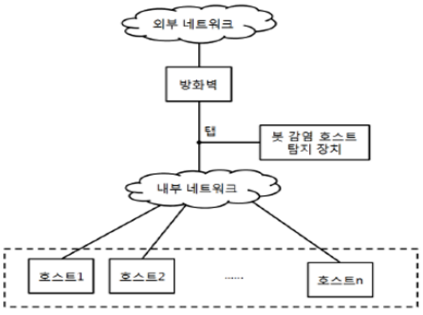
서는 앞서 논의한 전략적 접근방안1을 통한 탐지방법에 더하여 인간정보기법(HUMINT: Human Intelligence)을 통합적으로 적용해볼 수 있을 것이다. 하지만 여기에서 주의해야할 점은 이 인간정보를 전통적인의미로 해석하여 국가정보기관의 배타적 업무영역으로 이해해서는 안 될 것이며 국가정보기관이외에도 경찰과 다른 법집행기관, 여타 정부/공공기관 및 민간조직 및 민간 전문가등을 포함하는 통합적인 인간정보수집활동으로 받아들여야 할 것이다. 이는 테러분야에서 발생하는 정보패러다임의 변화 때문이다. 전통적인 개념의 정보활동은 정보기관의 배타적 영역이었다. 정보기관은 방첩활동을 통해 자국내 중대한 위협을 줄 수 있는 결정적 증거들을 확보하여 이를 법집행기관에 통보함으로서 법집행기관을 지원하고 법집행기관은 이 제공받은 결정적 증거를 사용하여 경비를 강화하거나 보안조치를 강화하거나 또는 주모자등을 체포하거나 제거함으로서 국가안보와 사회안전을 지켜낼 수 있었다. 하지만 테러의 경우는 이러한 결정적 증거에 해당하는 것들을 발견하기가 쉽지 않다는 데 그 딜레마가 있다. 대체로 테러에 관한 정보는 부정확하며 포괄적인 경우가 많다. 이와 함께 대부분의 테러관련첩보는 잠재적 테러리스트가 잠복해 있는 거주지역 단위에서 파악되는 중요하지 않아 보이는 여러 파편적 증거들의 총합일 경우가 많다. 이 경우 국가정보기관은 이 해당지역 단위에서 첩보 수집을 효과적으로 하기에는 인력과 비용의 한계 때문에 적합하지 않으며 오히려 이러한 형태의 탐문활동은 해당지역에 배정된 순찰경관이나 지역 주차단속공무원 또는 지역주민 등이 더 큰 역할을 할 수가 있다. 이러한 측면에서 전통적인 패러다임인 정보기관과 법집행기관과의 엄격한 역할분담에서 탈피하여 정보기관과 법집행기관과의 유기적 통합에 의한 적절한 역할분담과 계속적인 상호피드백을 통한 기관간의 긴밀한 협력이 필요하다고 할 수 있다. 한편 이러한 협력관계에서 국가정보기관의 업무는 정보수집보다는 정보분석으로 무게중심을 옮길 필요가 있다. 전통적인 국가정보나 군사정보, 또는 산업정보와는 달리 테러정보는 국제범죄정보의 경우처럼 어떤 결정적이고 핵심적인 정보가 특별한 정보출처로부터 완제품 형태로 입수된다기 보다는 어떻게 보면 사소해 보일 수도 있는 여러 파편화된 정보들을 조합하여 하나의 큰 그림을 만들어 가는 작업이라고 할 수 있다. 때문에 정보수집활동을 공개정보데이터베이스 활용과 지역사회에서 임무를 수행하는 순찰경찰관이 지역주민들로부터 수집한 자

질구레한 정보들의 중요성이 커지고 있다. 때문에 전통적인 정보수집업무는 다양한 개인과 기관들과 협력을 강화하고 미국 CIA의 경우처럼 사회과학적 방법론을 이용한 정보분석업무에 보다 업무역량을 집중할 필요성이 있다. 테러내부네트워크의 탐지는 정보의 수집과 분석이 지속적으로 반복되는 사이클을 통해 탐지할 수 있을 것이다.

다음으로 일단 의심가는 테러내부네트워크가 파악된다면 이 의심가는 node군들을 네트워크상에서 감시할 필요가 있다. 이와 관련해서는 사이버 보안분야에서 어떤 PC가 봇넷에 감염되어 있는 지를 알아내는 봇(bot)탐지 방법을 응용하여 테러네트워크에서 실제공격을 감행하고자하는 hub 또는 이를 둘러싼 서클을 탐지 할 수 있다. 이러한 방안은 최석우, 손춘호, 김경수, 그리고 유재형(2010)이 KNOM Review에 발표한 블랙리스트 접근 트래픽 감시를 통한 봇탐지 방법이라는 논문에서 주장한 내용에서 힌트를 얻은 것이다.

이상징후 탐지는 2단계로 접근 할 수 있다. 우선 마련된 scale-free네트워크 그림에서 극단주의 성향을 띠며 긴밀하게 결합된 hub과 node들을 점선의 동그라미로 묶어 블랙리스트로 지정한다. 이러한 블랙리스트에 등록된 서클은 테러내부네트워크로 지정하고 이 내부네트워크밖에 존재하는 모든 hub과 node들의 결합을 외부네트워크로 지정한다. 그리고 이러한 내부네트워크와 외부네트워크 사이의 communication traffic을 집중적으로 감시하며 이상 징후를 발견하는데 노력을 집중한다.

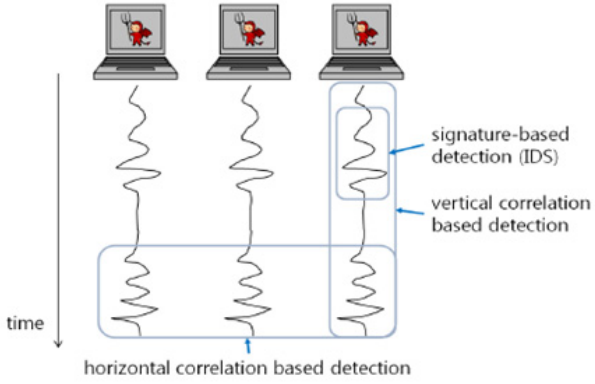
〈그림 11.〉 테러네트워크상의 이상징후 탐지를 위한 집중감시 위치



(출처 : 최석우, 손춘호, 김경수, 유재형, 2010)

위의 그림 11.은 최석우 등의 논문에서 제시한 봇탐지장치 설치위치에 대한 그림을 빌려온 것이다. 이 논문에서는 그림상의 내부네트워크를 블랙리스트에 오른 테러내부네트워크로 호스트를 각각의 테러 행위자로 외부네트워크를 주요 감시대상 테러내부네트워크와 연결되면서 이들의 외부에 위치하는 scale-free 네트워크상에서의 모든 hub과 node들을 의미하는 것으로 재해석 할 수 있다. 그리고 위의 봇감염 호스트 탐지장치의 설치위치를 테러관련 communication traffic을 탐지하는 개입포인트로 설정할 수 있다. 이 경우 일차적으로 내부와 외부 네트워크 사이의 communication traffic이상징후가 발견 되는 지를 파악하기위해 이 둘 사이의 트래픽을 감시하는 방법을 생각해 볼 수 있다. 따라서 감시의 개입 포인트는 이 둘 사이의 경계부분이 될 것이다.

〈그림 12.〉 네트워크상에서의 테러공격 감행행위 등의 이상징후 탐지방법



(출처 : 최석우, 손춘호, 김경수, 유재형, 2010)

위의 그림 12.에서 보이는 것처럼 이상징후의 탐지는 시간적 흐름에 따라 하나의 내부네트워크와 다른 외부네트워크와의 트래픽을 수직적으로 분석할 수도 있으며 아니면 수평적으로 동일한 시간대에 전체네트워크상에서의 여러 다른 네트워크 서클들과 트래픽 패턴을 비교해 봄으로서 이상징후를 발견할 수 도 있다. 위의 그림 역시 최석우등의 논문에서 빌려온 것으로 감염된 PC는 각각의 테러 내부네트워크들로 실선은 communication traffic을 나타내며 수직으로 길게 그려진 네모는 동일

한 대상에 대한 시간에 따른 트래픽패턴 비교를 수평으로 그려진 네모는 서로 다른 대상에 대한 동일한 시간대의 패턴 비교를 각각 나타낸다.

한편 봇넷 탐지에 있어서 communication traffic은 인터넷상에서는 전기 시그널을 의미하지만 테러네트워크상에서의 communication traffic은 행위자들 (nodes)간의 이메일, 인터넷접속 및 트위터나 facebook등의 social network 상에서의 결합을 포함하여 전화통화, 우편, 물리적 접촉, 또는 금융거래나 돈의 이동등 다양한 방식의 트래픽을 포함할 수 있다. 또한 봇넷 탐지에서 내부네트워크의 이상징후는 감염여부에 관한 이상행동을 의미하지만 테러내부네트워크에서의 이상징후는 행위자들의 일상적인 생활패턴이 갑작스럽게 바뀐다거나 의심가는 행위자들이 집중적으로 함께 시간을 보내거나 이슬람극단주의에 관한 강한 종교적성향을 보이거나 갑작스럽게 폭탄제조에 들어가는 화학물질등의 구매가 급증한다던가 하는 것들로 나타날 수 있다.

일단 1단계 감시에서 이상징후가 포착되면 2단계 감시로 넘어갈 수 있다. 이 경우 전체네트워크상에서 이상징후가 포착된 테러네트워크내부의 결합관계를 집중감시하며 특히 그 서클 내에서 hub의 기능을 하고 있는 행위자를 선택적으로 집중감시함으로서 테러공격기도에 관한 사전정보를 입수하거나 형사기소를 위한 법적 증거를 확보할 수 있을 것이다.

3. 전략적 접근방안 3: 선택적/차별적 처벌

Scale-free테러네트워크상에서 단순 node와 hub사이의 역할과 비중이 다르다는 것을 발견할 수 있다. 따라서 테러네트워크상에서의 위치와 기능에 따라 다르게 법적인 처벌을 적용하여야 하며 또한 이러한 네트워크상에서의 다른 비중과 역할을 법정에서 증거로 활용할 수 있을 것이다. 이 경우 단순 node는 보다 경미한 처벌을 hub은 보다 가중된 처벌을 고려해 볼 수 있다. 한편 이러한 제안이 기존에 시행되고 있는 단순가담자나 행동대원에 대한 경미한 처벌과 범죄/테러 지휘부나 행동대장에 대한 강력한 처벌로 이해해서는 안 될 것이다. 물론 그러한 차별적 처벌의 철학적 배경은 유사하다고 볼 수 있다고 하더라도 기존에 실행되던 방식은 특정조직내부에

서의 행위자의 직책이나 지위에 기초하여 처벌의 수위를 결정하고 있다. 이에는 특정조직의 존재여부를 염두에 두고 그 가담여부에 근거하여 판단을 내린다. 하지만 여기에서 제안하는 차별적 처벌은 이러한 조직에 근거한 지위나 직책과는 무관하다. 테러네트워크상에서 hub과 node들은 같은 조직에 속할 수도 있지만 전혀 다른 조직에 속할 수 도 있고 심지어 어떤 조직에도 속하지 않은 프리랜스로 활동할 수 도 있다. 따라서 hub과 node에 대한 판단은 네트워크상에서의 역할중요도에 따라 판단되어야 할 것이다. 때문에 기존의 관행과는 법철학적 바탕은 유사해 보이지만 그 실행되는 방식에서는 중요한 차이가 있다고 하겠다. 아울러 수사과정에서 테러행위자의 네트워크상에서의 역할을 파악하기 위한 노력이 이루어져야 할 것이다.

4. 전략적 접근방안 4: hub에 대한 선택적 공격을 통한 전일적(holistic) 접근

테러네트워크상에서 hub의 제거를 위해서는 이에 집중할 필요가 있으며 hub의 제거를 통한 전체네트워크의 무력화를 지향해야한다. 따라서 단순 node를 체포할 경우 이 node에게 hub 또는 hub과 보다 직접적으로 결합된 다른 node에 관한 정보를 법집행기관에 제공하는 대가로 죄를 사면하거나 감해주는 법적인 흥정을 시도해 볼 수 있다. 이를 통해 전체네트워크의 그림을 그려가는 작업과 그 네트워크상에서 중요한 역할과 기능을 하는 hub들을 파악하고 이들을 공격하는 작업을 통해 전체네트워크를 무력화 시키는 전일적(holistic)접근이 이루어져야 할 것이다. 여기에서 한 가지 주의할 점은 hub을 단순히 빈라덴이나 알-말리키, 그리고 유수프등의 상식적으로 받아들여지는 테러조직의 지휘부로 이해해서는 안 된다는 점이다. 물론 이들이 hub일 경우도 있지만 그렇지 않을 경우의 수도 존재한다. 네트워크상에서의 hub은 조직의 리더나 지휘부등의 직책이 아니라 node들과의 연결관계상에서 중요한 위치를 점유하는 실존적인 의미이다. 따라서 이 hub은 시간에 감에 따라 지속적으로 변동한다. 또한 이 hub은 네트워크상에서 단 하나만 존재하는 개념이 아니며 복수의 형태로 존재한다. 따라서 특정 hub의 제거는 전체네트워크에 영향을 미치겠지만 또 다른 관계망의 균형이 형성될 수 있다. 따라서 여러 중요한 hub들에 대한 전일적인 접근이 요구되며 hub들의 제거 이후 전체네트워크의 변화를 지속적으로 감시하

며 무력화시켜야하는 지속적인 작업으로 접근해야 한다.

Ⅵ. 맺음말

오늘날 테러조직은 네트워크형태로 진화했다. 그리고 이 테러네트워크는 무작위로 결합된 random네트워크가 아니라 선호도결합(preferential attachment)에 의해 이루어진 scale-free네트워크의 형태를 띤다. 때문에 대테러 전략은 이 scale-free네트워크의 독특한 특성에 기초해서 디자인되어야 하며 이를 위해서는 이러한 네트워크의 특성에 대한 이해가 선행되어야 한다.

이 논문은 scale-free형태인 테러네트워크가 hub에 대한 선택적 공격에 취약함에 착안하여 테러네트워크의 파괴나 무력화를 위해서는 우선 이 네트워크상에서 hub을 파악할 필요가 있으며 이 파악된 hub의 파괴에 대테러기관 또는 법집행기관의 역량을 집중할 필요가 있음을 제시하고 있다.

궁극적으로 이 논문은 테러네트워크에 대한 이해를 통해 대테러의 새로운 전략적 패러다임을 보여주고 있으며 구체적인 방안으로 4가지의 전략적 접근방안을 제시하면서 관계기관에 이러한 주제에 대한 보다 많은 관심과 노력을 촉구한다.

참고문헌

최석우, 손춘호, 김경수, 유재형. (2010). 블랙 리스트 접근 트래픽 감시를 통한 봇 탐지 방법. KNOM Review, vol. 13, no. 1.

Arquilla, John and Ronfeldt, David. (1996). The Advent of Netwar. Santa Monica, CA: RAND (National Defense Research Institute).

Barabasi, Albert-Laszlo. (2003). Scale-Free Networks. Scientific American, 288: 60-69.

Berkowitz, Bruce. (2003). The new face of war: how war will be fought in the 21st century. New York: The Free Press.

Bollobas, Bela. (2001). Random Graphs, (2nd ed.). Cambridge, UK: Cambridge University Press.

Caldarelli, Guido. (2004). The Structure of Biological and Social Systems. SIAM News, vol. 37, no. 3. Available at: http://www.mathaware.org/mam/04/essays/systemsstructure.html.

Continental Airlines Air Route. Available at: http://www.mslima.com/mfadt/thesis/2004/08/transportation-routes.html.

Fewer dragons, more snakes. (2010, November 13). The Economist, vol. 397, no. 8708: 27-30.

Jordan, Javier., Manas, Fernando M., and Horsburgh, Nicola. (2008). Strengths and weaknesses of grassroot jihadist networks: the Madrid bombings. Studies in Conflict & Terrorism, vol. 31, no. 1:17-39.

Magouirk, Justin., Atran, Scott., and Sageman, Marc. (2008). Connecting terrorist networks. Studies in Conflict & Terrorism, vol. 31, no. 1:1-16.

Miller, John., Stone, Michael., and Mitchell, Chris. (2002). The cell. New York: Hyperion.

Naim, Moises. (2005). The Illicit. New York: Anchor Books.

Newman, Mark., Barabasi, Albert-Laszlo., and Watts, Duncan J. (2006). The Structure and Dynamics of Networks. Princeton, NJ:Princeton University Press.

Porekar, Jan. (2002). Random Networks. Available at: http://www-f1.ijs.si/~rudi/sola/Random_Networks.pdf.

Reed, Donald J. (2008). Beyond the war on terror: into the fifth generation of war and conflict. Studies in Conflict & Terrorism, vol. 31, no. 8: 684-722.

Sageman, Marc. (2004). Understanding terror networks. Philadelphia, PA: University of Pennsylvania Press.

Shultz, Richard H. (2009). Insurgents, Terrorists, and Militias: The Warriors of Contemporary Combat. New York: Columbia University Press.

Toffler, Alvin. & Toffler, Heidi. (1993). War and anti-war: making sense of today's globalization. New York: Warner Books, Inc.

Wasserman, Stanley and Faust, Katherine. (1994). Social Network Analysis: Methods and Applications. Cambridge, UK: Cambridge University Press.

Williams, John P. (2009). 2009년 FDD 가 (Foundation of Defense of Democracies) 주최한 이스라엘에서의 대테러 교육과정에서 윤민우가 만나서 테러 네트워크와 이라크의 대테러 전쟁 양상에 관해 조언을 구함. John P. Williams 는 미국 대령을 이라크 전에 참전하였으며 이 해군사관학교 중동 이슬람 연구 센터의 Deputy Director를 역임한 대테러분야 전문가이다.

Yun, Minwoo. (2010). Insurgency warfare as an emerging new mode of warfare and the new enemy. The Korean Journal of Defense Analysis, vol. 22, no. 1: 111-125.

Understanding Terror Networks and Strategic Approaches: Cases of Taleban, Al Qaeda, and other Islamic Extrimists

Yun, Min-Woo

Today, the evolution of terrorist organizations generated a new type of terrorist network, which is scale-free network formed by preferential attachment rather than random attachment. Such emergence of scale-free terrorist network implies that counterterrorism policy makers need to understand the characteristics of scale-free network to develop effective counterterrorism policy. The current study responds to such necessity and suggests that terrorist networks, having characteristics of scale-free network, could be crack down by selectively attacking its hubs and thus disabling the functions of the entire scale-free network. This study provides four practical strategic considerations to policy makers and suggests that understanding the new type of terrorist network is critical to cope with evolving terrorism in the era of new counterterrorism strategic paradigm.

❖ Key words : Terror Network, Scale-free Network, Counterterrorism strategy, Social Network

투고일 : 2011. 02. 09 / 심사(수정)일 : 2011. 02. 28 / 게재확정일 : 2011. 03. 25