테러리스트의 인터넷 활용성 증대와 대응 과제

김응수

현대 테러리즘은 발생양상이 개별국가나 단체를 초월하여 초국가적 성격을 띠고 있다. 특히 9.11 테러 사태와 아프간· 이라크 전은 국가안보와 전쟁의 패러다임을 새롭게 변화시켰다. 테러리즘의 개념과 양상의 변화 추이와 더불어 테러리스트의 커뮤니케이션 수단 역시 시대적으로 많은 변화를 가져왔다. 카세트 테이프와 비디오 테이프 시대를 거쳐 오늘날 인터넷을 통하여 더욱 정교한 옵션을 선택할 수 있는 시대에 와있다. 작금, 과학기술의 발달과 함께 인터넷은 테러조직에게 신경조직으로써 활용성은 급격히 증대하고 있다. 테러조직들은 인터넷으로 의사소통을 하는 것은 물론 선전활동과 자금조달, 그리고 가상공간에 성전학습소를 설치하여 원격학습을 하는 등 다양하게 사용되고 있다. 그들은 인터넷을 통한 심리전으로 지지자들을 더욱 교화시키고 적을 혼란스럽게 하며 대중에게 공포감을 심어준다. 이러한 현상은 9.11 테러 이후로 급증하여 인터넷은 초국가적 테러리즘에 있어서 중요한 양상이 되었다. 그러나 테러리스트들이나 극단주의자들의 인터넷 활용성 증대에 비하여 정책결정자들은 그에 대한 인식과 대처방안이 상대적으로 현저히 낙후되어 있는 실정이다. 따라서 테러리스트들의 인터넷을 활용한 커뮤니케이션 실태를 정확히 인식하고 세계화의 흐름과 더불어 UN 등 국제기구들의 보다 적극적인 역할을 촉구한다. 또한 개별국가들은 사사로운 자국의 이해논리에 국한하기보다 국제법적 기초를 토대로 인류평화 유지 차원에서 대비책을 강구하도록 적극 노력하고 협조하는 자세가 필요하다.

주제어: 초국가적 테러리즘, 세계화, 신경조직, 국제 공조, 개별국가의 노력

I. 들어가는 말

전 세계를 사상 초유의 충격으로 몰아넣은 2001년 9월 11일 테러사건과 그로 인한 아프간·이라크전(戰)은 인류역사에 있어서 커다란 획을 그으면서 국제안보와 전쟁의 패러다임을 새롭게 변화시켰다(김응수, 2007: 174). 그동안 논의 차원에서만 머물러 왔던 초국가적 테러리즘이 현실로 나타난 것이다.

이와 같이 21세기에 있어서 발생하는 초국가적 테러리즘의 주체로써 테러리스트들은 첨단화된 커뮤니케이션을 필수 불가결한 도구로써 사용하고 있다. 비록 이슬람교도의 테러리스트들과 극단주의적인 조직들은 엄격한 이념을 바탕으로 활동하지만, 그들은 세계화(globalization)라는 현대적 기제를 활용하고 수용함으로써 그들의 임무를 수행함에 있어서 많은 진전을 꾀하고 있다. 1970년대 이후 테러리스트들은 많은 시행착오를 겪으면서 대중화된 현대의 통신수단을 활용하여 다양한 목적들을 달성할 수 있었다. Ayatollah Khomeini는 1970년대에 의사소통 수단으로써 카세트테이프를 많이 활용하였고 bin Laden은 1980년대와 1990년대에 비디오테이프를 이용하여 'jihad(聖戰)를 수행하는 것은 모든 이슬람교도들의 임무이자 본분' 이라는 그의 메시지들을 대중화 시켰다. 그리고 Abu Musab al-Zarqawi는 다양한 멀티미디어의 형식과 인터넷을 통하여 지금까지 전례가 없는 흉악함을 전파하였다(Abdelnasser, 2000: 45).

특히 인터넷은 al-Qaida 또는 그들과 연계되어 있는 조직들, 그리고 그 조직에 가입하려고 하는 세포조직들에게 필수적인 수단으로써 자리 잡게 되었다(Gruen, 2006). 인터넷은 초극단적 위협을 가진 '토착(home-grown)' 조직들에게 선전활동, 신규모집, 교의, 신앙, 이론, 원리 등의 주입, 자금 및 필수품 조달과 커뮤니케이션 수단 등의 용도로써 지속적으로 사용되고 있다. 그리고 과학기술이 발달함에 따라 테러리스트들이 사용하고 있는 위협도 함께 가중되고 있다. 즉, 그들은 카세트테이프 시대에서 비디오테이프, 그리고 인터넷을 통하여 더욱 정교하고 복잡한 옵션들을 선택할 수 있는 시대에 와 있다.

1989 - 2001년 아프가니스탄에서의 패배로 현대 테러리즘이 모진 시련을 겪은 이후 인터넷은 테러리스트들에게 제일 중요한 선전활동과 의사소통 수단과 방법이 되었다. 현대 jihadists가 인터넷을 지속적으로 신뢰하고 의존하는 것을 우리는 절대로 과소평가해서는 안 된다. 이제 테러리스트들의 활동은 물론 대테러 활동에 있어서도 인터넷은 의심할 여지없이 가장 중요한 정보 제공의 근원이라고 평가하게 되었다. 그러나 아직 반테러리즘 또는 대테러리즘 차원에서 인터넷이 중요한 역할을 하는 만큼보다 인식이 부족하다.

그러므로 테러리즘에 있어서의 커뮤니케이션 역할, 특히 인터넷의 기능에 대하여 심도 있는 연구는 국내는 물론 국제적인 관점에서도 상당히 미진한 실정이다. 일반적으로 인터넷을 테러리스트나 그와 관련된 조직들의 일반적인 케뮤니케이션 수단의 하나로 인식하는 경향이 있다.

오늘날 국제 테러리즘의 활동 영역이 전통적 테러리즘 개념의 범주를 넘어 초국가성을 띠게 됨에 따라 커뮤니케이션 수단도 광역화와 속도, 그리고 고도의 보안성을 필요로 하고 있다. 따라서 본 연구에서는 초국가적 테러리즘의 주 의사소통 수단으로써 활용되고 있는 현대 테러집단의 인터넷 등 웹을 이용한 케뮤니케이션의 발전 추이와 알카에다의 활용실태를 집중적으로 분석하고자 한다. 그리고 이러한 테러집단의 웹을 이용한 커뮤니케이션 수단으로써 점점 그 유용성이 높아짐에 따라 이를 해결함에 있어서 한계와 현실적인 대응책을 논의하고자 한다.

II. 테러조직의 인터넷 활용 양태

1. 테러리스트의 인터넷 활용 추이

오늘날 거의 모든 테러리스트들과 게릴라 조직들은 아주 특별한 경우를 제외하고는 통제받지 않는 웹을 사용한다. 일반적으로 테러리스트와 게릴라 조직은 좌익과 우익(left and right wing), 인종-민족주의자(ethno-nationalist), 정치-종교주의자(politico-religious), 그리고 단일 사안을 다루는 조직(single-issue group) 등 4가지 부류가 있으며, 그들은 모두 통제받지 않는 웹을 사용한다. 역동적 정보 기반인 인터넷은 다양한 용도로 쓰이고 있는 바, 예컨대 폭력적인 jihad의 이데올로기와 조직원의 신규모집, 조직을 정치화하고 과격하게 만드는 과정, 그리고 새로운 테러리스트들과 극단주의자들의 조직을 동원하는 주된 수단 등으로 사용하게 되었다. 그들은 인터넷을 활용하여 여러 논점들에 대한 토론과 학습은 물론, 그들의 비전을 제시하기도 한다(Chandler, 2007: 179-180). 즉, 인터넷을 활용하여 테러조직과 극단주의자들은 조직원들에게 심리전 교육을 할 뿐만 아니라 적에게도 심리전을 강요하여 그것을 일반적인 대중들에게 유포하도록 하였다.

<표 1> 테러리스트와 게릴라 조직의 인터넷 활용

ㅣ 대 상	조직원 (추종자, 지지자)	적	일 반 대 중
내 용	· 심리전 교육(사기고양) · 활동방향 제시 * 믿음과 생활방식에 비판 받음	· 이슬람 적대세력 혼란시킴 · 허의정보 유출 및 오보 제공	· 두려움 유발 · 신규요원 모집 · 국제여론 형성

자료: 본문 내용을 정리하였음.

좀 더 구체적으로 말하면 <표 1>에서 보는 바와 같이 그들은 자신의 추종자들이나 지지자들에게 심리전을 통하여 사기를 높임과 동시에 활동 방향을 제시하였는데 대부분의 경우 아주 과격하였다. 또한 그들은 이슬람교도의 극단주의자들을 제외한 다른 모든 사람들로부터 그들의 믿음과 생활방식에 대하여 비판을 받았다. 그리고 적에 대한 심리전은 사이버 상에서 이슬람의 적대세력을 혼란시키고, 허위정보를 유출하거나 오보를 제공하는 방식으로 진행되었다. 일반대중을 상대로 한 심리전은 대중들로 하여금 두려움을 유발하고, 신규 요원을 모집하거나 국제 여론을 형성하기 위한 것이다. 특히 2001년 10월 이후 아프가니스탄의 패배로 테러리스트와 극단주의 조직들은 추방되거나 이탈하였지만, 이들은 인터넷을 통하여 재건을 추진하였다. 더욱이 al-Qaida와 그들의 연합조직들은 인터넷에 가상 훈련기지를 설치하여 TATP(triacetone triperoxide)와 같은 폭발물 제조법을 게재하였으며, 장차 공격 목표에 대한 정찰과 지휘감독을 하였고, jihad의 땅으로 여행을 희망하는 자들에게는 자세한 정보를 제공해주기까지 하였다. 이와 같이 테러조직과 극단주의 조직들은 인터넷을 사용함에 있어서 안전보장과 비밀통신, 동조자들과의 실시간 대 의사소통 등 다양성을 띠고 있다. 웹 사용의 용이성과 효율성은 9.11 테러 사건의 지도자인 Khalid Sheikh Muhammad, 일명 'Mokhtar'에 의해 완벽하게 구현되었다. 그는 al-Qaida 내부적으로 통용되는 부호와 방법을 사용하여 '죽음의 편지'를 대중화 시켰다. 그의 부하인 al-Qaida 통신 담당자 Muhammad Naim Noor Khan과 영국 내의 al-Qaida 지도자로 알려져 있는 일명 Esa al-hindi라고 불리는 Dhiren Barot 등은 인터넷을 여러 분야에 이용하였다.

테러리스트의 인터넷 사용에 대한 학계 권위자인 Gabriel Weimann 교수는 테러리스트들이 인터넷 사용에 대한 교육을 하고 있는데 그것은 다음과 같은 장점이 있기 때문에 많은 관심의 대상이 된다고 하였다.

- 엄격하지 않은 이용 규칙과 통제, 전 세계에 많은 잠재적 이용자들이 접근하기가 용이함
- 의사소통에 대한 익명성 보장과 정보유통의 신속성
- 웹의 개발과 유지비용의 저렴함
- 문서・그래픽・오디오・비디오를 합성하여 사용할 수 있으며, 필름・노래・책・포스터 등을 다운로드할 수 있는 멀티미디어 환경
- 인터넷 기사를 출처로 사용하는 매스미디어 보도를 조종하는 능력(Weimann, 2005: 1-5)

여기에서 1990년대 중반 테러리스트와 극단주의자들의 초기 인터넷 사용에 대하여 살펴보기면 인터넷 초기 사용자들은 미국, 캐나다, 유럽등지에 분포되어 살고 있는 이민자와 이산자 중의 테러리스트의 지지자들이였다. 결국 오늘날까지 광범위하고 주요한 테러리스트들과 극단주의자들의 웹사이트는 서구에서 유래되었다고 할 수 있다. 미국에서 최초로 인터넷을 사용한 조직은 이집트 이슬람교 단체(IGE)의 정신적 지도자인 Sheikh Omar Abdel Raham, 일명 'Blind Sheikh'를 지지하는 집단이었다. 'Blind Sheikh'가 투옥한 후에 그들은 인터넷을 사용하여 반서구 선전활동을 널리 전파하였으며 미국과 캐나다에서 인터넷을 통하여 자금을 모으기 시작하였다. 점차 그들은 네트워크의 교류 범위를 프랑스, 독일, 이탈리아, 영국, 오스트리아 등 유럽의 지지자 및 후원자들에게로 확장시켜 나아갔다.

상용화된 웹을 사용하는 자들은 jihadist 조직들에만 국한되지 않았다. 예컨대 Liberation Tigers of Tamil Ealam (LTTE)는 최초로 인터넷을 사용하여 의사소통을 하였으며 세계를 무대로 선전활동을 하였고 정부의 정보 하부조직에 공격까지 한 그룹 중 하나이다. 한 LTTE 세포조직은 미국에 있는 대학을 기지로 하여 1990년 중반 동시다발적으로 스리랑카 외교부 파견단에 대한 공격을 선도했으며 정부의 통신 시스템을 혼란스럽게 만들었다. 또한 민족주의자들과 Neo-Nazis와 Ku Klux Klan과 같은 우익 조직, 그리고 필리핀의 New People's Army와 네팔의 Maoists와 같은 좌익 조직들도 인터넷을 사용한다. 폭력적인 jihadist가 같은 이념을 가진 jihadist 단체들과 단합하듯이, 같은 공산주의적인 이념으로 단합한 이들 또한 인터넷을 통하여 협력을 도모한다. 실례로 Revolutionary International Movement(RIM)는 인터넷을 이용하여 라틴아메리카부터 남동아시아의 테러리스트와 극단주의자들의 활동을 전 세계적으로 통합하고 조정하고 있다. '산업화된 서구' 지역으로부터 전 세계로 퍼진 인터넷의 악용은 테러리스트들과 게릴라 조직들에 의해서 라틴아메리카, 중동, 아시아, 아프리카, 그리고 그 외의 지역까지 확장되고 있다.

2. 테러리즘의 신경조직 (Nerve System): Al-Qaida

Al-Qaida는 웹과 다른 현대적인 도구들을 테러리스트들 사이에서 대중화한 것으로 유명하다. Bin Laden은 NATO-스타일 전투 재킷과 러시아의 AK-47 강습용 소총과 같은 현대적인 고성능 장비를 소지하기 위하여 과감하게 투자하였다. 또한 그는 애리조나에서 항공기를 구입하였으며, 뉴욕에서 인공위성 전화를 획득해서 사용했다. 비록 jihadist는 서구를 비난하지만, bin Laden처럼 서구의 현대 과학기술의 다양성은 개발하고 활용하여 그들의 의지와 목표를 이루려고 한다.

재정을 '테러리즘의 동맥(life-blood)'이라고 한다면, 통신과 커뮤니케이션은 이들의 '신경조직(nerve system)'이라고 할 수 있다. 마치 오늘날의 무장 세력들의 정교한 첨단 무기체계가 최첨단 정보통신기술에 의존하는 바와 같이, 테러리스트들 또한 첨단 기술에 의존한다. 한 동안 테러조직들은 인터넷의 사용으로 많은 이익과 도움을 얻었다고 알려져 있고 al-Qaida 또한 예외가 될 수 없다. '지구촌'의 성장에 대한 점진적 변화와 발달은 그 조직과 그와 연관된 모든 세포조직들에게 네트워크를 제공해 주었으며 아무리 느슨한 관계도 지속적으로 유지될 수 있도록 해주었다.

이슬람교도의 세계에 발표한 Usama bin Laden의 몇몇의 중요한 선언들은 그가 얼마나 '미디어에 정통한 사람'이라는 것을 알 수 있다. 이 부분은 그가 아프간이나 파키스탄의 국경지역으로 도피했다고 믿어지는 지금도 변함이 없다. 2001년 말 미국이 리드하는 연합군들이 발견한 아프가니스탄의 'CNN Tapes' 에서 al-Qaida가 천연 화학약품 개발을 시도한 것이 확인되었으며, 이러한 실험과정이 비디오로 녹화되었던 것으로 보아 천연 화학약품 개발은 지속적으로 개발되고 있다는 사실을 확신할 수 있었다. 비슷한 시기에 가면을 쓴 mujahidin의 훈련 장면과 그들의 투사적 무용을 찬양하는 비디오도 만들어졌다. 이것들은 물리적이거나 전자적인 다양한 방법으로 새로운 지하드 신봉자들을 모집하기 위해 al-Qaida가 배포한 것이었다. 이제 테러리스트들이 수백 개의 웹사이트를 악용하는 것은 하나의 현상이 아닌 일상적인 일이 되었다고 볼 수 있다.

이슬람교도 극단주의자 조직 웹사이트의 경우, 한결같이 다양한 권유를 하고 있는데, 그들의 권유는 jihad에 실질적으로 참여하거나 지지와 후원을 강요하고 있었다. 정부와 사설기관들은 특히 9.11 테러 사건 후에 al-Qaida와 관련된 사이트들을 집중적으로 추적해 왔다. 이러한 테러리스트 사이트들은 잘못된 정보들이나 근거 없는 이념을 전파하려고 만들어졌을 뿐만 아니라 신규 테러리스트들을 모집하거나 조직할 수 있도록 세뇌시키고 그들에게 훈련방법도 제공하였다. 'Muaskar Al-Battar'(훈련기지: 'The Training Camp') 라는 아랍어로 만들어진 한 사이트는 특별히 훈련잡지 사이트로 개설되었으며 그들은 테러리스트들에게 대중적인 무기류의 사용법을 제공해 주었다.(UN)[1] 이 두 달에 한 번 꼴로 출간된 인터넷 간행물은 첫 호에 AKM과 AK-47 돌격용 소총들에 대하여 집중 소개하였다. 그 후 MP-5 서브머신 권총, 그리고 3호에는 그 악명 높은 RPG-8 견착식 대전차 로켓 발사기에 대한 설명을 수록하였다. 이와 같이 가상공간에 있는 성전학습소는 공격의 효율성과 치명성을 높이기 위해 매복공격 감행으로부터 고성능 폭파장치 활용까지 테러활동의 전부를 예비 테러리스트들에게 전수하고 있다(하영선 2009: 446). 2006년 6월 현재 22호까지 존재하는데 이 사이트는 사라져버린 다른 많은 Al-Qaida와 관련된 사이트들과는 다르게 아무나 쉽게 접속할 수 있었다. Al-Qaida에 관련된 최초의 사이트 중 하나인 alneda.com에는 지금 접속을 하면 '추적되고 해킹 당해 현재는 미국이 소유하고 있다!'라는 문구가 뜬다. 다른 몇몇 사이트들도 비슷한 최후를 맞이한 것처럼 보인다. 상당한 테러리스트들의 웹사이트를 추적하는 것은 아주 까다로울 수밖에 없는데 이것은 인터넷 체계상의 본질 때문이었다. 이것은 사용자들이 수천 마일이 떨어진 곳에서 자신의 신분을 숨기고 쉽게 사이트를 유료로 개설할 수 있기 때문이다. 하지만 이러한 개설자들의 표면상의 익명성에 불구하고, 몇몇의 인터넷 서비스 제공자들(internet service providers, ISPs)이 사이트의 목적을 깨닫고 난 후에 폐쇄시킴으로써 어느 정도의 제제에 성공을 거두기도 하였다.

가끔은 풍선효과처럼, 테러리스트들은 그들의 사이트들을 폐쇄시키고 다른 곳에서 개설하는 경우도 있다. 어쨌든, 많은 사이트들이 다양한 기술적 합성을 통하여 '인터넷의 오용'을 보여주고 있다. 이와 관련한 최근의 예로써 Steganography라는 프로그램은 사용자들이 그들의 파일들을 아예 다른 내용이나 형식으로 바꾸어 전송할 수 있다. 사진이나 비디오 클립들은 최근에 jihadist 포럼인 mohajroon의 회원들로부터 암호가 걸려 보호받으면서 스크린을 찍어내는 방식으로 사용하도록 되어 있어 사용자들은 문서를 사진파일로 바꾸어서 전송할 수 있고, 해커들이나 수사관들의 추적으로부터 벗어나 비밀이 보장된 가운데 안전하게 의사소통이 이루어진다. 또한 그 프로그램에 대하여 사용이 용이하도록 단계적으로 회화적인 설명과 번역을 제공하였다. 이러한 소프트웨어들은 익명성 보장과 비밀스러운 의사교환이 가능하고, 보안상의 경계를 제공해 줄 수 있다는 이유로 jihadist 포럼들에게 빠르게 대중화 되었다. 이러한 사실들로 보아 그 회원들이 얼마나 컴퓨터에 대한 지식이 많고 기술적인 통찰력이 있는가를 알 수 있다. 이 예가 보여주듯이, 'greater al-Qaida' 회원들이나 그들의 후원자에 의해 사주된 많은 '사이버 전술가'들은 은밀하게 활동하지 않고 기술적 보호를 받으면서 공개적으로 활동하였다. 이러한 여러 가지 기술들은 al-Qaida에 한정되지 않고 대다수의 현대 테러리스트들에게 꾸준히 사용되고 있고, 하마스, 헤즈볼라와 이슬람교도 jihad들은 최근 몇 년간 세계적인 사건들을 통하여 많은 사람들의 생활을 혼란스럽게 만들었다. 이와 같이 이슬람 세계로 선전하는 행위는 인터넷을 이용하여 아주 쉽게 전파할 수 있었다(Chandler, 184-185).

인터넷 붐으로 인하여 우리의 일상생활에는 편리한 점들이 많지만 동시에 해악도 존재한다. 예컨대 해커들이 금융 관련 이익을 추구하기 위하여 인터넷 사이트에 불법적으로 존재하는 것이다. 지하로 숨어든 테러조직들이 감시를 피하면서도 서로간의 커뮤니케이션은 지속할 수 있도록 의심 없는 주인들의 사이트 시스템을 해킹하게 되었다. 또 다른 조직은 이와 비슷하게 위조 '통화료 서비스 코너'를 운용하여 이민자나 유럽 국가의 유랑 노동자들에게 할인된 국제전화 상품을 제공해 주었다. Continental Airlines 같은 저명한 업체를 해킹함으로써 '통화료 서비스 코너'는 이민 고객들에게 국제전화 요금을 국내전화 요금으로 제공해 줄 수 있었다[2]. 이렇게 '통화료 서비스'를 합법적인 사업으로

1) UN Security Council documents/2002/541, dated 15 May 2002.

가장해 마드리드 열차 폭파사건의 테러리스트들에게 은신처와 IED 기폭장치의 기술적 노하우를 공급해주었다.

3. 인터넷 커뮤니케이션의 만화경 현상(Kaleidoscope phenomenon)

인터넷 커뮤니케이션의 만화경 현상 (kaleidoscope phenomenon)[3]의 한 예로써 테러리스트들이 인터넷을 악용하여 그들의 목적을 내세우며 그들의 '신성하지 못한 전쟁'을 위한 새로운 회원들을 모집하는 일이 있다. al-Qaida는 자신들의 사이트를 칼, 언월도와 AK-47 등의 무기와 코란 구절들로 화려하게 장식하고, 순교의 보답으로 평생을 72명의 처녀들과 함께한다는 설명 등으로 그들의 사이트를 비젼 있고 호감이 가도록 만들었다. 이런 사이트들은 뚜렷한 미래가 없고 희망을 잃어버린 청소년들에게는 우울한 현실로부터 도피할 수 있는 공상적인 희망과 기회를 제공하는데 충분했다. 이를 통해 Usama bin Laden과 그가 지휘하는 집단은 십자군에 대항하여 용감하게 맞서 싸움으로써 명성을 유지했던 Salah al-Din(혹은 'Saladin')과 같은 위상으로 평가되고, 어떤 이들은 아예 Usama bin Laden을 현대의 새로운 Salah al-Din으로 추앙하게 되었다. 이 사이트들은 성인 남성이나 청소년들만 상대한 것이 아니라 동시에 여성들도 목표로 하였다.

2004년 8월 말에 새로운 al-Qaida 웹 사이트가 개설되었는데, 그것은 특별히 여성들을 겨냥한 사이트였다. 'al-Qaida 아랍반도 여성정보국(al-Qaida's Arabian Peninsular Women's Information Bureau)'에서 출판한 Al-Khansaa잡지에는 jihad를 따르는 여성들을 모집하는 광고를 하였다. 이것은 처음에 어떻게 남성들과 대등한 역할을 하는가에 대한 방법으로부터 시작하여 그들이 가정에서 어떠한 중요한 신념을 가질 것인가에 대한 내용을 제시하였다[4]. 그들 집단 고유의 호전적인 분위기에도 불구하고, Al-Khansaa는 이를 감추고 현대 '소녀풍의 어필'을 하기 위하여 핑크색으로 웹을 장식하였다. 하지만, 잡지 출판사들은 Al-Khansaa잡지를 개설하는 과정에서 그들의 의도대로 하지 못하고 al-Qaida의 주장대로 편집하였다. 그리고 사우디아라비아 여성들은 아라비아 반도 이교도에 대해 al-Qaida가 조장하는 반감을 가진 사우디와 아랍 여성 및 아이들을 겨냥하여 새로운 인터넷 잡지를 출간하는 것에 맹렬히 비난하였다. 왜냐하면 사우디아라비아 여성들에게 이슬람은 자비, 동정, 관용과 정의를 대표하는 것이라고 여겼기 때문에 여성들을 합류시키거나 Jihad에 대한 지지자로 만드는 것은 테러리스트들이 다시 한 번 이슬람교도의 신앙을 잘못 해석한 것으로 단정할 수밖에 없기 때문이다. 당시 전문가들은 그들이 추구하는 것은 전혀 이슬람적이지 않고 극단주의와 복수에 초점이 맞추어져 있다고 평가했다[5]. 비록 현재는 Al-Khansaa에 접속할 수는 없지만 인터넷을 통하여 급진적으로 여성들을 대상으로 설득과 개혁을 하고, 특히 서구 여성들을 이슬람으로 개종시키려는 그들의 노력은 지속적으로 추진되었다. 한 예로, Muriel Degauque라는 38세의 벨기에 여성은 백인의 기독교가정에서 태어났지만, 이슬람교도로 개종하였다. 극단주의자가 된 그녀는 한 이슬람교도의 채팅룸에 접속하여 이라크로 부름을 받고 결국 2005년 12월에 미국 호송차에 자살폭탄 테러를 감행함으로 죽음을 맞이했다.

하지만 테러리스트들에게 인터넷은 양날의 검이 될 수도 있다. 테러리스트들의 커뮤니케이션 활동에 관해 그들의 사용 흔적들과 그들의 신분을 감추기 위해 암호를 걸어 접근을 불가능하게 하는 방법을 강구함에도 불구하고, 정보보안 서비스들은 그들을 추적할 수 있는 방법을 찾아내고 있다. 현재 SIGINT 와 ELINT팀들은 최첨단 테크놀로지와 소프트웨어를 운용함으로써 테러리스트들의 통신 전송들을 추적하여 그들을 체포하거나 그들이 계획한 공격들을 좌절시키도록 하였다. 한 예로써 2006년 6월, 캐나다 경찰은 17명의 남아시아 남성들을 토론토에서 체포하였는데 그들은 전원 이슬람교도 테러리스트 세포조직의 회원이었고, 토론토 인근에 있는 중요한 시설을 공격할 계획을 세웠다는 혐의가 있었다. 그리고 그들은 암모니아 질산염을 3톤이나 소유하고 있었는데 체포되자 이를 원예 목적으로 소유하고 있었다고 변명하였다. 캐나다의 보안서비스는 그 용의자들의 활동계획을 한 인터넷 채팅 사이트를 감시하다가 발견하여 테러사건 발생을 예방할 수 있었다[6].

가장 위협적인 해커의 예로 'Irhabi 007(terrorist 007)'이란 필명으로 활동한 해커가 있었다. 이는 al-Qaida와 밀접하게 연합을 형성하여 수많은 인터넷 사이트에서 신뢰를 받으면서 활동하였다. 정보보안 서비스들은 2년여 동안 이 사이트가 잠적하기 전까지의 '사이버 상의 행적'들을 추적하였다. 그리고 2005년 10월 21일, 경찰이 22세의 남성 Younis Tsouli을 런던에서 체포하였다. 그는 '영국의 테러활동 2000지침(UK Terrorism Act 2000)' 에 의거하여 살인과 폭파, 협박을 통해 테러리스트 활동자금을 조달하였다는 혐의로 체포되었다. 다른 테러를 수사 중이던 당국이 Irahbi 007가 사이버 공간에서 잠적한 시점이 Younis Tsouli가 체포된 시점과 같고, Younis Tsouli의 집에서 발견한 정보 등의 정황으로 보아 그가 바로 그 사이버-테러리스트였다는 판단을 하게 되었다[7].

4. 테러리스트 커뮤니케이션과 미디어

정보보안 서비스들과 이와 관련한 민간기구들이 인터넷 해킹이나 테러리스트들을 지속적으로 추적하고 감시하는 데에는 언론의 역할을 또한 언급하지 않을 수 없다. 예컨대, 이라크에서 테러리스트들이 자행하는 도로상에서의 폭발물 테러와 자살폭탄 테러 등은 매 사건마다 텔레비전을 통하여 방송되

2) 'Steganography Instructions to Conceal a File Within the Contents of Another for Secret Data Transmission explained by Jihadist Forum Member', siteinstitute.org/news.html(2010. 6. 12 검색).

3) 만화경 현상(Kaleidoscope Phenonmenon)은 원통 속에 여러 가지로 물들인 유리 조각을 장치하고, 사각형의 유리판을 세모지게 짜 넣은 것으로 그 속을 들여다보면 온갖 형상이 대칭적으로 나타나게 된다. 여러 갈래의 다양한 것이 섞여 있음을 비유적으로 이르는 말이다.

4) Dr Udo Ufkotte, 'Telefonieren fur den Terror', Park Avenue Magazine, 2(February 2006).

5) See www.inteligence.org.il/eng/memri/sep_e_04.htm(2010. 6. 12 검색).

6) Javid Hassan, 'Women Come Out Against Extremist Internet magazine'. Arab News, 7 September 2004.

7) en.wikipedia.org/wiki/2006_Toroton-terrorism_arrests(2010. 6. 20. 검색).

므로써 결과적으로 전 세계에 테러리스트 조직들을 위한 무료광고를 제공해 주는 꼴이 된다. 하지만 전 세계에 많은 이슬람교도들은 정보의 결핍으로 이러한 사건들을 이라크를 침략하였던 국가에 대하여 정당성 있는 보복과 응징으로써 인식하게 된다는 것이다. 다행스럽게도 많은 이라크인들은 이와 같은 생각을 하지 않으며, 사담 후세인 정권이 더 이상 통치하지 않기를 원한다.

불행하게도, 특정 주제에 대해 잔인하고 끔찍한 사건들을 보도하는 텔레비전 방송들은 경쟁에서 살아남았다. 따라서 오직 al-Jazeera만 독점적으로 Usama bin Laden과 그의 대리인인 Ayman al-Zawahiri에 대한 오디오를 상영할 수 있었던 것은 al-Jazeera가 기존의 al-Qaida 지도자들 중 남아 있는 이들의 대변인 역할을 하기 때문이었다. 만약 al-Jazeera의 이 역할을 다른 방송국이 맡는다면 al-Qaida 테이프들이 인터넷을 통하여 다양한 방법으로 전파되었을 것이다. Al-Jazeera의 공정성 때문에 어떤 경우에는 al-Qaida 웹사이트로부터 이미 방출되었던 정보들을 그대로 보도하기도 하였다. Evan Kohlmann은 MSNBC 텔레비전을 통하여 bin Laden과 al-Zawahiri가 발표하기 위한 녹화 비디오테이프의 편집과 배포 과정에 대하여 조사하였던 것을 설명하였다(Katz 2006). 그 비디오테이프는 bin Laden과 Zawahiri가 비밀장소에서 녹화하였으며, 새로 모집한 카메라맨들로부터 제안을 받아 al-Qaida의 홍보담당자 As Saahab가 편집하면서 더욱 세련되게 완성하여 인터넷으로 전 세계에 배포시키게 된다. 그리고 이러한 내용들은 대테러리즘 블로그을 이용하여 참조할 수 있도록 구성되어 있다.

여하튼, 테러리스트들이 인터넷과 웹들을 불법으로 이용하는 것은 al-Jazeera가 테러리즘을 장려하고 있다는 것을 입증한다. 특히, 테러리즘이 잔혹한 양상을 띠고 있으며, 만약 그 방송국이 al-Qaida의 메시지들을 독점하여 방영할 경우에 그러한 경향이 더욱 강하다. 1999년 8월 러시아가 체첸을 재침공했을 때 체첸 야전군 사령관 샤밀 바사예프의 행동도 좋은 예로 볼 수 있다. 이러한 미디어의 독점 양상은 그 회사가 얼마나 bin Laden이나 그의 대변자에게 돈을 지불하는가에 달려 있다. 이러한 과정에서 만약 어떠한 돈이라도 거래가 되었다면 al-Jazeera는 마땅히 UN의 제재를 받아야 하고, 그 회사는 al-Qaida에 관련한 자금과 물질적인 지지와 후원으로 인하여 1267위원회의 통합목록에 등록되어야 한다. 확실히 국제사회와 미디어를 포함한 관련 요소들이 초국가적 이슬람교도의 테러리즘으로부터 받는 위협에 대해 어떻게 대처하는가를 파악하기 위해서는 테러리즘 개념에 대한 이해와 재정, 그리고 커뮤니케이션에 이르기까지 전반적인 과정을 고찰할 필요가 있다.

III. 테러조직의 인터넷 활용 확산 방지를 위한 대응과제

1. 테러단체의 웹 운용 문제 해결의 한계

UN 분석지원과 제재규약 감시팀(UN Analytical Support and Sanctions Monitoring Team: ASSMT)은 국제기구와 국제사회의 효과적인 활동과 그들의 활동결과에 초점을 맞추었고, 나아가 그 문제들의 범위와 한계에 대하여 강조하였다(UN Security, 2010) 그러나 그들의 견해가 다른 기관이나 기구들과 일치하지 않는 것도 있었다. ASSMT는 인터넷에 al-Qaida가 오늘날 2,600개 이상의 사이트들과 관련이 있다고 하였다.

<표 2> 웹사이트 개설 현황 (개망)

구 분	전체 웹사이트 수	테러단체 웹사이트 수
1998 년 9 월	2,636,000	12
2004 년 9 월	55,062,000	4,800

자료: Chandler(2007: 187)와 http://www.netcraft.com/survey2010의 데이터를 조합하였음

<표 2>에서 보는 바와 같이 1998년도 전체 웹사이트 2,636,000여 개 중 al-Qaida에만 국한되어 있는 것은 아니지만, 12개의 테러리스트 웹사이트들이 존재했으나 불과 6년 후인 2004년에는 55,062,000여 개의 전체 사이트 중 4,300개가 넘는 테러리스트 사이트가 존재하고 있다. 이것은 인테넷 망이 초기에 선진국 위주에서 운용되었으나 그 이후로는 개발도상국을 포함한 전 세계로 급속히 확산되고 있고, 테러리스트 웹사이트는 더욱 빠른 속도로 증가하고 있음을 나타낸다. ASSMT가 국제기구나 단체들에게 테러리스트 웹사이트 문제를 강조하였지만 이를 통제할 수 있는 특별한 대안은 없었다. 독자들의 관심을 끌게 하는 안전보장이사회의 결의 1617(2005)과 1624(2005)를 통하여 국제협력으로 테러리스트들의 테크놀로지 개발과 그들의 목적 추구를 차단하라고 강조하였지만 그 효과는 아주 미미하였다. 안전보장이사회가 '지정한 국가들은 모두 채택해야 한다.'는 방침에도 불구하고 개별국가들은 각국에 차별화된 이익이 없을 경우에는 거의 협력하지 않거나 아주 적은 수의 국가들만 이에 관심을 표명하였다. 그런 가운데 테러리스트들과 후원조직의 끊임없는 인터넷 개발은 초국가적 테러리즘을 시도하려는 노력이라고 볼 수 있고, 이에 대한 대응 또한 초국가적 방법과 수단을 공유함해야만 그 위협에 대응할 수 있다. 그러나 이것은 민주주의를 신봉하는 전 세계가 개인의 인권과 권리를 중요 시하는 관점에서 가장 중요하고 심각한 딜레마 중 하나로 직면하게 된다.

보안 및 정보기관들은 웹 사용을 감시하였지만 관료와 정치가들은 그 사용을 규제하는 활동을 하기는커녕 그것을 거의 이해하지도 못했다. 흥미로운 것은 UN감시조직이 테러조직의 자금공급에 대하여 추적하던 중 al-Qaida와 관련된 테러리스트들의 인터넷 사용에 대하여 처음으로 관심을 갖게 되었다.

9.11테러 사태 발생 이후 많은 국제사회와 공동체들이 테러조직의 자금 조달 통로에 대하여 추적하면서 확인된 테러리스트들이 현대 과학기술을 논리적으로 사용했다는 것을 확인하였다. 많은 일반시민들은 개인 신상정보가 인터넷에 노출된다는 위협을 감수하면서도 인터넷 뱅킹은 그 당시 아주 보편화되어 있었다. 테러리스트들이나 그들의 후원자와 지지자들은 그들의 신원을 숨기기 위하여 현대적

발달된 기술을 사용하였고, 결국 테러리스트들은 이미 '세계화(globalization)' 추세에 편승하고 있었다고 판단된다. 그들이 감시를 피하여 자금을 유통시킬 수 있는 수단은 곧 인터넷이었고, 인터넷을 통하여 재정적인 처리뿐만 아니라 지휘통신, 의사소통, 조직 관리와 병참지원까지 하고 있었다.[8)]

테러리스트들과 극단주의자들이 인터넷을 의도대로 사용할 수 있게 된 지 10년 이상이 지났지만 아직 정부의 정책과 의사결정자들은 이에 대하여 확고한 대처 방안을 마련하지 못한 실정이다. 이와 같은 문제의 핵심은 테러리즘에 대한 이해가 부족하고, 또한 의사결정자들의 역량이 부족하기 때문이다. 그리고 개별국가들은 테러리즘과 극단적인 경향에 대하여 강력한 이념적 대응을 개발하므로써 테러리즘을 예방하거나 억제책을 강구하기 보다는 사후 물리적 대응, 즉 테러 사건 발생 후 어떻게 대처하는가 하는 대테러리즘에 역점을 두고 있다. 국가나 정부조직이 테러리스트에 대한 이념적 대응을 간과하게 되면 이스라엘-팔레스타인의 경우처럼 테러리스트들은 물리적인 하부구조나 기본역량을 강화시켜 지속적으로 대응을 하게 될 것이다. 인터넷상에서 테러리스트들의 이념을 통제하기란 그 특성상 현실적으로 불가능한 실정이다. 사이버 공간에는 수천 개의 테러리스트와 극단주의자들의 웹사이트가 존재하고 있지만 대테러리즘과 대극단주의자들의 사이트는 아주 극소수만이 존재하고 있어 테러리스트들과 극단주의자들이 실질적으로 우세한 입장이라고 평가할 수 있다. 정부는 테러리스트들이나 관련 조직들이 불법으로 광범위하게 인터넷을 활용하는 행위에 대하여 효율적으로 대처하기에는 그들보다 기술적으로 몇 년이나 뒤쳐져 있다. 결과적으로 매일 수백 명의 청소년들이 테러리스트의 교리를 배우고, 일부는 이미 테러공격을 계획하고, 준비하며 시행하는 실정이다. jihadist 조직 스펙트럼에는 자기 학습을 통해 극단주의자적 성향이 증가하는 현상이 아주 중요한 위협으로 부상하고 있다. 따라서 정부와 관련기관, 그리고 기구들은 이와 같이 급증하는 위협에 효과적으로 대처할 수 있는 지속적이고 조직적인 대응책들을 발전시켜 나아가야 한다.

2. 소극적 대응책: 지혜로운 선택

세계 많은 산업국가들의 대다수 시민들은 개인의 자유와 국가 개입 사이에 균형관계를 잘 생각해 보아야 한다. 민주주의 사회에서는 일상생활에서 개인의 모든 사생활은 법적 보호를 받는다. 테러리즘이 과거에 주목을 받지 못하던 시대에는 국가 안전보장이나 법 집행 시 개인이 테러리즘 관련 혐의가 있는 경우에 국가는 일정한 범위 내에서 전화 감청 등 개인의 사생활을 침해할 수 있었다. 하지만 이러한 사생활 침해는 국가나 정부에 따라 아주 다르게 조명될 수도 있다. 사생활 침해와 관련한 유럽에서의 예로 독일 히틀러 시대나치정권의 비밀국가경찰 게슈타포(Gestapo) 역할과 냉전기 소련이 동독을 점령했던 기간 동안의 동독의 국가공안국 슈타지(Stasi)의 활동상을 들 수 있다. 시민자유 주창론자들은 개인이 사생활을 보장받는 권한은 인간의 기본권 중에서 가장 높은 가치라고 주장하고, 대다수의 시민들은 실제 사생활을 보장받을 수 있을 것이다. 그러나 문제는 보안당국이 극소수의 테러리스트들을 상대하면서 발생한다. 여기에서 명심해야 할 것은 인터넷은 테러리스트의 초국가적 커뮤니케이션 수단이기 때문에 이 문제에 대한 통제와 억제책 또한 초국가적이어야 한다. 테러리즘에 자금을 조달하는 것을 막기 위한 UN 안전보장이사회 결의안에 포함된 방법과 유럽연합과 같은 지역단체와 FATF 같은 국제기구가 후원하는 방법 등 테러리스트들에 의한 인터넷의 악용을 막기 위한 효과적인 대책이 수립되어야 한다. 이러한 방책들은 금융기관과 관련 국가들에게 요구되는 수준만큼 테러리스트의 근원지가 되는 국가들과 인터넷서비스 제공자들(ISPs)에게도 동등한 수준의 책임을 요구해야 한다.

3. 적극적 대응책: 국제적 협력을 통한 초국가적 대응

Weimann 교수는 그의 저서 '인터넷 상에서의 테러(Terror on the Internet)'에서 '오늘날의 사이버 공간에서 안전보장과 개인의 자유와의 균형을 유지하는 방법'에 대한 6가지의 접근을 제시하고 있다. 이러한 양자 간의 균형을 유지함에 있어서 가장 중요한 것은 '국제적인 협력과 공동제휴를 활성화 해 나아가는 것'이라고 하였다. 이와 관련된 내용은 '사이버 범죄와 테러리즘으로부터 보호하기 위한 국제협정(International Convention to Enhance Protection from Cyber Crime and Terrorism)'에서 보다 구체적으로 제시하였으며, 그것은 보호수단과 대응수단, 그리고 이것을 활용한 방책들을 망라하여 언급하였다. Hoover 협회의 지지를 받은 이 제안은 이미 2000년 8월에 완성되었다(irwar, 2010). 그러나 이에 대한 산물은 아무것도 나오지 않았지만, 이 제안은 이러한 문제에 대한 효시이면서 가장 논리적인 대안이었다는데 의미가 있다.

국제협약을 체결하여 테러리스트와 테러조직들의 인터넷과 미디어 악용에 대한 대응책으로 국제적 협력은 기본이면서 필수적이다. UN의 후원 아래에 13개의 국제협약들이 이미 채택되어 회원국들이 자국의 입법을 통하여 다양한 활동을 하는 테러리즘과 대응할 수 있도록 회원국들에게 기본적인 지침을 제공해 준다.

국제사회는 국제공동체들이 현재의 테러리스트들을 철저히 추적하고, 감시하도록 하기 위해서는 이러한 협약들을 더욱 발전시켜야 한다. 테러리즘에 대한 일치된 국제적 정의가 없어서 오랜 기간 동안 테러리즘에 대하여 총괄하는 기관이 부재할 수밖에 없었다는 것은 어불성설이다. 국경 없는 웹의 특성상 이러한 국제적 통제책은 분명히 있어야 한다. 언론의 자유와 표현의 자유는 항상 옹호되어야 하나, 테러리즘에 관련된 행위들을 행하거나 이를 지지 또는 후원하는 행위는 당연히 법으로 금지해야 한다. 이미 그러한 사례는 많이 있고, 예컨대 영국에서도 현재 다음과 같은 규약이 통용되고 있다. '테러리즘 같은 행위를 직접 하거나, 직·간접적으로 사주하는 행동은 범죄 및 위반행위로 규정하며... 이것은 테러리즘을 칭송하거나 찬미하는 것을 포함한다.' 따라서 이러한 협약들을 채택하여 수용하는 것이 매우 어려움에도 불구하고, 현재의 혼란스러운 상황을 극복하는 것에 더 큰 가치를 둘 필요가 있다. '테러리즘 자금조달 억제에 관련한 국제협약(International Convention on the Suppression of

8) www.iwar.org.uk/law/resouces/cybercrime/standford/cisacdraft.htm(2010. 6. 19 검색).

the Financing of Terrorism)'에 많은 국가들이 소극적으로 참여했던 것과 같이, 인터넷과 테러리즘에 관한 국제협약의 대안 또한 실질적이지 못하고 현학적(pedantic)인 모습을 띠겠지만, 그렇더라도 협약은 계속 체결되고 실행되어야 한다.

UN 총회를 통한 협약 채택은 그 자체가 구속력을 가지지는 않지만, 전 세계적로부터 인정을 받는 것이라고 해석될 수 있다. 따라서 이 협약은 인터넷의 테러리즘에 대한 국가적 법률제정의 기초가 되는 것뿐만 아니라 필요하다면 제재규약 권한 등 다양한 수단과 방법을 사용하도록 제시해 준다. 여기서 이 협약에 대하여 개별국가나 단체들이 책임을 지는가 여부는 매우 중요하다. 따라서 이러한 수단과 방책들은 UN 안전보장이사회가 총괄해서 실행하여야 한다. 물론 개별국가들이 자체적으로 관련 법규를 제정하는 것을 장려하지만, 자국의 이익만을 위하기 때문에 '국제적 기준'에 미달하는 경우가 자주 발생한다. 따라서 자체적으로 테러리스트 웹사이트를 감시하고 필요에 따라 폐쇄시킬 수 있는 ISPs의 존재는 허용하되, 무책임한 자들을 규제할 수 있는 발전된 기준 마련이 필요하다. 또한 이런 기준을 충족시키기 위하여 개별국가에 방향 및 규정을 제시하고 감시하는 FATF와 유사한 기관들의 설립이 필요하다. 또한 국제사회에서 개별국가들의 노력 또한 중요하다. 범세계적 역할을 하고 있는 미국은 2010년 4년 주기 국방검토보고서에서 사이버 공간에서 효과적인 작전 수행을 위하여 국방전략의 방향성을 제시하고 추진하고 있는 것도 그 좋은 예라고 할 수 있다. 초국가적 테러리즘에 대비한 국제사회의 노력과 이를 지향한 개별국가들의 노력 또한 절실히 요구된다.

Ⅳ. 맺는 말

테러리스트들은 커뮤니케이션을 위하여 항상 새로운 통신기술을 활용하고 그 이전에 이용 가능했던 대중매체를 부가적으로 사용해 왔다. 앞에서 살펴본 바와 같이 현재 테러리스트들에게 있어서 그들의 활동 영역이 초국가적 현상을 띠게 됨에 따라 인터넷은 단순히 임무수행의 효율성(efficiency of performance)에 한정되지 않고 조직의 존립 여부에까지 긴요하게 영향을 미치는 긴요한 수단으로 인식된다. 테러리스트들은 인터넷을 통하여 정보 유통과 회원 확보, 자금 조달, 조직관리 뿐만 아니라 가상공간에 성전학습소를 설치하여 원격학습을 하고 있다.

그럼에도 불구하고 이에 대응할 수 있는 대안은 너무도 미흡한 수준이다. 인터넷의 은닉성을 전제로 첨단 과학기술을 도입하여 급격한 성장세를 구가하는 초국가적 테러리즘에 대응하기 위해서 다각적인 노력이 필요하다.

우선, 현실적으로 매우 빠른 속도로 증가하는 테러리스트들의 인터넷 사이트 개설에 비해 현저히 뒤지는 테러 대처 방안과 정책결정자들의 낮은 인식도, 상대적으로 느린 테크놀로지 개발 등이 현실적인 걸림돌로써 작용한다. 따라서 9.11테러 사건을 포함하여 지금 이 시각에도 지구촌 곳곳에서 발생하고 있는 첨단화된 테러사건들에 대하여 어떻게 대처해야 할 것인가에 대하여 인식을 새롭게 하여야 한다.

다음으로, 인간의 기본권 보호 측면에서 편중된 주장을 들 수 있다. 사생활 보호는 분명 중요시되어야 하고 존중되어 하나, 보안기관이 소수의 테러리스트와 상대하여 대테러 활동할 때 상충되는 문제가 발생할 수 있다. 따라서 이것을 어떻게 극복하는가가 관건이라 하겠다. 중요한 것은 인터넷은 테러리스트들의 초국가적 커뮤니케이션 수단이므로 이에 대한 대처도 초국적이어야 한다는 것이다. 우리나라도 대테러 법안이 아직 장기간 입법 계류 중인 표면적인 이유 중의 하나가 인권 침해 논란이고, 한시적으로 금년 5월 'G20 정상회의 성공적 개최를 위한 경호안전과 테러방지 특별법'이 국회에서 가결되었다.

끝으로, 개별국가들은 테러리스트들의 인터넷을 활용하여 그들의 기능 활성화를 억제하고 차단하려는 진정성이 있다면 지나치게 자국의 이해관계에만 집착하는 시각에서 벗어나 초국가적 협력적 대응책을 모색해야 한다. 이것은 강한 통제력을 가진 새로운 협의체를 구성하여 보다 적극적인 대응을 하는 것이 당연하다. 그러나 세계화의 흐름에 편승하여 급성장세를 보이고 있는 테러리즘의 특성 상 우선적으로 기존의 협의체인 UN을 중심으로 국제적인 노력이 이루어져야 한다. 만약 안전보장이사회의 결의를 포함한 국제적인 필요조건들이 충족되어 테러위협에 대처한다면, 그것은 단순한 정치적 선언에 그쳐서는 안 되고 실질적으로 구속력 있게 이행되어야 한다. 따라서 UN 회원국가들이 UN 규약을 준수하지 않거나 책임과 의무를 다하지 않으면, 그들은 제재를 받아야 마땅하다. 회원국들이 실질적으로 관련 규약을 잘 이행하는 것과 효과적으로 감시를 하는 것은 매우 중요하지만 그것은 회원국들의 높은 도덕적 수준이 반드시 전제되어야 한다.

우리가 늘 경험했던 것처럼 평화와 안보에 영향을 주는 위협에 대하여 결정적인 행동을 취할 때 일반적으로 수반되는 불안(malaise)은 항상 존재해 왔다. 현 시대에 있어서 발생 가능성이 가장 높고 예측하기 어려운 테러리즘의 신경조직인 인터넷을 활용한 커뮤니케이션 통제책을 강구하는 데에는 이에 대한 정확한 현실 인식과 억제 및 차단하겠다는 국제사회와 개별국가들의 강력한 의지, 그리고 첨단 과학기술이 절실하게 요구되며 지구상의 모든 국가들은 명확하게 방향성을 설정한 가운데 대비해야 한다.

참고문헌

김영호. 2008. 9/11 이후 다자적 대테러 협력의 형성과 향후 전망. 대테러연구 논총. 통권(5): 1-42.

김응수. 2009. 탈냉전 이후 테러리즘의 초국가성 확산과 대응전략. 軍史. 국방부 군사편찬연구소. 통권(73): 173-207.

여영무. 2006. 국제 테러리즘 연구. 서울: 한국해양전략연구소.

유현석. 2009. 국제정세의 이해. 서울: 한울 아케데미.

조성권. 2007. 9/11 이후 국제테러리즘의 경향 및 전망. 대테러연구논총. 통권(4). 93-116.

하영선 외(역). 2009. 세계정치론. 서울: 을유문화사(Baylist, John and Steve Smith, The Globalization of World Politics: An Introduction to International Relations).

현승수. 2009. 체첸 테러리즘과 이슬람 사이버 지하드. 對테러 政策硏究論叢. 서울: 국가정보원. 통권 (6): 288.

Abdelnasser, Walid M. 1997. Islamic Organizations in Egypt and the Iranian Revolution of 1979: The Experience of the First Few Years. *Arab Studies Quarterly*. Issue 19.

Chandler, Michael and Rohan Gunaratna. 2007. *Countering Terrorism: Can We Meet The Threat of Global Violence?*. London: Reaktion Books.

Nacos, Brigitte L. 2006. *Terrorism and Counterterrorism: Understanding Threats and Responses in the Post-9/11 World*. New York: Pearson Longman.

U.S. Department of Defense. 2010. *The Quadrennial Defense Review Report*. Washington DC: Department of Defense.

Simonsesn, Cliffford E. and Jeremy R. Spindlove. 2007. *Terrorism Today*, 3rd Edition. New Jersey: Pearson Education.

Gruen, Madeleine. New York City Police Department, June 2006. Interview. Counter Terrorism Analyst, Counter Terrorism Bureau.

Katz, Rita and Michael Ker. Washington Post. 26 March 2006, BOI. Terrorist 007, Exposed.

UN Security Council documents/2002/541, dated 15 May 2002.

Weimann, Gabriel. 2006. Terror on the Internet. Washington DC: United States Institute of Peace.

http://www.iwar.org.uk/law/resouces/cybercrime/standford/cisacdraft.htm

http://www.lauramansfield.com/j/007.asp

http://mypetjawa.mu.nu/archives/160985.php

http://equilibrium.tistory.com/39?srchid=BR1

金應洙: 경남대학교 대학원(서울)에서 "테러리즘의 초국가성 확산과 대응전략에 관한 연구"로 정치학박사학위를 받았다. 합동참모본부 대테러 관련 과장 직책을 수행하였고, 현재 특공부대에 재직 중이면서 충남대 평화안보대학원과 한성대 국제대학원에서 강의를 병행하고 있다. 주요 관심연구분야는 국제 정치학적 관점에서의 이론과 실무 차원의 병행된 테러리즘, 남북한 관계, 군사학 등이다. 최근 연구 산물로는 "테러리즘과 대테러리즘", "테러리즘의 현재", "글로벌 테러 대응전략" 번역서와 "탈냉전 이후 초국가적 테러리즘의 확산과 대응전략", "탈냉전 이후 초국가적 테러리즘의 확산과 군사적 대응", "남북한 문화교류를 통한 동질성 회복 방향" 외 다수의 논문이 있다 (kkkk5604@hanmail.net).

투 고 일: 0000년 00월 00일
게재확정일: 0000년 00월 00일

Increase in Usage of Internet in Terrorism and Counter-measures

Eung Soo Kim

The modern terrorism is not limited to individual counties or organizations but occurs in transnational nature. The security environment and the paradigm of war has been changed especially after 9.11 crisis and Afghan-Iraq war. Along with the dramatic changes in the concept and the aspect of terrorism, the world has faced to various changes in communication over the centuries. As technology has progressed, terrorist groups have moved from the cassette tape era to that of videotape, and to that of the sophisticated options available across the internet. As the high-end technology has made progress and terrorists have taken advantages, internet has become as their 'nerve system.' Not only do they communicate through the internet, but use it for may different areas such as propaganda, transfer of funds, and installing holy-academies to support self-indoctrination of terrorists. By using the internet the terrorists wage psychological warfare to confuse their enemies and instill fear in the minds of the public. Such phenomenon has increased rapidly over after the events of 9/11 and has become a very important factor in transnational terrorism. However, even a decade after the terrorists or extremists mastered the use of the internet, government policy and decision-makers have done little to address the problem. Therefore, it requires more progressive actions from UN and other institutions that will influence governments to develop effective and enduring policies. Furthermore, each government should not only take their actions for a clear and distinct benefit for themselves, but also need to take their attitudes based on international law and prepare the restrictive counter-measures for the reason of peacekeeping.

key word: transnational terrorism, glibalization, nerve system. international cooperation, effort of individual nations