사이버 테러리즘에 대한 국제적 대응에 관한 연구
A Study on International Countermeasures to Cyber-terrorism

김정태, 이현우
한국전자통신연구원
{acroo, lhwoo}@etri.re.kr

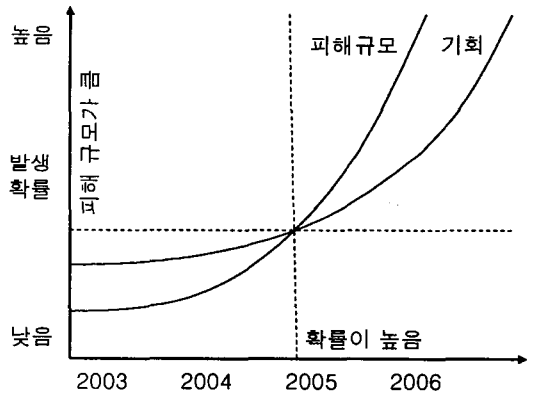
Abstract

Developing into information oriented society, dependency on network systems increases gradually in the area of economy, society and so on. Under that circumstance, temporary stop or damage of integrity of network system may have a strong impact on economic activities and overall society. Recently, threat of cyber terrorism, organized hostile action to government or industry through network, is increasing. Because of the features of network, it is not sufficient only a nation's countermeasure against Cyber terrorism, so international cooperation is needed We review the status of countermeasure against cyber terrorism and examine several considerations for policy establishment.

1. 서론

2001년의 9·11 테러 이후, 현실 세계와 사이버 공간의 특별한 구분 없이 테러리즘에 대한 우려가 점진적으로 고조되고 있다. 금융, 운송, 항공, 전력 등 사회 주요 기반시설에 대한 물리적 테러뿐만 아니라, 사이버 테러리즘에 의한 위협에 따라 체계적인 정보보호 대책의 수립이 무엇보다도 중요하게 인식되고 있다. 이로 인해, 국내외 여러 정부는 사이버 테러리즘에 대응하기 위한 대책을 마련하려는 노력을 기울이고 있으며, 지속적인 검토와 실험을 수행해 오고 있다. 물론, 물리적 또는 사이버공간상의 어떠한 위협에 대해서도 체계적인 대응을 수립하는 것이 중요한 일이겠으나, 9·11 테러 이후 각국이 서둘러 발표하고 있는 대책은 논리성이 결여된 급조된 것이라는 시각도 많다. 사이버 테러리즘이 지닌 물리적 테러리즘과의 차이를 고려하지 않고서 해결책만을 찾으려 한다면, 이는 미봉책에 그칠 공산이 크다.

네트워크 인프라가 구축되고, 개개인과 국가가 네트워크에 상당부분을 의존하기 시작하면서, 이를 통한 테러는 테러리스트들에게는 매력적인 경로를 제공해주게 되었다. 그럼에도 불구하고, 9·11 테러 이전부터 현재까지 사이버 테러리즘이라 명확히 규정될 만한 사건은 발생하지 않았다. 국제적 테러의 주요 대상국이었던 미국에서도 지난 10년 동안 네트워크를 이용해 대규모 파괴도 일어거나 사망과 같은 인명피해가 있었던 사건은 아직 발생하지 않은 상황이다. 9·11 테러에 대해, 국제적 정세가 테러리즘에 의해 위협을 받게 되는 단계로 들어섰다는 신호탄이 되었다는 해석도 있었으나, 현재까지의 상황을 종합해 볼 때 9·11 테러는 단발성 사건에 지나지 않다고 해도 과언이 아니다. 그렇지만, 사이버 테러리즘은 단 한 차례의 사건으로도 그 피해가 예상치 못한 규모로 확산될 가능성이 있기 때문에, 국가 안보에 대한 개념에 사이버 테러리즘을 중요하게 고려해야하는 상황이 도래한 것은 확실하다 (그림1). 국가 안보가 보다 예측 불가능한 국면으로 전환됨에 따라, 국가 안보에 위협을 주는 대상을 명확히 규정하고 정확한 대응책을 마련하여야 한다.



(그림 1) 사이버 테러리즘의 기회와 피해규모의 관계 (출처: Kevin Coleman, "Cyber Terrorism", 2003. 10.)

사이버 테러리즘의 대상을 규정하는 과정에 있어서의 장애물로는, 네트워크를 이용한 테러는 그 주체를 규정하기 곤란하고 시작점을 파악하는데 많은 시간이 소요된다는 점을 들 수 있다. 테러의 주체가 악의적인 목적이 없는 단순한 의도의 해커 (recreational hacker)인지, 특정 집단이나 특정 국가가 양성한 정규군에 의한 것인지를 파악하기 어렵기 때문에, 대응의 수위를 결정하기가 난해한 상황

이 된다. 또한, 테러의 배후가 파악되었을 경우에, 이에 대한 반격이 가능한 것인가를 결정하는 것도 쉽지 않다. 국제법과 관련된 문제나, 사이버 테러를 물리적 보복으로 연결시킬 수 있는 가에 대한 문제 등이 명확하지 않기 때문이다. 사이버 테러가 행해지는 형태가 다양하고, 그 피해의 규모 또한 다양하기 때문에 정확한 원칙이 적절히 세워져 있어야만 한다.

본 논문에서는 이러한 사이버 테러리즘에 대한 문제들에 대한 논의에 앞서, 논의의 대상을 명확히 하기 위해 사이버 테러리즘의 정의와 특징을 살펴보고, 사이버 테러리즘의 어떠한 요소가 우리에게 위협이 될 수 있는지 살펴본다. 이어, 국제적인 대응이 어떻게 이루어지고 있으며, 추가적으로 고려해야할 사항들에 대해 검토해 보고자 한다.

2. 사이버 테러리즘의 정의와 특징

1990년대 여러 국가들이 점차적으로 네트워크 의존적으로 변화함에 따라서, 여러 전문가들은 네트워크가 집단간, 또는 국가간 공격의 새로운 대상이 될 수 있다는 예상을 내어놓기 시작하였다. 이러한 걱정스런 예상은 9·11 테러 직후부터 점진적으로 과장되기 시작하였으며, 위협적인 예상으로 변모하기 시작하였다. 사이버 테러리즘의 개념 정의에 대한 애매함은 대중들을 호도하고 본질을 왜곡해 왔다. 이러한 개념의 변질을 고려할 때 사이버 테러리즘을 명확히 규정하는 것은 매우 중요하다. 네트워크를 이용하여 특정 대상에 대해 이루어지는 모든 공격이 사이버 테러라고 보기는 어려우며, 개인의 이익을 추구하고자 이루어지는 사이버 범죄와는 달리 사이버 테러는 네트워크와 네트워크에 연결된 사회 기반시설의 위협을 목적으로 한다는 차이를 고려하여야 한다. 근래 웜이나 바이러스가 국제 네트워크의 위협요소로 대두되는 일이 잦아졌다. 이러한 악성코드는 대부분 개인의 장난이나 호기에 의한 단순 범죄에 지나지 않은 상황이지만, 만약 이러한 사건이 특정 집단이나 국가가 의도적으로 관여하여 테러의 대상을 위협하려 한다면, 국가의 안보에 있어 매우 중대한 위협 요소가 될 수 있을 것이다.

현재 주로 사용되고 있는 사이버 테러리즘에 대한 정의에 따르면, '사이버 테러란, 정부나 시민을 위협하려는 목적으로, 사이버 툴을 사용해 에너지, 수송, 공공시설 등의 주요 국가 기반시설을 중지시키려고 하는 행위'이다. 공포심과 불안감을 조장하기 위한 목적을 지녀야 한다는 점과, 사이버 툴의 사용, 즉 물리적 수단이 아닌 소프트웨어와 네트워크를 이용한다는 점에서 물리적 테러와 차이를 두고 있다.

사이버 테러리스트들이 기존의 물리적 공격 수단을 버리고 새로운 공격 방법을 선택하게 만드는, 사이버 테러리즘의 장점은 여러 가지가 있다. 물리적 테러에서 그 위협의 실체나 어떠한 위협 세력이 실행한 것인지에 대해서 명확한 검증을 하기는 쉽지 않다. 사이버 테러의 경우에는 이러한 검증이 보다 어렵다. 사이버 테러를 수행하고 있는 곳과 공격의 피해를 입고 있는 곳이 지리적으로 상당한 거리를 두고 있는 경우가 대부분이기 때문에, 위협 세력의 실체뿐만 아니라, 어디에서 공격을 가하고 있는지, 언제 시작된 것인지 파악하는 것이 거의 불가능하다. 사이버 테러리스트들은 자신의 신분과 위치를 위장하기 용이하다는 장점에서 사이버 테러를 선택하게 된다. 또한, 물리적 테러는 자금과 인력의 준비 단계가 중요하지만, 사이버 테러는 최소한의 인원과 컴퓨터 몇 대만으로도 공격을 시작할 수 있다. 테러를 자행하는 집단과 국가가 대부분 많은 자금을 운용하기 어려운 상황에서 이러한 이점은 크게 작용할 수 있다.

물리적 테러는 인명이나 특정 시설에 대한 물리적 파괴를 대상으로 한다. 그러나 사이버 테러는 피해규모가 국가 규모의 기능 마비가 가능하며, 상황에 따라서는 그 이상도 가능하다. 사이버테러리즘의 피해는 테러리스트들이 예상하지 못한 규모로 증폭될 가능성도 있다. 또한, 사이버 테러는, 공격의 형태가 다양하게 변화할 수 있다. 공격 코드의 일부 수정을 가하는 것만으로도 몇 분에서 몇 일간 공격을 하는 것도 가능하며, 특정 목표에서 다수의 목표로 대상을 확대할 수 있다.

사이버 테러로 인한 피해는, 사이버 테러리즘을 계획한 주체의 의도에 따라 다양하게 나타난다. 금융 네트워크나 시스템의 마비를 통한 경제의 붕괴에서부터 국가 방호 체계의 혼란을 일으켜 물리적 공격을 유도하는 것에 이르기 까지 예상하지 못한 범위에 이를 수 있다. 이러한 사이버 테러로 인한 직·간접적인 피해로는 다음과 같은 것들이 있다.

- 테러로 인해 중단된 기반시설의 재가동 비용
- 테러의 주체 파악을 위한 시간과 비용
- 사회 기반시설에 대한 신뢰의 하락
- 국민의 정부와 정보통신 산업에 대한 불신
- 국가의 국제적 이미지 손실

3. 사이버 테러리즘에 대한 대응

최근 세계 각국은 사이버 테러리즘을 국가 안전 보장의 중대한 위협으로서 인식하고 자국 내의 대응 체계와 조직 정비뿐만 아니라, 국제적인 대응에도 많은 노력을 기울이고 있다.

이는 모두 세계적으로 우리들이 직면한 여러 테러리스트 위협을 저지하기 위하여 국가 간의 역량을 강화해야할 부분이다.

- 국제적인 조직의 유기적 활동

현재, 아시아태평양경제협력체(APEC)나 경제협력개발기구(OECD) 등의 국제기구들은 사이버 테러리즘 문제에 대해 유기적인 관계를 유지하며, 국제회의에서의 사이버 테러리즘 대응 문제의 우선순위를 높이는 데 주력하고 있다.

- 테러리즘 대응 지원 프로그램

물리적 테러나 사이버테러의 주 대상이 되고 있는 국가나, 향후 테러가 발생할 가능성이 높은 국가를 중심으로, 테러리즘 대응 지원 프로그램 등을 통해 재정적 지원이 이루어지고 있다. 이러한 프로그램들은, 사이버 테러리즘에 대한 대응 기법 확보,

사이버 테러리즘을 조사·분석하는 기법의 발굴, 사이버 사건의 문제를 다루는 기관들 간의 공조 등에 필요한 지원을 수행하고 있다.

- 연구·개발 지원

주요 사회기반 시설을 향한 위협을 저지하기 위한 기술의 연구·개발에 대한 지원활동이 이루어지고 있다. 사이버 보안, 정보 분석, 물리적 방위 등의 영역에서 기술 발전에 필요한 각 기구간의 협조가 진행되고 있다.

여러 연구·개발 프로젝트를 통해 국방, 운송 및 주요 기반시설과 중대한 관련이 있는 컴퓨터 네트워크이 대한 위협을 방어하고 완화하는 것에 집중하고 있다. 또한, 사이버 테러리즘에 맞서 컴퓨터 시스템들을 강화하기 위한 검출, 방어, 응답, 경보 능력을 강화하는 데 목표를 두고 있다.

- 외교.

외교는 사이버 테러리즘의 확산을 차단하는 핵심적인 요소이다. 테러리스트들은 각국을 누비며 테러 행위를 자행하며, 세계의 어느 지역에라도 영향을 미칠 수 있다. 북대서양조약기구(NATO), 서방7개국정상회담(G7), 국제연합(UN), 동남아시아국가연합(ASEAN), 미주기구(OAS), 유럽안보협력기구(OSCE) 등의 다양한 조직들은 국제적 또는 지역적인 수준에서 유기적으로 밀접하게 공조해 나가고 있다.

- 테러리즘에 대한 자금조달의 저지

9·11 테러 이후, 170개 이상의 국가와 사법권은 테러리스트의 자산들을 동결하기 위하여 자금 조달과 관련한 금지령을 발하였다. 이를 통해 테러리스트들이 자금을 모으거나 이동시키는 것을 저지하고 있다. 테러리즘과 관련한 문제를 다루고 있는 국제법의 수가 증가하고 있으며, 30여개 국가가 9·11 테러 이후에 수립된 10여개의 주요 국제법에 서명한 상태이다. 국제법 뿐만 아니라, 국내법을 통해서도 여러 국가들이 테러리스트의 조치를 제한하는 법을 제정하고 있으며, 이러한 법을 기꺼이 실시해 나가고 있다.

4. 사이버 테러리즘에 대한 고려 사항

현재 사이버 테러리즘과 관련한 국제적 대응책을 살펴보면, 대부분이 테러 발생이전에 테러의 발생을 차단하는 것에 주력하고 있다. 그러나 테러리즘의 발생 이후 이를 어떻게 해결할 것인가에 대해서는 별다른 노력을 기울이지 못하고 상황이다.

현재 사이버 범죄에 대한 국제적 조약은 몇 가지 수립되어 있으며, 많은 국가들이 이러한 조약에 체결되어 있다. 이를 통해 이미 발생한 범죄 행위에 대해서, 국가간 공조와 협력을 통해 사이버 범죄에 효과적으로 대응하고 있다. 그러나, 소수에 의해 이루어지는 사이버 범죄와는 달리 사이버 테러리즘은 조직적인 체계를 갖추고 이루어지는 경우가 많기 때문에, 사이버 범죄와 관련한 조약으로 사이버 테러리즘에 다루기는 어려우며, 사이버 테러리즘만의 특성에 대한 고려와 논의를 통해 신규 조약 체결 등의 해결책이 필요하다.

4.1 사이버 테러와 물리적 테러의 혼합 공격에 대한 대응

사이버 테러리즘의 대응을 어렵게 만드는 문제들 중의 하나는 사이버 테러가 물리적 테러와 연계하여 발생하는 경우, 이를 어떻게 해석하고 대응해야 하는가이다. 일반적인 사이버 테러는 독립적으로 행해진다는 것을 염두에 두고 있으나, 실제로 물리적 테러와 병행해 수행되는 경우도 고려되어야 한다. 물리적 테러리즘에 대한 대응과 사이버 테러리즘에 대한 대응을 별개로 구분하여 법안이나 조약을 제정할 경우, 두 가지 형태의 테러가 같은 집단이나 국가에 의해 동시에 행해진다면, 두 가지 형태를 구분해서 대응할 것인지 또는 어느 하나를 다른 쪽에 포함시켜 대응해야 할 것인지에 대한 우선적인 기준 정립이 필요하다.

국제연합헌장의 2조 4항, '무력행사금지 원칙'에 따르면, '다른 국가의 영토보전이나 정치적 독립에 대하여 어떠한 방식이든 무력의 위협이나 무력행사를 금지'하고 있다. 정치적 목적 등의 사이버 테러에 대해 어떠한 대응을 할 수 있느냐는, 이러한 조항에서의 무력 의미하는 바를 규정하여야 한다. 무력이 물리적 군사력을 말하는 입장이 통설이 되고 있기 때문에, 네트워크를 통한 사이버 공격이나 보복은 국제연합헌장에서 금지하고 있는 무력의 범위에 포함되지 않게 된다. 이러한, 새로운 공격의 형태가 나타난 이상, 기존의 물리적 공격과 사이버 공격을 명확하게 구분 지을 필요가 있다.

4.2 공격의 주체에 따른 대응

사이버 테러를 감행한 주체가 누구인가에 따라서 대응이 달라질 수 있다. 사이버 테러를 감행한 주체가 개인인지 혹은 국가인지에 따라서 처벌을 할 것인지, 보복 공격을 할 것인지가 결정되게 된다. 개인의 테러 행위를 국가에 귀속하여 해석할 것인지, 이를 다른 차원의 행위로 볼 것인지에 대한 체계적인 검토가 필요하다.

공격의 주체가 집단이나 국가로 규정되었을 경우에는, 공격에 가담한 사람을 전투원으로 볼 것인지, 비전투원으로 볼 것인지에 구별 기준이 필요하다. 제네바 협약에 따르면, '전투원은 이를 식별할 수 있는 복장이나 표지를 착용 또는 부착해야한다'고 되어 있다. 비정규전인 물리적 테러에서는 이러한 의무가 무시되어 테러리스트들이 민간복장이나 적군 군복을 입고 공격을 가하는 경우도 있으나, 최소한 무기의 휴대 등에 의해 일반인과는 구분되는 특징을 가지고 있게 된다. 그러나 네트워크를 이용한 공격에서는 이러한 규정으로 전투원과 비전투원을 구분하기는 현재로서는 불가능하다.

4.3 공격의 개시 시점에 대한 해석

사이버 테러를 무력공격의 한 종류로 규정한다면, 어느 시점에서 공격이 시작되어, 교전 상태에 들어갔는지에 대한 판단이 필요하다. 국제 무력분쟁법에서는 교전을 시작한 주체와 더불어 교전의

시작 시기를 규정하도록 하고 있는데, 물리적 공격과는 달리 사이버 테러에는 명확한 개전의 시기가 명확하지 않기 때문에, 교전의 시작 시기와 관련된 국가간 해석의 이견이 발생할 소지가 있다.

4.4 공격이 이루어진 곳에 따른 대응

공격의 주체가 어디에서 공격을 감행하였는지에 따라 처벌을 달리 하여야 한다. 사이버 테러리즘은 공격하는 장소와 공격을 당하는 장소가 서로 다른 법적 관할권에 있을 수 있기 때문에, 공격의 주체를 어느 국가에 귀속시켜야 하는 가에 대한 명확한 판단이 필요하다. 현재 국제법상 범죄행위는 소극적 속인주의에 따르고 있기 때문에, 범죄행위의 주체가 개인인 경우 피해국이 관할권을 설정할 수 있으나, 사이버 테러리즘을 단순한 범죄행위로 간주해 처리하는 것은 곤란하다. 피해국이 사이버 테러를 행한 사람의 인도를 요구할 경우에, 용의자를 억류하고 있는 국가와의 협상에서 문제가 발생할 경우, 용의자를 억류하고 있는 국가가 테러 지원국으로 비난받을 수 있으며, 새로운 문제를 야기할 수도 있다. 또한, 사이버 범죄 조약을 체결한 국가들 간에서는 협조 체제가 이루어질 수 있으나, 어느 한 국가가 국제 조약을 체결하지 않은 국가일 경우에는 큰 분쟁 요인이 될 수 있다.

4.5 테러 대응의 결정

국제연합헌장 41조, '보충성의 원칙'에는 '안전보장이사회는 그의 결정을 집행하기 위하여 경제관계 및 철도·항해·항공·우편·전신·무선통신 및 다른 교통통신수단의 전부 또는 일부의 중단과 외교관계의 단절을 포함하는 등의 병력의 사용을 수반하지 아니하는 조치를 취하도록 의결할 수 있다'고 규정하고 있으며, 51조, '자위권 발동 요건'에는 '회원국에 대하여 무력공격이 발생한 경우 개별적 또는 집단적 자위권 행사가 가능하다'고 기술되어 있다. 사이버 테러를 당한 국가가, 사이버 테러를 무력공격으로 자의적으로 규정하거나, 병력의 사용을 수반하지 않았다는 해석을 통해 자국의 안보를 위한 조치로 사이버 보복이 허용되는 것인지에 대한 문제 등 발생할 수 있다. 또한, 사이버 보복이 금지된 행위가 아니라 하더라도, 상대국에 대한 국내 문제 불간섭 의무에 반하는 것이 되어 국제 위법행위에 해당하는지에 대한 판단이 내려져야 할 것이다.

5. 결론

현재, 일반적인 사람들이 인지할 만한 사이버 테러 사건이 발생한 적이 없기 때문에 네트워크 인프라가 상당히 구축되어 있는 국가에서도 사이버 테러리즘에 대한 인식의 수준이 낮은 상황이다. 사이버 테러리즘이 발생할 수 있는 충분한 조건이 이미 만족되어 있다는 것을 각국 정부나 국민들에게 인식시켜 나가는 것이 필요하다. 또한, 사이버 범죄와 사이버 테러리즘이 사회의 윤리에 반하는 것임을 각인시키고, 사이버 공간에서도 일정한 규칙을 지켜야 한다는 것의 중요성을 이해할 수 있도록 하는 노력이 필요하다.

사이버 테러리즘의 공격은 사회 주요 기반시설을 대상으로 한다. 이러한 기반시설은 국가가 관리하고 있는 영역만을 대상으로 하는 것이 아니라, 민간의 시설도 포함될 수 있다. 따라서 사이버 테러리즘을 차단하는 노력을 기울이거나, 또는 테러 이후의 피해와 원인을 분석하기 위해서는 정부와 민간의 협력 체제 확립이 필요하다. 국내의 경우를 살펴볼 때 정보보호와 관련한 생산업체들이 작은 규모의 벤처기업의 형태인 경우가 많다. 정부는 한 공업 중심의 방위 산업 뿐만 아니라 이러한 부분이 대해서도 산업 육성의 노력을 기울여 나가야 할 것이다.

사이버 테러리즘은 사이버 테러리즘과 관련한 조약을 체결한 동맹국 중에서 가장 취약한 지점을 노리 경로를 확보한 다음 다른 동맹국의 정보 통신망이나 사회 기반시설에 위해를 가할 수 있다. 이를 방지하기 위해 사이버 테러리즘에 관한 각국의 기술 격차를 최소한으로 줄이고, 정보보호와 관련한 국가간 기술적 협력을 꾀하는 것이 중요하다. 또한, 사이버 테러리즘은 새로운 형태의 행위이기 때문에, 법적인 측면에서 완전한 정비가 되어 있지 않다. 본 논문에서 살펴본 사이버 테러리즘에 대한 국제적인 고려사항과 함께 자국법과 관련한 미비점에 대해서 어떻게 해결해 나가야 하는지를 명확하게 할 필요가 있다.

사이버 테러리즘에 대한 각국의 여러 가지 대응책이 마련되고 실시됨에도 불구하고, 새로운 난관이 나타날 수 있다. 대응책이 성공적이면 성공적일수록, 테러리스트들은 보다 새롭고 취약한 목표물을 물색해 나갈 것이다. 여러 영역에서 대응책을 마련하는 등의 철저한 준비와 지속적인 경계가 필요할 것이다.

참고문헌

[1] Department of Defense, Office of General Counsel, "An Assessment of International Legal Issues in Information Operations", 1999. 5.

[2] US-CERT, "International Coordination for Cyber Crime and Terrorism in the 21st Century", 1999. 12.

[3] Christopher C. Joyner and Catherine Lotrionte, "Information Warfare as International Coercion: Elements of a Legal Framework", EJIL, Vol. 12 (2001) No. 5

[4] Abraham D. Sofaer, Seymour E. Goodman, "The Transnational Dimension of Cyber Crime and Terrorism", 2001.

[5] Anthiny H. Cordesman, "Cyber-Threats, Information Warfare, and Critical Infrastructure Protection", CSIS, 2002

[6] Rohas Nagpal, "Cyber Terrorism in the Context of Globalization", 2002. 9.

[7] Kevin Coleman, "Cyber Terrorism", 2003. 10.