한국경호경비학회 – 제40호(2014): 109–145
투고일 2014. 07. 30, 심사일 2014. 09. 07, 게재확정일 2014. 09. 14

새로운 안보환경을 둘러싼 사이버 테러의 위협과 대응방안

윤 민 우

새로운 안보환경을 둘러싼 사이버 테러의 위협과 대응방안: 쟁점들과 전략적 접근 틀에 대한 논의*

윤 민 우**

〈요 약〉

그 동안 사이버 테러와 관련하여 우리나라에서 많은 양질의 지식이 축적되어 왔음에도 불구하고 몇 가지 매우 중요한 취약점이 지적될 수 있다. 그리고 이러한 취약점을 극복해 보려는 시도가 이 논문의 주요 논제이다. 기존 사이버 테러관련 논의나 연구를 살펴볼 때 아쉬운 점으로 파악되었던 사항은 사이버 테러와 관련된 여러 현상들이 빚어내는 미래의 안보환경에서 국가안보전략 개발이라는 거시적 프레임에서 사이버 테러문제를 접근하는 논의가 없었다는 점이다. 이 논문은 이러한 사항에 중점을 두고 사이버 테러에 대한 논의를 전개할 것이다. 바꾸어 말하면 이 논문의 목적은 안보위협의 한 양식으로서 사이버 테러가 던지는 국가안보위협의 의미를 재평가하고 미래안보환경에서 국가안보전략 개발이라는 틀 속에서 사이버 테러의 문제를 재조명 한다.

이 논의에서 다루는 사이버 테러에 관련된 몇 가지 쟁점들은 사이버 공간이 추가된 미래 안보환경에서 국가안보의 전략적 접근 틀의 구성에 중요한 메시지를 전달한다. 미래 환경에서 사이버라는 새로운 특성을 가진 공간 환경이 국가안보와 사회 및 개인안전에 중요한 외부조건의 하나로 추가되었다는 사실을 직시하고 기존의 4차원에 사이버가 추가된 5차원 공간환경에서 어떻게 새로운 국가안보전략이 마련되어야 하는지에 대한 기본 전략 틀이 마련되어야 한다. 이러한 전제위에 미래의 기술진보의 양상과 방향이 파악되어야 하고, 위협의 주체와 성격과 유형이 분석되어야 한다. 사이버 테러의 위협과 성격은 이런 맥락에서 다루어져야한다. 한편 이러한 기반위에 다시 사이버 테러를 포함한 여러 미래사회에 예상되는 위협들과 위협 주체들에 대응하기 위한 방안들이 기능과 시스템 면에서 동시에 수립되어야 한다.

주제어 : 테러리즘, 사이버 테러, 국가안보, 사이버 안보, 사이버 범죄, 사이버 전쟁

* 이 논문은 현재 진행 중인 한반도 사이버 테러 위협과 대응방안에 대한 연구의 일부를 발췌하여 작성되었음.

** 가천대학교 경찰안보학과 부교수, 범죄학 박사, 국제정치학 박사수료.

목 차

Ⅰ. 머리말

지난 10, 20년간 국내에서 사이버 테러가 던지는 위협과 이에 대한 적절한 대응의 필요성을 제안하는 지적들은 많이 있어왔다. 많은 연구자와 전문가들 (김상욱·신용태, 2010; 김승권·김상국·최종화, 2008; 김홍석, 2010; 서동일·조현숙, 2011; 윤해성·윤민우·Freilich·Chermak·Morris, 2012; 이재은·양기근·류상일, 2008; 임영갑, 2010; 조성현·이택규·이선우, 2014; 최광복, 2011; 홍성표, 2011)이 사이버 테러가 던지는 문제의 심각성과 까다로운 속성들을 지적해 왔으며, 이와 관련된 법률적 제안과 국가제도나 정책적 제언, 그리고 구체적인 대응기술 개발에 대한 소개나 제안 등이 여러 논문이나, 보고서 등의 형태로 이미 나와 있다. 사이버 테러 분야에 관심을 가지는 누구라도 적은 수고를 들이면 그러한 많은 이 분야 전문가들이 생산해 낸 참고할 만한 자료들을 쉽게 이용할 수 있고 이 분야에 대한 이해도를 높일 수 있다.

이제까지 축적되어온 국내의 사이버 테러 관련 지식들을 정리해보면 대체로 다음

과 같은 사실을 알 수 있다. 우선 사이버 테러는 전통적인 적성국가로부터의 전쟁위협이라는 국가안보위협과는 다른 새로운 특성을 가지는 국가안보에 대한 주요한 위협이다. 사이버 테러는 적성국가 뿐만 아니라 개인과 조직화된 사적 집단에 의해서도 행해질 수 있으며, 이는 국가의 기간시설 마비나 대규모 재난, 주식 시장이나 전기 공급 등의 대규모 혼란과 같은 경우를 통해 국민의 삶과 생명, 안녕과 사회질서, 국가 안위에 심각한 위협을 초래할 수 있다. 이러한 사이버 테러는 기존의 전통적 안보위협처럼 시간적 지리적 제약이 없으며 언제, 어디서든 발생할 수 있는 지리적, 시간적 무경계성 또는 무제한성을 띠며 가해자 역시 신속히 파악할 수 없는 은밀성을 띤다. 이처럼 전통적 국가안보 시스템이 작동하기 어려운 새로운 형태의 안보위협을 초래하지만 아직 우리사회는 이러한 위협에 대한 인식과 대응이 부족하다 (김홍석, 2010; 윤해성 외, 2012).

둘째, 사이버 테러가 주는 새로운 성격의 안보위협은 정부, 군, 사법기관, 민간, 학계 등의 긴밀한 협력과 이러한 국가 전 부문의 포괄적이고 통일된 대응을 요구한다. 이러한 총체적, 체계적, 포괄적 대응을 위해서는 단일화된 포괄적으로 정비된 법률조항과 이에 기반을 둔 국가 컨트롤 타워가 작동해야 한다. 미국, 영국, 독일 등 여러 주요 동맹국들의 사례는 그러한 사실을 단적으로 보여준다. 하지만 우리나라는 아직 단일화된 형태의 총괄적인 법률 조항이 존재하지 않으며, 컨트롤 타워 역시 사실상 작동하지 않는다. 즉, 우리나라의 사이버 테러 대응은 결정적으로 취약하고 미비하다. 때문에 산만하고 파편화된 법률의 통합과 정비, 그리고 국가 컨트롤 타워의 구축과 작동은 시급히 요구되는 사항이다 (김홍석, 2010; 이재은 외, 2008).

셋째, 사이버 테러에 대한 효과적 대응을 위해서는 인적, 물적 인프라 구축과 육성이 절실하다. 특히 이는 사이버 테러 부문에서의 빠른 기술 발전과 북한, 중국 등의 우리 주변의 실제적, 잠재적 위협국가 들이 사이버 테러 혹은 사이버 전쟁 부문에 막대한 투자와 노력을 경주하고 있다는 사실을 감안할 때 더욱 그러하다. 하지만 우리의 경우 군에서 주도하는 사이버 사령부 역시 아직 상대적으로 초기 단계에 불과하며, 국정원, 경찰, 검찰, 인터넷 진흥원 등 사이버 테러 관련 주요 담당 기관들에서 인적, 물적 자원의 부족과 열세가 공통적으로 주요한 문제점으로 지적되고 있다. 이 때문에 사이버 수사, 사이버 테러 대응, 사이버 위협거부 및 방호, 사이버 정보활동, 사이버 전쟁 수행 등 사이버 테러 대응과 관련된 많은 분야에서 지속적인 기술과 장비 개발, 그리고 우수한 인력자원의 양성은 우리국가가 시급히 관심을 기울이고

노력을 경주해야 할 사안이다 (김승권 외, 2008; 배달형, 2011; 홍성표, 2011).

한편, 주로 법학자나 법률 전문가 또는 행정학 등의 사회과학자 들이 생산해 낸 논문이나 보고서 등이 위에 제시한 그러한 내용들을 지적해온 것과는 달리 IT(Information Technology) 분야 전문가들이나 학자들이 생산한 논문이나 보고서 등은 특정 사이버 공격 방법에 대한 대응기법이나 기술 개발을 제안하는 내용들을 주로 담고 있다. 해킹이나 스파이 웹, 분산거부공격 등과 같은 외부적 침해로부터 장비와 시스템을 어떻게 방어할 것인가의 기술적 문제나 네트워크 시스템 전반에 대한 보호와 관련된 기술적 제안 등이 이들이 생산해 낸 정보나 지식의 주를 이룬다 (서동일·조현숙, 2011; 조성현 외, 2014).

하지만 그 동안 사이버 테러와 관련하여 우리나라에서 많은 양질의 지식이 축적되어 왔음에도 불구하고 몇 가지 중요한 취약점이 지적될 수 있다. 그리고 이러한 취약점을

극복해 보려는 시도가 이 논문의 주요 논제이다. 첫째, 그 간 생산된 논문이나 보고서의 취약점 가운데 하나는 사이버 테러 또는 사이버 테러리즘이라는 용어가 불분명하게 일관되지 않게 다루어지고 있다는 점이다. 이러다 보니 실제로 같은 표현이더라도 글쓴이에 따라 다른 내용을 담고 있는 경우가 빈번하다. 예를 들어, 사이버 테러라는 주제로 어떤 논문은 사이버 전쟁과 네트워크 통합전쟁에 대해 논의하고 있는가 하면 (김승권 외, 2008; 김승주, 2013; 김홍석, 2010), 해킹이나 봇넷, 분산거부공격과 같은 특정 기술에 대해 논의하기도 하며 (문종식·이임영, 2010; 정기석, 2012), 경우에 따라서는 사이버 테러가 실제로는 사이버 범죄를 의미하기도 한다 (김연준·옥정석, 2011; 안유성, 2013). 또한 사이버 테러가 이처럼 글쓴이의 인식에 따라 실제로 담고 있는 내용들이 결정되다 보니 사실상 주요한 안보위협 사안임에도 불구하고 사이버 테러의 논의에서 제외되는 경우도 발생한다. 보다 구체적으로, 최근 들어 서유럽이나 북미 등에서 주요한 문제로 대두되고 있는 테러리스트의 사이버 공간의 이용문제나 사이버 도박이나 사이버 심리전 같은 범죄자나 적성국가에 의한 사이버 공간의 이용문제는 그 문제가 심각하며 사이버 테러논의와 밀접한 관련이 있음에도 불구하고 논의 자체에서 빠지는 경우들이 나타났다.

물론 테러리즘이나 사이버 테러 같은 용어의 정의가 사실상 어렵고 정의하는 주체의 주관적 인식에 의해 크게 좌우되고 있음은 사실이다. 하지만 엄밀한 용어의 정의를 목적으로 하지는 않더라도 가급적 현재 주요한 위협이 되는 사이버와 관련된

여러 현상들을 포괄적으로 수집하여 그 특징과 속성을 논의함으로서 사이버 테러가 갖고 있는 복잡하고 포괄적인 속성을 보여주려는 노력은 의미가 있을 것이다.

그러나 아쉽게도 그 간의 우리나라 연구에서는 이러한 노력이 부족하다고 판단된다. 특히 범죄자나 테러리스트에 의한 공간으로서의 인터넷 사용 문제는 그 문제의 근원적 심각성에 불구하고 사이버 테러의 논의에서 거의 다루어지지 않았다. 또한 사이버 범죄, 사이버 테러, 사이버 전쟁과 같이 혼용되어 사용되는 여러 사이버 위협의 문제도 어떻게 유형별로 구분하고 그 속성과 대응방법의 차이점에 대해 접근할 것인지의 모색도 있어야 할 것이다. 이 문제 역시 그 간의 국내 논의에서는 명쾌하게 해소되지 않았다.

사이버 테러와 관련한 기존 연구보고서나 논문의 또 다른 아쉬운 점은 특정 법률적, 정책적, 기술적 대응이라는 파편화된 지엽적 논의에 그치고 있다는 것이다. 사이버 테러와 관련하여 대체로 특정 법률안이 필요하다거나 (김연준·옥정석, 2011; 김홍석, 2010; 정기석, 2012) 특정 정부 기구나 협력 시스템이 만들어 져야 한다거나 (김연준·옥정석, 2011; 이재은 외, 2008; 정기석, 2012) 아니면 특정한 기술적 대응방식이 적용되어야 한다거나 (김승권 외, 2008) 하는 식의 논의가 주류를 이루고 있다. 물론 이러한 논의가 주요한 의미가 있다. 그러나 사이버 테러의 문제는 21세기 환경조건의 변화와 새로운 폭력 또는 파괴양식의 한 징후로서 나타나는 위협이라는 보다 근본적인 성격을 가진다는 것에 주목해야할 필요가 있다. 때문에 미래사회에서 전반적인 국가안보의 리모델링이라는 총괄적이고 거시 전략적 관점에서 사이버 테러문제를 전일적으로 접근하는 노력이 필요하다고 할 수 있다. 그리고 이는 앞서 언급된 법적, 정책적, 기술적 대응방안들을 어떻게 유기적으로 결합하고 조율하여 국가안보전략이라는 거시적 틀에서 재창조 할 것인가의 문제와 연결된다. 하지만 지금까지 이러한 근본적이고 거시적 국가안보전략의 틀을 리모델링하는 시각에서 사이버 테러나 안보위협을 접근하는 연구보고서나 논문은 드물었다. 이러한 근본적 안보전략 틀에 대한 논의의 부재는 사이버 테러 대응을 단기적 상황에 대한 대응이나 파편적인 현상 대응에 매몰되도록 유도하며 이는 미래사회에서의 국가안보의 치명적 공백으로 이어질 위험성을 초래한다.

이는, 이 논문에서 앞으로 보다 구체적으로 논의하겠지만, 사이버 테러의 문제는 폭력수단의 민주화 (Democratization of Violence)라는 21세적 시대현상과 미래전쟁에서의 사이버 공간의 전쟁공간으로의 편입 (Reed, 2008), 그리고 범죄, 테러, 전쟁이라

는 각기 다른 폭력 양식의 전일적 통합화라는 여러 시대적 환경조건이 변화하는 추세 속에서 미래사회의 국가안보를 담보해내기 위해 우리국가의 형사사법제도와 군, 정보기관 등의 전체 시스템을 어떻게 리모델링할 것인가의 보다 근원적인 틀에서 접근해야만 할 연구주제이다. 즉, 국가의 미래 안보전략과 형사사법 전략이라는 전체 그림 속에서 사이버 테러의 문제가 접근되어야 한다.

사이버 테러의 위협과 대응이라는 주제로 논문을 쓰면서 갖게 되는 가장 큰 부담감은 이미 기존에 많이 보고된 지식이나 정보를 다시 되풀이하여 제시하지 않을까하는 점이다. 흔히 '수레바퀴의 재발명'이라고 알려진 이러한 이미 알려진 지식의 되풀이 된 제안은 비록 표절은 아니라 할지라도 논문의 가치 그 자체를 심각하게 훼손시키게 된다. 따라서 이 논문에서는 가급적 사이버 테러와 관련하여 기존에 이미 제시된 사항들에 대해서는 논의를 회피한다. 같은 맥락에서 이 논문은 주로 기존의 사이버 테러관련 논의나 연구에서 지적되지 않았던 사항들을 중심으로 논의를 전개할 것이다.

앞서 지적한 것처럼 기존 사이버 테러관련 논의나 연구를 살펴볼 때 아쉬운 점으로 파악되었던 사항들을 고려하여 사이버 테러에 대한 논의를 전개할 것이다. 바꾸어 말하면 이 논문의 목적은 안보위협의 한 양식으로서 사이버 테러가 던지는 국가안보위협의 의미를 재평가하고 미래안보환경에서 국가안보전략 개발이라는 틀 속에서 사이버 테러의 문제를 재조명한다.

Ⅱ. 테러리즘과 사이버 테러리즘

사이버 테러리즘은 구체적으로 그 용어가 무엇을 의미하는지 명확히 정의되어 있지 않다 (김홍석, 2010: 321-326). 때문에 사이버 테러 또는 사이버 테러리즘이라는 용어는 이 용어를 쓰는 전문가나 연구자, 또는 학자의 주관적 인식에 따라 매우 다양한 의미로 쓰이고 있다. 어떤 경우에 사이버 테러리즘은 사이버 공간상에서의 개인이나 네트워크망 또는 국가나 민간기관에 피해를 야기하는 특정 기법이나 기술을 지칭한다 (문종식·이임영, 2010). 또한 어떤 경우에는 개인 컴퓨터나 포털 사이트, 웹사이트 또는 정보통신망 자체에 대한 파괴나 기능마비, 또는 침해 행위 자체를 의미하기도 한다 (서동일·조현숙, 2011). 이 밖에도 경우에 따라서는 사이버 공간을

통해 야기되는 국가기반시설에 대한 파괴나 불법적 점유, 통제나 파괴 행위를 의미하기도 하며 어떤 경우에는 사이버 공간을 활용한 실제 범죄나 테러 공격행위를 의미하기도 한다 (윤해성 외, 2012). 한편, 사이버 테러는 행위주체에 따라 판별하기도 하는데 그 가해자가 개인이나 범법조직에 의한 범죄행위일 경우에는 사이버 범죄로 테러 행위자에 의한 침해행위의 경우는 사이버 테러로 국가행위자에 의한 조직적 행위는 사이버 테러 또는 사이버 전쟁행위로 받아들여진다 (문종식·이임영, 2010). 경우에 따라서는 사이버 공간을 활용한 정보수집활동이나 심리적 선전, 선동 행위등도 사이버 테러로 불리기도 한다 (이상호, 2011). 이처럼 사이버 테러는 컴퓨터 장치나 디바이스, 사이버 공간, 인터넷, 정보통신망 등과 연관된 여러 서로 다른 유형의 문제 행동 또는 행위들을 지칭하는 명확하지 않은 어떤 용어로 통용되고 있다.

사이버 테러리즘의 용어 정의가 이처럼 불분명한 근본적인 이유는 이 용어가 의미가 불분명한 테러리즘이라는 용어를 기반으로 하여 생성된 데다가 사이버라는 또 다른 불분명한 개념을 포함하여 만들어진 합성어라는 사실 때문이다. 따라서 이중의 불분명성을 동시에 가지고 있기 때문에 사실상 사이버 테러리즘이 무엇을 구체적으로 의미하는지 정의하기가 쉽지 않다. 여기에 더불어 사이버 테러리즘에 대한 논의나 연구를 수행하는 전문가들이나 연구자들의 배경이 IT, 법학, 행정학, 사회학, 범죄학, 국제정치학, 군사학 등 이질적인 다양한 분야를 포함하여 각기 서로 다른 의미로 사이버 테러리즘에 접근하고 있다. 이는 개념의 혼란을 더욱 증폭시킨다. 이외에도 문제를 더욱 복잡하게 만들고 있는 것은 대체로 2001년 9.11 테러를 기점으로 이후 약 14-5년 동안 기술적, 전략적, 환경적 조건이 너무 빨리 급변하여 그간 테러리즘과 사이버, 그리고 사이버 테러리즘의 의미가 모두 상당한 질적 변화를 경험했다는 점이 사이버 테러리즘의 정의문제를 더욱 어렵게 한다.

우선 테러리즘은 9.11 당시의 테러리즘의 개념에서 상당한 질적 변화가 있어왔으며, 현재는 질적으로 다른 의미로 테러리즘이 사용되는 경향이 나타난다 (윤민우·김은영, 2012). 대체로 전통적인 의미에서 테러리즘은 9.11 테러 당시 까지만 하더라도 가해자로서 비국가 행위자 조직이나 개인이 상정되었고 정치적, 사회적, 또는 종교적 목적과 같은 비경제적 또는 비금전적 목적을 달성하기 위해 실행되는 인명살상과 시설물 등의 파괴로 나타나는 불법적인 폭력의 사용이나 사용의 위협으로 정의되었다. 또한 이 과정에서 공공이나 사회, 또는 국가에 대한 심리적 강박이나 위협, 또는 공포의 조장이 주요한 요소로 지적되었으며, 때문에 공공이나 여론과 같은 청

중에 대한 영향력을 미치려는 의도가 주요하게 다루어졌다. 그리고 다중이용시설이나 건물, 교통시설 등과 같은 비군사부문에 대한 공격이 테러리즘 정의의 주요한 한 요소로 간주되었다. 하지만 이러한 전통적인 테러리즘의 이해는 지난 14-5년간 거의 모든 테러의 구성요소들에서 상당한 질적 변화가 일어났으며 전통적인 정의에 벗어나는 많은 다양한 형태의 테러리즘행위가 테러의 정의에 포함되는 경향이 전개되었다. 예를 들면, 원유나 가스 파이프 등을 폭파하거나 주식시장을 교란하는 행위, 국가의 정상적 형사사법기능을 마비시키려는 행위 등은 체제 흔들기 (system disruption) 전략으로 불리는데 이는 공포의 조장이나 협박, 강박 등을 목적으로 하지 않으며 국가의 기능 자체에 대한 공격을 수행한다. 또한 최근 들어 나타나는 단순한 불특정 다수에 대한 증오의 표출이나 공격, 금전적 수입을 목적으로 한 용병고용 형태의 테러가담이나 범죄-테러의 융합으로 나타나는 테러조직의 범죄조직화 경향 등은 증오나 분노의 표출이라는 심리적 목적이나 금전적, 경제적 목표를 추구한다는 점에서 정치적, 사회적, 종교적 권력 추구를 목표로 한다는 전통적 테러의 개념에서 벗어나 있다. 또한 USS Cole에 대한 테러공격이나 천안함 폭침이나 연평도 포격과 같은 군사목표를 공격하는 행위 등은 테러나 이러한 유사행위가 군사 타깃에 대해서도 전투나 전쟁의 형태와는 별개로 발생할 수 있음을 보여준다. 이와 더불어 아프가니스탄과 이라크 등에서 나타나는 현상은 테러가 전쟁과 뚜렷이 구분되기 어렵다는 사실을 경험적으로 보여주며, 테러가 오늘날 네트워크 전쟁이라는 전쟁양식의 한 형태가 되고 있음을 보여준다. 또한 테러 가해자 역시 전통적인 비국가 비밀 조직 이외에도 북한과 같은 민족국가 단위나 알 카에다와 같은 초국가 네트워크, 그리고 lone-wolf 테러나 leaderless resistance, 또는 homegrown 테러와 같은 돌출 개인 등의 다양한 유형이 있음을 보여준다. 또한, 최근 독일의 National Socialist Underground (NSU)의 사례처럼 공공에 영향을 미치려는 의도를 전혀 갖지 않고 은밀하게 자신들의 정체를 숨긴 채 테러 공격을 지속하는 테러유형도 발생할 수 있음을 알 수 있다. 또한 실제 현실세계에서의 폭력이나 살상이 전혀 발생하지 않고도 효과적인 테러 공격이 발생할 수 있다는 사실도 나타나고 있는데 사이버 테러의 경우는 이에 해당할 수 도 있다. 대표적으로 DDoS 공격의 경우는 사이버 테러로 지칭되지만 실제로 현실세계에서 인명의 살상이나 시설물의 파괴 등 실제 폭력은 발생하지 않는 경우가 대부분이다. 단지 사이버 공간상에서 일정정도의 불편함이 초래된다. 이처럼 지난 14-5년 동안 테러리즘의 전통적 개념 자체에 많은 다양한 변화들이 일어났고 오늘날

이러한 다양한 많은 행위 유형들이 테러리즘이라는 불명확한 개념 하에 통칭되고 있다.

사이버라는 개념 역시 불분명한 요소를 가진다. 사이버 테러에서 의미하는 사이버는 인터넷, 하이테크, 전자적 침해 등의 유사 용어들과 뒤섞여 쓰이고 있다. 사이버는 사실상 공간으로서의 의미를 가진다 (윤해성 외, 2012). 이는 하늘, 땅, 바다로 이루어진 실제 현실공간에 대비되는 정보통신망의 정보들이 축적되고 유통되는 의식의 가상공간을 의미한다. 하지만 이 사이버라는 말은 이러한 가상공간을 운용하거나 가상공간에서 활동하는데 필요한 기술이나 장비, 장치, 단말기, 기법 등을 의미하기도 한다. 또한 사이버라는 용어는 네트워크망이나 정보통신 기반시설이라는 물리적 설비를 지칭하는 의미도 포함한다. 결국 간추려 보면 사이버는 가상공간으로서의 의미와 이에 관련된 장치, 장비, 설비, 기법이거나 정보통신 기반시설과 같은 물리적 인프라를 포함하는 포괄적 개념으로 두루 쓰이고 있다.

테러리즘과 사이버라는 두 불분명한 개념이 결합된 사이버 테러 또는 사이버 테러리즘은 따라서 용어가 구체적으로 무엇을 의미하는지 상당한 어려움을 던진다. 가장 일반적으로는 사이버 테러리즘은 해킹, 불법바이러스 유포, 봇넷, 그리고 DDoS 공격과 같은 특정 기법을 이용한 사이버 공간상에서의 전자적 침해행위가 된다. 주로 피해 대상은 컴퓨터 단말기나 웹사이트, 또는 정보통신망 등의 장애나 시스템다운 등으로 피해 대상이 사이버 공간이나 물리적 장비나 기반시설 등에 한정된다. 사이버 테러리즘으로 불리는 또 다른 유형은 피싱이나 사이버 불법도박, 개인정보유출, 산업기술유출, espionage 등의 형태로 나타나는 침해 행위이다. 이 경우 개인정보유출이나 금전적, 안보적 범죄피해 등과 같이 피해자에 대한 물리적 피해가 실제 발생한다. 하지만 사이버 공격은 가상공간에서 발생하며 사용되는 기법역시 사이버 관련 기술이라는 특징을 가진다 (김승주, 2013). 사이버 테러의 범주에서 다루어지는 또 다른 문제 유형은 이른바 전자적 제어시스템의 장악을 통한 물리적 살상 또는 파괴행위이다. 발전소나 교통시스템, 전기, 가스, 금융 등의 인프라는 기본적으로 정보통신망에 의해 전자적으로 컨트롤된다. 악성 바이러스 유포 등을 통해 이러한 전자적 컨트롤 시스템을 허가받지 않은 자가 장악하고 컨트롤 시스템에 고의로 장애를 일으키거나 비정상적으로 작동하도록 유도함으로서 앞서 언급한 다양한 인프라 시스템의 사고나 붕괴, 폭발, 혼란과 같은 물리적 파괴를 유도하는 것이다 (김홍석, 2010; 323). 한편 사이버 테러는 현실공간에서의 물리적 행위를 포함하기도 한다. 사

이버 공간에서의 공격을 위해 현실공간을 이용하거나 현실공간에서의 공격행위를 위해 사이버 공간을 수단으로 이용하는 경우 모두 사이버 테러에 포함될 수 있다. 전자는 현실에서의 사회 공학적 방법을 통해 획득한 정보나 접근권한 등을 통해 사이버 공간상에서 정보유출이나 여러 형태의 사이버 공격을 실행하는 경우이며 후자는 현실에서의 실제 파괴나 살상 행위를 위해 사이버 공간을 정보수집, 커뮤니케이션, 자금조달, 교육, 훈련, 인력 채용 등의 여러 공격준비와 지원활동의 통로나 수단으로 활용한다 (윤해성 외 2012). 이밖에도 사이버 테러는 사이버 공간을 활용한 심리전 또는 프로파간다 활동을 의미하기도 한다 (이상호, 2011). 이는 기존의 방송이나 신문, 출판물 등의 커뮤니케이션 채널을 활용한 전통적인 심리전이나 프로파간다 활동을 그대로 사이버 공간으로 옮겨 놓은 것이다. 웹사이트 운용이나 댓글, SNS (Social Network Service) 등의 통로를 통해 여론이나 정치적, 사회적 상황을 테러 행위자에게 유리한 방식으로 조성하고 이를 통해 자신들의 목적을 실현하려는 행위역시 사이버 테러의 범주에 포함된다 (윤해성 외, 2012). 마지막으로 아직은 현실에서 구현된 사례는 없지만 사이버 공간을 통한 원격 장악과 통제를 통해 인터넷에 연결된 장비나 장치 자체가 파괴나 살상행위를 하도록 유도하는 것 역시 가까운 장래에 사이버 테러의 범주에 포함될 것이다. 예를 들면 세탁기, 청소기, TV, 냉장고 등의 스마트 가전제품이 직접 인터넷에 연결될 경우 원격 장악과 통제를 통해 오작동이나 과부하를 유도함으로서 자체 폭발시켜 살상을 유도할 수 있을 것이다. 또한 가사도움이 로봇이나 전투로봇, 드론이나 전투슈트 등이 인터넷에 연결된 경우 원격장악과 통제를 통해 그러한 장비나 장치를 살상이나 파괴의 목적으로 이용할 수 도 있을 것이다. 이 역시 미래에는 사이버 테러의 범주에 포함될 것이다.

살펴본 것처럼 사이버 테러리즘 또는 사이버 테러가 가지는 의미는 매우 다양하고 복잡하다. 이는 테러리즘이 가지는 다양성과 복잡성과 함께 연동되어 있다. 결국 사이버 테러를 다룰 때에는 이러한 복잡하고 다양한 여러 관련 행위들을 모두 총괄하여 다루어야 하는 어려움에 직면한다. 또한 이러한 다양한 유형의 문제 행위나 공격행위는 현실공간에서의 살상, 파괴, 또는 문제행위들을 포함하여 함께 고민해야 한다. 더욱이 그러한 공격을 주도한 주체가 개인인가 범죄조직인가, 테러조직인가, 아니면 적성국가 인가에 따라 사이버 범죄, 사이버 테러, 사이버 전쟁 등이 결정될 수 있기 때문에 사이버 테러의 범주에 사이버 범죄와 사이버 전쟁 문제를 포함하여 함께 다루어야 한다 (문종식·이임영, 2010). 바꾸어 말하면 사이버 테러의 정의는

사이버 공간이나 사이버 공간에 연결된 물리적 장비, 설비, 장치, 기기, 소프트웨어, 정보통신망 설비 등이 연루된 국가안보와 사회 일반의 안전, 그리고 다수 개인의 안녕과 안전을 위협하는 가상공간과 현실공간의 문제 행동들을 함께 포괄적으로 다루어야 한다.

Ⅲ. 사이버 테러 위협에 대한 평가

오늘날 사이버 테러의 문제는 분명하고 실존하는 안보위협인 것처럼 보인다. 2009년 7/7 DDoS (Distributed Denial of Service) 사건, 2011년 3/4 DDoS 사건, 2011년 농협 해킹사건, 그리고 2012년 중앙일보 해킹사건 등의 사례들은 사이버 테러의 위협에 대한 경험적 증거가 된다 (김홍석, 2010). 더욱이 주요 안보위협 세력들인 북한과 중국 등의 사이버 전쟁 또는 사이버 테러 수행 능력과 발전추이를 감안할 때 사이버 테러의 위협은 상당히 심각한 문제라고 평가할 수 있다 (임영갑, 2010; 홍성표, 2011).

대체로 국내의 대다수 관련 분야 전문가들의 의견과 논문, 그리고 연구 보고서 등은 사이버 테러가 던지는 이러한 중요한 안보위협의 문제에 대해 동의하고 공감한다. 사이버 테러는 국가 안보와 사회 안정, 그리고 개인의 안녕과 행복에 대한 심각한 위협으로 인식된다. 이런 맥락에서 이 논문에서도 앞서 제시된 사이버 테러가 오늘날 제기하는 국가안보에 대한 심각한 위해라는 점은 이론의 여지가 없는 하나의 현실로 받아들일 수 있다.

하지만 이 논문은 사이버 테러가 주요한 국가안보의 위협이라는 사실 자체가 아니라 그러한 위협을 어떤 시각에서 판단하고 이해해야 하는지에 관해서 기존의 많은 유사한 주장들과 본질적으로 다르다. 우선, 기존의 주장들은 사이버 테러의 위협을 단편적인 현상으로 이해하려는 측면이 있다. 즉, 주로 해킹, 바이러스 유포, 웜바이러스 유포, 논리폭탄 전송, 대량정보전송 및 서비스 거부공격, 고출력 전차총 등의 기술적 방법을 통한 전산망의 교란, 붕괴, 특정 컴퓨터 단말기에 대한 공격, 교통, 금융, 전기, 수도 등의 전자적으로 제어되는 인프라 시스템에 대한 교란 및 공격, 스미싱, 보이스 피싱 등의 형태로 나타나는 대규모의 전산망을 통한 범죄행위 등의 특정한 유형의 테러공격의 한 양식 또는 범죄 행위의 한 양식을 다루는 것으로 문제를 접근

하는 경향들이 전형적으로 나타난다 (문종식·이임영, 2010; 서동일·조현숙, 2011; 이재은 외, 2008; 정기석, 2012; 정태명, 2001). 하지만 이러한 인식은 사이버 테러가 미래사회의 환경조건과 결합된 복잡하고 다차원적인 속성을 가진다는 사실을 간과하는 측면이 있다.

또 다른 한편은, 기존의 주장들 가운에 한 걸음 더 깊이 있게 진전된 시각으로, 주로 군사부문에서 사이버테러를 바라보는 시각이다. 이들은 사이버 테러를 미래전쟁의 한 형태로서의 사이버 전쟁으로 이해하고 있다. 이들의 사이버테러에 관한 이해와 주장들은 기존의 법률적, 기술적, 사회과학적 주장들 보다는 좀 더 깊이 있는 이해를 추구하고 있는 것을 보여준다. 사이버 테러를 기존의 육, 해, 공, 우주에 추가된 또 다른 제 5의 공간으로 보고 이 새로운 전장공간에서 이루어지는 전략적 정보전으로 이해한다. 이를 좀 더 발전 시켜 미래전의 주요 특징인 네트워크 중심전의 한 양식으로 까지 사이버 테러를 이해한다 (김승권 외, 2008; 배달형, 2011).

하지만 이러한 시각 역시 사이버테러를 바라보는 시각이 여전히 단편적인 이해에 그친다는 한계를 가진다. 즉, 사이버 테러의 문제를 군사와 전쟁부문에 국한시켜 이해하면서 범죄, 테러, 그리고 전쟁의 속성이 공존하며 민간 부문과 군사 부문의 구분이 불명확하며 함께 연동되어 있는 이중적 성격을 가지는 사이버 테러의 문제를 통합적으로 다루지 않고 있다는 한계를 노출한다.

이 논문은 사이버테러의 위협이 보다 복합적이고 다차원적이며 그 때문에 우리 삶과 안보의 근본적 속성을 뒤바꿀 수 도 있을 정도로 심각한 안보의 위협을 제기하고 있다는 사실을 보여주려고 시도한다. 사이버 테러가 던지는 안보의 위협은 이제까지 우리가 이해하는 것 보다 훨씬 더 본질적이고 심각하며 근본적이다. 이는 미래사회로의 이행과정에서 나타나는 우리 삶의 근본적인 패러다임 변환과 연동되어 있기 때문이다. 따라서 본 연구는, 사이버 테러에 대한 대응이 이러한 본질적 이해를 바탕으로 해야 하며, 그와 같은 전제아래에서 국가안보 전체의 개념과 틀을 전반적으로 리모델링하는 작업이 함께 수반되어야만 진정 의미 있는 사이버 테러에 대한 대응을 모색할 수 있다.

최근에 심심치 않게 보도되고 있는 인공지능, 속칭 아이언 맨 슈트로 불리는 전술공격용 전투슈트, 전투로봇, 드론, 인터넷으로 연결된 스마트 가전제품, 3-D 프린트기, 각종 최첨단 단말기 등은 미래사회의 폭력의 주요한 한 양식으로서의 사이버 테러 문제의 심각성을 암시하는 한 단초를 보여준다. 비록 각기 다른 기술적 발전을

보여주지만 이러한 의미 있는 기술적 진보들은 통합적으로 이해해야 한다. 예를 들면, 전술 공격용 전투슈트나 전투로봇, 드론, 스마트 가전제품, 그리고 각종 최첨단 단말기 등의 확장은 사이버 공간의 확장을 의미한다. 즉, 미래 환경에서는 지금 보다 더욱 빠르게 확장된 사이버 공간이 펼쳐질 것이며 이러한 가상공간은 현실공간과 거의 실시간으로 평행하게 동시 존재할 것이다. 그리고 더 나아가 이러한 평행적이고, 동시적으로 공존하는 가상공간과 현실공간은 모든 실생활과 전장의 전투 현장에까지도 긴밀하게 결합될 것이다. 이러한 상황은 곧 더욱 폭발적으로 팽창된 가상공간에서의 사이버 안보위협이 더욱 심각한 위협이 될 것이며 이러한 위협은 현실 공간에 대한 직, 간접적 위협으로 긴밀하게 연동될 것임을 의미한다.

또한 전술 공격용 전투슈트와 전투로봇, 드론, 각종 스마트 가전제품 등의 확장과 상용화는 이러한 여러 디바이스 들을 통제하는 인공지능과 결합됨으로서 미래사회에서는 사이버 테러가 이러한 여러 실제 현실공간에서의 디바이스를 통해 실제 폭력으로 이어질 수 있음을 의미한다. 곧 현재 보여 지는 가상공간에 한정된 사이버 테러가 현실공간에서의 실제 살상, 파괴와 연결될 수 있는 상황이 미래사회에서 전개될 가능성이 매우 높다. 이와 더불어 3-D 프린트와 각종 최첨단 단말기의 상용화는 생산부문에서 생산자와 소비자의 구분이 무너지고 생산자가 곧 소비자가 되는 현상이 폭력적 파괴부문에서도 진행될 것임을 암시한다. 즉, 폭력적 무기나 수단을 소비하는 공격 행위자가 직접 그 수단을 생산하여 사용할 수 있는 가능성을 열게 될 것이다. 이는 곧 폭력의 민주화 경향을 의미하는데 폭력적 공격을 의도하는 개인이건 집단이건 손쉽게 그 의도를 현실화할 수단을 획득하고 이를 가상공간과 현실공간에서 실제 사이버 테러 또는 공격을 집행할 수 있게 되는 것을 의미한다.

결국 사이버 테러의 위협은 앞서 지적한 이러한 미래사회에서의 환경 조건의 변화라는 근본적 변화의 연장선상에서 이해하여야만 한다. 그리고 이는 사이버 공간의 확장과 현실공간과의 결합 그리고 사이버 공간과 현실 공간의 밀접한 결합이라는 조건으로 인해, 우리는 지금까지 우리인류가 전통적으로 다루어오던 안보위협과 이에 대한 대응이라는 근본적 패러다임을 다시 짜고 전반적인 리모델링을 해야 하는 상황에 직면하게 되었다는 것을 의미한다. 그러므로 사이버 테러에 대한 대응은 이러한 근본적 문제인식과 현실공간과 사이버 공간을 함께 포함하는 전반적인 틀 속에서 안

보위협과 이에 대한 대응이라는 전체 틀을 다시 짜는 방향에서 접근하여야 한다.

사이버 테러에 대한 이해와 이에 대한 전반적인 리모델링 작업은 몇 가지 세부 부문으로 나누어 접근될 수 있다. 하지만 이러한 세부 부문들은 궁극적으로 전체적인 틀 속에서 유기적으로 통합된 각 부문으로 이해되어야 하며 전체적인 통합 속에서 미래사회에서의 안보프레임의 전략적 틀 구축이라는 방향으로 전개되어야 한다. 사이버 테러는 이러한 방향성 안에서 자연스럽게 녹아들어야 할 것이다. 각 세부 부문들은 사이버 공간에 대한 이해와 사이버 범죄, 사이버, 테러, 그리고 사이버 전쟁의 융합이라는 측면, 공간이라는 측면에서 사이버 부문이 가지는 전략적 의미. 생산양식과 파괴양식의 변화와 폭력의 민주화라는 측면, 미래전쟁의 한 양식으로서의 사이버 테러가 가지는 성격, 그리고 가상폭력의 현실폭력과의 유기적 결합이라는 여러 특징들을 포함한다.

Ⅳ. 사이버 공간에 대한 이해

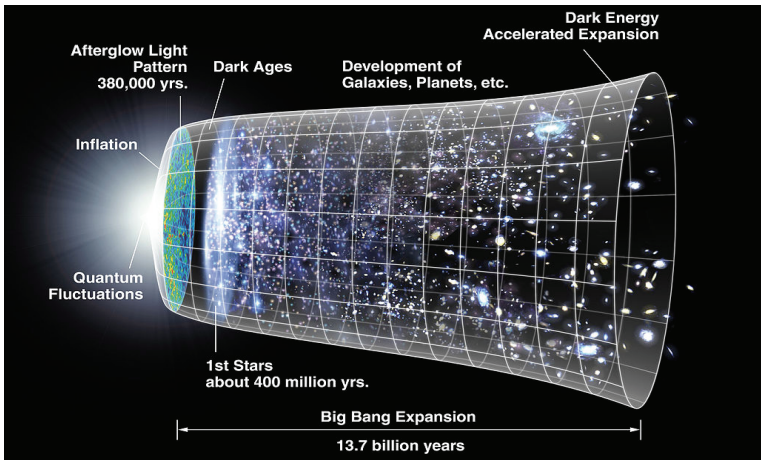
사이버 테러의 문제를 명확히 이해하기 위해서는 사이버 공간 자체에 대한 명확한 이해가 선결된다. 사이버 공간은 기존의 현실공간인 땅, 바다, 하늘, 그리고 우주라는 4개의 서로 다른 공간에 추가된 제5의 공간이다 (김승권 외, 2008: 75-76; 최광복, 2011: 7-8). 때문에 사이버 공간은 하나의 독특한 별개의 공간으로서의 의미를 가진다. 기존의 땅, 바다, 하늘, 우주 등의 현실공간이 각기 그 고유한 특성을 가지는 것처럼 사이버 공간역시 별개의 하나의 공간으로서 독특한 특성을 가진다. 그리고 이러한 독특한 특성은 대체로 사이버 공간에서 발생하거나 사이버 공간이 관련된 테러위협의 성질을 결정한다.

사이버 공간이 가지는 가장 명백한 특성은 물리적으로 실존하지 않는 의식의 공간이라는 점이다. 사이버 공간이 존재한다는 물리적 증거는 광케이블과 컴퓨터 단말기와 무선 랜 포트와 같은 장치나 설비뿐이다. 하지만 의식의 공간으로서의 사이버 공간은 이러한 물리적 장치나 설비를 훨씬 뛰어넘는 실존하는 드넓은 영역이다. 사이버 공간은 물리적으로 존재하지 않는 의식의 공간이기 때문에 무경계성, 전일성,

무시간성, 그리고 동공간성이라는 특징을 가진다. 이는 현실공간과 구별되는 특성이다. 땅, 바다, 하늘, 우주와 같은 현실공간은 공간의 분할이 가능하다. 또한 현실공간은 모든 공간이 다른 공간과 결합되어 전일적으로 존재하지는 않는다. 즉, 한 공간에서 다른 공간으로 이동하기 위해서는 연속적으로 이어진 제3의 공간을 통과하여 이동해야 한다. 이러한 특성은 A지점에서 B지점으로 이동하기 위해서는 시간의 소요와 그 둘 사이에 끼어있는 또 다른 지점 즉, C라는 지점을 통과해야만 이동할 수 있다는 것이다. 하지만 가상공간인 사이버 공간에서는 위에 언급한 모든 물리법칙이 적용되지 않는다. 사이버 공간에서는 물리적 경계가 의미를 상실한다. 또한 전체의 사이버 공간이 분할될 수 없는 하나의 전일적인 덩어리로 존재한다. 따라서 한 공간에서 다른 공간으로의 이동에 소요되는 시간은 거의 zero에 가까우며 한 지점에서 다른 지점으로의 이동이 다른 제3의 지점을 거치지 않고 바로 이루어질 수 있다. 따라서 모든 공간이 모든 다른 공간과 직접 맞닿아 있는 특성을 가진다. 결국 사이버 공간은 전체가 하나의 공간 덩어리로 이루어지는 것처럼 형성되며 이 곳 에서의 이동시간은 거의 zero에 수렴하게 된다.

사이버 공간의 또 다른 특성은 사이버 공간이 물리적 법칙을 뛰어넘는 공간이라는 특성에서 비롯되는데 서로 다른 현실공간을 직접 이어주는 웜 홀의 기능을 한다. 현실 공간에서의 A 지점과 B 지점이 서로 떨어져 있음으로 해서 정보의 교환이 시간과 공간적 이동을 필요로 하게 된다. 하지만 사이버 공간은 이러한 시간과 공간이동의 소요라는 물리적 법칙을 극복하게 만들고 현실 공간의 A 지점과 B 지점을 실시간으로 직접연결 시켜 정보 교환을 하도록 만든다. 이는 A 지점에 위치한 a 가 물리적 법칙이 부여하는 한계를 극복하고 거의 0에 가까운 비용으로 시간과 공간의 제약을 극복하고 B 지점에 위치한 b 에게 직접 영향을 미칠 수 있음을 의미한다.

사이버 공간은 시간의 흐름에 따라 지속적으로 확장된다. 다시 말하면 시간이 미래로 흐를수록 사이버 공간의 전체 크기는 지속적으로 확장되는 하나의 방향으로 움직인다. 이런 점에서 사이버 공간은 빅뱅이론과 시간의 역사와 관련된 이론에서 주장하는 우주 대폭발과 우주팽창가설과 닮아있다.



(출처: http://wmap.gsfc.nasa.gov/media/060915/)

〈그림 1〉 우주팽창과 시간에 대한 개념도

위의 그림은 최초의 우주 대폭발과 급격한 우주팽창과 이후 시간의 흐름에 따른 지속적인 우주팽창과정을 그래픽으로 나타낸 것이다. 이 그래픽에서 주요한 점은 우주 공간이 계속 팽창되는 과정에 있으며 이러한 진행은 미래의 무한대 시간으로 흐를 때까지 계속될 것이라는 점이다. 우주 공간의 팽창은 이론적으로 우주의 사멸 또는 종말시점에서 멈추게 된다. 하지만 이 경우는 공간자체가 0으로 수렴되는 것을 의미한다. 또한 지속적인 확장과정에서 새로운 공간과 새로운 별과 행성이 지속적으로 만들어지고 탄생하고 기존의 항성과 행성이 소멸하는 현상들이 나타난다. 사이버 공간은 이러한 우주 공간의 특성과 닮아 있다. 최초의 빅뱅으로 간주될 수 있는 것은 논쟁의 여지는 있지만 대체로 1960년대 후반 또는 1970년대 초반 미국에서 탄생한 ARPANET (Advanced Research Projects Agency Network) 으로 간주될 수 있다. 이는 오늘날 글로벌 인터넷의 모태로 알려져 있다. 20세기 중반 최초의 사이버 공간의 출생이후 사이버 공간은 지속적으로 빠르게 확장되어 왔다. 오늘날 전 세계를 아울러는 사이버 공간의 크기는 엄청나게 확장되었으며 미래로 갈수록 이러한 공간의 규모는 지속적으로 빠르게 팽창할 것이다. 이 팽창은 팽창하는 한 방향으로 흐르는 경향이 있으며 사이버 공간자체의 소멸이 있기 전까지 지속될 것처럼 보인다. 또한 이 사이버 공간상에서 사라지는 웹사이트나 정보와 새로이 탄생하고 생산되는 웹사

이트와 정보가 지속적으로 교차되는 과정에 있다. 이는 우주 공간과 마찬가지로 사이버 공간에서 알 수 없는 영역들이 지속적으로 만들어 지고 확장되며 또한 부분적으로 알려진 공간이 소멸하기도 하는 경향이 나타남을 의미한다.

사이버 공간은 또한 공간 자체의 무정부성을 가진다. 현실공간은 공해나 우주 등 특수한 공간을 제외하고는 특정한 국가권력의 배타적 관할권에 속한다. 따라서 대체로 발생하는 공격이나 피해 등의 위치에 따라 배타적인 관할권을 가지는 국가권력이 존재하며 그 영향과 통제를 받게 된다. 하지만 사이버 공간의 경우는 이러한 특정 국가권력의 배타적 관할권이 배정되기가 쉽지 않다. 가해자와 피해자, 그리고 공격이나 피해발생 지점 등이 사실상 어느 특정한 국가권력의 독점적 영역에 속하지 않는 경우가 대부분이다. 또한 현실공간에서 일반적으로 기대할 수 있는 순찰이나 경계활동, 정찰 및 감시, 실질적, 잠재적 피해자의 보호나 피해예방과 같은 통상적인 국가권력의 보호활동이 존재하기가 어렵다. 때문에 사이버 공간은 현실 공간과는 달리 사실상 국가가 존재하지 않는 것과 같은 상황이 만들어진다. 이 공간에서는 국가권력이 존재하지 않으면서 잠재적 가해자와 잠재적 피해자만 존재하는 사실상의 무정부 상태가 연출된다.

마지막으로 사이버 공간이 가지는 특성은 은밀성이다. 실제 행위자의 아이덴티티가 가려지는 특성이 존재한다. 때문에 공격이나 침해행위의 가해자는 좀 더 심리적으로 안전하고 편안하게 공격이나 침해행위를 수행할 수 있다. 단지 어떤 컴퓨터나 장치, 단말기 앞에서 어떤 특정 개인이 공격이나 침해 행위를 하였는지를 밝힐 수는 있지만 그러한 개인의 행위가 실제로 어떤 조직이나 집단의 명령체계에 의해 수행되었는지 단지 일탈된 개인의 행위인지, 그 동기는 무엇인지 파악하기가 매우 어렵다. 또한 공격이나 침해 행위를 한 개인을 밝혀내는데도 상당한 시간과 돈과 노력이 투입된다.

결과적으로 사이버 공간이 가지는 위와 같은 특성들은 사이버 테러의 위협을 매우 쉽고, 치명적으로 만들며 반대로 이에 대한 효과적인 대응을 매우 어렵게 만드는 경향이 있다. 사이버 공간이 가지는 무정부성과 은밀성은 가해자에게는 심리적으로 좀 더 편안하고 손쉽게 처벌이나 억제의 위험 없이 사이버 테러를 실행할 수 있는 유인 요건을 제공한다. 반대로 이러한 특성들은 국가권력이 스스로나 그 구성원들의 안보를 확보하기 매우 어렵게 만든다. 더욱이 사이버 공간의 지속적인 팽창과 부분적인 생성, 소멸은 사이버 공간 내에 국가권력이 파악할 수 없는 미지의 공간이 계속

만들어지는 것을 의미하며 반대로 공격가해자에게는 이용 가능한 잠재적 공격 타깃이나 공격통로가 지속적으로 증가하는 것을 의미한다. 더불어 사이버 공간이 가지는 무경계성, 전일성, 무시간성, 그리고 동공간성 등의 특성은 실시간으로 거의 이동비용이나 기회비용을 치르지 않고 사이버 공간 내에 존재하는 모든 대상을 직접공격하거나 공격통로로 이용할 수 있는 이점을 사이버 테러 공격행위자에게 제공한다. 더욱이 서로 떨어져 있는 현실공간의 두 지점을 실시간으로 연결해주는 웜 홀의 기능을 함으로서 현실공격을 위한 매우 효과적인 공격통로이자 지원 공간을 제공한다. 이러한 주요한 사이버 공간의 특성들은 사이버 테러의 위협의 심각성을 증폭시킨다. 더욱이 기술의 발달로 미래사회로 갈수록 사이버 공간이 가지는 특성은 사이버 테러의 위협을 증가시키는 방향으로 작용할 가능성이 크다. 더욱이 사이버 공간은 의식의 공간이기 때문에 사이버 공간을 활용한 공격 대상의 의식에 대한 직접영향을 목표로 한 사이버 심리전의 무한한 가능성까지 열려 있다. 만약 미래사회에서 인공지능이나 인간 뇌의 생체정보와 인터넷 공간의 전자정보 간에 호환이 가능해 진다면 이러한 문제는 매우 심각해 질 것이다. 돌이켜 보면 전쟁의 궁극적 목표는 살상이나 파괴의 위협이나 실행을 통한 상대방에 대한 나의 의지의 관철이다 (Clausewitz, 2009). 만약 의식의 공간을 통해 상대방의 의식에 영향을 미침으로서 나의 의지를 직접 관철시킨다면 그 수단이 되는 폭력사용이나 그 사용의 위협은 불필요하거나 우회될 수 있다. 이 경우 사이버 공간을 통한 의식의 조작은 궁극적인 전쟁무기가 될 것이다. 사이버 테러의 위협에 대한 평가는 이러한 사이버 공간이 가지는 고유한 특성과 미래사회로의 전진에서 그 사이버 공간과 관련기술이 어떻게 변모할 것인가에 대한 종합적 판단 하에 이루어져야하며 그러한 전제하에서 사이버 테러의 위협은 매우 근원적이고 심각한 사항이라고 판단할 수 있다.

Ⅴ. 사이버 범죄, 사이버 테러, 그리고 사이버 전쟁

사이버 테러와 관련되어 고려되어야 할 가장 중요한 사항 가운에 하나는 사이버 테러와 사이버 범죄, 그리고 사이버 전쟁간의 연관성과 개념 설정이다. 많은 경우에 해킹과 DDoS, 봇넷, 바이러스 유포나 스파이 웨어, 고출력 전자총, 또는 스턱스 넷 등과 같은 공격용 사이버 무기를 활용한 침해 사례들이 사이버 테러로 받아들여진

다. 하지만 문제는 똑같은 행위가 논의를 전개하는 전문가나 학자, 또는 실무자에 따라 사이버 범죄나 사이버 전쟁으로 간주되기도 한다. 이러한 개념상의 혼란과 중복은 농협이나 국민은행 개인정보유출사건에서도 나타나듯이 개인정보유출이나 보이스 피싱 등과 같은 사이버 공간을 통한 실제 피해사례에서도 사이버 범죄 또는 사이버 테러와 같은 정의가 두서없이 중복되어 나타난다. 만약 같은 행위가 북한과 같은 적대국가의 군 조직에 의해 발생된다면 사이버 전쟁으로 간주될 지도 모른다.

이러한 사이버 범죄, 사이버 테러, 또는 사이버 전쟁과 같은 개념상의 혼란은 사이버 피해 발생 시 대응과정에서 어떤 정부기관이 주도해야 하는지에 대한 혼란을 야기한다. 사이버 범죄의 경우는 일반 수사기관이 사이버 테러의 경우는 국가 방첩기관이나 정보기관 또는 수사기관의 중앙부처에서 담당하게 된다. 한편 사이버 전쟁의 경우는 사이버 사령부와 같은 군의 전담부대에서 다루어야 할 사항이다. 하지만 문제는 실제로 현실에서 발생하는 사이버 공격이나 사이버 침해사례는 사이버 범죄나 사이버 테러 또는 사이버 전쟁이라고 뚜렷이 구분하기가 어렵다는데 있다. 앞서 언급한 여러 침해사례가 발생 했을 시 초기 단계에서 이러한 침해나 공격사례들이 사이버 범죄인지 아니면 사이버 테러나 사이버 전쟁인지 사실상 구분이 불가능하다. 실제로 현실에서 나타나는 침해 행위 자체는 개념 정의의 차이에도 불구하고 동일하다. 그리고 많은 경우에 피해의 직접 당사자는 포털 사이트나 웹사이트, 정보통신 기반설비나 발전소나 교통시스템, 방송국 등의 민간 부문이거나 민간인 사이트나 개인 컴퓨터나 스마트 폰 등이다. 특정한 실제 피해사례가 범죄인지, 테러인지, 아니면 전쟁 행위인지에 대한 판별은 사태 발생이후 지난한 수사나 피해조사 과정에서 밝혀지게 될 가능성이 농후하다. 따라서 사이버 범죄, 사이버 테러, 또는 사이버 전쟁 등을 개념적으로 엄밀하게 구분하고 담당 대응기관을 구분하여 설정할 수 있지만 실질적 의미에서는 이러한 개념의 구분은 어렵거나 실효적 이익이 제한적이다. 따라서 자연스럽게 사이버 테러의 개념이나 이에 관련된 논의는 사이버 범죄와 사이버 전쟁을 포함하게 된다.

사실상 사이버 범죄, 사이버 테러, 사이버 전쟁의 개념을 구분할 수 있는 기준은 공격행태나 내용이아니라 가해자의 성격과 의도 피해대상의 성격과 피해정도에 달려 있다 (김홍석, 2010; 문종식·이임영, 2010). 사이버 공격의 가해자가 개인이나 일반 범죄자이며 개인의 분노표출이나 재미의 충족 또는 금전적 이익의 추구가 동기일 경우 이는 사이버 범죄로 정의된다. 대체로 이 경우 피해대상은 일반 시민들이나

민간 기업이 대상이 되며 피해 규모도 개인적 침해에 머무른다. 비슷한 유형의 공격의 주체가 테러리스트 이거나 테러집단 또는 국가 행위자라 할지라도 평화 시에 단순한 일회성 공격을 기도할 경우에는 사이버 테러에 해당한다. 이 경우 이들 가해자들의 동기는 대체로 공격 대상이 되는 피해주체의 사회의 혼란이나 중대한 피해 등을 기도한다. 이를 통해 그들이 추구하는 정치적, 사회적, 또는 심리적 목표를 실현하려 한다. 공격 대상의 피해 정도는 중간 정도이며 사회적 혼란을 야기할 정도의 충분한 피해 규모이다. 다수의 사람들이나 기업, 또는 정부기관이나 사회 기반시설에 대한 피해를 초래하는 것을 목표로 한다. 사이버 전쟁의 경우는 국가단위의 행위자이거나 초국가적 테러 네트워크 세력과 같은 대규모 집단 행위자가 전쟁의 승리를 통해 공격대상 국가에 대해 자신들의 정치적 의지를 관철시키려 하는 것을 목표로 한다. 이 경우 공격 대상은 국가 전체가 되며 국가급 규모의 대규모 피해를 초래하는 것을 목표로 한다. 또한 공격역시 단발성이라기보다는 일정기간 지속된 전체적인 전략 하에 다발성 공격이 지속될 수 있다.

하지만 앞서 언급한 사이버 범죄, 사이버 테러, 사이버 전쟁의 구분은 그러한 개념의 구분에 포함되는 주관적, 평가적 요소 때문에 실질적 의미에서는 이들을 구분할 판단의 여지가 희박하다. 사실상 공격의 초기 단계에서 사이버 공간 저편에 있는 공격 시발점의 컴퓨터 단말기 앞에 앉아있는 공격 행위자가 범죄자인지, 테러리스트인지, 전쟁을 수행하는 한 국가의 정규군 병력인지 판단할 근거는 없다. 또한 공격 초기단계의 여러 사이버 공격 현상들은 범죄와 테러, 그리고 전쟁이라고 구분할 수 없을 정도로 비슷한 행태이다. 따라서 초기 단계에는 사이버 범죄나 테러, 그리고 전쟁으로 구분할 수 없으며 대부분의 경우에 사이버 범죄로 피해 대상자가 인식하여 경찰과 같은 수사기관에 그 침해 사실을 보고하게 된다. 때문에 대부분의 경우에 일차 대응 기관은 경찰과 같은 수사기관이 된다. 많은 경우에 경찰의 수사가 진행되는 과정에서 사이버 범죄인지 아니면 사이버 테러 또는 사이버 전쟁인지의 실체가 드러나고 판단되게 된다.

결국 사이버 범죄, 사이버 테러, 사이버 전쟁은 하나의 현상으로 다루어야 한다. 하지만 그 위협의 정도나 대응과정에서 중요한 차이가 나타난다. 때문에 서로 다른 개념들을 하나의 현상으로 함께 다루지만 그 개념을 유형별로 구분하여 처리할 필요가 발생한다. 보다 적절한 방법은 평면적이고 도식적인 개념별 유형 구분 보다는 사이버 범죄 ↔ 사이버 테러 ↔ 사이버 전쟁으로 이어지는 하나의 스펙트럼으로 이

해하여야 할 것이다. 그리고 그 스펙트럼은 가해자의 성격, 목표, 그리고 피해 대상과 피해 규모에 따라 낮은 단계에서 높은 단계로 이어지는 것으로 파악하고 판단해야 할 것이다. 그리고 그 단계별로 대응기관과 대응주체가 결정되어야 할 것이다. 다음은 그러한 스펙트럼을 보여준다.

사이버 공격의 유형	사이버 범죄	↔	사이버 테러	↔	사이버 전쟁
가해자 성격	일반 범죄자 개인이나 조직	↔	테러조직, 국가행위자	↔	국가행위자 또는 초국가적 테러 네트워크
가해자 동기	금전적 이득, 단순 흥미, 개인적 보복	↔	정치적, 사회적, 종교적 목표	↔	국가 전략적 목표, 정치적 목표
피해 대상	개인, 민간 기업	↔	사회의 불특정 다수, 주요 국가 기간시설, 교통, 전기, 수도, 금융, 방송 등 인프라, 정부기관, 국가급 주요 민간 기업	↔	국가전체, 군사 부문, 국가전략 기반시설
피해규모	개인이나 민간 기업에 대한 심각한 침해	↔	사회전체나 사회의 불특정 다수, 국가의 일부 부문	↔	국가 전역
대응 주체	검찰, 경찰 등의 일반 수사기관	↔	검찰청이나 경찰청 등의 중앙부서의 사이버 테러 전담기구, 국가정보원 등의 국가급 정보, 방첩기관	↔	대통령 직속의 국가안전보장회의, 국가안보실, 육, 해, 공군 등 국가최고전쟁수행 지도부

〈그림 2〉 사이버 범죄, 사이버 테러, 사이버 전쟁의 스펙트럼

Ⅵ. 생산양식의 변화와 파괴양식의 변화

엘빈 토플러 (Toffler & Toffler, 1993)는 이미 20여 년 전에 미래사회의 전쟁을 예견하면서 생산의 양식이 파괴의 양식을 결정한다고 지적한바 있다. 사이버 테러라는

오늘날의 파괴양식은 오늘날의 사회와 미래사회를 특징짓는 정보화 된 생산양식과 밀접한 관련이 있다. 즉 생산양식 또는 경제활동과 관련된 일상생활을 지배하는 기본법칙이 사람을 살상하고 사회를 파괴하는 폭력행위 역시 지배한다. 이는 정보통신망에 의해 통합되고 조율되는 생산양식과 파괴양식이 서로 다른 것이 아니라 동일한 기본법칙이라는 한 뿌리에서 자라난 두 개의 서로 다른 가지이기 때문이다.

오늘날과 미래사회를 특징짓는 정보화된 생산양식은 사이버 공간을 통해 통합되고 조율된다. 여기서 사이버 공간은 생산자와 소비자를 연결하며 그러한 연결은 모든 생산자 개인과 모든 소비자 개인을 실시간으로 zero 비용으로 결합시킨다. 소비자와 생산자 양자는 실시간으로 소통하며 상거래 행위를 수행한다. 한편 사이버 공간은 로봇, 세탁기, 전화기, 청소기, 에어컨, 컴퓨터 등의 각종 디바이스를 실시간으로 연결한다. 사용자는 자신 또는 다른 사람의 디바이스에 실시간으로 접속하고 그러한 디바이스를 작동할 수 있다. 또한 특정 기업이나 기관의 구성원들이나 각 부문은 실시간으로 사이버 공간을 통해 결합되고 조율된다. 그리고 이러한 소통의 비용은 시간적이건, 금전적이건 zero에 가까워진다.

이러한 사이버 공간에 의해 결합된 정보화된 생산양식은 두 가지 뚜렷한 특징을 가지며 이는 산업사회가 시작된 이래 지속되어 왔던 우리 삶의 기본 틀을 근본적으로 변혁시킨다. 그 특징들 가운데 첫 번째는 특정 개인에 대한 맞춤형 생산이 가능해졌다는 것이다. 정보화된 생산 시스템은 각 소비자 개인의 특성이나 구매패턴, 기호 등에 대한 정보의 수집과 분석을 가능하게 한다. 사이버 공간은 그러한 정보의 수집과 분석의 값싸고 효과적인 통로이자 도구가 된다. 즉 이는 대량생산과 대량소비의 산업사회에서 맞춤형 생산과 소비로의 이동을 의미한다. 또 다른 특징은 보다 근본적이고 중요한 변혁이다. 이는 생산자와 소비자가 일체화 되는 방향으로의 이동이다. 인터넷의 발달과 3D 프린트의 개발은 이러한 변혁을 가능하게 한다. 인류는 산업혁명의 시작과 함께 지난 100-200년 동안 생산자와 소비자가 분화되는 경험을 해왔다. 전 산업단계에서 생산자와 소비자는 동일했다. 스스로 필요한 물품은 개인이 직접 제작하여 충당했다. 가내 수공업이나 가정에서 옷을 만들거나 신발을 만드는 따위는 그러한 일체화의 현상이다. 하지만 산업사회의 등장으로 생산자는 대량생산에 집중하고 소비자는 단지 소비하고 사용하는 역할에 충실한 수동적인 존재의 역할을 수행했다. 하지만 사이버 공간의 발달과 3D 프린트의 등장은 스스로 물품을 만들어 쓸 수 있는 가능성을 다시 열었다. 사이버 공간을 통해 획득된 물품생산의 설계도

와 노하우는 3D 프린트를 통해 손쉽게 소비자 스스로 생산이 가능하도록 만들었다. 이는 혁명적인 변혁이며 미래사회에는 이러한 방식으로의 이동이 더욱 촉진, 심화될 것이다. 이는 미래사회의 생산양식이 다시 생산자와 소비자가 일체화 되는 개인 맞춤형으로 변혁할 것임을 의미한다.

생산부문에서의 이러한 두 가지 특징적인 변혁은 다가올 미래사회의 파괴부문을 특징짓는 동일한 특징이 될 것이다. 사이버 공간은 이러한 소통과 조율의 통로로 생산부문에 영향을 미쳤던 것과 같은 방식으로 파괴양식을 결정하는데 영향을 미칠 것이다. 새로운 정보화 시대의 폭력양식의 하나인 사이버 테러는 이런 맥락에서 이해되어야 한다. 사이버 공간을 통해 모든 공격의 감행자와 모든 공격대상은 실시간으로 결합될 것이다. 이들의 소통 또는 연결에 들어가는 시간과 비용은 이론적으로는 zero에 가까울 것이다. 또한 공격 즉 사이버 테러에 사용되는 모든 공격용 디바이스들 예를 들면 개인용 단말기, 컴퓨터, 노트북, 스마트폰, 봇넷, 스틱스 넷, 바이러스, 스파이 웨어, 드론, 전투로봇, 전술 공격용 전투슈트, 항공 관제장치, 교통통제 시스템 등은 실시간으로 거의 zero cost로 사이버 공간을 통해 결합될 수 있다. 사이버 테러 또는 실제 테러를 수행하는 테러네트워크나 조직의 각 부문 예를 들면 전술공격팀, 정보수집 및 분석 팀, 지휘부, 지원팀, 프로파간다 담당 등은 사이버 공간을 통해 서로 실시간으로 거의 zero 비용으로 서로 유기적으로 결합될 수 있다 (윤해성 외, 2012).

파괴부문 역시 앞서 언급한 두 가지 특징에 의해 결정 지워진다. 첫 번째는 맞춤형 생산과 마찬가지로 맞춤형 파괴가 가능하다는 것이다. 사이버 공간은 거의 zero 비용과 노력으로 적절한 공격 대상의 특성과 취약점을 파악할 수 있게 해준다. 그리고 적절한 전략적, 전술적 목적에 맞추어 적절한 양과 정도의 폭력 수단을 사용해서 공격 대상을 타격하도록 허락한다. 따라서 이전 산업사회와 같이 대량파괴 형식의 전면전이나 총력전을 수행할 필요가 없으며 적절한 형태의 적절한 정도의 파괴능력을 사용하여 적절한 대상을 타격하도록 허락한다. 사이버 테러는 그러한 맞춤형 타격 방식의 파괴양식이다. 또 다른 특징인 생산자와 소비자가 결합된 현상이 생산부문에서 진행된 것처럼 파괴부문에서도 무기의 생산자와 소비자가 일체화 되도록 허락한다. 전 산업사회에서는 무기의 제작 또는 생산은 무기를 사용하는 소비자가 스스로 해결할 수 있었다. 화살이나 칼, 검, 등은 이러한 유형의 무기이다. 때문에 개인이 스스로 무장할 수 있는 조건이 허락되었으며 국가의 무장 역시 변변치 않았으므

로 개인이나 사적인 집단이 국가와 같은 강력한 적을 상대로 무장공격을 수행하는 것이 허락되었다. 하지만 산업사회로의 이행은 기관총, 전투기, 탱크 등 무기의 생산은 특정한 공장형태의 생산자가 독점하도록 만들었다. 무기의 소비자는 생산 능력을 상실했으며 단지 소비만을 할 수 있을 뿐이었다. 이러한 변화는 무기의 생산을 독점하는 국가가 압도적인 폭력 능력의 우위에 설 수 있게 만들었고 사적인 개인이나 집단은 무장력 면에서 현저한 열세를 극복할 수 없었다. 이러한 생산자와 소비자의 분화는 테러리즘과 같은 파괴양식이 제한되는 결과를 만들었고 대규모 파괴는 단지 국가 간의 전쟁에 국한되었다. 하지만 사이버 공간의 등장과 3D 프린트의 등장은 다시 무기의 생산자와 소비자가 결합될 수 있는 가능성을 열었다. 사이버 공간을 통해 총기류나 폭발물 또는 드론이나 전투로봇 등의 설계도와 제작 방법을 확보할 수 있는 값싼 가능성이 열렸으며 3D 프린트의 등장은 이러한 무기들의 제작 역시 손쉽게 할 것이다. 이는 폭력의 소비자가 곧 스스로 폭력 수단인 무기를 생산하는 생산자가 될 수 있는 가능성을 의미한다. 최근 나타나는 3D 프린트를 사용한 플라스틱 총기류의 제작과 사용은 그러한 새로운 시대의 도래를 암시하는 징후일지 모른다. 이러한 변혁은 그간 국가에 의한 폭력수단의 독점화라는 근간을 흔들고 있으며 폭력의 사유화 또는 민주화과정을 촉진시킬 것이다. 이는 곧 폭력적 공격을 감행할 수 있는 주체가 사적 개인과 집단으로 확산되는 것을 의미하며 국가 행위자에게는 무기를 들려서 병사를 다른 국가의 영토내로 진격시켜야 하는 부담감을 들어내고 먼저 인적 에이전트를 다른 국가 내에 확보하고 사이버 공간과 3D 프린트를 통해 무기를 사후에 실시간으로 공급하는 다른 방식의 전쟁수행이나 테러 수행이 가능해졌다는 것을 의미한다. 결국 이러한 모든 변혁은 폭력적 공격인 테러나 전쟁 가능성과 위험성을 높이는 방향으로 작용할 것이다. 사이버 테러는 이러한 맥락에서도 이해되어야 한다. 여기에서 사이버 테러는 사이버 공간이 무기를 생산하고 공급하고 확보하는 통로로서의 의미를 가지며 실제 파괴는 현실공간에서 일어날 수 있을 것이다.

Ⅷ. 미래전쟁의 새로운 한 양식으로서의 사이버 테러

사이버 테러는 미래 전쟁의 한 양식이라는 성격을 가진다. 이는 4세대 전쟁 (Lind, 2004) 혹은 Reed (2008)의 개념에 따르면 5세대 전쟁이라는 개념으로 이해되는 미래

전의 모습을 의미한다. 이러한 논리에 따르면 생산양식이 농업생산, 산업생산, 정보화 생산 양식으로 변화하는 것처럼 전쟁의 양식 역시 변화한다 (Toffler & Toffler, 1993). 전쟁양식의 변화는 생산양식의 변화에 영향을 받으면서 동시에 무기와 직접 관련된 기술과 무기와는 직접 관련이 없지만 일상적인 생산기술의 변화에 함께 영향을 받는다 (Morgenthau, Thompson, & Clinton, 2005; Taylor, 1969). 또한 전쟁양식의 변화는 이데올로기의 변화와 전략적 혁명과 같은 무형의 비물질적 요인의 변화에 의해서도 영향을 받는다 (Morgenthau et al., 2005). 1, 2차 세계대전은 산업사회의 대량생산 방식이 전쟁의 변화를 이끈 대량파괴였다. 기관총, 탱크, 전투기, 폭격기와 전략폭격 같은 기계화 산업화된 대량파괴 전쟁이었다. 개인 병사가 휴대가능하고 분당 발사속도가 획기적으로 개선된 라이플의 도입은 기병 돌격 전쟁을 종식시키고 보병전쟁위주로 전쟁의 모습을 변모시켰다. 항공기과 항공모함의 도입은 해전에서 무겁고 느린 전함을 전장에서 퇴역시켰다. 비군사 부문의 철도의 발명은 전쟁전개 속도의 획기적 개선을 가져왔고 이는 프랑스-프로이센 전쟁에서 보듯이 전쟁의 전개 양상을 혁명적으로 바꾸어 놓았고 1차 대전의 원인이 되었다. 민족주의의 확산은 이전의 용병군에 의한 전투를 종식시키고 대규모 병력동원과 한 국가의 모든 부문이 동원되는 국가 총력전의 양상을 역사무대에 등장시켰다. 2차 대전 초반의 독일군의 빛나는 승리는 독일군 참모부의 전략적 혁신의 결과였다. 이는 1차 대전의 참호전위주의 전쟁양식에서 대규모 기동부대의 집중을 통한 기동전과 육군-공군의 합동전 양식으로의 획기적인 변모였다 (Morgenthau et al., 2005; Taylor, 1969). 같은 맥락에서 사이버 테러는 정보화 사회의 도래와 네트워크 중심사회로의 발전 사이버 공간의 확장과 정보통신의 각종 디바이스의 발달과 정보통신망의 획기적인 발전, 그리고 인공지능과 로봇, 인공위성 등의 각종 정보통신망으로 결합된 기술 장비들의 도입과 확산이라는 여러 미래사회의 환경조건에 영향을 받는 새로운 얼굴의 전쟁양식의 한 모습이다.

사이버 테러가 새로운 전쟁양식의 한 모습이라는 것은 두 가지 측면에서 그러하다. 하나는 사이버 테러가 앞으로 네트워크 중심 전으로 전개될 미래전쟁에서 주요한 공격과 방어양식의 하나라는 점이다. 이는 정보전의 한 형태로 사이버 테러를 사이버 전쟁으로 바라본다. 여기서 사이버 전쟁은 컴퓨터와 네트워크 시스템에서 이루어지는 전쟁의 양상을 띤다. 네트워크 중심 전으로서의 사이버 전쟁의 가치는 미래 전장에서의 전투력이 정보의 공유, 정보에 대한 접근, 그리고 정보 흐름의 속도로

부터 나오기 때문이다 (김승권 외, 2008). 이는 미군이 전쟁을 수행했던 2001년 이후의 최근의 경험에서도 지지되고 있다.

전쟁의 결과에서 차지하는 정보전의 비중이 갈수록 증가하면서 사이버 위협의 파괴력이 군사력과 국가안보, 그리고 전쟁의 결과에 직접적인 위협이 되고 있다. 미래전에서는 네트워크 중심 전이 더욱 심화되는 방향으로 전개될 것이다. 전투현장에서의 최일선 보병, 포병, 기갑 등의 병사 개개인과 전투기, 헬기, 지원기 등의 항공전력, 이지스함, 잠수함 등의 해상 전력이 모두 네트워크망으로 결합되고 실시간으로 상호 정보 교환과 공유를 하게 될 것이다. 또한 이러한 통합 전력망은 전투 현장을 지휘하는 현장 지휘부를 거쳐 전장 전역을 관리하는 국가급 최고 지휘부까지 실시간으로 연결될 것이다. 더불어 정보, 병참, 수송 등 여러 전투지원체계 역시 네트워크망으로 결합되어 실시간으로 전투지원이 가능하게 될 것이다 (배달형, 2011). 이러한 통합전력망의 극적인 사례는 최일선 보병 전투원 개개인의 전술공격용 전투슈트에서 구현될 전망이다. 이 슈트는 최근 개봉된 영화 “Edge of Tomorrow”에서 잘 보여 진다. 이 슈트는 개인 전투원의 전투 능력을 극적으로 높여줌은 물론 실시간으로 사이버망에 결합될 수 있도록 해주는 휴대용 컴퓨터 단말기나 유사한 디바이스, 그리고 모니터와 카메라가 달리게 될지 모른다. 즉 이렇게 되면 개개 전투원은 전투 현장에서도 실시간으로 사이버 공간에 접촉함으로서 정보에 접속하고 다른 전투 및 지원, 지휘 체계와 실시간으로 정보를 교환하며 또 반대로 지휘부 역시 개개 병사에 달린 영상장비를 통해 실시간으로 현장 상황을 보고받고 지휘를 수행하게 될 것이다. 이러한 미래전장환경의 그림에서 사이버 테러와 같은 사이버 공격은 적의 통합전력네트워크망을 궁극적으로 마비시키게 되는 매우 강력한 무기가 될 것이다. 보다 극적인 경우에는 해킹이나 바이러스 유포 등을 통해 적의 탱크나 항공기 등의 무기를 원격 장악하거나 전투 수행 병력에게 잘못된 역정보를 전송하여 적군끼리 서로 교전하게 하거나 하는 등의 심각한 혼란을 야기할 수 있다. 가능성은 희박하지만 사이버 공격을 통해 적의 미사일이나 핵무기 등의 전략무기를 스스로 폭발하게 하거나 잘못된 타깃을 공격하도록 유도함으로서 마치 자신의 무기처럼 사용할 수 있을지도 모른다. 이러한 여러 가능성 등은 사이버 공격이 주요한 공격방법이 될 수 있음을 보여주며 반대로 자신의 통합전력 네트워크망을 적의 사이버 공격으로부터 어떻게 효과적으로 방어하는 가는 주요한 관심분야가 될 것이다.

사이버 테러가 새로운 전쟁양식의 한 측면이라는 주장의 또 다른 측면은 사이버

라는 새로운 또 하나의 공간에서의 전쟁이라는 점이다. 이는 기존의 땅, 바다, 하늘, 그리고 우주라는 네 개의 공간에 추가하여 사이버라는 또 하나의 공간이 추가됨을 의미 한다 (최광복, 2011). 또 하나의 전장 공간이 추가된다는 의미는 기존의 전쟁에 새로운 공간이 추기됨으로서 이 공간의 특성을 반영하는 독특한 전쟁이 이 공간에서 수행될 것이라는 점과 그리고 이 공간에서의 전쟁이 기존의 다른 공간에서의 전쟁과 통합되어 전체 전쟁수행에서의 군사조직, 전략, 작전, 운영체계 등 제반 군사 분야 전반에 근본적인 변혁이 일어날 것이라는 점을 내포한다. 이러한 추정은 20세기 이후에 항공 전력의 탄생으로 하늘이라는 공간이 전쟁공간으로 추가되면서 나타난 현상을 통해 유추해 볼 수 있다.

기존의 공간들에서 보여 지는 전쟁의 특성은 육전이 전쟁승패의 핵심이라는 사실이다. 전쟁의 궁극적 결전은 육군전력에 의해 수행되고 적의 의지를 최종적으로 굴복시키고 마지막 승리를 이끌어내는 것 역시 육전에 의해 달성된다. 반면 해전과 공중전은 육군전력을 지원하는 전력강화 (force multiplier) 역할이 핵심이다. 물론 해전과 공중전 전력만으로 적의 의지를 굴복시키고 전쟁의 최후승리를 이끌어 낼 수 있다는 주장도 있다. 해군 전력은 해상봉쇄 (blockades)를 통해 또한 항공 전력은 전략폭격 (strategic bombing campaign)을 사용하여 독자전력으로 적의 의지를 굴복시킴으로서 전쟁의 승리를 결정지을 수 있다는 논리이다. 하지만 Mearsheimer (2001)에 따르면 이는 역사적 경험을 통해 지지되지 않는다. 그에 따르면, 전쟁의 궁극적 승패는 육군 전력에 의해 육전에서의 결과에 의해 결정된다. 반면 해군과 공군 전력은 제해권 및 제공권 장악을 통한 병력수송, 물자지원, 함포사격, 공중폭격, 정찰 및 정보수집, 지원, 상륙작전과 공수작전을 통한 적의 취약점 장악 등과 같은 형태로 육전 수행에서의 결정적 승리를 지원하는 역할을 수행한다. 물론 핵무기를 사용한 전략공격을 통해 전쟁에서의 승패를 육전의 결전 없이 독자적으로 수행할 가능성도 존재한다. 하지만 이 역시 상호확증파괴라는 형태로 전쟁 당사자의 핵무기 사용에 제한이 걸리기 때문에 육군전력의 활용 없이 독자적으로 전쟁의 승패를 결정짓기에는 제한적이다. 독자적 공간에서의 전쟁으로서의 사이버 전은 해전이나 공중전과 유사한 성격을 갖는다. 좀 더 이론적으로 발전되어야 하겠지만 해전에서의 봉쇄나 공중전에서의 전략폭격에 유사한 사이버 전에서 독자전력에 의한 전쟁승리의 전략은 적의 통합 정보 네트워크망의 교란, 마비, 장악을 통해 적의 전쟁의지를 굴복시키고 항복을 받아내는 것이다. 여기서 한발 더 나아가면 사이버 공간을 통한 기술적 심리

적 공격을 통해 적의 주요 기반시설을 마비 또는 파괴시키거나 DDoS 공격이나 사이버 심리전 등을 통해 적의 민간인들에게 불안, 공포, 혼란을 야기함으로서 적의 전쟁 의지를 꺾어 항복을 받아낼 수 있을 것이다. 하지만 실제 국가 총력전 양상이 전개되는 실제 전쟁에서 이러한 조치만으로 적이 항복할 것이라고 기대하는 것은 지나치게 낙관적이다. 이미 해전과 항공전에서의 한계를 통해 실제 경험적으로 이러한 식의 전쟁 승리가 가능하지 않을 수 있다는 점이 파악될 수 있다. 지난 10년간의 이라크, 아프가니스탄 전쟁에서 보 듯 적의 강력한 전쟁 수행 의지는 정보 통신전력 뿐 만 아니라 해상 및 항공 전력의 도움이 전혀 없는 상황에서도 창의적인 육군 전력만으로 효과적인 전쟁 수행이 가능하다는 것을 입증했다. 때문에 사이버 전력만으로 전쟁의 승리를 이끌어 내는 것은 사실상 어렵다. 이런 맥락에서 사이버 전력은 기존 해상 전력과 항공 전력이 수행하는 병력 이동, 물자 수송, 정보 수집, 분석, 지원, 육전을 지원하는 보조적인 지원공격 등과 같은 형태의 역할을 담당할 것이다. 최근 들어 국, 내외에서 제기되는 테러리스트의 사이버 공간 이용에 관한 논의는 이런 맥락에서 이해되어야 한다. 테러리스트는 사이버 공간을 인력 채용, 선동, 극단화, 자금 조달, 교육, 훈련, 기획, 계획, 비밀 통신, 테러 공격 집행의 지원수단, 무기 조달, 사이버 공격 등의 여러 형태로 이용하고 있는데 (윤해성 외, 2012) 이는 기본적으로 실제 육전을 지원하는 여러 방식을 보여준다.

Ⅷ. 가상폭력과 현실폭력의 결합

아직까지는 사이버 테러의 피해는 가상공간에 머무른다. 사이버 테러에 대한 통상적인 이해 방식은 공격이 가상공간상에서 머무르고 공격의 대상과 피해 역시 가상공간의 타깃인 정보통신망, 포털 사이트, 웹사이트, 컴퓨터 단말기 또는 여러 종류의 디바이스들로 한정된다. 아직 이제까지의 사이버 테러라고 분류되는 사건들 가운데 실제적인 폭력피해가 현실공격으로 나타난 경우는 없다. 피해의 대부분은 불편을 초래하고 나 심리적인 불안, 정보유출을 통한 범죄적 피해 등에 국한된다. 물론 공격용 사이버 무기로 분류되는 스턱스 넷의 경우처럼 사이버 무기가 현실의 피해를 초래할 것으로 예상되는 경우도 있으나 아직 이러한 실제 사례는 사실상 나타나지 않고 있다.

하지만 사이버 테러를 가상공간에 국한되는 가상폭력으로 단정하는 것은 오류다.

사이버 또는 정보통신과 관련한 급격한 기술의 발전과 전략적 혁신은 점차 가상폭력을 현실폭력과 결합시키는 방향으로 나아가게 할 것이다. 우선 공격용 사이버 무기의 개발은 향후 이러한 사이버 무기를 통해 교통시스템, 발전시설, 주요 산업설비 등의 통제시스템을 장악하고 오작동 시킴으로서 치명적인 폭발과 같은 인위적인 재난을 초래하게 만들 수 있을 것이다. 또한 실제 현실폭력을 지원하는 통로로서 사이버 공간이 활용될 수 있으며, 인터넷 망에 결합된 단말기 자체가 사람을 살상할 수 있는 효과적인 무인무기로 사용될지 모른다. 즉, 사이버 공간에 결합된 컴퓨터 자체가 이동할 수 있고 무기를 사용할 수 있게 된다면 사이버 테러는 그러한 살상용 컴퓨터를 통해 직접 폭력을 행사하는 수단이 될지 모른다. 사이버 공간을 통해 원격 조종되는 전투로봇은 바꾸어 말하면 살상용 컴퓨터 단말기이다.

가상공간과 땅, 바다, 하늘 등의 현실공간의 폭력은 양방향으로 연결되어 있다. 하나는 가상공간에서의 사이버 테러가 현실공간의 실제 폭력과 파괴를 결과하는 것이다. 여기서 가상공간은 두 가지 서로 다른 방식으로 현실폭력으로 연계된다. 하나는 스턱스 넷과 같은 공격용 사이버 무기를 통해 현실공간의 목표물에 직접 파괴나 살상 등의 피해를 가하는 것이다. 마치 사이버 공간에서 발사된 공격무기가 현실공간에서 실제 살상 무기로 변환되어 실제 폭력과 파괴를 야기하는 모양새를 띤다. 또 다른 방식은 앞서 전쟁양식에서 잠시 논의한 것처럼 사이버 공간이 현실 폭력의 행위자들을 지원하는 정보수집, 분석, 교육, 훈련, 병력모집, 심리적 혼란과 세뇌, 물자 및 무기제공, 지휘통제 등의 실제 현실의 파괴 및 살상을 위한 지원 및 준비 기능을 담당하는 것이다. OSINT (Open source Intelligence) 오퍼레이션이나 빅 데이터 분석을 통한 데이터마이닝, Internet vetting, 웹사이트의 운용, steganograhy, 3D 프린터, 사이버 심리전, 온라인 자금세탁이나 송금 등의 다양한 방법과 기술 등은 이러한 준비 및 지원기능을 위한 여러 모습들이다. 미래사회에는 기술의 급격한 발전과 함께 보다 진보된 형태의 가상폭력과 현실폭력의 결합이 나타날 것이다. 드론이나 전투로봇 같은 여러 살상용 컴퓨터 디바이스가 개발된다면 이는 사이버 테러가 매우 치명적이고 효과적인 현실공간의 살상과 파괴로 전환될 것임을 예고한다. 날아다니거나 표면으로 이동하는 여러 종류의 살상용 컴퓨터 디바이스 등은 사이버 공간을 통한 원격조종에 의해 특정 타깃을 저격하거나 폭파시키는 임무를 수행할 것이다. 이와 함께 사이버 공간을 통한 공격 지원 기능에 관련된 기술 등도 매우 놀랄만한 속도로 진보할 것이다.

현실공간의 폭력역시 사이버 공간에서의 파괴와 폭력으로 전이되는 결합현상이 나타날 것이다. 고출력 전자총 (High Energy Radio Frequency Gun), EMP (Electro Magnetic Pulse) 폭탄, 드론 등과 관련된 기술의 발전을 이러한 가능성을 갈수록 현실화 시키고 있다. 고출력 전자총은 강력한 전자파를 발사하여 컴퓨터 전산회로에 이상 현상을 일으켜 전산망에 시스템 오작동을 유발하거나 정지시키는 전파무기이다. EMP 폭탄은 EMP Shock를 통해 전자장치를 파괴하는데 사용되는 것으로 고출력 전자총에 비해 그 범위와 면적이 넓어 해당 컴퓨터 및 정보통신망 전체를 일시에 파괴시킬 수 있다. 한편 드론 기술의 발달은 초소형 드론을 통해 핵심 전산망 자체에 접근하여 물리적으로 외부에서 직접 악성 바이러스 등을 침투시키거나 정보를 빼내거나 해킹 또는 시스템 장악 등에 이용될 수 있다. 또한 목표로 선정된 개인용 컴퓨터 등에 직접 물리적으로 접근하여 외부에서 접속함으로서 정보유출이나 봇 넷 구축, 스파이 웹이나 악성 바이러스 등을 유포할 수 있게 될 것이다. 이러한 여러 기법의 공통점은 현실공간에서의 공격수단을 통해 현실공간으로부터 사이버 공간을 파괴하가니 마비시키는 방향성을 띤다는 점이다. 기술적인 문제는 아니지만 사회 공학적 접근을 통한 사이버 공간에 대한 공격 역시 현실공간에서 사이버 공간으로 폭력이 전이된다는 점에서 같은 유형을 이해할 수 있다.

이처럼 가상폭력과 현실폭력이 양방향으로 결합되어 있다는 사실은 중요한 시사점을 준다. 이는 사이버 테러를 가상공간에서의 기술적 문제로만 제한적으로 이해해서는 안 된다는 분명한 사실이다. 이러한 제한적인 사이버 테러에 대한 접근은 문제의 심각성과 성격을 제대로 이해하지 못하게 만들며 궁극적으로 사이버 테러 대응에서의 심각한 결함을 만들어 내기 쉽다. 때문에 사이버 테러를 접근하기 위해서는 가상폭력과 현실폭력의 양방향 결합이라는 보다 입체적인 관점에서 사이버 테러의 심각성을 이해하고 그에 따른 전략개발과 대응전략이 추진되어야 할 것이다.

Ⅸ. 맺음말: 전략적 접근 틀에 대한 제안

결국 이제까지 논의한 사이버 테러에 관련된 몇 가지 쟁점들은 이와 관련된 전략적 접근 틀의 구성에 중요한 메시지를 전달한다. 이제까지 논의한 쟁점들인 테러리즘이 범죄이자 테러, 그리고 새로운 전쟁양식의 한 형태라는 세 가지 속성을 동시에

가지고 있는 복합적인 현상이며 이러한 성격은 그대로 사이버 테러리즘에서도 나타난다는 사실, 따라서 사이버 테러는 그것이 범죄인지 테러인지, 또는 전쟁인지의 성격이 유동적이며 때문에 실존적으로 판단해야 되는 동일한 스펙트럼 상의 지속적으로 변동하는 성격이라는 점, 사이버는 또 하나의 공간이라는 성격을 가지며 그러한 공간적 특성에 의해 조건 지워지고 있다는 점, 21세기 정보화 시대라는 같은 특성에 의해 조건 지워지는 생산양식과 긴밀히 결합된 파괴양식의 하나라는 점, 미래전쟁의 한 양식이라는 점, 그리고 마지막으로 현실공간의 폭력과 사이버 공간의 폭력이 결합된 형태로 전개되는 현상이라는 점 등이 전일적, 통합적으로 고려되어 사이버 테러에 대한 이해와 이해 대응한 전략적 접근 틀이 마련되어야 한다. 이를 좀 더 이해하기 쉽게 정리하면 미래 환경에서 사이버라는 새로운 특성을 가진 공간 환경이 국가안보와 사회 및 개인안전에 중요한 외부조건의 하나로 추가되었다는 사실을 직시하고 기존의 4차원에 사이버가 추가된 5차원 공간 환경에서 어떻게 새로운 국가안보 전략이 마련되어야 하는지에 대한 기본 전략 틀이 마련되어야 한다. 이러한 전제위에 미래의 기술진보의 양상과 방향이 파악되어야 하고, 위협의 주체와 성격과 유형이 분석되어야 한다. 사이버 테러의 위협과 성격은 이런 맥락에서 다루어져야한다.

한편 이러한 기반위에 다시 사이버 테러를 포함한 여러 미래사회에 예상되는 위협들과 위협 주체들에 대응하기 위한 방안들이 기능과 시스템 면에서 동시에 수립되어야 한다. 우선 확장하는 사이버 공간에 대한 파악과 장악을 위해 OSINT operation과 빅 데이터 분석, 데이터 마이닝, 인터넷 베팅, 그리고 SNS (Social Network Service) 모니터링 등의 지속적 작업과 데이터베이스 구축, 그리고 사이버 심리전 전개와 대응 해킹, DDoS 공격 등의 방법 등이 모색될 수 있다 (윤해성 외, 2012; 이완희·윤민우·박준석, 2013; Appel, 2012). 또한 검찰, 경찰 등의 형사사법기관과 정보기관, 군 등의 범죄-테러-전쟁을 다루는 여러 국가 권력기관들을 유기적으로 통합하고 유연하게 대응할 수 있도록 리모델링하고 역량구축을 강화해야 한다. 또한 지속적인 과학기술과 장비개발 등을 통해 군사용 사이버 무기와 첨단무인장비와 법집행용 또는 정보활동용 무기 및 장비 개발을 함께 추구하면서 상호호환성의 문제를 고려해야 할 것이다. 또한 인력 양성에 주력하고 형사사법, 정보, 군 등의 전문 인력의 상호호환성과 유동성을 확보해야 할 것이다. 또한 기존의 현실공간에서 작동하는 검찰, 경찰, 정보기관의 각 부문과 육, 해, 공군 등의 각 전투부문, 그리고 여러 민간 기관들과 회사, 그리고 대학이나 연구소 등의 전문기관들과 통합적인 사이버 테러의 예방과

대응, 그리고 수사 및 법집행과 민방위를 포함한 통합전투 역량을 구축하는 방향으로 전략적 접근의 기본 틀의 방향성이 모색되어야 할 것이다 (이홍기, 2013; 주성빈·최응렬, 2013; Park & Kim, 2011).

참고문헌

1. 국내문헌

김상욱·신용태. (2010). 국가 사이버재난관리 시스템 구축 방안. 정보과학회지, 37, 5, 351-362.

김승권·김상국·최종화. (2008). 미래 사이버전 및 대응방안. 정보과학회지, 26, 11, 75-85.

김승주. (2010). 세계 각국의 사이버전 수행능력과 국내 피해사례. 군사논단, 75, 19-35.

김연준·옥정석. (2011). 국가위기관리를 위한 사이버테러 대응체계 구축 방안. 인문사회논총, 18, 43-71.

김홍석. (2010). 사이버 테러와 국가안보. 저스티스 통권, 121, 319-356.

문종식·이임영. (2010). 사이버테러의 동향과 대응방안. 정보보호학회지, 20, 4, 21-27.

배달형. (2011). 국가군사전략급 수준에서 북한 사이버 위협과 한국군의 대응방향. 전략연구, 52, 147-174.

서동일·조현숙. (2011). 사이버전을 위한 보안기술 현황과 전망. 정보보호학회지, 21, 6, 42-48.

안유성. (2013). 사이버공격에 대비한 국방체계 발전방안 연구. 정보보호학회지, 23, 2, 48-54.

윤민우·김은영. (2012). 다차원 안보위협과 융합안보: 탈근대 사회에서의 안보와 치안의 융합현상에 대한 이해. 한국경호경비학회지, 31, 157-185.

윤해성·윤민우·Freilich Joshua·Chermak Steven·Morris Robert M. (2012). 사이버 테러의 동향과 대응방안에 관한 연구. 한국형사정책연구원 연구총서, 12-B-03.

이상호. (2011). 북한 사이버 심리전의 실체와 대응방향. 한국정치외교사논총, 33, 1, 263-290.

이완희·윤민우·박준석. (2013). 인터넷 시대의 정보활동: OSINT의 이해와 적용사례분석. 한국경호경비학회지, 34, 259-278.

이재은·양기근·류상일. (2008). 국가 사이버 위기관리체계 강화 방안에 관한 연구. 한국위기관리논집, 4, 2, 69-93.

이홍기. (2013). 국가위기관리체제의 효율성 제고 방안 연구. 한국경호경비학회지, 36, 493-523.

임영갑. (2010). 사이버전의 양상 및 대응전략. 저스티스 통권, 121, 357-362.

정기석. (2012). 최근의 사이버테러에 대한 대응방안. 정보·보안 논문지, 12, 1, 89-96.

정태명. (2001). 사이버테러와 정보보호: 창과 방패의 끝없는 전쟁. 디지털 행정, 24, 4, 26-36.

조성현·이택규·이선우. (2014). TCP/IP 네트워크 프로토콜의 DoS 공격 위약점 및 DoS

공격사례 분석. 정보보호학회지, 24, 1, 45-52.

주성빈·최응렬. (2013). 국가 통합위기관리체계(IEMS)의 구축방안에 관한 연구. 한국경호경비학회지, 34, 279-311.

최광복. (2011). 사이버전 대응을 위한 국방 정보보호환경 분석과 보안관리모델 연구방향 고찰. 정보보호학회지, 21, 6, 7-15.

홍성표. (2011). 북한 사이버 공격수법, 고도화·지능화. The Unified Korea, 34-35.

Park, D. K. and Kim, T. M. (2011). Mutual Cooperation between USA Police and Private Security: Actual Status and Meaning. 한국경호경비학회지, 28, 207-228.

2. 국외문헌

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

Clausewitz, C. V. (2009). *On War*. New York: Brownstone Books.

Lind, W. S. (2004). "Understanding fourth generation war." *Military Review*, September-October: 12-16.

Mearsheimer, J. J. (2001). *The Tragedy of Great Power Politics*. New York: W. W. Norton & Company.

Morgenthau, H., Thompson, K., and Clinton, D. (2005). *Politics Among Nations: The Struggle for Power and Peace*. 6th ed. New York: McGraw-Hill.

Reed, D. J. (August, 2008). "Beyond the War on Terror: Into the Fifth Generational War and Conflict." *Studies in Conflict and Terrorism*, vol. 31, no. 8: 684-722.

Taylor, A. J. P. (1969). *War by Time-Table: How the First World War*. New York: American Heritage Press.

Toffler, A. and Toffler, H. (1993). *War and anti war: Survival at the dawn of the 21st century*. Boston, MA: Little, Brown and Company.

자료출처

Timeline of the universe NASA Website http://wmap.gsfc.nasa.gov/media/060915/

【Abstract】

The threats and responses of cyber-terrorism in a new security environment: Issues and propositions on strategic frameworks

Yun, Min-Woo

Despite much discussions on cyber-terrorism in South Korea, several missing issues could be addressed. This paper attempts to deal with such missing but important issues. In South Korea, there has been little attentions on cyber-terrorism with the respects of national security strategy development under macro framework responding to future security environment. This article focuses on such issues. In other words, the purpose of this paper evaluates the meaning of national security threats raised from cyber-terrorism as a mode of security threats and proposes the matter of cyber-terrorism within the development of national security strategy in the future security environment.

several issues in this discussion pass some important messages for the construction of national security strategic approach framework within the future security environment adding cyber-space. in the future environment, a new space called cyber is added as an important external condition which might determine the security of individuals, societies, and nations. Therefore, the fundamental strategic framework should be prepared. After that, the trend and direction of future technological advancement should be understood and the identity, nature, and types of threat should be analyzed. Also, after that, various responses and countermeasures are together constituted in the aspect of function and system regarding various anticipated threats of the future human society including cyber-terrorism.

Key words : terrorism, cyber-terrorism, national security, cyber-security, cyber-crime, cyber-warfare