

사이버테러 대응체계와 법치주의

정준현* · 김귀남**

요약

사이버테러는 넓게는 “네티즌 사이에 공포감을 조성할 목적으로 행하는 사이버상의 일체의 만행(act of Vandalization of cyber)”으로 새길 수 있고 오프라인 상의 테러리즘에 근접하는 좁은 개념으로는 “특정한 집단이나 개인이 자신의 정치적 목적이나 이념을 관철시킬 목적으로 대중, 정부요인 또는 정부기관이나 공공기반시설 등에 대해 위협을 가할 수 있는 무기로서의 컴퓨터 사용”으로 각각 새길 수 있다. 사이버테러가 갖는 파급효과의 연쇄성(개인적 법익침해가 사회적 법익의 침해로 그리고 사회적 법익의 침해가 국가질서의 혼란으로 이어지는 연쇄성)과 공간초월성(개인적 법익침해를 매개로 하는 국가기반질서의 파괴도 가능)을 감안할 때 국가정보원은 일 반경찰권한에 속하는 것에 대한 것에 대하여도 초기단계에서부터 가급적 경찰청이나 관련 국가 기관과 정보를 공유하거나 모니터링하면서 국가질서에 대한 위협으로 전이되지 아니하도록 예방작용을 해야 한다.

Encounter Measure System Against Cyber-Terror And Legalism

Jun-hyeon Jeong* · Kui-nahm Kim**

ABSTRACT

Preventive measures and control over cyber terrorism in Korea is a complex problem. Today laws should meet requirements made by modern technologies development. Law enforcement, special services and judicial system cooperation, their efforts coordination and their material security are priority directions. None of the country is able to prevent cyber terror independently and international cooperation in this field is vital. Taking the above into consideration, we propose and insist that National Intelligence Service(NIS) should share cyber terror data with Police Agency and have top police authority over the cyber terror.

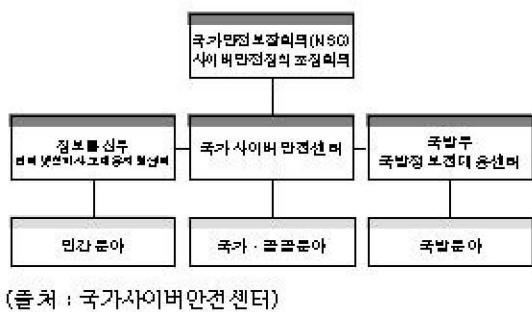
Key words : Cyber Terror, National Information Service(NIS), Legalism, Cyber Police

* 천문대학교 법학과

** 경기대학교 정보보호기술공학과

1. 문제의 제기

현재 우리나라의 사이버테러대응체계는 아래의 그림에서 보는 바와 같이 국가안정보장회의를 축으로 크게 국가정보원을 중심으로 하는 국가공공분야의 정보보안체계(국방분야의 경우에는 국방부를 중심으로 하는 국방정보대응센터가 담당)와 정보통신부를 중심으로 하는 민간분야의 정보보호체계로 이원화되어 있다. 그밖에 경찰청도 별도의 사이버테러대응센터를 운영하는 등 2003년도에 발생한 1·25인터넷 대란을 계기로 국가안보차원에서 사이버안전확보를 위한 제도정비가 착수되었다.



(그림 1) 국가사이버테러 대응체제도

그러나, 이러한 제도정비는 헌법과 정부조직법 및 국가정보원법 등 조직법에 의한 국가행정권한의 분배기준이나 사이버테러에 대한 개념의 정립 및 경찰행정에 대한 법체계의 인식 없이 부처간 이기주의식으로 이루어져 법치행정의 틀을 위협받기에 이를 것으로 평가된다.

이러한 점에서 이하에서는 사이버테러에 대한 개념의 정립을 시도하고 그에 상응하는 경찰법체계상의 권한청을 현행 조직법상 각 기관의 직무범위를 토대로 사이버테러의 집행기관과 향후의 입법개선점을 간단하게나마 검토해보기로 한다.

2. 사이버테러의 개념

이하에서는 사이버테러의 개념을 도출하기 위해 먼저 오프라인상의 테러리즘에 대한 개념논의를 먼저 살펴본 후에 온라인의 특성을 감안한 사이버테러리즘에 대한 개념의 정립에 노력해보기로 한다.

2.1 테러리즘의 의미

현실공간에서 이루어지는 테러리즘의 의미에 대해 Thornton은 “폭력의 사용이나 그 위협을 수반하는 불법적인 수단에 의해 정치적 행동에 영향을 행사하려는 의도의 상징적인 행위”[1]로 규정하고 있으며, Kaiser는 “정치적 권력투쟁의 폭력범죄 형태”[2]로 그리고 미 중앙정보국(CIA)에서는 “정치적 상징효과를 얻기 위한 폭력의 사용 또는 그 위협으로서 직접적인 피해자보다는 다수 대중에게 심리적인 충격을 가하려는 목적을 가진 것(여기에는 국가 내에서 행하여지는 전복활동 또는 반란적 군사활동을 모두 포함)”으로 각각 정의하고 있다[3].

우리나라의 경우에도 테러범죄에 관한 통일된 이론이나 실정법은 없고, 1982년 대통령령령 제47호로 발하여진 “국가대테러활동지침” 제2조에서는 “국가이익과 국민에 대하여 국제테러분자 등이 각종의 목적을 위하여 국내외에서 불법적으로 지행하는 각종 범죄행위”를 국제테러로 규정하고 있고[4], 2001년 11월 26일 차관회의에서 의결된 “테러방지법(안) 제2조제1호에서는 “‘테러’라 함은 정치적·종교적·이념적 또는 민족적 목적을 가진 개인이나 집단이 그 목적을 추구하거나 그 주의 또는 주장을 널리 알리기 위하여 계획적으로 행하는 ① 대통령령이 정하는 국가요인·각계 주요인사·외국요인과 주한 외교사절에 대한 폭행·상해·약취·체포·감금·살인, ② 국가중요시설, 대한민국의 재외공관, 주한 외국정부시설 및 다중이용시설의 방화·폭파, ③

항공기·선박·차량 등 교통수단의 납치·폭파, ④폭발물·총기류 그 밖의 무기에 의한 무차별한 인명살상 또는 이를 이용한 위협, ⑤대량으로 사람과 동물을 살상하기 위한 유해성 생화학 물질 또는 방사능물질의 누출·살포 또는 이를 이용한 위협 등 행위로서 국가안보 또는 외교관계에 영향을 미치거나 중대한 사회적 불안을 야기하는 행위를 말한다고 개념을 정의하여 테러의 보호법익을 국가안보 또는 외교관계 및 사회적 안정으로 규정하고 있는 실정이다.

이러한 관점에서 테러리즘의 개념징표를 찾는다면 “특정한 정치적 또는 이념적 목적으로 행하여지는 폭력 등의 불법적인 수단”으로 요약할 수 있을 것이다.

2.2 사이버테러리즘(사이버테러)

앞에서 살펴본 바와 같이 테러리즘에 대하여는 “정치적 목적으로 행하여지는 폭력을 수반한 각종 불법행위”로 어느 정도 공통점을 도출할 수는 있지만, 사이버테러리즘의 의미에 대해 일반적으로 받아들여지고 있는 개념정의는 현재 존재하고 있지도 않고 사이버공간과 오프라인 공간의 차이로 인하여 현실공간에서 이루어지는 테러리즘의 개념을 그대로 도입할 수도 없는 실정이다.

그렇다고 하여 단순히 컴퓨터 공격을 사이버테러로 규정짓는 것도 문제가 있다[5]. 왜냐하면, 어떠한 사건이 발생한 후 상당한 시간이 경과하지 아니하고는 컴퓨터 공격자의 의도, 동일인 여부 또는 정치적 동기나 목적을 확실하게 확정하기가 어렵기 때문이다[6]. 그러나, 사이버테러의 개념정의를 논의하기 위해 다음과 같은 몇 가지의 개념논의를 참조해볼 수 있을 것이다.

첫째, 미국법전 제22권 제2656조에서는 테러리즘을 “통상 대중에게 영향을 미칠 의도로 하

위 민족단체나 비밀결사에 의해 비전투원을 목표를 하여 범하여지는 계획적이고 정치적 동기를 가진 범행”으로 개념을 정의하고 있고, 국제테러는 한 국가 이상의 국민이나 영토와 관련있는 테러를 의미하는 것으로 이해되고 있다는 점이다.

이 경우 테러리스트 집단은 국제테러를 실행하는 집단이나 그 하부집단을 의미하게 된다[7].

이와 관련하여, 미국의 국토안보부(DHS : The Department of Homeland Security) 내에 설치되어 있는 국가기간시설보호센터(NIPC)는 사이버 테러리즘을 “정부를 위협하여 정부정책을 변경시킬 목적으로 컴퓨터를 통하여 폭력, 사망, 파괴를 초래하여 공포감을 생기게 하도록 계획된 범죄행위”로 개념을 정의하기도 한다[8].

둘째로, 정보화사회가 고도화되면 될 수록 다른이 접하게 되는 공공시설의 통신기반 의존도는 커질 수밖에 없고 그만큼 정보화사회는 곳곳에 전자적 아킬레스건(Electronic Achilles' heel)을 많이 가질 수밖에 없다. 이러한 점에서 격대적인 국가나 세력이 이를 취약성을 악용하여 부실한 컴퓨터 네트워크에 침입하거나 주요기능을 와해시키거나 전복시키고자 획책할 것임을 상정할 수 있다.

따라서 사이버테러의 전제는 국가 주요기간 시설의 운용은 컴퓨터 네트워크에 의존할 수밖에 없고 그 의존도는 향후 더욱 점증하고 새로운 취약점도 발생할 것이라는 점에 착안해야 할 것이고, 이러한 착안점에서 출발할 때 사이버테러는 “에너지, 운송 및 정부기능 등 중대한 국가기간시설을 마비시키거나 정부나 일반대중을 협박 또는 강압하기 위해 컴퓨터 네트워크 도구를 사용하는 행위”를 의미하는 것으로 새겨야 한다는 입장이다[9].

셋째로, 보안전문가의 보고서에 의하면[10] 컴퓨터의 공격이 물리적 테러리즘행위에 비견하는 파괴적 효과와 공포의 효과가 잠재해 있다면

사이버테러로 보아야 한다고 하면서, 이러한 효과의 엄격성을 전제로 사이버테러가 일정한 범위에 제한되어야 하겠지만 사망, 부상, 정전의 확산, 비행기충돌, 물의 오염으로 이어지거나 경제에 대한 신뢰기반을 위축시키는 컴퓨터공격 또한 사이버 테러리즘으로 규정하여야 한다고 한다.

이러한 입장은 오늘날 인터넷의 생활화에 따라 사이버 공간이 네티즌에게 있어서는 경제의 중요활동무대라는 점을 감안할 때, 인터넷상 공포감(Panic)을 확산하고 매체에 대한 불신을 야기할 정도의 네티즌 자산에 대한 공격은 사회적 혼란을 야기할 우려가 있는 행위라는 차원에서 사이버테러리즘으로 간주하여야 한다는 견해와 흐름을 같이 하는 것이라고 할 것이다.

예컨대, 주식시장의 분열(disruption), 은행사이트의 조작, 소문유포와 은행시스템의 실행(Run), 바이러스 유포를 통한 네트워크의 파괴 등은 모두 사이버 공간상의 사이버테러리즘의 행위로 파악할 수도 있다는 것이다. 이러한 행위가 생명의 손실을 야기하지는 않지만 생명의 손실이 없는 전자적 은행폭격으로 간주할 수 있는 것이다.

아울러, 오늘날 상당수의 병원과 의료기관이 사이버 공간에서 서비스를 제공하고 있다는 점과 병원의 사이버 자산에 대한 테러리스트의 공격은 생명의 손실로 이어질 수 있다는 점 또한 감안되어야 한다고 한다.

2.3 사건

전술한 개념을 종합해보면, 사이버테러리즘은 좀계는 “특정한 집단이나 개인이 자신의 정치적 목적이나 이념을 관철시킬 목적으로 대중, 정부요인 또는 정부기관이나 공공기반시설 등에 대해 위협을 가할 수 있는 무기로서의 컴퓨터사용” 또는 여기에는 현대 정보전과 관련하여 컴퓨터설비와 전송선에 대한 물리적 공격을 포함

하는 것도 가능하다[11].

넓은 의미에서의 사이버테러는 오늘날 네트워크 시스템이 정보화사회의 아킬레스 건으로 기능한다는 점에 착안하여 컴퓨터 네트워크 시스템에 장애를 초래하는 물리적 또는 소프트웨어적인 일체의 불법적 행위로 개념을 정의할 수 있을 것이다.

요컨대, 사회일반의 건전한 사이버이용관계의 보장이라는 측면에서는 사이버 테러리즘의 개념을 폭넓게 정립하고자할 경우에는 네트워크 이용에 있어 이용자에 대해 당혹감이나 공포감을 조성하거나 조성할 목적으로 행하여지는 사이버상의 일체의 만행(act of Vandalization of cyberspace)으로 새길 필요가 있는 것이다.

3. 경찰의 개념과 종류

3.1 경찰의 개념

경찰은 그 실질내용에 관계없이 조직법상 경찰의 권한으로 된 것을 의미하는 형식적 의미의 경찰과 법령상 경찰기관의 담당업무와는 관계없이 작용의 성질에 착안하여 학문적으로 성립된 개념으로서 “공공의 안녕과[12] 질서[13]를 유지하기 위한 위험의 방지 및 이미 발생한 장애의 제거 등을 목적으로 일반통치권에 근거하여私人에 대해 국가가 행하는 명령 또는 강제작용”을 의미하는 실질적 의미의 경찰[14]로 구분된다. 이러한 실질적 경찰작용은 국민의 자연적 자유를 제한하는 외관을 갖기는 하지만 그 실질은 개인의 권리와 자유를 지켜주고 보호해주는 의의를 갖는다[15].

3.2 경찰의 종류

경찰은 다음과 같은 구별이 가능하다.

첫째로 행정경찰과 사법경찰의 구별인바, 전자는 실질적 의미의 경찰, 즉 사회공공의 안

녕·질서를 직접 목적으로 하는 작용을 의미하는 데 대하여, 후자는 범죄수사·범인체포 등을 행하는 작용을 의미한다(다만, 현행 형사소송법 제196조는 이러한 사법경찰의 임무를 경찰행정 기관에 맡기고 있다).

둘째로, 보안경찰과 협의의 행정경찰의 구별인바, 전자는 공공의 안녕·질서를 유지하기 위하여 자신의 업무로서 독립하여 행하여지는 경찰작용을 의미하고, 후자는 건설교통부장관이 불법건축물을 단속하는 것과 같이 행정청이 자신의 업무를 수행하는 과정에서 발생하는 위해를 방지하기 위하여 행하여지는 부수적 경찰작용을 말한다[16].

마지막으로, 이 글과 관련하여 중요한 고등경찰과 보통경찰의 구별이 있는바, 전자는 국가정보보원과 같이 국가조직의 근본에 대한 위해의 예방 및 제거를 목적으로 하는 경찰작용을 말하며, 후자는 경찰청과 같이 일반사회의 안녕·질서의 유지를 위한 경찰작용을 말한다[17].

4. 현행조직법상 사무영역별 경찰권의 소재

현행법상 실질적 경찰권으로서의 질서유지작용과 관련한 조직법으로는 정부조직법과 경찰관직무집행법 및 국가정보원법 등이 있는바, 이를 법규정을 사이버질서와 관련하여 개략적으로 살펴보면 다음과 같다.

첫째, 정부조직법 제34조에서는 행정자치부의 소관업무로 제1항에서는 “행정자치부장관은 국무회의의 서무, 법령 및 조약의 공포, 공무원의 복무 및 연금관리 상운, 정부조직과 정원의 관리, 행정개혁, 행정능률, 전자정부, 정부청사의 관리, 지방자치제도, 지방자치단체의 사무지원·재정·세제, 지방자치단체간 분쟁조정, 선거, 국

민투표, 민방위·재난관리 제도에 관한 사무를 장리한다”고 규정하고 있다.

다른 한편, 제2항에서는 “국가의 행정사무로서 다른 중앙행정기관의 소관에 속하지 아니하는 사무는 행정자치부장관이 이를 처리한다”고 규정하여 특정업무의 소관부처가 불분명할 경우 행정자치부의 소관사무로 되고 이러한 소관업무를 수행함에 있어서 예상되는 위험의 예방과 장해의 제거에 대해서는 행정자치부장관이 행정경찰권을 갖게 됨을 알 수 있다.

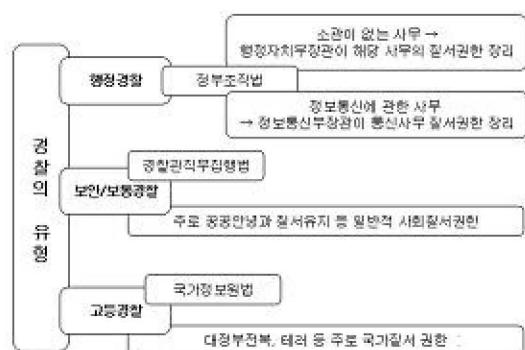
둘째로, 정부조직법 제38조는 “정보통신부장관은 정보통신·전파관리·우편·우편환 및 우편대체에 관한 사무를 장리한다”고 규정함으로써 정보통신업무의 수행상 예상되는 부수적인 위험의 예방과 장해의 제거와 관련한 정보통신질서권은 정보통신부장관에게 귀속시키고 있는 것으로 새길 수 있다.

셋째로, 경찰관직무집행법 제2조에서는 “경찰관은 ①범죄의 예방·진압 및 수사, ②경비·요인경호 및 대간첩작전수행, ③치안정보의 수집·작성 및 배포, ④교통의 단속과 위해의 방지 및 ⑤기타 공공의 안녕과 질서유지 등의 직무를 행한다”고 규정함으로써 경찰은 자신의 독립목적으로서의 국가질서가 아닌 사회질서유지업무(보안경찰작용)를 근간으로 부수적으로 사법보조업무 등을 행하고 있음을 알 수 있다.

끝으로, 국가정보원법 제2조에서는 “국정원은 ①국외정보 및 국내보안정보(대공·대정부전복·방첩·대테러 및 국제범죄조직)의 수집·작성 및 배포, ②국가기밀에 속하는 문서·자재·시설 및 지역에 대한 보안업무(각급기관에 대한 보안감사는 제외), ③형법중 내란의 죄, 외환의 죄, 군형법중 반란의 죄, 암호부정사용죄, 군사기밀보호법에 규정된 죄, 국가보안법에 규정된 죄에 대한 수사, ④국정원직원의 직무와 관련된 범죄에 대한 수사 및 ⑤정보 및 보안업무의 기획·조정 등의 직무를 수행한다”고 하여 국정원

은 주로 국가질서유지와 관련된 예방작용과 사법작용으로서의 국가질서를 파괴하는 범죄주사작용을 각각 수행함을 알 수 있다.

이러한 내용을 그림으로 표시하면 아래와 같다.



(그림 2) 경찰의 유형과 협행 조직법상 소관부처

5. 맺는 말

앞에서 살펴본 바와 같이 사이버테러는 넓게는 “네트워크 이용관계에 있어 이용자에게 당혹감 또는 공포감을 조성하거나 조성할 목적으로 행하는 사이버상의 일체의 만행(act of Vandalization of cyber)”으로 새길 수 있고 오프라인 상의 테러리즘에 근접하는 좁은 개념으로는 “특정한 집단이나 개인이 자신의 정치적 목적이나 이념을 관철시킬 목적으로 대중, 정부요인 또는 정부기관이나 공공기반시설 등에 대해 위협을 가할 수 있는 무기로서의 컴퓨터사용”으로 각각 새길 수 있다.

이러한 개념 분류에 의하면, 국가정보원법상 국가정보원은 주로 후자에 관한 질서유지권한을 갖는 반면에 후자를 제외한 전자는 정부조직법상 정보통신부장관의 행정경찰사무 또는 경찰관직무집행법상 일반경찰의 사무에 각각 속하게 되나, 정보통신부장관의 경우 사무는 조직법상

장리하고 있으되 사무집행의 근거가 되는 집행법(작용법)적 근거가 마련되지 아니하여 통신질서위반을 단속할 수 있는 경찰권한을 현재 갖고 있지 못함을 알 수 있다.

다른 한편, 사이버 공간의 행위는 네트워크라고 하는 하나의 망으로 연결되어 있는 결과 오프라인 공간상의 행위처럼 행위 자체의 현장한정성을 갖지 아니하고 공간초월성을 갖는 점에서 특정개인에 대한 사이버테러가 사회전반 또는 국정운영시스템 자체에 대한 위협으로 이어질 소지를 배제하기 어렵게 된다는 점에서[18] 경찰권한이 물리적으로 엄격하게 구별된다고 보기 어렵다.

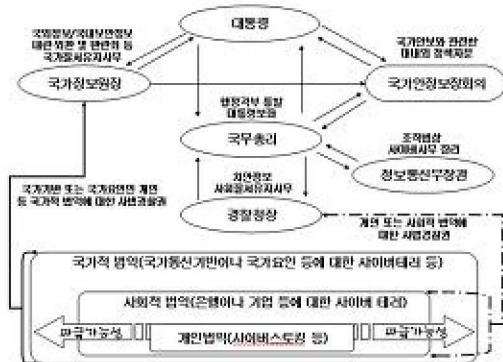
이러한 제반 사정을 고려할 때 사이버테러에 대응할 질서유지권한청은 경찰 또는 국가입법정책상의 판단에 의한 정보통신부장관(예컨대, 경제경찰권을 가진 공정거래위원회나 식품의약경찰권을 가진 식품의약청과 같은 외청을 두고 그에 상응하는 집행법을 둘 경우)은 통상의 네트워크 기능장애를 야기하는 일체의 사이버테러 행위에 대해 그리고 국가정보원은 국가안정 등 국가의 기간을 위협하는 통신기반네트워크 시스템 등에 대한 장애를 야기하는 사이버테러에 대해 각각 경찰권을 갖는다고 하여야 할 것이다[19].

따라서 국가법령의 기본 틀을 무시하고 가변적인 일부의 주장에 얹매여 정상적이고 일반적인 행정조직을 무시하고 옥상옥의 별도조직을 생산하는 정부조직의 무리한 확장이나 정략적인 소관기관의 지정은 자제되어야 한다.

요컨대, 아래의 그림에서 보는 바와 같이 사이버테러대응기관으로서의 경찰청은 주로 개인 및 사회적 차원의 법익침해에 한정되는 정보의 수집을 통한 예방작용과 발생된 장애의 제거와 관련한 경찰권을 갖는다고 할 것이다(현재 경찰청 산하의 사이버테러대응센터가 가동 중에 있는 점을 감안하더라도 행정경찰로서 정보통신부장관을 별도로 상정할 필요는 상존한다).

다만, 사이버테러가 갖는 파급효과의 연쇄성(개인적 법익침해가 사회적 법익의 침해로 그리고 사회적 법익의 침해가 국가질서의 혼란으로 이어지는 연쇄성)과 공간초월성(개인적 법익침해를 매개로 하는 국가기반질서의 파괴도 가능)을 감안할 때 국가정보원은 일반경찰권한에 속하는 것에 대한 것에 대하여도 초기단계에서부터 가급적 경찰청이나 관련 국가기관과 정보를 공유하거나 모니터링하면서 국가질서에 대한 위협으로 전이되지 아니하도록 예방작용을 해야 한다.

이와 동시에 국가이익에 대한 사이버테러와 관련된 정보수집과 수집된 정보의 분석을 대통령에게 직접 보고하거나 대통령의 요청에 따라 국가안정보장회의를 거쳐 국가안보정책에 관해 대통령에게 자문하며 발생된 국가적 장애의 제거에 대한 사법경찰권한과 수립된 정책의 집행을 담당하여야 한다고 할 것이다.



(그림 3) 현행법제에 의거한 사이버테러에 대한 경찰권한도

참 고 문 헌

- [1] T. P. Thornton, "Terror as a Weapon of Political Agitation", in H. Eckstein(ed.), *Internal War : Problems and Approaches*,

p. 73 1964, 죄인섭, "테러리즘의 실태에 관한 일 고찰", *국제법논총*, 제6권, p.35에서 재인용, 1992

- [2] G. Kaiser, *Kriminologie : Eine Lehrbuch*, S.658, 1988.
- [3] 국제문제조사연구소, 테러대책과 관련한 국내법상 미비점 검토, p. 15, 1986.
- [4] 현재의 대테러시스템은 법률이 없는 상태에서 1982년 대통령훈령 제47호에 의거한 '국가대테러 활동지침'에 기반하고 있다는 점에서 법률적 근거를 갖는 테러방지법의 제정이 시급한 실정이다고 일단 평가할 수 있다.
- [5] 예컨대, 2004년 국가정보원이 발간한 백서의 목차 및 그 내용에 의하면 제1편 총론 제2장에서는 사이버침해 위협과 사례를 제시한 후 사이버테러에 대한 개념정의없이 제2편 "제1장 국가정보보호체계" 제1절에서 사이버테러대응이라는 항목을 설정함으로써 "사이버 위협 = 사이버테러"로 오인할 여지를 두고 있음은 큰 문제라고 할 것이다. 국가정보원, "2004 국가정보보호백서", pp. 14-26, 35, 2004.
- [6] CRS Report for Congress(Oct. 17, 2003.), p. 4, 2003, 10.
- [7] 미국 정부는 1983년 이래로 테러리즘에 대한 이러한 개념정의를 채택하여 사용하고 있다. Patterns of Global Terrorism, <<http://www.state.gov/s/ct/rls/pgtrpt/2001/html/10220.htm>>, 2003.
- [8] 2002 Director of NIPC, Scott Berinato, The Truth About Cyberterrorism, CIO, March 2002.
- [9] James A. Lewis, Assessing the Risks of Cyber Terrorism, "Cyber War and Other Cyber threats", CSIS, 2002.
- [10] Dorothy Denning, Is Cyber War Next?, November 2001.
- [11] 이와 관련 중국의 경우에는 '제4군' 사이버

- 부대를 창설하여 “點穴(급소)전략”이란 이름으로 해킹전술을 개발하고 있음을 주지하는 바이다. 중앙일보, “중국 ‘제4군’ 사이버부대 유학파 등 2000명 활약”, p. 3, 2004. 7.
- [12] 공공의 안녕이라 함은 한편으로 개인의 생명·신체·건강·자유·재산과 같은 개인적 법익과 다른 한편으로 국가적 공동체의 존속 및 기능과 같은 국가적 법익이 침해되지 않는 상태를 의미한다. 김남진, 행정법 II, p. 251.
- [13] 공공의 질서란 지배적인 사회·윤리관에 비추어 그것을 준수하는 것이 원만한 공동생활을 위한 전제로 간주되는 법규범 이외의 규범의 총체를 의미한다. 김남진, 앞의 책, p. 251.
- [14] Wolff/Bachof, Verwaltungsrecht III, S. 26f, 1978.
- [15] 김남진, 행정법 II, pp. 250-251.
- [16] 전통적인 경찰국가인 독일 등의 경우 2차 대전 후 실질적 의미의 경찰임무가 대폭 일반 행정기관에 이양되었다고 한다(위생·건축·산업·경제경찰 등). 김남진, 경찰행정법, 경제원, p. 17, 2002. 9.
- [17] 김남진교수는 개인의 안전을 보호하는 통상의 경찰을 보통경찰로 그리고 국가의 안전을 보호하는 경찰을 고등경찰로 설명하고 있다. p. 21.
- [18] 사이버 테러에 관한 많은 문헌들은 컴퓨터 네트워크의 취약성과 주요기간시설의 취약성은 동일한 것이며, 이를 취약성은 국가안전을 현저하게 위협할 것임을 지적하고 있으나, 공격에 취약하다는 컴퓨터 네트워크 및 주요기간시설과 국가안전에 대한 그 결과의 영향의 관계를 좀더 자세하게 살펴보면, 취약성의 지적은 잘못된 것이라고 한다. 즉, 많은 컴퓨터 네트워크는 쉽게 공격받을 수 있 는 상태에 있는 반면 주요시설의 경우에는 쉽게 공격받을 수 있는 상태에 있는 것이 거의 없다는 점이 감안되지 않았다고 한다. James A. Lewis, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber threats”, CSIS, 2002.
- [19] 미국의 경우 바이러스 제작자나 해커 겸거예 FBI나 NSA 같은 수사 및 첩보기관의 공이 크다는 사실은 널리 알려져 있다. 하지만 국정원내에 국가사이버안전센터를 두는 것은 신중하게 추진돼야 한다. 김현아, 국정원 ‘국가사이버 안전센터’ 구축, 신중해야, inews, 2003. 9.



정준현

1978년 성균관대학교
법률학과(법학사)
1982년 성균관대학교
대학원(법학석사)
1991년 고려대학교 대학원
(법학박사)

1986년 ~1996년 법제처 법제연구담당관
1997년 ~현재 선문대학교 법학과 교수



김귀남

미국 캘리포니아 대학교 수학과
(응용수학사)
미국 콜로라도주립대학
통계학과(통계학 석사)
미국 콜로라도주립대학
기계산업공학과
(기계산업공학박사)

현재 경기대학교 정보보호기술공학과 주임교수