이슈 보고서

2021 19

주요국 정부의 사이버보험 시장 참여 배경 및 동향

송윤아·홍보배

KiRi 보험연구원

머리말

정보통신기술(ICT)의 급속한 발전으로 사람과 공간·생물·정보·비즈니스 등 사물이 물리·가상공간의 경계 없이 서로 유기적으로 연결되어 소통하고 상호작용하는 초연결사회로 진입하였다. 네트워크는 사물인터넷(IoT), 인공지능(AI)과 같은 혁신 기술에 힘입어 더욱 고도화하면서 시공간 압축을 통해 지능과 정보에 기반을 둔 4차 산업혁명을 이끌며 새로운 기회와 가치를 창출하고 우리 삶의 변화를 가속화하고 있다.

초연결사회가 진행됨에 따라 사이버공격의 접점이 급증하여 통제 불가능한 사물들의 사이버 무기화가 개인 및 기업을 넘어 국가·사회적 문제로 부상하고 있다. 단 한 건의 성공적인 사이버공격이 거대 자연재해에 버금가는 수준의 피해를 초래하고 국가 주요 기반시설을 타격하며 기업 생존 및 국가안보를 위협하는 상황에 이르렀다. 초기 사이버공격이 주로 정보 유출 피해를 초래하였다면, 초연결·초지능·초고속화가 진행됨에 따라 물리적 피해와 막대한 기업활동중단 손해가 현실화되고 있다.

이처럼 사이버리스크 증가와 함께 동 리스크 관리 수단으로서 보험에 대한 기대가 커지고 있다. 그러나 사이버사고의 대재해 가능성이 예견되는 상황에서 보험산업의 보험담보 공급 축소는 불가피하다. 본 보고서는 최근 기업이 직면한 사이버리스크의 양적·질적 변화, 그로 인한 사이버보험 시장 내 수요 및 공급의 변화와 보장공백을 분석한다. 그리고 동 보장공백에 대한 미국, 호주, 영국, 프랑스 등 세계 보험시장을 주도하는 국가들의 대응을 면밀히 검토함으로써 우리나라에의 시사점을 도출한다.

마지막으로, 본 보고서에 수록된 내용은 연구자 개인의 의견이며, 우리원의 공식 의견이 아님을 밝혀 둔다.

2021년 12월

보험연구원 원장 **안 철 경**

목 차

표 차례

그림 차례

요 약

이 보고서는 최근 기업이 직면한 사이버리스크의 양적·질적 변화, 그로 인한 사이버보험 시장 내 수요 및 공급상의 변화와 보장공백을 분석하고, 동 보장공백에 대한 미국, 호주, 영국, 프랑스 등 사이버보험 시장을 선도하는 주요국의 대응을 검토하였다.

분석 결과, 2010년대 들어 사이버사고의 공격자는 개인 또는 범죄조직에서 국가·준정부조직·테러조직으로, 공격 동기는 호기심·금전·과시욕에서 정치적·군사적 동기로, 공격표적은 개인 또는 보안이 취약한 중소기업에서 공급망 및 산업제어시스템 공격을 통한 대기업과 국가기반시설로, 피해 유형은 정보 유출 및 개인정보 침해에서 재물·신체·영업중단 손해 등으로 확대되고, 피해심도는 통제가능한 수준에서 파괴적인 수준으로 진화하였다. 파괴적 사이버공격의 빈도 및 심도 증가와 기업의 사이버 관련 규제리스크 증가에 따라, 사이버보험에 대한 수요도 급격히 증가할 것으로 예상된다. 사이버리스크의 양적·질적 변화에 대응해 보험업계는 사이버보험 공급에 보수적 기조를 취할 것으로 보인다. 구체적으로, ① 사이버사고의 빈도 및 심도 증가, 대재해 가능성 등에 따른 보험업계의 공급 기조 변화, ② 암묵적 사이버담보의 언더라이팅 리스크 가시화와 그에 따른 포괄위험 담보방식 재물·배상책임보험의 사이버면책 확대 움직임, ③ 정보 유출 피해 등 배상책임과 비용보장에 집중된 단독 사이버보험의 비포괄성, ④ 2017년 낫페트야 공격으로 촉발된 국가배후 사이버공격에 대한 재래식 전쟁면책 적용 논란과 그로 인한 보험업계의 사이버 대재해 및 전쟁면책 움직임, 그리고 ⑤ 벌금 및 랜섬담보의 반공익성에 따른 규제 강화와 동 담보 제공 자제의 움직임 등이 관찰된다. 이에 따라 사이버사고로 인한 재물 및 영업중단 손해, NDBI, 신체손해, 국가 배후 사이버공격, 사이버 대재해, 그리고 벌금 및 랜섬담보에 대한 보장공백이 커질 것으로 예상된다.

이에 세계 사이버보험 시장을 선도하는 미국, 영국, 프랑스, 호주 등에서는 자국에서 이미 운영 중인 공사협력 테러보험 프로그램을 통해 '일부 사이버공격'으로 인한 손해에 대해 재보험담보 및 유동성을 제공하는 방식을 취하고 있거나 논의 중이다. 이미 테러보험 프로그램이 존재하는 상황에서는 사이버사고를 동 프로그램의 손인으로 추가하는 것이 정

책적으로 가장 용이한 접근일 뿐만 아니라, 사이버리스크에 대응한 공사협력 보험 프로그램을 새로이 구성하기에는 사이버리스크와 사이버보험 시장이 단기간에 급격하게 변하였기 때문으로 사료된다. 그러나 기존 테러보험 프로그램은 물리적 테러리즘과는 이질적인 사이버테러리즘의 특성을 반영하고 심각한 보장공백이 예상되는 사이버공격을 포섭하는 데 있어 여러 한계를 보였다. 무엇보다도 문제의 사이버사고가 테러리즘 요건을 충족해야 하므로, 인간의 실수에 의한 대규모 사이버사고, 범죄조직의 대규모 금전 목적 랜섬웨어 공격, 또는 국가 배후 사이버공격은 프로그램 적용대상에서 배제될 수 있다. 국가 배후 사이버공격, 경제적 목적의 사이버공격 등은 기존 '테러리즘'의 정의에 부합하지 않을 뿐만 아니라, 공격주체를 특정하기 쉽지 않아 특정 사이버공격을 '테러리즘'으로 인정하는 것에도 불확실성이 존재한다. 주요국은 이러한 한계를 이미 인지하고 있으며, 현 시점에서는 미국이 기존 테러보험 프로그램에 매몰되지 않고 사이버리스크에 대한 보장공백 해소 방안을 적극적으로 탐색 중이다. 미국에서는 재난적 규모의 사이버사고, 국가 배후 사이버공격, 사이버공격으로 인한 NDBI(물적 손해를 동반하지 않은 영업중단손해) 등에 대한 정부의 재보험담보 제공을 심도 있게 검토하고 있다. 호주에서도 테러리스트의 사이버공격으로 인한 기업의 재물손해 및 영업중단손해에 대해 정부가 재보험담보 및 지급보증을 제공하는 방안이 현재 긍정적으로 논의 중인 가운데, 보장범위에 국가 배후 사이버공격을 포함될 수 있도록 '공격자에 상관없이 정치적·종교적·이념적 목적을 가진 악의적 사이버공격'으로 논의 범위를 확대하고 있다.

자연재해나 물리적 테러리즘과 달리, 사이버사고로 인한 피해는 국경이 없고, 손해보험은 업의 속성상 활발한 국경 간 거래가 불가피한 산업이라는 점에서, 전술한 사이버보험 시장 상황이 특정 국가에 국한된 것은 아니다. 특히, 국내 사이버보험은 세계 보험시장을 선도하는 주요 국가의 보험제도 변화, 손해율, 보험요율, 인수전략 등에 상당한 영향을 받기 때문에 사이버리스크에 대한 보장공백의 문제가 특정 국가에 국한된 이슈는 아니다.

Ⅰ 서론

1. 연구 배경 및 목적

사이버리스크는 데이터 또는 서비스의 무결성·가용성·기밀성을 통합하는 정보통신기술(Information and Communication Technology; ICT)을 사용함으로써 발생하는 모든 리스크를 의미한다. 사이버공격으로 인해 당사자가 직접 입은 유·무형의 자산 손실, 영업중단손실, 인적 피해, 벌금 등 규제비용뿐만 아니라, 제3자에 대한 손해배상책임 등으로 구체화된다(〈표 Ⅰ-1〉 참조). 사이버공격으로 인한 직접비용과 파생적 간접비용(Systemic cost)은 7,990억~22.5조 달러로, 세계 총생산의 1.1~32.4%를 차지하는 것으로 추정된다(Dreyer et al. 2018).[1] 보험업계는 20여 년 전부터 사이버리스크의 일부를 보장하는 단독 사이버보험을 판매해왔다. 또한 보험회사가 의도했는지 여부에 상관없이, 포괄위험(Open-peril 또는 All-risk) 담보방식의 재물·배상책임보험을 통해 사이버담보를 암묵적으로 보장해 왔다.

2010년 중반부터 세계 사이버보험 시장에서는 정부가 공급자로 언급되는 이례적인 현상이 관찰된다. 2018년, 국내에서는 정보통신서비스 제공자가 업무수행 과정 중 소유·사용·관리하는 개인정보 유출 등으로 발생하는 제3자에 대한 배상책임에 대해 보험가입 의무화 논의가 한창이었다. 반면 동 기간 유럽에서는 개인정보 침해에 대해 실효적 수준의 벌금이 부과되는 법률이 시행되고, 매우 위험할 수 있으니 전통적인 포괄위험 담보방식의 재물 및 배상책임보험 증권에 '사실상' 사이버사고 면책을 명시적으로 표기하라는 신호를 정부가 보험업계에 보냈다. 영국에서는 테러리스트의 사이버공격으로 인한 재물손해 및 영업중단손해에 대해 정부의 유동성 제공을 결정하였다. 호주에서는 악의적 사이버공격으로 발생한 재물손해 및 영업중단손해에 대해 정부의 재보험담보 및 지급보증이 심도 있게 논의되었다. 미국에서는 테러리스트의 사이버공격에 대한 정부의 재보험담보 제공을

1) 사이버리스크에 대한 추정은 모수에 매우 민감하여 추정값의 편차가 크므로, 추정액 정보는 수치로서 의미를 두기보다는 사이버사고가 '대규모 리스크'를 초래하는 손인 중 하나라는 개념으로 받아들이기는 것이 적절함. 세계적 재보험회사 및 중개사 등이 추정값을 제시해왔으나, 이들은 직접적인 이해당사자인데다 추정방법론을 공개하지 않은 반면, Rand Corporation은 추정방법 및 모수를 상세히 공개한다는 점에서 분석 결과를 본문에 인용함

승인하는 데 그치지 않고 정부의 재보험담보 제공을 국가 배후 사이버공격, 재난적 피해를 유발하는 사이버공격 등으로 확대하는 방안을 검토하였다.

우리나라가 사이버사고로 인한 개인정보 침해에 대한 보상방안에 집중하는 동안, 수요와 공급 측면에서 세계 보험산업을 선도하는 국가들에서는 일부 조건을 충족하는 사이버공격에 대해 정부가 보험 공급자를 자처하거나, 원활한 보험공급을 지원하였다. 우리가 놓치고 있는 것은 무엇일까? 보험선도국의 정부들이 사이버보험 시장에 왜 이토록 적극적으로 참여한 것일까? 시장실패 및 보장공백이 존재한다면, 그 원인은 무엇이며 구체적으로 어느 부분에 공백이 존재하는 것일까?

최근 기업의 사이버리스크에 양적·질적 변화가 있었고, 그로 인해 사이버보험 시장에 심각한 보장공백이 발생하여, 그 방안으로서 정부의 적극적인 시장 참여가 결정 및 논의된 것이라면, 그 구체적인 방법 및 범위, 논의 과정, 쟁점, 기저논리 등을 살펴볼 필요가 있다. 자연재해나 물리적 테러리즘과 달리, 사이버사고로 인한 피해는 국경이 없고,[2] 손해보험은 업의 속성상 활발한 국경 간 거래가 불가피한 산업이라는 점에서, 작금의 시장 상황이 특정 국가에 국한된 것은 아닐 것이기 때문이다.

이 보고서는 먼저, 최근 기업이 직면한 사이버리스크의 양적·질적 변화, 그로 인한 사이버보험 시장 내 수요 및 공급상의 변화와 보장공백을 분석한다. 그리고 동 보장공백에 대한 미국, 호주, 영국, 프랑스 등 주요 보험선도국의 대응을 면밀히 검토함으로써 우리나라에의 시사점을 도출한다.

본 보고서는 2010년대 중반 이후 본격적으로 드러난 새로운 유형의 사이버리스크와 사이버보험 시장의 변화에 초점을 맞춘다는 점에서, 임준 외(2018)와 차별되는 상호배타적 연구범위를 가짐과 동시에 사이버리스크 및 보험에 대한 연구문헌(Literature)상으로는 임준 외(2018)의 연장선상에 있다. 임준 외(2018)는 국내 사이버사고 관련 현황과 미국, 유럽, 일본, 중국 등 주요국의 사이버보험 현황 및 활성화 전략을 살펴보고 정책적 시사점을 도출하였다. 그들의 연구는 국내 현황과 관련하여 사이버사고, 사이버보험 시장, 사이버의무보험, 사이버사고 관련 공적 규제 및 손해배상 등을 살폈는데, 분석 항목에서 짐작할 수 있듯이, 그들의 주요 논의 대상 손해는 정보 유출 및 개인정보 침해로 인한 배상책임인 반면, 이 연구의 논의 대상 손해는 재물·신체·영업중단손해로 상호배타적 연구범위를 형

2) 2017년 워너크라이(WannaCry) 랜섬웨어 공격은 150개국에 30만 대의 PC 감염을 초래하였고, 2017년 낫페트야(NotPetya) 공격은 러시아가 적성국인 우크라이나를 표적으로 한 공격이었지만, 그 피해가 전 세계로 확산되었음

성한다. 또한 임준 외(2018)의 핵심 의제 중 하나는 사이버보험의 수요 진작, 즉 사이버보험 가입 활성화로, 이 연구의 핵심 의제인 보장공백과는 대척점에 있다. 2018년 이전까지는, 적어도 정보 유출 및 개인정보 침해로 인한 배상책임손해에 대해서 수요가 상대적으로 중요한 문제였겠으나, 향후 문제는 수요가 아니라 수요를 따라잡지 못하는 공급이다. 독자에게는 임준 외(2018)와 더불어 이 연구가 사이버리스크와 사이버보험 시장의 발전 과정을 이해하는 데 도움이 될 것이다.

〈표 Ⅰ-1〉 기업의 사이버리스크

당사자		제3자
직접손실	비용	
• 금융 도난 및 사기 • 지적재산 도난 • 영업중단손해 • 사이버 협박 • 평판 손실 • 물적 자산 손실	• 법률비용 • 계약상 벌금 • IT 포렌식 • 통지 • 데이터 및 소프트웨어 손실 • 평판 손실 관리 • 물적 자산 손실로 인한 비용	• 데이터 Compromise • 금융 도난 및 사기 배상책임 • 네트워크 서비스 실패 배상책임 • 지적재산 도난 배상책임 • 인격권 침해 배상책임 • D&O 배상책임 • 일반자산손실 배상책임

자료: Wrede et al.(2020)

2. 연구 내용 및 방법

2장에서는 최근 기업이 직면한 사이버리스크의 양적·질적 변화, 그로 인한 사이버보험 시장 내 수요 및 공급의 변화와 보장공백을 분석한다. 이를 위해 사이버보안보다는 보험의 관점에서 게임체인저가 되는 사이버사고를 중심으로 주요 공격자, 공격동기, 공격표적, 손해 유형 및 심도 등의 변화를 파악하고 동 리스크의 양적·질적 변화에 대응한 수요 변화를 분석한다. 다음으로, 사이버리스크의 양적·질적 변화에 대응한 공급 부문의 주요 변화를 살펴본다. ① 사이버사고의 빈도 및 심도 증가, 대재해 가능성 등에 따른 보험업계의 공급 기조 변화, ② 암묵적 사이버담보의 언더라이팅 리스크 가시화와 그에 따른 보험업계의 포괄위험 담보방식 재물·배상책임보험 내 사이버면책 확대 움직임, ③ 정보 유출 피해 등 배상책임과 비용보장에 집중된 단독 사이버보험의 비포괄성, ④ 2017년 낫페트야 공격으로 촉발된 국가 배후 사이버공격에 대한 재래식 전쟁면책 적용 논란과 그로 인한

보험업계의 사이버 대재해 및 전쟁면책 움직임, 그리고 ⑤ 보험회사의 벌금 및 랜섬(Ransom) 담보의 반공익성에 따른 규제 움직임이다. 마지막으로, 수요는 존재하나, 보험업계가 위험평가역량 부족 또는 대재해가능성으로 담보제공을 꺼려, 수요와 공급 간 공백이 존재하는 손해유형을 분석한다.

3장에서는 미국, 호주, 영국, 프랑스 등 보험선도국 정부의 사이버보험 시장 참여 동향을 살펴본다. 구체적으로, 각국 정부의 사이버리스크에 대한 보장공백 해소 방법 및 범위, 기저논리와 근거, 의사결정의 과정, 한계 및 추가 논의사항 등을 살펴본다. 4개국 모두 기존 공사협력 테러보험 프로그램 내에서 테러리스트의 사이버공격으로 인한 재물손해와 영업중단손해에 대해 정부가 재보험담보 및 유동성을 제공하고 있거나, 제공 여부를 논의 중이다. 저자가 파악한 바로는, 현 시점에서 사이버사고로 인한 보장공백을 해소하고자 기존 테러보험 프로그램과 상관없이 정부가 시장에 공급자로 참여한 사례는 없다. 전술한 4개국은 동일한 문제에 직면하여 궁극적으로 동일한 해결방안을 가지나, 국가별로 진척도에 차이가 있다. 예를 들어, 미국의 경우 정부가 사이버 테러리즘에 대해 재보험담보를 이미 제공하고 있는 가운데, 현재 정부의 재보험담보 제공 범위 확대가 심도 있게 논의되고 있다. 무엇보다도, 사이버사고의 보장공백을 물리적 테러리즘을 계기로 설립된 기존 테러보험 프로그램을 통해 해소하려다 보니, 많은 한계에 봉착하게 되었다. 미국은 현재 이러한 한계를 인지하고 극복하는 방안을 다각도에서 검토하고 있다. 반면, 호주는 사이버 테러리즘으로 인한 재물손해에 대해 정부가 재보험담보 및 지급보증을 제공하는 방안을 검토 중이다. 국가별로 진척도가 상이하기 때문에, 진행단계별로 핵심의제나 고려사항을 살펴볼 수 있을 것으로 기대된다. 또한, 미국과 프랑스는 문제의 사이버공격이 일정 조건을 충족하면 자동적으로 기존 공사협력 테러리즘 프로그램의 적용대상이 되는 구조이기 때문에 사이버사고를 기존 테러리즘 프로그램의 적용대상 손인(Peril)으로 추가할 것인지에 대한 사회적 논의 자체가 생략되었다. 반면, 영국과 호주의 경우 특정 사이버사고를 기존 공사협력 테러보험 프로그램의 적용대상 손인으로 포함할지 여부에 대한 의사결정이 별도로 이뤄져야 하는 구조로서, 영국은 2018년에 그러한 결정이 이뤄졌으며, 호주는 현재 검토 중이다. 영국과 호주의 의사결정 과정과 기저논리 및 선결요건 등을 엿봄으로써 향후 우리의 논의에 참고할 수 있을 것으로 기대한다.

4장에서는 보고서를 요약하고, 정책 제언으로 마무리한다. 자연재해나 물리적 테러리즘과 달리, 사이버사고로 인한 피해는 국경이 없다. 우리나라도 국제사회가 경험하고 있는 유형의 사이버리스크에 심각하게 노출되어 있다(〈표 Ⅰ-2〉 참조). 더불어 국내 사이버보

험은 세계 보험시장을 선도하는 주요 국가의 보험제도 변화, 손해율, 보험요율, 인수전략 등에 영향을 받기 때문에 사이버리스크에 대한 보장공백의 문제가 특정 국가에 국한된 이슈는 아니다. 이에 우리나라 정부의 정책적 대응에 앞서 국내 기업의 사이버리스크 실태 분석과 국내 사이버보험 수요 및 공급 분석의 필요성을 제언하는 것으로 보고서를 마무리 한다.

〈표 Ⅰ-2〉 우리나라의 사이버공격 피해 사례

공격	주체 및 수단	대상 및 피해
2003. 1. 25 인터넷 대란	슬래머 웜	MS사 DB, 한국 8천여 대·전 세계 7만여 대 PC 다운
2004	중국 해커조직	원자력연구소 등 국책연구기관, 국회 등 10개 국가기관 시스템, 6개월간 중요 기밀 유출
2009. 7. 7 DDoS 공격	북한 (최초 확인)	청와대 등 국가 주요기관, 언론사·은행 등 21개 사이트
2011. 3. 4 DDoS 공격	북한	국회·통일부 등 20개 정부 주요기관 홈페이지, 증권사·은행·포털 등 20개 사이트 마비
2011. 4. 12	북한·APT 공격	농협 전산망
2013. 3. 20	북한	YTN, 신한은행 등 방송·금융 6개사 4만여 대 PC·서버, ATM기기 3천여 대 손상
2013. 6. 25	북한·DDoS 공격	청와대 홈페이지, 정당, 언론사 전산시스템
2014	북한·해킹	한국수력원자력
2015. 6	북한·DDoS 공격	서울지하철, 청와대, 국회, 통일부, 대구은행 등
2016	북한·악성코드	서울지하철, 청와대, 국회, 통일부, 대구은행 등
2017. 3	DDoS 공격	롯데 인터넷 면세점
2017. 5	워너크라이	150개국 30만 대 PC

자료: 채재병(2019); 신영웅(2020)

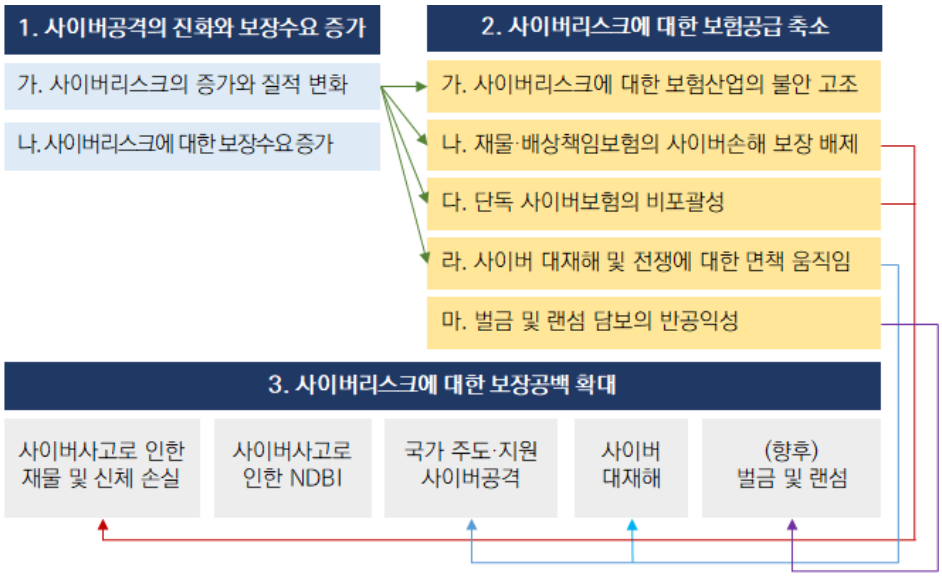
Ⅱ 사이버리스크에 대한 보장공백 확대

최근 미국, 영국, 프랑스 등에서는 기존 공사협력 테러보험 프로그램을 이용하여 '테러리스트'의 사이버공격으로 인한 직접적인 재물손해 및 영업중단손해에 대해 정부가 보험회사에 재보험담보 또는 단기유동성을 제공하기로 하였다.[3] 여기에 그치지 않고, 기존 공사협력 테러보험 프로그램에서 보장하는 사이버공격의 범위와 손해유형을 확대하는 방안을 적극적으로 논의하고 있다. 예를 들어, 미국에서는 재난적 규모의 사이버사고, 국가 배후 사이버공격, 사이버공격으로 인한 물적 손해를 동반하지 않은 영업중단손해 등에 대한 보장을 다각도에서 검토하고 있다. 호주에서도 테러리스트의 사이버공격으로 인한 기업의 재물손해 및 영업중단손해에 대해 정부가 재보험담보 및 지급보증을 제공하는 방안이 현재 긍정적으로 논의 중이며, 국가 배후 사이버공격을 포함할 수 있도록 '공격자에 상관없이 정치적, 종교적, 이념적 목적을 가진 악의적 사이버공격'으로 논의 범위를 확대하고 있다.

이처럼 정부가 특정 시장에 공급자로 참여하는 것은 매우 이례적인 현상이다. 정부가 사이버보험 시장에서 원보험자, 재보험자, 유동성제공자, 지급보증자 등 공급자로서 기능한다면, 이를 정당화할 수밖에 없는 불가피한 시장환경이 존재할 것이다. 주요국 정부의 사이버보험 시장 참여 동향을 논의하기에 앞서, 참여 배경을 살펴볼 필요가 있다. 이 장에서는 구체적으로, 최근 기업이 직면한 사이버리스크의 양적·질적 변화, 그로 인한 사이버보험 시장 내 수요 및 공급의 변화와 보장공백을 분석한다.

3) 미국, 영국, 프랑스, 독일, 스페인, 호주 등 주요국의 공사협력 테러보험 프로그램에 대한 상세한 내용은 송윤아·홍보배(2021)을 참조하기 바람

〈그림 Ⅱ-1〉 정부의 사이버보험 시장 참여 배경



자료: 저자가 작성함

1. 사이버사고의 진화와 보장수요 증가

가. 사이버리스크의 증가와 질적 변화

1) 사이버사고의 스펙트럼

컴퓨터 시스템과 통신망으로 만들어진 영역을 사이버공간(Cyberspace)이라 한다. 사이버공간을 지탱하는 것은 컴퓨터 시스템과 통신망(Network)이다. 국가, 기업 혹은 개인에게 있어 중요한 기능을 하는 컴퓨터 시스템과 통신망이 내·외부 공격으로 훼손 혹은 마비되는 경우에 해당 국가, 기업 혹은 개인에게 중대한 피해가 발생하게 된다. 따라서 사이버공간을 구성하는 컴퓨터 시스템과 통신망의 안전에 대한 침해는 현대 정보사회의 안전에 대한 심각한 위협이라고 할 수 있다.

사이버사고는 인간의 실수 또는 부주의(시스템 결함 포함)로 인한 비악의적 사이버사고와

악의적인 사이버사고, 즉 사이버공격으로 구분할 수 있다(〈그림 Ⅱ-2〉 참조). 공격자, 공격표적, 피해양상, 공격동기 등을 종합적으로 고려할 때 사이버공격은 사이버범죄(일반 정보시스템 및 정보 침해), 사이버 테러리즘, 사이버전쟁으로 대별할 수 있다. 사이버범죄는 전통적으로 개인 또는 사인의 집단이 자신의 경제적 이익을 획득할 목적으로 실행되며, 특정 업무 마비 및 정보 유출 피해를 초래한다. 사이버 테러리즘은 국가·사회적으로 공포 내지 불안을 조성하기 위한 컴퓨터시스템 운영 방해, 정보통신망 침해 또는 전자적 침해 행위로서, 한 사회나 국가에 공포심 내지 불안감을 조성할 수 있는 정도에 도달하는 사이버공격으로 볼 수 있다. 일반적으로 테러리즘은 한 건의 공격으로 피해를 극대화하는 데 공격의 방점이 있기 때문에 주요 사회기반시설이 표적이 되고, 성공적인 테러리즘은 사회기능 마비와 공포를 극대화한다. 2010년대 들어서는 특정 국가가 사이버공격을 배후에서 주도 또는 지원하는 등 국가가 사이버공간에 공격자로 참여하면서 사이버 테러리즘과 구분하여 사이버전쟁이라는 용어가 등장하였다.

사이버 테러리즘에 대해 국제적으로 합의된 일반적인 정의가 아직 존재하지 않고, 사이버 테러리즘이 국가를 공격자로 포함하는지 여부에 대한 학술적 합의가 없는 가운데, 국가가 공격의 주체 또는 배후로 등장하면서 사이버 테러리즘과 사이버전쟁의 개념적 구분에 혼란이 존재한다.[4] Plotnek and Slay(2021)은 사이버 테러리즘을 비국가 행위자들이(Non-state actors) 정치적·사회적 목적을 추구하고자 정부나 사회를 협박 또는 강제하기 위하여 정보시스템을 대상으로 고도의 손상을 야기하는 컴퓨터에 기반을 둔 공격이나 위협으로 규정한다. Plotnek and Slay(2021)의 정의에 따르면, 공격자가 국가인지 여부에 따라 사이버 테러리즘과 사이버전쟁을 구분할 수 있을 것이다. 이 보고서 제3장에서 살펴보겠지만, 국가가 원보험자, 재보험자, 지급보증자, 또는 유동성제공자 등으로 참여하는 각 국의 테러보험 프로그램에서도 해당 프로그램의 발동 요건인 '테러리즘'을 정의함에 있어, 행위 주체에 '국가', '국가 주도 또는 지원' 등에 대한 언급이 없다.[5]

4) 사이버범죄·테러리즘·전쟁에 대해 국제적으로 합의된 단일의 정의는 존재하지 않으며, 개별 국가의 법률 혹은 국제·지역적 협약에서 사이버범죄에 대한 정의를 포함하는 경우는 많지 않음. 실무와 학계에서는 사이버공격에 대한 다양한 정의를 제시하고 있으나, 사이버공격의 개념은 이에 대한 정의를 내리기 위한 목적에 따라 그 범위 및 구체화 정도가 다르게 나타남. 예를 들어, 국가사이버안전관리규정(제2조)은 사이버공격을 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위로 정의하며, 표적을 국가정보통신망으로 한정함

5) 2002년 유엔 총회에서는 "개인 또는 집단의 행위가 실제로 해당 국가의 지시 또는 통제하에 수행되었을 경우 국제법에 따라 국가의 행위로 간주된다"는 원칙을 포함하는 국제적 위법 행위에 대한 국가의 책임에 관한 결의안(Resolution on the responsibility of States for internationally wrongful acts)을 채택함

그러나 범죄, 테러리즘, 전쟁이라는 개념을 정의함에 있어서 애매모호하고 중첩되는 현상들이 나타나 상호배타적인 개념적 구분은 사실상 어렵다. 이러한 애매모호함은 특정 행위자가 동시에 서로 다른 종류의 행위에 연루되어 있기 때문에 나타나기도 하며, 특정 행위가 중첩되는 의미를 동시에 내포하고 있는 데에서 기인한다. 예를 들면, 북한으로부터 시도되었다고 의심되는 사이버공격과 같은 경우 적성국가에 의한 적대적 행위 즉, 전쟁 행위로 간주될 수도 있으나, 순수하게 경제적 이익을 위해 실행됐을 가능성을 배제할 수 없다는 점에서 사이버 테러리즘·전쟁이자, 사이버범죄의 특성을 동시에 가지기도 한다.[6] 이처럼 범죄와 테러리즘, 그리고 전쟁은 일련의 연속되는 스펙트럼상에서 연속적으로 배치되어 있는 폭력적 행동양식이다. 각 행동양식은 서로 중첩되는 애매모호한 교집합의 형태로 포함되는 다중적 성격을 동시에 가지고 있으므로 공통된 행동양식 또는 현상들을 포함하고 있다.

현재로서는 어떠한 사이버공격이 전쟁행위로 간주되어야 하는지에 대한 국제적인 법적 지침은 없지만, 다수의 국가와 국제기구는 어떠한 특정 유형의 사이버공격이 기준점을 충족하는지를 밝히고 있다(OECD 2020b). 예를 들어, EU는 2017년 악의적 사이버행위는 유엔 헌장(Charter of the United Nations)에 의거, 무력 사용 또는 무력 공격과 동일하게 간주될 수 있다고 보았다.[7] 영국 검찰(Attorney General)은 2018년, 무력 공격과 동등한 규모의 살상과 파괴를 초래하거나 이와 같은 위협을 주는 사이버공격에 대해 유엔 헌장 제51조에서 인정한 대응 행동을 취할 권리를 갖는다고 보았다(U.K. Attorney General's Office 2018).[8] G7은 2017년 사이버공간에서의 책임 있는 국가의 행동에 관한 선언문(Declaration on Responsible States behavior in Cyberspace)을 통해 같은 취지의 내용을 발표했으며(G7 2017), 북대서양조약기구 NATO도 2014년, 사이버공격은 NATO의 집단방위(Collective defense) 협정을 발동시킬 수 있다고 발표하였다(NATO 2014).

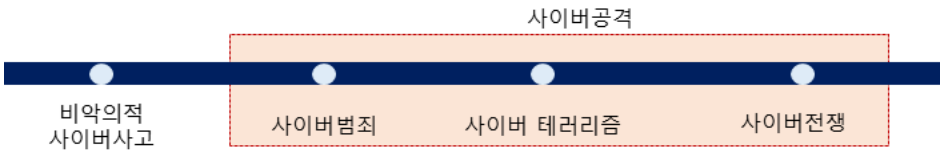
6) 미국 CISA(Cybersecurity&Infrastructure Security Agency)는 UN 보고서(UN Security Council 1718 Committee Panel of Experts' 2019 mid-term report)를 인용하여, UN의 대북제재로 경제난을 겪고 있는 북한은 사이버공격을 외화벌이 수단으로 사용하기도 한다고 밝힘; Cybersecurity&Infrastructure Security Agency(2020. 6. 23)

7) General Secretariat of the Council of the European Union(2017)

8) 유엔헌장 제51조는 다음과 같음. 이 헌장의 어떠한 규정도 국제연합회원국에 대하여 무력공격이 발생한 경우, 안전보장이사회가 국제평화와 안전을 유지하기 위하여 필요한 조치를 취할 때까지 개별적 또는 집단적 자위의 고유한 권리를 침해하지 아니함. 자위권을 행사함에 있어 회원국이 취한 조치는 즉시 안전보장이사회에 보고됨. 또한 이 조치는, 안전보장이사회가 국제평화와 안전의 유지 또는 회복을 위하여 필요하다고 인정하는 조치를 언제든지 취한다는, 이 헌장에 의한 안전보장이사회의 권한과 책임에 어떠한 영향도 미치지 아니함

용어 선택에 따라 보험금 지급여부가 달라지는 만큼 보험약관 용어는 배타적인 개념적 구분을 필요로 한다. 사이버범죄, 사이버 테러리즘, 그리고 사이버전쟁 등의 개념 간 애매모호함 및 중첩성은 보험산업의 전쟁면책 적용여부에도 논쟁을 초래한다.[9] 사이버범죄·테러리즘·전쟁 간 중첩성 및 애매모호함을 해소하기 위해, 2020년 제네바협회(Geneva Association; GA)와 국제 테러리즘 리스크 (재)보험풀 포럼(International Forum of Terrorism Risk Reinsurance and Insurance Pools; IFTRIP)은 사이버공격을 사이버범죄, 사이버 테러리즘, 적대적 사이버행위(Hostile Cyber Activity; HCA), 사이버전쟁으로 구분하였다. 즉, 사이버 테러리즘과 사이버전쟁 사이에 적대적 사이버행위를 삽입하여 사이버전쟁의 개념을 보다 명확히 구분하고자 하였다. GA·IFTRIP는 공식적으로 전쟁으로 선포되었거나, 선포가 없더라도 누가 보더라도 전쟁이 자명한 공격을 사이버전쟁, 국가가 연루된 것은 맞으나 연루 정도가 애매한 공격을 적대적 사이버행위로 규정하였다. 그러나 이러한 구분은 사이버귀책에 대한 문제 등 여전히 논쟁의 여지를 가진다.

〈그림 Ⅱ-2〉 사이버사고의 스펙트럼



자료: 저자가 작성함

9) 상세한 내용은 이 보고서 2장 2절 라.를 참고하기 바람

〈표 Ⅱ-1〉 사이버공격의 스펙트럼

구분	사이버범죄	사이버 테러리즘	사이버전쟁
공격자	개인, 범죄단체	비국가 행위자, 준정부 테러조직	국가
공격동기	경제적 이익, 호기심, 과시욕구	정치, 종교, 민족, 군사, 이데올로기적 이익	정치, 군사, 경제, 전반 국가이익
공격표적	일반 정보시스템	주요 국가기반시설	주요 국가기반시설
피해양상	특정 업무 마비 및 정보 유출	사회기능 마비 및 공포 조장	국가기능 및 전쟁수행력 파훼
공격수법	해킹, 악성코드 유포, 서비스 거부 공격, 기타 유형 등	해킹, 악성코드 유포, 서비스 거부 공격, 기타 유형 등	해킹, 악성코드 유포, 서비스 거부 공격, 기타 유형 등
공격 근원지	국내외	국내외	국외

주: 국제사회 및 학술 논의에 근거하여 개념적 특성을 구분한 것으로, 국제적·학술적·법적으로 합의·확정된 개념은 아님
자료: 저자가 작성함

2) 공격자 및 표적 확대

사이버공격은 초기 개인 단위의 일반적인 공격형태를 넘어 기업 단위의 범죄형 공격이나 준정부 테러조직 및 국가 단위의 공격으로 발전하였다. 초기 정보사회에서는 해킹 능력의 과시욕구, 호기심이 사이버공격의 주된 동기였으나 2010년대 들어서는 경제적 이익, 그리고 정치적·이념적·군사적 동기의 사이버공격이 실행되고 있다. 공격동기와 함께 공격자의 범위도 확대되었다. 경제적 이익을 목표로 하는 범죄조직, 산업기밀을 훔치기 위한 산업 스파이, 대부분의 시간을 비밀 정보를 훔치는 단 한 가지 일에만 전념하는 해킹 그룹 배후에 준정부 테러조직, 국가 등이 사이버 공격자로 참여한다. 사이버공격은 비용 및 위험 대비 효과가 큰 대표적인 비대칭전력으로 간주되기 때문이다.

범죄조직이 악성 프로그램을 이용하여 시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 만들고 이를 풀어주는 대가로 금전을 요구하는 공격사례가 2010년대 들어서 빈번해지고 있다. 예를 들어, 워너크라이(WannaCry), 낫페트야(NotPetya), 록커고가(LockerGoga) 랜섬웨어 공격이 기업 및 정부기관에 상당한 피해를 초래하였다. OECD(2020a)에 따르

면, 2017년 이전까지는 사이버보험 지급보험금 중 랜섬과 사이버 협박에 대한 보험금은 10~20% 수준이었으나, 2017년 워너크라이와 낫페트야 공격으로 21~31% 수준으로 증가하였다. 뿐만 아니라 랜섬 요구액도 점차 높아져서 보험회사가 랜섬웨어 보상한도를 보수적으로 설정하거나 보험료를 인상한 것으로 알려져 있다.

사이버공간에서 국가가 공격자 또는 배후로 참여하여 타국의 안보에 실체적 위협으로 작용한 것은 2010년대 들어서이다. 2010년, 이란은 미국과 이스라엘의 스턱스넷(Stuxnet) 공격으로 원자력발전소와 우라늄 농축시설의 가동이 중단되는 물리적 피해를 입었다. 공격자가 국가기관이고 피해목표가 물리적 시설이었다는 점에서 사이버 보안의 관점에서는 이정표가 되는 사건이었다. 스턱스넷은 지멘스(Siemens)에서 제조한 특정 PLC(Programmable Logic Controller, 프로그램 가능 로직 제어기)의 프로그램을 변경하여 원심분리기의 작은 속도 변화 및 마모를 초래하였다. 스턱스넷은 악성코드가 PLC를 어떻게 장악하는지를 전 세계에 보여준 첫 사례가 되었다.

사이버공격의 표적도 개인 및 중소기업 대상 정보 공격에서 주요 기업의 산업제어시스템(Industry Control System; ICS) 및 국가기반시설로 확대되었다. ICS는 그동안 외부 접근이 차단된 폐쇄적인 환경과 특정 회사의 기술로 구축되어, 대중적인 사이버공격이 통하지 않았다. 그러나 최근 IoT 센서, 인공지능(Automatic Intelligence; AI), 빅데이터, 5G 등 다양한 정보통신기술(Information Communication Technology; ICT)과의 융합에 따른 스마트화로 시스템의 외부 연결이 늘어남에 따라 공격의 표적이 되고 있다(최윤성 2021). 운영기술(Operation Technology; OT)[10] 및 ICS에 대한 표적 공격은 물리적인 피해와 직접적으로 연결되어 있어, 공격자는 단 한 번의 성공적인 공격으로 파괴적인 피해가 발생할 수 있는 점을 노린다. ICS 공격은 생산 중단으로 인한 매출 손실, 작업자 인명 피해 사고 등 파괴력을 가진다. 2018년 대만 TSMC의 워너크라이 랜섬웨어 감염, 2019년 세계 최대 알루미늄 제조기업인 노르웨이 노르스크 하이드로(Norsk Hydro)의 록커고가(LockerGoga) 랜섬웨어 감염,[11] 2020년 일본 혼다 자동차공장 Ekans 감염[12] 등 OT 시스

10) OT는 산업제어시스템(ICS)의 자동화 및 이를 실행하는 데 필요한 모든 시스템 환경을 의미함

11) 노르스크 하이드로는 세계 곳곳에 지사가 있었는데, 이를 연결하는 글로벌 IT 네트워크 시스템이 록커고가 랜섬웨어에 감염됨. 록커고가는 공장 시스템의 데이터를 사용할 수 없도록 암호화함. 이에 알루미늄 공장의 운영을 수동 모드로 전환하였지만 알루미늄 원재료를 뜨거운 열로 녹여 가공하는 작업의 특성상 생산 및 운영 차질이 불가피했음. 결국 이 회사는 75만 달러(약 900억 원)에 이르는 피해를 보게 되었고, 이 사고로 전 세계 알루미늄 생산량이 감소하여 알루미늄 가격이 상승함

12) 2020년 6월, 사이버공격을 받은 사내 네트워크 시스템이 장애를 일으켜 미국과 인도, 브라질, 터키 등 전 세계 공장 여러 곳의 생산라인 관리시스템이 마비되었고, 일본 공장에서는 완성차 출하가 중단되었음

템 사고가 빈발하고 있다.

특히, 주요 사회기반기설이 전략적 공격 목표로 부상하여 이와 연결된 OT 및 ICS에 대한 사이버공격이 더욱 증가하고 있다. 우크라이나 정전사태, 독일 원자력 발전소 악성코드 감염, 우크라이나 공항 공격, 영국 철도 사이버공격, 미국 콜로니얼 파이프라인의 송유관 공격[13] 등 사회기반시설을 표적으로 하는 사이버공격 시도가 점점 증가하고 있다. 사회기반시설에 대한 OT·ICS 공격은 파괴적 피해를 초래한다는 점에서 금전 목적의 범죄조직이나 정치적·군사적 목적의 테러조직, 나아가 국가 단위 공격자에게 가장 매력적인 표적이다. 금융, 통신, 의료, 교통, 정부시설, 에너지, 상수도, 제조 등 주요 사회기반시설은 해당 시스템 및 자산의 불능상태나 파괴가 안보·국가경제안보·국가보건 및 치안 또는 이러한 문제가 결합한 부분을 약화시킬 수 있는 물리적·가상적 시스템 및 자산이다. 언급된 분야 중 어떠한 것이라도 그 기능을 방해하거나 불능상태에 빠뜨리는 사이버공격은 잠재적으로 파괴적인 효과를 가지고 있는 것이 사실이다. 그 효과는 인명손실에서부터 재정손실에 이르며, 민간기관과 정부기관 모두 해당된다. 이처럼 주요 사회기반시스템이 본질적으로 갖는 취약성은 공격자에게 매력적인 표적이 된다.

3) 피해 유형 및 심도 확대

가) 피해 유형

물리적 현실세계와 디지털 가상세계를 연결하는 사물인터넷으로 발현되는 초연결사회에서는 피해의 범위가 더 이상 사이버공간에 국한되지 않는다. 초기 사이버공격은 정보의 유출, 훼손, 변조, 도용, 개인정보 및 저작권 침해 등으로 주로 금전적·정신적 손해를 초래하였다. 최근에는 ICT기술을 매개로 공격의 강도를 높이고 공격범위를 확장하여 물리적 자산과 인명을 위협하는 수준에 이르렀다. 특히, ICS에 대한 표적 공격은 물리적인 피해

13) 2021년 5월 7일, 미국 대형 송유관 업체인 콜로니얼 파이프라인(Colonial Pipeline)사가 다크사이드(DarkSide)라는 러시아 기반 랜섬웨어 범죄 집단의 공격을 받음. 콜로니얼 파이프라인은 총 길이 5,500마일(약 8,800km)로, 동부 일대 가솔린·디젤 연료 소비량의 45%를 공급해 온 송유관 업체임. 제품 생산에서 판매까지 산업 시스템 자동화가 이루어진 상황에서 랜섬웨어 공격이 발생하자 시스템이 전면 중단되는 사태가 벌어졌음. 해당 지역 주유소의 물량 공급이 6일 동안 중단되면서 휘발유 가격이 폭등함. 랜섬웨어 공격 이후 6~7월 국제유가 선물시장의 체결 시세가 뛰고, 미국 현지 주유소에선 '사재기'가 벌어졌으며, 석유 재고 부족 등으로 조지아·노스캐롤라이나·플로리다·버지니아주에서는 비상사태가 선포되는 등 파장이 컸음. 콜로니얼 파이프라인은 해킹당한 사실을 알게 된 당일, 운영시스템을 복구하기 위해 해커들에게 75비트코인(당시 440만 달러 상당, 50억 원)을 지불함. FBI는 공격자들의 자금 추적을 통해 6월 7일 230만 달러(26억 원, 63.7비트코인) 상당의 비트코인을 회수함

와 직접적으로 연결되어 있어, 영업중단으로 인한 손실과 작업자 인명 피해 사고 등을 초래하고, 국가기반시설과 연결된 ICS 공격은 대규모 정전 사태, 방사능 유출, 시장교란으로까지 이어진다.

2010년대 들어서면서 사이버공격으로 인한 재물피해 및 영업중단손해, 배상책임손해 등이 급격히 증가하였다. 2010년 스턱스넷은 악성코드로 원격에서 물리적 피해를 초래하여 세간의 주목을 받은 최초의 공격으로 상징성을 가지지만, 1,000여 개에 달하는 고농축 우라늄 원심 분리기에 과부하를 일으켜 사용불가 상태로 만드는 피해에 그쳤다. 2014년 독일 제철소 공격은 사이버공격의 목표가 정보 유출이 아니라 물리적 시설에 대한 타격이었으며 공격이 성공했다는 점에서 보안 및 보험의 관점에서 이정표가 되는 사건이다(〈그림 Ⅱ-3〉 참조). 2014년 익명의 해커그룹이 독일의 제철소 직원에게 스피어피싱(Spear-phishing) 이메일을 보내, 열어 보는 순간 직원의 아이디와 패스워드가 유출됐다. 해커그룹은 훔친 아이디와 패스워드로 용광로 컨트롤 통신망에 접속했다. 해커들이 제어시스템 기능을 차단해 용광로가 적절한 폐로 과정을 거치지 못함으로써 막대한 손실이 발생했다. 2015년에는 우크라이나에서 발전소로부터 전력을 공급받아, 가정이나 상가, 공장 등에 분배하는 배전망 회사 ICS에 대한 사이버공격이 발생하였고, 총 3곳의 배전 회사 IT시스템이 사이버공격을 받아 결국 변전소와의 전기 연결이 3시간 동안 끊어졌고, 약 225,000가구가 피해를 보았다.[14] 2019년에는 세계 최대 알루미늄 제조사가 록커고가 랜섬웨어에 감염되어 생산 및 운영에 차질이 빚어져 국제 알루미늄 가격이 인상되었다. 2020년에는 미국 최대 송유관 업체의 ICS 시스템이 공격받아 석유 공급이 중단되면서 미국 휘발유 평균가격이 6년 반 만에 처음으로 1갤런당 3달러를 상회하였다.

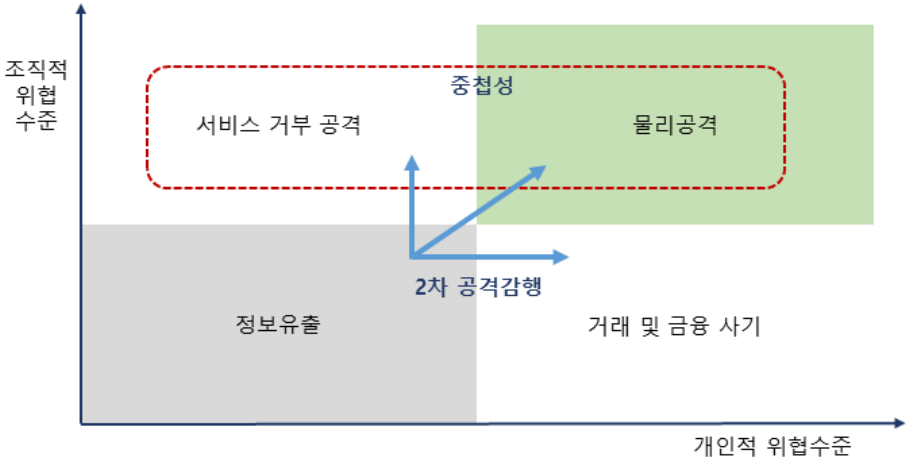
사이버공격으로 인한 인명피해의 가능성도 커졌다. 2021년 2월 플로리다 소도시에 위치한 정수처리 시설이 사이버공격을 당했다. 해당 사이버공격을 시도한 공격자는 데스크톱의 공유 소프트웨어인 팀뷰어(TeamViewer)를 통해 원격으로 제어시설에 접근해 주거용 및 상업용으로 사용되는 식수의 수산화나트륨 농도를 정량보다 100배 높게 설정하였다. 직원에 의해 발각되지 않았다면 주민들이 음독 사고를 겪을 수도 있는 사건이었다.

14) 미국 CSIS(Center for Strategic and International Studies)는 2006년 이후 발생한 심각한 사이버사고를 시간 순으로 정리·공개함. 사이버공격의 상세 내용은 이를 참조하기 바람

〈그림 Ⅱ-3〉 보험 관점 주요 사이버사고

자료: 저자가 작성함

〈그림 Ⅱ-4〉 사이버사고의 피해 유형



자료: 유성민(2016)

나) 피해 심도

대규모 랜섬웨어 공격으로 인한 손실액은 자연재해 피해액과 유사한 것으로 나타난다. 2017년 워너크라이와 낫페트야 공격으로 발생한 경제적 손실은 각각 80억 달러, 100억 달러로 추정되는데, 미국에서 발생한 자연재해 손실액은 100~250억 달러에 달한다(〈그림 Ⅱ-5〉 참조). 공격기법이 보다 정교해지고 파괴적인 방향으로 발전한다는 점에서 랜섬웨어 공격의 손실액이 거대자연재해를 넘어설 것이라는 전망도 있다. Lloyd's와 University of Cambridge의 공동연구는 랜섬웨어의 전 세계적 감염 시 경제적 손실이 850억~1,930억 달러에 이르며, 이 중 보험으로 보장되는 손실이 2억~4억 달러에 불과할 것으로 추정하였다(Lloyd's&University of Cambridge 2015). Lloyd's는 리스크 모델링업체인 AIR Worldwide와의 공동연구에서 미국에서 사이버공격으로 3일간 클라우드 사용이 중단될 경우 미국 내 1,250만 개사에서 150억 달러의 잠재적 손실이 예상된다고 발표하였다(Lloyd's 2018).

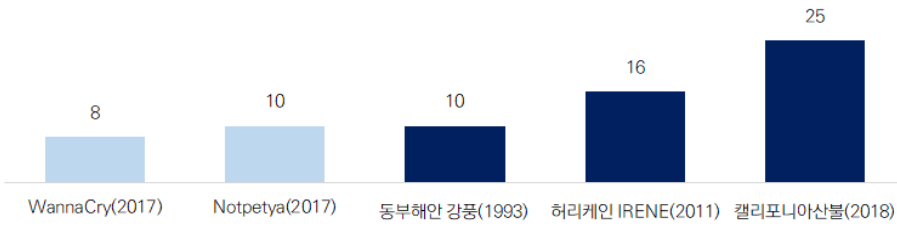
보안강화에도 불구하고 공급망을 통한 사이버공격이 실행되면서, 피해 규모·범위·기간 등이 걷잡을 수 없이 커지고 있다. 공급망 공격(Supply chain attack, third-party attack)은 자사의 시스템 및 데이터에 접속할 수 있는 외부 협력업체나 공급업체를 통해 누군가가 시스템에 침투하여 피해를 야기하는 형태의 공격이다. 상대적으로 보안체계가 강력한 대기업, 금융·안보기관 등을 우회 공격할 수단으로 공급망 공격이 쓰이는 상황으로 2017년 낫페트야, 2020년 솔라윈즈 공격이 대표적이다. 낫페트야 공격에서 공격자는 우크라이나에서 주로 사용되는 회계 프로그램 미독(MeDoc) 업데이트 서버를 변조하여, 프로그램 업데이트 시 낫페트야 악성코드가 전달되도록 설정하여 그 피해가 세계적으로 확산되었다. 솔라윈즈는 IT 모니터링 솔루션 오리온(Orion)을 공급하는 공급업체로, 공격자는 오리온 업데이트 버전에 악성코드를 심어 미국 주요 안보기관을 포함한 공공기관과 마이크로소프트(MS), 파이어아이 등 보안 기업까지 해킹하였다. 공급망 공격은 표적인 기업·기관의 보안 체계를 직접적으로 접근하지 않기 때문에 해킹 사실을 인지하기 어렵다는 특징을 가진다. 2020년 2월 오리온 업데이트 버전에 악성코드가 포함된 이후, 이런 사실이 드러나기까지 10개월의 시간이 걸렸다. 이로 인해 솔라윈즈의 SEC filing에 따르면 18,000개사가 공격에 노출되었다(SolarWinds 2020).

사이버공격의 피해범위가 물리적 공간으로 확대되면서, 단 한 건의 성공적인 사이버공격이 초래하는 손실규모가 가공할 만한 수준으로 증가하였다. Lloyd's는 2015년 연구에서

사이버사고로 인해 영국 본토에 정전이 발생할 경우 직접적인 경제적 손실은 72억~536억 파운드, 향후 5년 동안 GDP 감소분은 490억~4,420억 파운드에 이를 것으로 추정하였다(Lloyd's and University of Cambridge 2015). 호주의 정부출자 테러보험 재보험회사 ARPC는 공격자가 펌웨어(Firmware) 업데이트 등을 통해 정보통신장비에 내장된 리튬이온 과열을 유도하여 호주 상업지구에서 대규모 폭발이 일어날 경우 최대손실이 833억 호주 달러에 이를 것으로 추정하였다. 이는 정교한 생화학공격의 최대손실액(920억 호주 달러)에 근접한 수준이다(OECD 2020b).

〈그림 Ⅱ-5〉 주요 자연재해 및 사이버공격 손실액

(단위: 십억 달러)



주: 손실액은 2020년 기준으로 실질화함
자료: Bateman(2020)

〈표 Ⅱ-2〉 세계 주요 사이버공격

사이버공격	위험	손해	공격자
터키 송유관 (터키, 2008)	물리적 시설 파괴	물적 피해	-
스턱스넷 (이란, 2010)	물리적 시설 파괴	물적 피해	미국, 이스라엘
사우디 아람코 (사우디아라비아, 2012·2016)	데이터 및 시스템 파괴	자본자산 파괴, 수익상실	-
야후 데이터침해 (미국, 2013·2014)	고객데이터 유출	배상책임, 평판손해	-
Sony Pictures (미국, 2014)	기업데이터 유출	지적재산, 수익상실	북한
독일 제철소 (독일, 2014)	물리적 시설 조작	영업중단손해	-
우크라이나 배전소 (우크라이나, 2015·2016)	기업활동중단, 데이터 및 시스템 마비	기업활동중단, 서비스중단	러시아
낫페트야 (글로벌, 2017)	기업활동중단, 데이터 및 시스템 파괴	유무형 자산손해, 영업중단손해	러시아
워너크라이 (글로벌, 2017)	기업활동중단, 데이터 및 시스템 파괴	유무형 자산손해, 영업중단손해	북한
록커고가 (글로벌, 2019)	기업활동중단, 데이터 및 시스템 파괴	유무형 자산손해, 영업중단손해	-
솔라윈즈 (미국, 2020)	기업활동중단, 데이터 및 시스템 파괴	유무형 자산손해, 영업중단손해	러시아
콜로니얼 파이프라인 (미국, 2021)	기업활동중단, 데이터 및 시스템 파괴	유무형 자산손해, 영업중단손해	-
JBS 정육업체 (호주·북미, 2021)	기업활동중단, 데이터 및 시스템 파괴	유무형 자산손해, 영업중단손해	-
플로리다 정수장 (미국, 2021)	물리적 시설 조작	인적 피해	-

자료: 저자가 작성함

〈표 Ⅱ-3〉 2010년 미국·이스라엘의 스턱스넷 공격

스턱스넷(Stuxnet) 사건은 2007년부터 2012년 사이에 이뤄진 일련의 사이버공격으로 인해 이란의 나탄즈(Natanz) 핵시설에 위치한 원심분리기가 파손된 사건이다. 스턱스넷 공격은 2010년 컴퓨터 바이러스가 이란 밖으로 유출되며 최초로 밝혀졌다. 이 사건은 국가 주도 사이버공격이자, 악성코드로 산업제어시스템을 감염시켜 원격으로 물리적 시설을 타격하여 세간의 주목을 받은 최초 사례로 알려진다. 스턱스넷은 MS 윈도우를 통해 감염돼 지멘스(Siemens)의 소프트웨어 및 장비를 공격하는 바이러스였다. 장비를 제어하고 감시할 수 있는 특수 코드를 포함하고 있는 이 웜 바이러스는 지멘스의 SCADA(Supervisory Control And Data Acquisition) 시스템만을 감염시키는 특징이 있었다.

스턱스넷 1.0 버전은 원심분리기의 속도를 현격하게 높이거나 낮추는 등 잦은 속도변화를 야기함으로써 원심분리기가 마모되도록 하였다. 스턱스넷 0.5버전은 원심분리기의 차단(Isolation) 및 배기(Exhaust) 밸브를 공격하여 원심분리기의 압력을 높이는 것을 목적으로 하는 것이었다. 원심분리기는 여러 농축 단계를 거치는데, 스턱스넷은 처음 두 단계와 마지막 두 단계의 차단밸브를 잠궈 가스 유출을 막음으로써 나머지 원심분리기들의 압력을 높였다. 압력 상승은 결국 더 많은 우라늄이 원심분리기 안으로 들어가게 만들고, 결과적으로 회전자에 더 높은 압력을 가하게 되었다.

2011년 4월 이란정부의 조사 결과 미국과 이스라엘이 공격의 배후에 있는 것으로 결론지었다. 스턱스넷으로 인한 경제적 손실은 크지 않았지만, 악성코드가 물리적 주요 기반시설을 표적으로 삼는 것을 보여줬다는 점에서 게임체인저였다.

※ 이란의 원자력발전소 사이버공격 이전부터 사이버무기를 활용한 물리적 공격이 존재한 것으로 알려져 있다. 일례로 스턱스넷에 앞서 2008년 터키 경유 석유송유관이 사이버공격을 받아 폭발한 사건이 있다. 이 송유관은 1,760km 길이 전체에 센서와 카메라를 가지고 있다. 공격자는 감시카메라의 통신 소프트웨어 취약점을 통해 시스템에 접근하여 대규모 네트워크에 침투한 후, 이를 이용하여 알람관리 네트워크를 통제하고 악성코드를 삽입하였다. 공격자는 알람을 무력화한 후 석유 압력을 변조하여 폭발을 유도하였다.

자료: 최윤성(2021)을 참고하여 작성함

〈표 Ⅱ-4〉 2015년 우크라이나 정전 사태

2015년 12월, 우크라이나의 전력망 시스템이 공격당한 사건이 발생하였다. 이 사건은 발전소로부터 전력을 공급받아, 가정이나 상가, 공장 등에 분배하는 배전 회사 ICS에 대한 사이버공격이었다. 총 3곳의 배전 회사 IT시스템이 사이버공격을 받아, 결국 변전소와의 전기 연결이 3시간 동안 끊어졌고, 약 225,000가구가 피해를 보았다. 이 사건은 적성국에 의한 전력망 공격으로 민간인 체감 수준의 물리적 피해가 발생한 전쟁 개념에 부합한 사이버공격으로서 의미를 가진다.

공격자는 마이크로소프트 오피스 문서를 조작하여 블랙에너지 3(BlackEnergy 3) 악성코드가 포함된 스피어피싱(Spear-phishing) 이메일을 보내 해당 회사의 IT 네트워크를 장악하는 1단계 공격을 수행하였다. 침투 성공으로 거점을 확보한 공격자는 2단계로 킬디스크(KillDisk) 악성코드를 사용해 핵심 시스템의 마스터 부트 레코드(MBR)를 삭제하여 배전 시스템과 연결 복구를 지연시키고, 흔적이 남지 않도록 관련 로그 기록을 삭제하였다. 변전소의 필드 장비를 대상으로는 맞춤형 악성 펌웨어를 삽입하여 직렬-이더넷(Serial to Ethernet) 변환 장치를 작동 불가능하게 만들고, 무정전 전원공급장치(UPS)를 비활성화하는 등 SCADA(Supervisory Control And Data Acquisition) 시스템 운영에 지장을 주기 위한 다각도의 공격을 수행하였다. 정전 피해가 발생한 이후에도 공격자는 고객이 정전 사실을 회사에 알리는 것을 지연시키기 위해 회사 콜센터에 전화 서비스 거부 공격(DoS)을 수행하여 피해 지속시간이 늘어나도록 하였다.

공격자는 2015년 공격 때 획득한 정보를 바탕으로, 2016년 12월에는 ICS에 대한 직접적인 공격이 가능한 인더스트로이어(Industroyer) 악성코드를 퍼트려 우크라이나의 수도 키예프의 송·변전소를 사이버공격하여 도시의 약 20%에 한 시간 가량 정전 피해가 발생했다.

이는 러시아 군부 정보그룹 샌드웜(Sandworm)의 소행으로 밝혀졌으며, 우크라이나 국가안보국(SBU)은 러시아가 이 사건의 배후에 있다고 주장하였다.

자료: 최윤성(2021)을 참고하여 작성함

〈표 Ⅱ-5〉 2017년 낫페트야 공격

낫페트야(NotPetya) 공격은 2017년 6월, 적성국인 러시아가 우크라이나를 상대로 벌인 사이버공격으로, 우크라이나 외에도 다국적기업들이 피해를 입었다. 이 사건은 역대 사이버공격 중 피해규모가 가장 큰 공격으로, 보험 관점에서는 사이버 대재해리스크를 현실화하고, 보험회사가 전쟁면책 적용을 주장하며 보험금 지급을 거절하면서 사이버 대재해 및 전쟁면책 도입을 촉발시켰다.

공격자는 우크라이나 정부기관이 의무적으로 사용하는 회계프로그램 미독(MeDoc)의 업데이트 서버에 침투해 악성코드를 퍼뜨렸다. 이후 랜섬웨어를 흉내 내 암호화폐인 비트코인을 요구했다. 하지만 국가기반시설을 공격하면서 300달러 송금을 요구한 것으로 미루어 금전취득이 원래의 목적은 아니었다. 일부 파일만 암호화하고 돈을 요구하는 랜섬웨어와 달리 낫페트야는 시스템 자체를 파괴해 데이터를 되살릴 여지를 남기지 않았다. 또한 공격 당시 악성코드 유포에 사용했던 이메일 계정을 폐쇄하는 등 막상 몸값을 받는 데는 신경 쓰지 않았다. 결국 낫페트야는 금전을 요구하는 랜섬웨어 모양만 갖춘 파괴형 악성코드인 것으로 밝혀졌다.

시스템 파괴 공격의 일종인 낫페트야를 퍼뜨려 정부기관을 비롯한 금융·전력·통신·교통 등 수많은 기반시설이 운용에 차질을 빚거나 가동이 중단되어 기업들에게 영업중단손실을 초래하였다. 우크라이나 전역으로 퍼진 악성코드는 64개국 이상의 다국적기업으로 급속히 확산됐다. 세계 최대 해운사인 덴마크 머스크(Maersk)의 컨테이너 터미널 17곳은 가동을 중단했다가 복구됐다. 영국·프랑스·스페인·네덜란드·인도·스페인 등의 기반시설과 기업들이 피해를 입었고, 미국의 특송·법률·제약회사도 공격을 받았다.

Crosignani et al.(2020)에 따르면, 낫페트야 공격으로 인한 미국 상장사의 직접 손실은, Beiersdorf(자산 76.9억 달러) 4,300만 달러, Fedex(자산 330.7억 달러) 4억 달러, Maersk(자산 688.4억 달러) 3억 달러, Merck(981.7억 달러) 6.7억 달러, Mondelez(자산 668.2억 달러) 1.8억 달러, Nuance(자산 58.2억 달러) 9,200만 달러, Beckitt Benckiser(자산 241.9억 달러) 1.17억 달러, WPP(자산 415.5억 달러) 1,500만 달러에 이른다.

2018년 2월, 미국·영국·캐나다·호주 등 다수의 국가는 공동성명서를 통해 낫페트야 사이버공격을 러시아 정부차원의 공격 행위로 발표하였다.

자료: Crosignani et al.(2020)을 참고하여 작성함

〈표 Ⅱ-6〉 2020년 미국 솔라윈즈 해킹

2020년 12월 솔라윈즈(SolarWinds)는 미국 증권위원회(SEC)에 해킹공격을 받은 사실을 보고하였다. 솔라윈즈는 미국 군대, 정보기관, 재무부 등 공공기관 및 포춘 500대 기업 다수가 사용하는 보안 솔루션 소프트웨어(오리온즈)를 제공하는 회사이다. 이 사건은 공급망 공격(Supply chain attack, third-party attack)의 심각성을 보여주는 사건이다. 공급망 공격은 자사의 시스템 및 데이터에 접속할 수 있는 외부 협력업체나 공급업체를 통해 누군가가 시스템에 침투하여 피해를 야기하는 형태의 공격이다.

이 공격은 사이버보안 업체인 파이어아이(FireEye)에 의해 처음 인지되었다. 2020년 12월 8일, 파이어아이는 자체 레드팀의 공격도구를 도난당했다는 사실을 발표하면서 해당 도구 자체를 모두 공개했다. 2020년 12월 13일, 파이어 아이는 자체 레드팀 공격도구에 대한 국가 주도 공격을 조사하는 과정에서 공급망 공격을 발견했다. 연구진은 공격자가 솔라윈즈 소프트웨어인 솔라윈즈 오리온 비즈니스 소프트웨어 업데이트를 트로이 목마화해 악성코드를 유포하는 백도어(Backdoor)에 진입했다는 증거를 우연히 발견하였다.

2020년 12월 15일, 월스트리트 저널은 미국 상무부와 재무부·국토안보부·국립보건원·국무부가 모두 영향을 받았다고 보도했다. 2020년 12월 17일, 미국 DOE(Department Of Energy)와 미국 핵무기 비축량을 관리하는 NNSA(National Nuclear Safety Administration)가 이 공격의 추가 피해자로 공개 지명됐다. 2020년 12월 31일, 마이크로소프트는 러시아 공격자가 소스코드의 일부를 침해했다고 밝혔다. 그리고 솔라윈즈의 SEC filing에 따르면 33,000고객사 가운데 18,000개 사가 공격에 노출되었다. 피해자는 북미, 유럽, 아시아, 중동의 여러 정부기관, 컨설팅, 기술, 통신, 석유 및 가스 업체 등이 포함된 것으로 알려졌다.

2020년 12월 14일, 워싱턴포스트는 이 공격이 러시아 해외 정보기관인 SVR(Russian Foreign Intelligence Service)과 연관이 있는 코지베어(Cozy Bear, APT 29)로 알려진 러시아 해커 그룹에 의한 공격이라고 보도했다. 2021년 4월 16일, 바이든 미 행정부는 솔라윈즈 공격이 러시아의 해외 첩보 수집 기관인 SVR의 소행이라고 공식 발표했다. 이에 대한 보복으로 러시아 일부 단체와 인물들에 대한 제재를 시작하고 외교관 10명을 추방했다.

자료: The Whitehouse(2021. 4. 15), "FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government"

나. 사이버리스크에 대한 보장수요 증가

사이버보험 시장은 여전히 초기 단계로 단독 사이버보험 상품이 출시된 것은 약 20년 정도 되었다. 초기 사이버보험 시장은 기술 기반 서비스를 제공하는 기업에 하자(Error and omission) 담보를 제공하는 것이었다. 즉, 직무수행상의 과실이나 태만으로 제3자에게 정보유출 등의 피해를 입혀 법률상 배상책임을 부담하게 됨에 따른 손해를 보상하였다. 점차 사이버사고가 증가하고, 2002년 미국 캘리포니아를 시작으로 개인정보 유출에 대한 통지의

무와 처벌을 담은 법규 도입이 전 세계적으로 확산되었다.[15] 사이버사고와 관련된 신규 손해가 발생하자, 사이버담보를 별도로 제공하는 전용보험이 본격적으로 판매되었다.

사이버보험은 ① 사이버리스크 전용의 단독 사이버보험(Stand-alone), ② 기존 재물보험 또는 배상책임보험에 사이버리스크에 대한 보장을 특약으로 부대하거나, 열거위험(Named-peril) 담보방식의 기업보험에 사이버담보를 명시적으로 열거하여 보장하는 패키지보험, ③ 기존 포괄위험(All-risk) 담보방식의 재물보험과 배상책임보험처럼 사이버리스크에 대한 보상이 명시되어 있지는 않지만 약관상 포함된다고 해석되는 상품 등 크게 3가지로 구분가능하다. ①과 ②를 명시적(Affirmative) 사이버보험, ③을 암묵적 또는 비명시적(Silent or non-affirmative) 사이버보험으로 구분한다.

사이버보험의 역사는 비교적 짧아서 미국 이외 지역에서는 사이버보험 시장규모가 공식적으로 집계·공개되고 있지 않으나, 사이버보험 시장이 빠른 속도로 확대되고 있는 것은 분명하다. OECD는 여러 자료를 토대로 명시적 사이버보험 수입보험료가 2018년 기준 40~50억 달러에 이르며 향후 4~5년 내에 3배 이상 규모로 증가할 것으로 보고 있다(OECD 2020b). 2018년 기준 OECD 회원국의 보험종목별 수입보험료는 기업 재물보험 3,239억 달러, 일반배상책임보험 1,984억 달러로, 사이버보험의 시장규모는 상대적으로 작은 편이다(OECD 2020b). 〈그림 Ⅱ-6〉에서 보는 바와 같이 미국이 명시적 사이버보험 시장의 대부분을 차지하나 그 외 시장도 2015년 이후 빠른 성장을 보이고 있다.

사이버보험의 원수보험료 증가세는 손해율 증가에 따른 보험요율 인상에 일부 기인한다. 2017년 워너크라이, 낫페트야, 2019년 록커고가 공격 등으로 보험회사의 보험금 지급부담이 증가하면서 사이버보험 요율이 단기간에 급격히 인상되었다. 보험요율은 2019년 2분기에 1.2%에 불과하였으나, 불과 2년만인 2021년 2분기에는 25.5%에 이르렀다(CIAB, 2021).

향후 사이버리스크가 급증함에 따라 사이버보험에 대한 수요도 급격히 증가할 것으로 예상된다. 그 이유로는 무엇보다도, 파괴적 사이버공격의 빈도 및 심도 증가에 따른 기업의 보장수요 증가이다. 사이버보안 강화와 보험요율 인상에도 불구하고, 개인정보 침해에 수반되는 제비용, 랜섬웨어 감염에 따른 랜섬, 영업중단손해, 데이터 및 시스템 복구비용,

15) 2002년 미국 캘리포니아주는 개인정보를 유출시킨 기업이 정보주체와 감독기관에 그 사실을 즉각 통보하도록 하고 불이행 시 범칙금 부과, 사적소송 제기근거를 입법화함(California Security Breach Notification Act 2002, California SB 1386). 이후 전 세계적으로 이러한 입법례가 증가하였음

법률비용, ICS 공격에 따른 재물손해 등 기업의 보장수요의 범위 및 규모가 늘어날 것으로 예상된다.

다음으로, 국제적으로 개인정보보호 및 사이버보안 강화 기조를 반영하여 관련 법 위반에 따른 벌금을 대폭 상향조정하는 추세로, 기업의 사이버 관련 규제리스크가 커졌다. EU는 2018년 5월 일반개인정보보호법(General Data Protection Regulation; GDPR)을 시행하였다. GDPR은 1995년에 제정된 개인정보보호지침(Directive 95/46/EC)을 개정해 2016년 4월 EU 의회가 승인한 법률이다. 2년간의 유예기간을 거쳐 2018년 5월부터 효력을 발휘하게 되었고, 그와 동시에 기존의 개인정보보호지침은 폐기되었다. 개인정보보호지침의 경우 개별 회원국 내에서의 입법화 여부에 따라 기업 등은 국가별로 대응을 달리해야 했으며, 국가별 법 내용 또한 상이할 수 있어 EU 회원국 간 정보 이동과 활용에도 제약이 되었다. 이와는 달리 GDPR은 28개 EU 회원국들이 단일 법률하에서 동일한 규제를 받게 되었다. GDPR은 EU 내 사업장을 운영하는 기업뿐만 아니라 전자상거래 등을 통해 해외에서 EU 주민의 개인정보를 처리하는 기업에도 적용되며, 정보주체의 권리와 기업의 책임성 강화 등을 주요내용으로 한다. GDPR은 위반 시 과징금 부과를 규정하고 있으며, 최대 과징금은 일반적 위반사항인 경우 전 세계 매출액의 2% 혹은 1천만 유로 중 높은 금액이며, 중요한 위반 사항인 경우[16] 전 세계 매출액의 4% 혹은 2천만 유로 중 높은 금액이다. GDPR 시행 이전 영국 데이터보호법 1998(Data Protection Act of 1998)이 위반에 따른 최대 벌금을 50만 파운드로 제한하였다는 점을 감안하면, GDPR은 기업의 벌금에 대한 부담을 심각한 수준으로 증가시켰다. 2019년 프랑스의 개인정보 감독기구(Commission Nationale de l'Informatique et des Libertés; CNIL)는 Google에 GDPR 위반 혐의로 5,000만 유로의 벌금을 부과하였다. 이는 Google의 2017년 한해 매출액을 기준으로 매출액의 약 0.05%에 해당하는 금액이다.[17] 우리나라도 2021년 1월, 국내외 기업의 역차별 해소를 위해[18] 국제적 기준에 맞춰 개인정보 침해사고를 낸 기업에 부과할 수 있는 과징금을 '침해사고 매출액의 3% 이하'에서 '전체 매출액의 3% 이하'로 상향하는 개인정보보호법 개정안을 입법예고한 바 있다. 호주는 최대벌금을 현행 210만 호주 달러에서 '1천만

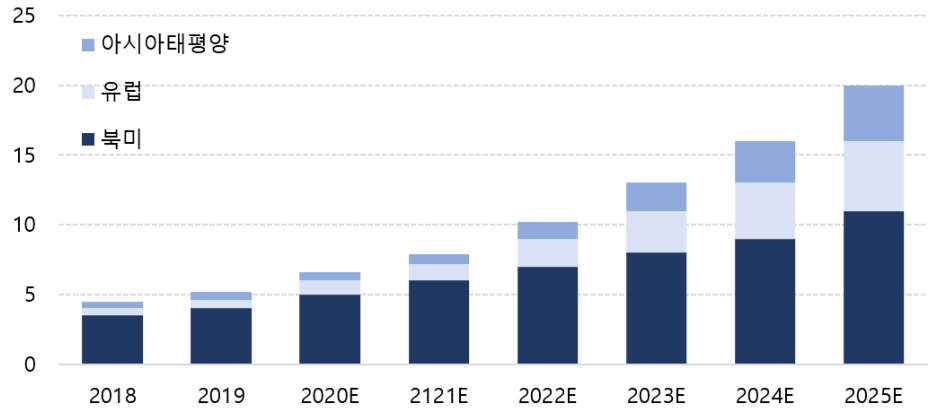
16) 소비자의 동의를 구하지 않고 개인 데이터를 처리·활용하거나 설계 및 기본설정에 의한 개인정보보호(Privacy by Design) 개념의 핵심원칙을 위배한 경우임

17) 2021년 8월에는 룩셈부르크가 아마존의 전자상거래 플랫폼 이용자 개인정보관리 미흡이 GDPR에 위반된다고 판단, GDPR 관련 사상 최대 금액인 7억 4,600만 유로의 과징금을 부과함

18) 국내 기업이 해외에서 과징금을 전체 매출의 4%를 받는 사이 국내에 들어오는 해외기업은 '관련' 매출의 3%를 받을 경우, 국내 기업에 대한 역차별이 발생함. 이러한 역차별 문제는 비단 우리나라만의 문제는 아니어서 개인정보보호법 위반에 대한 벌금 상향은 국제적 흐름이며, 벌금 수준의 국제적 수렴이 불가피함

호주 달러, 법 위반으로 인한 부당이득의 3배, 또는 매출액의 10% 중 큰 금액'으로 상향조정하는 것을 검토 중이다. 중국·캐나다도 개인정보보호법을 제·개정하여 전체 매출의 5%를 부과하는 방안을 검토 중이다.

〈그림 Ⅱ-6〉 세계 명시적 사이버보험 원수보험료



주: 1) 단위는 십억 달러임
2) 2020년부터는 추정치임
자료: IAIS(2020)

2. 사이버리스크에 대한 보험공급 축소

가. 사이버리스크에 대한 보험산업의 불안 확산

최근 일련의 사이버공격을 목도한 보험산업은 사이버리스크에 대한 과소평가와 이해부족을 우려하는 분위기이다(EIOPA 2018). 두려움의 실체는 먼저, 리스크 측정이 어렵다는 점이다. 사이버사고는, 특히 사이버공격은 기술발전과 함께 피해를 극대화하는 방향으로 그 수법이 계속해서 진화하기 때문에 모델링에 필요한 경험데이터가 부족하다. 기술발전과 새로운 공격자 및 공격동기 출연으로 리스크가 지속적으로 변한다는 점은 외생적인 요소로, 보험산업이 통제하기 어려운 부분이다. EIOPA 조사에서 보험회사들은 리스크의 속성상 경험데이터 부족으로 사이버리스크 모델링 자체가 어려워, 보험산업이 사이버리스크를 과소

평가해왔고, 실제 리스크를 요율에 제대로 반영하지 못했을 가능성이 있다고 응답하였다.

다음으로, 사이버사고는 연쇄적인 손실을 초래하여 대재해 가능성을 내포한다. 2017년 워너크라이처럼 불특정 다수를 감염시키는 사이버공격, 2017년 낫페트야, 2020년 솔라윈즈 사건과 같은 공급망 공격은 연쇄적인 피해를 초래한다. 낫페트야는 우크라이나에서 시작하여 단기간에 세계적으로 확산되었고, 솔라윈즈는 미국 내 18,000개 사에 피해를 초래하였다. 전통적으로 보험산업에서는 거대 자연재해의 경우 지리적 분산을 통해 위험을 관리해왔지만, 사이버리스크는 감염병리스크와 같이 지리적 분산을 통한 위험관리가 불가능하다. Berliner(1982)에 따르면 부보가능성 여부를 판단하는 계리적 기준은 다음과 같다. ① 손실발생이 우연하고 독립적이어야 하고, ② 손실노출도가 커야 하고(동질위험을 가진 다수 존재), ③ 최대가능손실이 관리 가능한 수준이어야 하고, ④ 사고당 평균손실이 적정해야 하고, ⑤ 도덕적 해이와 역선택이 과도하지 않아야 한다. 사이버리스크는 인적재해로서 손실발생이 우연하지 않고 손실 간 상호의존성이 높으며 최대가능손실이 관리가능한 수준을 벗어나는 사례가 이미 발생하고 있다.

이에 보험회사는 사이버담보 제공에 보수적인 입장을 취하고 있다. 미국 (명시적) 사이버보험 시장에서는 2020년 손해율이 67.8%로 전년(44.8%) 대비 23%p 증가하였다. 이미 담보별 보상한도를 축소하거나 인수심사를 보다 까다롭게 진행하며, 손실발생 가능성이 큰 사이버담보를 제공하지 않는 경향이 관찰된다(GAO 2021).

나. 재물·배상책임보험의 사이버손해 보장 배제

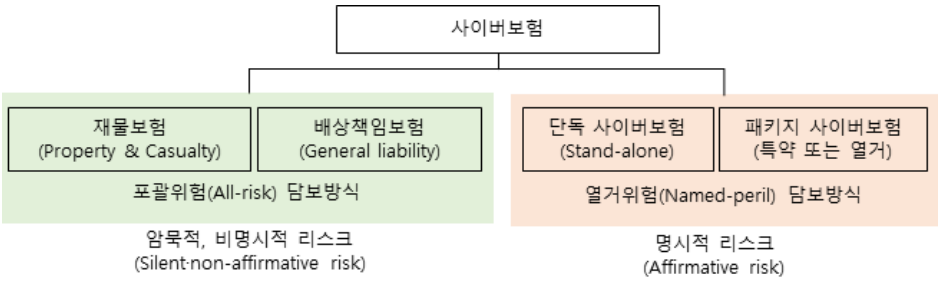
1) 암묵적 사이버보험 인수리스크 가시화

손해보험 계약은 손인(Peril)으로 인하여 우연하게 발생한 경제적 손해를 보상하는 계약이므로, 모든 보험증권은 담보하는 손인의 범위를 분명하게 하고 있다. 기업 재물보험 약관에서 손인의 범위를 규정하는 방식은 크게 포괄위험 담보방식과 열거위험 담보방식으로 구성된다. 포괄위험 담보방식은 담보손인을 열거하는 대신 비담보손인이나 면책위험을 열거하고, 이에 해당하지 않는 모든 손인에 의한 손해를 보상하기로 약정하는 방식이다. 열거위험 담보방식은 보험약관에서 담보하는 손인을 일일이 열거·기재하여 담보하기로 명시한 위험에 대해서만 보험회사가 담보하는 방식이다. 열거위험은 보험약관에서 부담하는 손인의 종류가 명시적으로 열거되므로 보험회사의 보상범위가 분명하다.

전술한 바와 같이 포괄위험 담보방식의 기업 재물 및 배상책임보험은 보험약관에 사이버 담보에 대한 보장 및 면책 여부를 명시적으로 표기하지 않는 한, 약관상 사이버사고로 인한 재물 및 배상책임 손해를 보장하는 것으로 해석된다. 물론 ISO 등이 처음 기업보험 약관을 작성할 때 오늘날 재물담보와 배상책임담보에 영향을 미치는 사이버리스크의 존재를 숙고하지는 않았을 것이다. 즉, 사이버리스크의 부재, 사이버리스크에 대한 인식의 부재로 이에 대한 부담보(면책) 조항이 약관상 존재할 이유가 없었던 것이다.

근래 사이버공격으로 인해 컴퓨터 파손 등 재물손해가 발생하고 나아가 물리적 시설 파괴를 초래하는 사이버공격 가능성이 커짐에 따라, 암묵적 사이버보험의 인수리스크(Underwriting risk) 역시 커지고 있다. 사이버사고에 대한 명시적인 면책이 없는 포괄위험 담보방식 재물보험은 사이버공격에 따른 재물손해 및 영업중단손해를 보장해야 하기 때문이다(〈그림 Ⅱ-7〉 참조). 예를 들어, 사이버사고를 명시적으로 면책하지 않은 재물보험의 경우, 악성소프트웨어 공격으로 인해 컴퓨터 시스템이 훼손되거나 생산설비에 화재가 발생한 경우 직접적인 재물손해와 그로 인한 영업중단손해를 보장해야 한다. 사이버사고를 명시적으로 면책하지 않은 일반책임보험의 경우, 사이버공격으로 인한 배상책임손해를 보상해야 한다.

〈그림 Ⅱ-7〉 사이버보험의 유형 및 언더라이팅 리스크



자료: 저자가 작성함

2) 약관상 사이버리스크 보장여부 명확화

전통적인 기업보험에서 암묵적 사이버담보는 보험계약자와 보험회사 모두에게 불확실성을 가져온다. 이에 최근 몇 년 동안 보험산업은 암묵적 사이버위험 노출도를 확인하고 전통적 기업보험에서 물리적·비물리적 사이버 노출을 제외하거나 담보를 명시적으로 표기하는 방안을 모색해왔다. 미국에서는 NAIC(National Association of Insurance Commissioners,

전미 보험감독자 협의회)와 ISO가, 영국에서는 영란은행 내 건전성감독청(Prudential Regulation Authority; PRA)과 Lloyd's가 다양한 기업보험 종목에서 사이버 면책조항을 발표, 이를 보험증권에 반영하도록 하고 있다. 미국 기업은 사이버보험 시장의 주 수요자이며, 영국 보험회사는 세계 보험시장의 주 공급자로서 두 시장에서 상품, 약관, 인수전략 등의 변화는 세계 시장에 영향을 미친다.

가) 영국

2001년 이후 재물보험에서는 보험목적물에 대한 직접적인 물리적 멸실 및 손상에 한해 보상하고 '전자 데이터(Electronic data)의 멸실·손상·변형·삭제·변조·변경의 결과에 따른 손실'은 통상 명시적 특약으로 부담보하였다. 데이터 및 소프트웨어 손실에 대한 면책을 확인하는 약관 문구로는 Electronic Data Endorsement C(NMA 2914)와 Electronic Data Endorsement D(NMA 2915)(전자데이터 부담보 조항)가 있다. 대부분의 기업보험에서 데이터 및 소프트웨어는 재물보험 약관에서 보장하는 유형자산으로 간주되지 않는다. 따라서 NMA 2914와 2915는 이러한 손실이 면책됨을 명확히 한다. 구체적으로 NMA 2914는 "증권안의 어떠한 반대의 조항과 그 배서에도 불구하고 다음과 같은 내용이 선행하는 것으로 한다: 이 증권은 어떠한 원인에 의한 것이든지(컴퓨터 바이러스를 포함하나 이에 국한되지 않는다) 전자데이터의 손실·손상·파괴·변형·삭제·오염·대체를 보상하지 않으며, 그로 인한 사용상 손해·기능상 저하·모든 형태의 비용 및 지출을 보상하지 않는다. 이는 손해 발생에 동시적 또는 순차적으로 기여를 한 다른 원인 또는 사고에 구애받지 않는다."[19]

이후 2003년 해상보험에서 사이버공격 면책 약관(Institute Cyber Attack Exclusion Clause, CL 380)이 등장하였다.[20] CL 380은 해상보험에서 시작하여 여러 보험종목에서

19) Electronic Data Endorsement A (NMA 2914) 25/01/2001: "1(a) This policy does not insure loss, damage, destruction, distortion, erasure, corruption or alteration of ELECTRONIC DATA from any cause whatsoever (including but not limited to COMPUTER VIRUS) or loss of use, reduction in functionality, cost, expense of whatsoever nature resulting therefrom, regardless of any other cause or event contributing concurrently or in any other sequence to the loss."

20) Institute Cyber Attack Exclusion Clause (Cl. 380) 10/11/2003: Any loss, damage, liability, costs or expenses directly or indirectly caused by or contributed to or resulting from the cyber incidents as set forth in the following provisions a) to g) are not covered by this Policy, regardless of any other cause or event contributing concurrently or in any other sequence to the loss, damage, liability, costs or expenses: a) Damage to or Loss of Data occurring on the Insured's Computer Systems,

활용되었다. 이 약관은 컴퓨터, 소프트웨어 프로그램 기타 전자시스템 등이 피해를 주는 수단으로 이용됨에 따라, 혹은 직·간접적으로 이에 기인하여 보험목적물에 발생한 멸실, 손상, 배상책임 및 비용에 대하여 보험회사의 절대적 면책을 다룬다. 다만 전쟁, 정치적 동기에 따른 적대적 행위, 테러리즘 등을 특약으로 담보하는 경우에는 컴퓨터, 소프트웨어 등이 유도장치나 무기로 이용되는 경우가 많아 사이버 절대면책을 적용하지 않고 이에 따른 멸실, 손해, 비용손실 등을 보상한다. CL 380은 컴퓨터 등 IT시스템이 피해를 발생시키는 수단으로 사용되기만 하면 보험회사의 면책을 적용함에 따라 약관이 지나치게 포괄적이라는 비판을 받았다.

2010년대 들어 사이버보험 시장이 급격히 성장하자, 영국의 PRA는 사이버보험 인수리스크에 주목하여, 기존 기업보험에서 사이버리스크에 대한 구체적인 약관내용의 불분명함에 관하여 살펴보기 시작하였다. PRA는 2015년 10월부터 2016년 6월 기간 동안 산업 관계자들과 사이버보험 인수리스크를 분석하였다. 사이버사고를 명시적으로 담보하는 사이버보험뿐만 아니라, 사이버사고를 명시적으로 면책하지 않는 포괄담보 방식의 재물보험과 배상책임보험에 내재된 리스크를 진단하였고, 그 결과를 2016년 11월 보험회사 CEO에게 보내는 서신을 통해 공개하였다.[21] 당시 주요 분석 결과는 다음과 같다. ① 암묵적 사이버리스크가 심각한 수준이나 대부분의 보험회사가 암묵적 사이버리스크를 관리하거나 계량화하지 않고 있다. ② 암묵적 사이버보험의 존재에 대한 인식이 확산되고 사이버 공격이 빈번해짐에 따라 암묵적 사이버손실이 향후 증가할 것으로 예상된다. ③ 본질적으로 광범위한 리스크를 보장하는 특종(Casualty) 라인 보험상품의 암묵적 사이버리스크 노출이 심각하다. ④ 재보험회사의 경우 암묵적 사이버리스크를 인지하고는 있으나 P&C 재보험계약에서 사이버면책이 널리 사용되거나 암묵적 사이버리스크가 요율에 적극적으로 반영되고 있지는 않았다. ⑤ 대부분의 보험회사가 사이버리스크 관리를 위한 명확한 전략이나 리스크 수용범위(Appetite)를 가지고 있지 않았으며, 사이버 관련 전문성 제고를 위한 투자도 충분하지 않았다. ⑥ 보험회사는 명시적 사이버담보에 대해서도 집합리스크와 꼬리리스크를 과소평가하였다. ⑦ 주요 대재해 모델링업체도 재난적 사이버사고에 대한 모델링은 아직 개발 초기 단계에 있다. ⑧ 2018년 GDPR이 도입됨에 따라 유럽에서도 사이

---

or b) a Computer Malicious Act on the Insured's Computer Systems, or c) Computer Malware on the Insured's Computer Systems, or d) a Human Error affecting the Insured's Computer Systems, or e) a System Failure occurring on the Insured's Computer Systems, or f) a Defect of the Insured's Computer Systems, or g) a Cyber Extortion.

21) PRA(2016. 11. 14), "Dear CEO"

버보험에 대한 수요가 증가하고 이에 따라 명시적 담보의 리스크 노출도도 증가할 것이다.

사이버보험 인수리스크에 대한 상기 진단에 근거하여, PRA는 리스크 완화를 위한 구체적인 조치가 필요하다고 판단하고, 2016년 11월 '사이버보험 인수리스크'라는 자문보고서(Consultation paper, CP39/16)를 발간하였다(PRA 2016). PRA는 성명서를 통해 기존 보험계약에서 잠재적으로 의도하지 아니하거나 불분명한 사이버리스크 보상 가능성에 대한 우려를 표명하였다. PRA는 사이버보험 인수리스크를 사이버공격 또는 악성코드로 인한 IT시스템 감염 등 악의적 행위와 데이터 손실 또는 우연한 사고 및 누락(Omissions) 등 비악의적 행위에 노출된 보험계약을 인수함으로써 생긴 잠재적 리스크로 정의하고 다음을 요구하였다. 무엇보다도 각 보험회사가 명시적 사이버담보와 암묵적 또는 비명시적 사이버담보의 리스크를 식별·계량화·관리할 것을 요구하였다. 둘째, 각 보험회사의 이사회가 회사의 사이버 전략과 리스크 성향을 명확히 규정하도록 지시하였다. 셋째, 보험회사가 사이버리스크에 대한 전문성을 지속적으로 개발하고 구축할 것 등을 요구하였다.

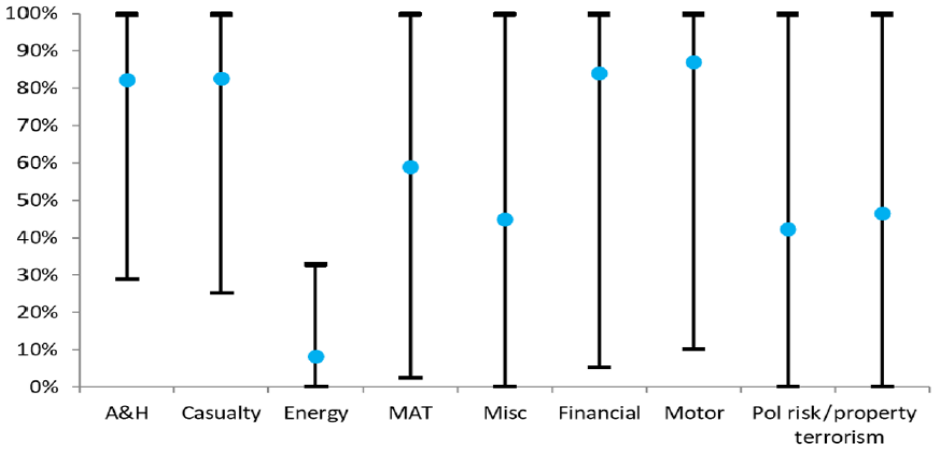
이어 2017년 4월에는 감독성명서(Supervisory statement, SS4/17)를 통해 CP39/16를 보완하였다(PRA 2017b). 암묵적 사이버리스크 관리를 위해, 기존 포괄위험 담보방식 P&C 보험에 내재된 사이버리스크를 보험료에 반영하거나, 사이버면책을 약관에 명시적으로 기입하거나, 사이버담보에 적용되는 보상한도를 명시적으로 기입하는 방안을 제안하였다. 만약 보험회사가 추가보험료 없이 사이버담보를 기존 재물보험에서 제공키로 하였다면, 그로 인한 잠재적 손실에 대해 이사회가 포괄적으로 평가하도록 하였다. 또한 PRA는 각 보험회사가 최대 200년 빈도로 발생하는 극단적인 손실을 고려한 사이버보험 인수리스크 스트레스 테스트를 수행하는 등 사이버리스크에 대한 명확하고 구체적인 전략 및 수용범위를 설정하도록 요구하였다.[22]

2018년 PRA는 보험업계와 공동으로 기업규모별 사이버리스크를 조사하였다(PRA 2019), 조사에 따르면 암묵적 사이버리스크에 노출된 총 보험가입금액(Policy limit)의 비율은 보험회사별·보험종목별로 편차가 매우 크다. A&H, 특종보험, 금융보험, 자동차보험 등에서 암묵적 사이버리스크가 평균적으로 매우 큰 것으로 나타난다(〈그림 Ⅱ-8〉). 또한 대부분의 보험회사는 암묵적 또는 명시적 사이버리스크에 대한 정량적 평가를 수행하지 않는 것으로 나타났다. 암묵적 사이버리스크에 대한 일부 보험회사의 스트레스 테스트에 따르면,

22) 2017년 7월에는 정책성명서(Policy statement, PS15/17)를 통해 CP39/16과 SS4/17에 대한 피드백을 제공함(PRA 2017a)

사이버사고는 보험회사의 다양한 보험종목에 영향을 미치며 그 추정손실이 미국에서 발생한 주요 거대자연재해의 피해액과 유사한 수준이다. 또한, 명시적 사이버리스크에 대한 스트레스 테스트에 따르면 총 손실액이 연간 사이버보험료의 수배에 이를 수 있다. PRA는 2019년 1월 보험회사 CEO에게 보내는 서신을 통해 모든 보험회사들이 명시적 사이버리스크 담보로 인해 발생할 수 있는 의도하지 않은 위험노출을 감소시키기 위한 실행계획을 수립하여야 함을 재차 강조하였다.

〈그림 Ⅱ-8〉 영국 보험산업의 보험종목별 암묵적 사이버리스크 노출도



주: 영국 PRA가 샘플링한 보험회사의 암묵적 사이버리스크에 노출된 총 보험가입금액의 비율을 나타내며, 그래프에서 점은 평균임
자료: Cartagena et al.(2020)

2019년 1월 이후 감독당국의 요구에 대응하여 영국의 두 보험산업 단체는 사이버리스크에 대한 명확한 보장 혹은 면책을 위한 기존 약관의 단계적 개선을 추진하고 있다. 2019년 7월 4일 Lloyd's는 모든 보험계약에 사이버담보 제공 여부를 명확히 하도록 요구하였다.[23] 구체적으로, 2020년 1월 1일자에 개시되는 재물관련 보험종목(First-party property damage lines of business)에 대하여, 보험회사가 포괄위험 담보방식인지 여부에 상관없이 모든 보험계약에 사이버리스크에 대한 보장 혹은 면책의 입장을 확정하여 명기하도록 요구하였다. 배상책임과 특약재보험에 대해서는 2020~2021년 동안 사이버담보 보

23) Lloyd's Market Bulletin Y5258, "Providing clarity for Lloyd's Customers on Coverage for Cyber Exposures"

장여부를 명확히 하도록 요구하였다.[24]

런던 보험시장의 사업자단체인 로이즈보험시장협회(Lloyd's Market Association)와 IUA(International Underwriting Association, 국제언더라이팅협회)는 사이버 관련 보험금 청구를 제한 및 축소하기 위해 새로운 사이버 면책조항을 발표하였다.[25] LMA는 2019년 11월에 새로운 4종의 사이버 보장·면책 표준약관을 발표하였다.[26] LMA 5400은 사이버 행위 및 사고로 인해 발생한 손실을 보장하지 않으나, 사이버사고로부터 발생한 화재 및 폭발손해를 보장한다. 데이터 복제비용 또는 손상된 데이터 처리장치의 교체 및 수리비용을 보장한다. LMA 5401은 행위의 악의성 여부에 상관없이 사이버 행위로 인한 손해를 보장하지 않는 절대면책(Absolute exclusion)이다. LMA 5400과 달리, 물리적 손인으로 인한 데이터 손실 또는 데이터 교체 및 복구 비용을 보장하지 않는다. 이와 관련하여 Lloyd's는 사이버리스크를 행위의 악의성 여부에 상관없이 '사이버 관련 모든 손실'로 정의한다. 즉, 사이버리스크는 사이버손실이 사이버공격, 악성코드를 이용한 IT시스템 감염 등과 같은 악의적 행위와 데이터 손실, 우연한 행동에 의한 비악의적 행위를 모두 포함한다.

2019년 런던 보험시장에서 로이즈를 제외한 보험회사 단체인 IUA에서는 별도의 절대적 사이버손해면책약관(Cyber Loss Absolute Exclusion Clause, reference: IUA 09-081)과 제한적 사이버손해면책약관(Cyber Loss Limited Exclusion Clause, IUA 09-082)을 발표했다.[27] 제한적 사이버손해면책약관에서는 컴퓨터 시스템, 통신망 또는 데이터 등의 사용에 따라 '직접적으로 발생한 손해에 한해' 담보하지 아니하며[28] 절대적 사이버손해면책약

24) Lloyd's는 2020년 1월 29일 사이버담보 제공 여부 명확화 작업의 추진 일정을 업데이트함(Lloyd's Market Bulletin Y5277: Update-Providing clarity for Lloyd's customers on coverage for cyber exposures)

25) IUA는 국제적인 대형 보험회사와 재보험회사들을 위한 세계에서 가장 큰 대표기구로서, 런던국제보험·재보험시장연합(London International Insurance and Reinsurance Market Association; LIRMA)과 런던보험자협회(Institute of London Underwriters; ILU)의 합병을 통하여 1998년 12월 31일 설립됨. 이 연합은 런던 기업보험시장의 해상보험부문과 일반 손해보험부문을 위한 대표 기구들을 하나로 통합함

26) Property D&F Cyber Endorsement(LMA 5400), Property D&F Cyber Exclusion(LMA 5401), Marine Cyber Exclusion(LMA5402), Marine Cyber Endorsement(LMA 5403)

27) IUA Cyber Loss Absolute Exclusion Clause (IUA 09-081) 17/05/2019), Cyber Loss Limited Exclusion Clause(IUA 09-082)

28) 2. Cyber Loss means any loss, damage, liability, expense, fines or penalties or any other amount directly caused by: the use or operation of any Computer System or Computer Network; the reduction in or loss of ability to use or operate any Computer System, Computer Network or Data; access to, processing, transmission, storage or use of any Data; inability to access, process, transmit, store or use any Data; any threat of or any hoax relating to 2.1 to 2.4 above; any error or omission or accident in respect of any Computer System, Computer Network or Data

관은 직접 혹은 간접적으로 발생한 손해를 면책하는 것으로 구분한다.[29]

IMIA Cbyer Exclusion 2018은 보다 최근의 면책조항으로 International Association of Engineering Insurers가 엔지니어링 보험시장에서 사용하기 위해 개발하였다. 동 조항은 ① 피보험자의 컴퓨터 시스템에 발생한 데이터 손실, ② 피보험자의 컴퓨터 시스템에 악의적 행위, ③ 피보험자의 컴퓨터 시스템에 컴퓨터 악성 소프트웨어, ④ 피보험자 컴퓨터 시스템에 영향을 미치는 인간의 실수, ⑤ 피보험자 컴퓨터 시스템에 발생한 시스템 실패, ⑥ 피보험자 컴퓨터 시스템 결함, ⑦ 사이버 협박(Extortion)로 인한 일체의 손실을 보장하지 않는다.

Cyber Loss Exclusion(Property Treaty Reisurance) LMA 5240은 Lloyd's Market Association이 개발하여, 재물특약 재보험(Treaty reinsurance)시장에서 사용된다. 사이버사고로 인한 일체의 손실을 보장하지 않는다.

〈표 Ⅱ-7〉 영국의 사이버사고 관련 면책조항

약관	약관 명칭	공표연도
NMA 2914/5 NMA 2914A/5A	Electronic Data Endorsement	2001, 2015
CL 380	The Institute Cyber Attack Exclusion Clause	2003
LSW 555	Aviation Hull 'War and allied perils'	2006
LMA 5272/3/4/5	Cyber Incident Exclusion	2016
LMA 3150	Insurance Act 2015 Endorsement-General Liability	2015
LMA 3141	Electronic and Computer Crime Policy	2016
LMA 3127	HIP 2015 Policy	2015
LMA 3092/30	Terrorism Exclusion(Including Cyber Terrorism)	2006, 2010
NMA 2912/28	IT Hazard Clarification Clause	2010
JSC 2015/8	Cyber Attack Exclusion Clause and Write-Back	2015, 2018
AVN 124	Data Event Clause	2018

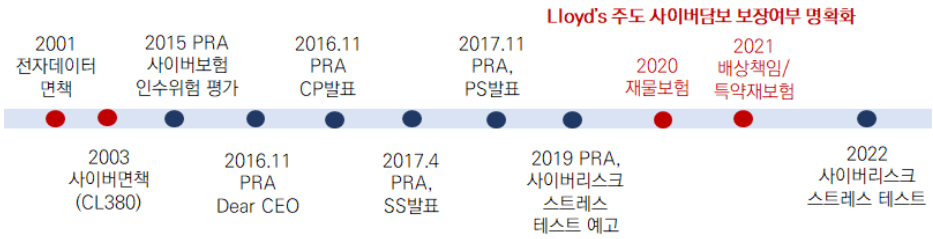
29) 2. Cyber Loss means any loss, damage, liability, expense, fines or penalties or any other amount directly or indirectly caused by

〈표 Ⅱ-7〉 계속

약관	약관 명칭	공표연도
LMA 5240	Cyber Loss Exclusion (Property Treaty Reinsurance)	2015
LMA 5241	Cyber Loss Limited Exclusion	2015, 2018
LMA 5247	Cyber Act Exclusion (Casualty Treaty Reinsurance) - LMA5274	2016
LMA 5327	Cyber Loss Limited Exclusion	2018
LMA 5359	Cyber Loss Exclusion	2019
IUA	Cyber Exclusion	2019
IMIA	Cyber Exclusion	2018
JC 2019-004	Cyber Coverage Clause	2019

자료: 저자가 작성함

〈그림 Ⅱ-9〉 PRA의 사이버보험 인수리스크 감독과정



주: 2020년 사이버리스크에 대한 스트레스 테스트를 수행할 예정이었으나 COVID-19으로 인해 연기됨
자료: 저자가 작성함

나) 미국

미국에서 판매되는 영업배상책임증권(Commercial General Liability Policy)의 보통약관은 ① 담보 A: 신체상해 및 재물손해에 대한 배상책임(Bodily Injury and Property Damage Liability), ② 담보 B: 인격침해 또는 광고침해에 대한 배상책임(Personal and Advertising Injury Liability), ③ 담보 C: 의료비(Medical payment) 등 세 개의 담보로 구성된다(〈그림 Ⅱ-10〉 참조). 신체상해 및 재물손해에 대한 배상책임은 타인에게 신체상해 또는 재물손해를 입힘으로써 발생한 법률상 배상책임을 보상한도액 내에서 보상한다. 인

격침해 및 광고침해에 대한 배상책임은 영업활동 중 불법구금, 중상 및 비방, 사생활 침해, 저작권 및 타이틀(권원) 침해 등으로 발생한 배상책임을 담보한다. 의료비 담보는 피보험자의 구내에서 타인이 신체상해 사고를 입은 경우 피보험자의 과실이 없어 배상책임이 없는 경우에도 피해자가 입은 손해를 보상한다.

영업배상책임보험의 담보 A에서 타인에게 입힌 재물손해에 대한 배상책임은 유형재물(Tangible property)에 입힌 손해에 대한 배상책임만을 의미하며, 타인의 상표권, 특허권, 영업권 등의 권리라든지 열·풍력과 같은 무형재물(Intangible)에 입힌 손해는 담보하지 않는다. 또한 전자데이터(Electronic data)를 유형재물로 간주하지 않아 전자데이터에 입힌 배상책임은 영업배상책임보험 담보 A에서 보장하지 않는다. 영업배상책임보험의 담보 A는 2006년부터 전자데이터 면책조항을 명시적으로 포함한다(CG 00 01 12 07, 2.p). 전자데이터 면책에 따라, 영업배상책임보험은 전자데이터의 손해·사용손해·파손·접근 및 조작 불가로 인해 제3자에게 발생한 신체상해나 재물손해에 대한 배상책임을 담보하지 않는다.

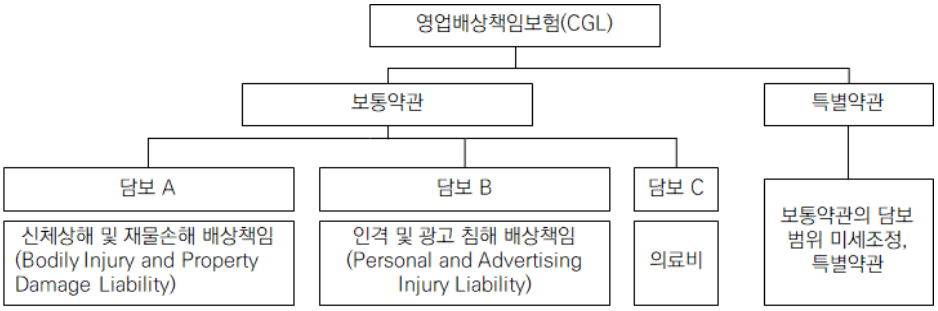
그러나 이후 사이버사고가 급증하자, ISO는 영업배상책임증권 담보 A와 담보 B에 '기밀 또는 사적 정보의 접근 및 공개 면책(Access Or Disclosure Of Confidential Or Personal Information)' 조항을 추가하였다.[30] 동 면책은 특허권, 영업기밀, 공정방법, 고객명단, 금융정보, 신용카드 정보, 건강정보, 그 외 모든 비공개정보 등 개인 또는 조직의 기밀 또는 사적정보에 접근 또는 공개함으로써 발생한 재물손해에 대한 배상책임, 인격침해 및 광고침해에 대한 배상책임을 담보하지 않는다.

ISO의 권고는 보험회사에 구속력을 가지지 않지만, ISO 발표 한 달여가 지난 2014년 6월 16일, 54개주 중에서 메릴랜드를 제외한 53개주에서 동 면책조항을 받아들였다. 전통적으로 기업은 데이터 침해(Data breach) 관련 리스크를 영업배상책임증권의 담보 B: 인격침해 또는 광고침해에 대한 배상책임을 통해 관리하였다. 그런데 2013년 담보 B에 대해 기밀 또는 사적정보의 접근 및 공개 면책이 추가됨에 따라, 기밀 또는 사적정보 접근 및 공개에 따른 인격침해 및 광고침해에 대한 배상책임을 관리하기 위한 별도의 단독 사이버보험에 가입할 수밖에 없게 되었다. 바꿔 말하면, ISO는 사실상 2013년에 이르러서 진정한 의미의 암묵적 사이버면책(Silent cyber exclusions)을 도입한 셈이다.

30) CG 21 06 05 14(Exclusion-Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability-With Bodily Injury Exception)

2020년 ISO는 재물보험(Commercial property insurance)에서 사이버담보를 명확히 제거하기 위해 Cyber Incident Exclusion endorsement(BP 15 60)과 Cyber Incident Exclusion with Ensuing Cause(s) of Loss Exceptions (BP 15 61) endorsement를 발표하였다. 미국 대부분의 주는 기업보험(Commercial property 또는 Businessowners policy)을 판매하는 보험회사가 해당 증권에 2021년 2월부터 전술한 두 개의 면책조항 중 하나를 의무적으로 포함하도록 하고 있다. Cyber Incident Exclusion(BP 15 60)은 사이버사고로 인해 발생한 모든 손실을 면책하나 사이버사고로 인해 화재 및 폭발이 일어난 경우에 한해 그 손해를 보장한다. BP 15 60는 BP 15 61에 비해 사이버사고로 인한 면책의 범위를 보다 넓히고 있다. 2021년 6월부터는 기계결함증권(Equipment breakdown policy)에 Cyber Incident Exclusion(EB 10 01)을 의무적으로 포함해야 한다.

〈그림 Ⅱ-10〉 미국 영업배상책임보험의 구성



자료: Insurance Services Office(ISO)(2006)을 참고하여 저자가 작성함

〈표 Ⅱ-8〉 미국 영업배상책임보험 담보 A의 면책조항 변화

2006년(CG 00 01 12 07)	2013년(CG 21 06 05 14)
2. p. Electronic Data Damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.	2. p. Access Or Disclosure Of Confidential Or Personal Information And Data-related Liability Damages arising out of: (1) Any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information; or (2) The loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data. This exclusion applies even if damages are claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by you or others arising out of that which is described in Paragraph (1) or (2) above. However, unless Paragraph (1) above applies, this exclusion does not apply to damages because of "bodily injury".

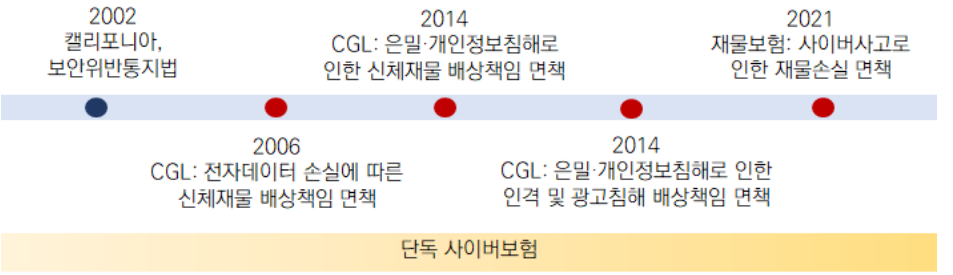
자료: ISO(2006); ISO(2013)

〈표 Ⅱ-9〉 미국 ISO의 사이버사고 관련 면책조항

약관	약관 명칭	공표연도
CG 00 01 12 07	Exclusion-Electronic Data(Coverage A Only)	2006
CG 21 06 05 14	Exclusion-Access or Disclosure of Confidential or Personal Information And Data-Related Liability-With Bodily Injury Exception	2013
CG 21 07 05 14	Exclusion - Access or Disclosure of Confidential or Personal Information And Data-Related Liability-Limited Bodily Injury Exception Not Included	2013
CG 21 08 05 14	Exclusion-Access or Disclosure of Confidential or Personal Information(Coverage B Only)	2013
BP 15 60	Cyber Incident Exclusion endorsement	2021
BP 15 61	Cyber Incident Exclusion with Ensuing Cause(s) of Loss Exceptions	2021
EB 10 01	Cyber Incident Exclusion	2021

자료: 저자가 작성함

〈그림 Ⅱ-11〉 미국 ISO의 사이버사고 면책



자료: 저자가 작성함

다. 단독 사이버보험의 비포괄성

〈그림 Ⅱ-12〉에서 보는 바와 같이 단독 사이버보험에서 보장하는 손해는 기존 손해보험에서 보장하는 유형을 모두 포함할 수 있다. 계약마다 상이하나, 단독 사이버보험은 재물손해, 영업중단손해, 배상책임, 신체상해를 보장하고 사이버랜섬을 보장한다.

그러나 실제로 시장에서 거래되는 손해 유형은 매우 제한적이다. 주로, 배상책임과 랜섬 및 비용 담보에 집중되어 있다. OECD(2017)에 따르면 26개 보험회사에 대한 조사 결과, 응답한 보험회사의 50% 이상이 개인정보 침해, 데이터 및 소프트웨어 손실, 사고대응 비용, 사이버 협박, 영업중단손해, 멀티미디어 배상책임, 규제 및 방어비용을 보장하는 것으로 나타났다(〈표 Ⅱ-10〉 참조). Romanosky et al.(2019)에 따르면, 2009~2016년 기간 동안 미국에서 판매된 단독 사이버보험 상품을 분석한 결과 단독 사이버보험은 배상책임액, 언론대응 비용, 통지 비용, 피해자 서비스 비용, 데이터복구 비용, 영업중단손해, 포렌식 비용, 랜섬, 데이터손실 등을 주로 보장하는 것으로 나타났다. OECD(2020b)에 따르면, 지역에 상관없이 사생활·미디어·통신망 보안 배상책임, 사고대응 비용, 데이터 복구, 사이버협박으로 인한 손해를 기본적으로 보장한다(〈그림 Ⅱ-13〉 참조).

반면, 사이버사고로 인한 재물손해와 신체상해 및 정신적 손해, 지적재산 도난에 대한 보장은 매우 제한적이다. OECD(2017)에 따르면, 지적재산 도난, 물적 자산 손실, 신체 손실에 대한 보장을 제공하는 보험회사의 비율은 12~23%에 불과하다(〈표 Ⅱ-10〉 참조). OECD(2020b)에 따르면, 재물손해, 신체상해, 금융도난, 정신적 손해 등에 대한 보장이 현저히 낮게 나타난다(〈그림 Ⅱ-13〉 참조).

현재 보험산업은 진화하는 사이버공격을 보장하는 데 명백한 한계를 보인다. 사이버공격의 표적이 사이버공간에서 물리적 공간으로 확장되고, 정보 유출 피해에 그치지 않고 재물 및 신체손해를 초래하는 상황에 이르렀다. 그러나 기존 재물 및 배상책임보험에서는 사이버사고로 인한 재물·신체·배상책임담보를 면책하는 추세인데다, 단독 사이버보험은 정보손실 관련 배상책임 또는 랜섬 보장에 집중한 채 재물 및 신체 손해에에 대한 담보 제공에는 소극적이다.

다만, 단독 사이버보험은 사이버 테러리즘으로 인한 손실을 대체로 보장하는 것으로 나타난다. 약관상 ① 테러리즘에 대한 보험회사의 면책조항을 규정하지 않거나, ② 사이버 테러리즘을 부보위험으로서 구체적으로 명시하거나(Affirmative coverage), ③ 일반 테러리즘에 대한 면책조항이 있으나 이것이 구체적으로 사이버 관련 사고에는 적용되지 않는 것으로 나타났다. OECD(2020b)가 검토한 단독 사이버보험 약관 중 단 한 건만 일반 테러리즘 면책조항이 사이버 관련 사고에도 적용되는 것으로 해석되었다.

〈그림 Ⅱ-12〉 보험종목별 사이버리스크 담보

자료: OECD(2020a)

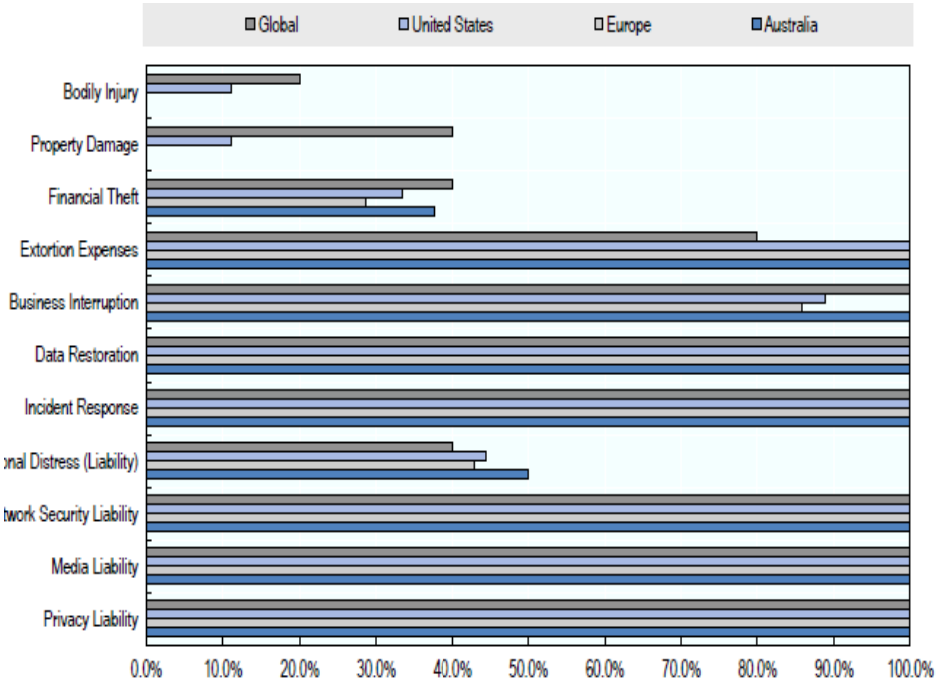
〈표 Ⅱ-10〉 명시적 사이버보험의 보장손해 유형

손해유형	당사자	제3자	보장내용	담보 제공 비율
개인정보보호 위반	○	○	개인정보 유출 시 발생하는 제비용	92%
데이터 및 소프트웨어 손실	○	-	손상 데이터 및 소프트웨어 복구 및 교체 비용	81%
사고대응 비용	○	-	사고 후 손실최소화 및 대응을 위해 소요된 직접 비용	81%
사이버 협박	○	-	사이버 협박의 종결을 위해 범죄자에게 지불하는 비용 및 관련 비용	73%
영업중단손해(BI)	○	-	부보된 사업활동의 중단 또는 방해로 인한 수익상실액과 고정비	69%
멀티미디어 배상책임 (명예훼손)	○	○	명예훼손 등으로 인한 배상책임, 조사비용, 방어비용	65%
규제 및 방어 비용	○	-	벌금, 법률비용 등	62%
평판 손실	○	-	보안위반사실이 공개되어 고객불만, 매출액 감소 손해	46%
통신망 서비스 실패 배상책임	-	○	IT 통신망 내에서 발생한 보안사고로 인한 배상책임	42%
거래상대방으로 인한 영업중단손해(CBI)	-	○	제3자(거래상대방)의 IT실패에 따른 영업중단손해	33%
배상책임: 기술 E&O	-	○	기술 서비스 및 상품 제공 실패에 따른 배상책임	27%
배상책임: 전문서비스 E&O	-	○	전문 서비스 및 상품 제공 실패에 따른 배상책임	23%
금융 도난 및 사기	○	-	컴퓨터 이용 도난 및 사기로 인한 금전손실	23%
지적재산 도난	○	-	시장점유율 감소 결과 손상된 IP자산의 가치	23%
물적 자산 손실	○	-	사이버공격으로 인한 물리적 시설 손실 회복 비용	19%
배상책임: 임원	○	-	임원의 과실, 선량한 관리자로서 주의의무 위반에 따른 클레임 보상	13%
사망 및 신체 상해	-	○	사이버공격으로 인한 사망 및 신체손해	12%
배상책임: 상품·운영	-	○	사이버사고로 인한 제품 및 운영 결함과 관련된 배상책임	8%
환경적 손실	○	-	사이버사고로 인한 환경적 영향과 관련된 배상책임, 청소, 회복 비용	4%

주: 각 담보를 제공하는 상품의 비율로서, 샘플은 26개임

자료: Univeristy of Cambridge(2016); OECD(2017)

〈그림 Ⅱ-13〉 단독 사이버보험 증권에서 보장하는 손해의 유형



주: 1) 특정 담보를 제공하는 증권의 비율을 나타냄
2) 다음 보험회사에서 제공한 정보를 이용하여 작성됨(AIG(Australia, UK, US); Allianz Global Corporate& Specialty(Global); Allied World(US); AXA XL(Australia, US); Beazley(UK, US); CFC Underwriting (Global); Chubb(Australia, UK, US); DUAL(Australia); Emergence Insurance(Australia); Hiscox (UK, US); Liberty International Underwriters(Australia); Munich Re Corporate Insurance Partner (Global); BE(Australia, Europe, US); Swiss Re Corporate Solutions(Global); Tokio Marine HCC (Europe); Zurich Insurance(Australia, Netherlands, US))

자료: OECD(2020b)

라. 사이버 대재해 및 전쟁에 대한 면책 움직임

1) 국가 연루 사이버공격에 재래식 전쟁면책 적용 논쟁

낫페트야는 2017년 6월, 우크라이나를 대상으로 벌인 러시아의 사이버공격이며, 우크라이나 외에도 다국적기업들이 피해를 입었다. 시스템 파괴 공격의 일종인 낫페트야를 퍼뜨려 정부기관을 비롯해 금융·전력·통신·교통 등 수많은 기반시설이 운용에 차질을 빚거나

가동이 중단되어 기업들에 막대한 영업중단손해와 그로 인한 배상책임을 초래하였다. 피해기업들은 사이버리스크를 담보하는 보험계약을 보유하고 있었고, 사고 직후 보험회사에 보험금을 청구하였다. 그러나 복수의 보험회사는 낫페트야 공격이 국가 차원의 적대적 전쟁 행위로, 보험약관에 규정된 전쟁면책 적용을 주장하며 보험금 지급을 거절하였다.

세계적 제약회사인 머크(Merck&Co)는 약 20억 달러의 손실을 보았다. 머크는 2.5억 달러 가치의 사이버보험과 17.5억 달러 가치(1.5억 달러 자기부담금 공제 후)의 20여 개 다른 영업중단보험을 통해 상당 부분을 보상받을 수 있을 것으로 기대했지만, 대부분의 보험회사가 전쟁면책을 이유로 보험금 지급을 거절하였다. 미국 식품 대기업 몬델레즈(Mondelez)는 낫페트야 공격으로 1,700개의 서버와 24,000대의 랩탑에 영구적인 손상을 입었다. 물리적 손해, 공급 및 유통 실패, 고객주문 대응 실패, 마진 감소 등이 1억 달러에 이를 것으로 보았다. 몬델리즈는 보유 중인 보험이 악성 소프트웨어 코드에 의한 물리적 손해를 포함하여 전자데이터, 프로그램, 소프트웨어에 발생한 모든 물리적 손실을 보장함에 따라 취리히 보험회사에 보험금을 청구하였으나, 상대 보험회사는 전쟁면책을 들어 보험금 지급을 거절하였다.

이에 2018년 10월 12일, 머크는 20개 이상의 보험회사와 재보험회사를 상대로 미국 뉴저지 고등법원(Superior Court)에 계약불이행 확인판결을 구하였다.[31] 또한 미국 식품 대기업 몬델레즈(Mondelez)는 취리히 인슈어런스(Zurich Insurance)를 상대로 미국 일리노이 법원에 1억 달러의 소송을 제기하였다.[32] 이 소송은 아직도 미국의 법원에서 계류 중이다.

머크와 몬델레즈가 가입한 포괄위험 담보방식의 재물종합보험(Property insurance package)은 정부나 주권 국가에 의해 시작된 적대적이거나 군사적인 행위를 보장하지 않는다. 낫페트야가 전쟁 행위라는 취리히의 주장은 주장하기는 쉽지만 법정에서 입증하기 쉽지 않다. 그러나 보험회사가 사이버공격으로 인한 보험금 지급을 피하기 위해 이러한 면책조항을 주장할 가능성이 커지고 있다. 두 사건에 대한 법원의 판결은 사이버보험 역사에 이정표가 될 것이다. 이하에서는 국가 연루 사이버공격에 재래식 전쟁면책을 적용하는 것의 문제점을 살펴보고 이를 극복하기 위해 보험산업에서 논의 중인 대안을 살펴보기로 한다.

31) Response of Generali in Merck and Co., Inc. and International Indemnity Ltd. v. ACE American Insurance Company et al, Superior Court of New Jersey Law Division: Union County, October 12, 2018(Merck & Co., Inc. v. Ace American Insurance Co., No. UNN-L-002682-18)

32) Complaint in Mondelez International, Inc. v. Zurich American Insurance Company, Circuit Court of Cook County, Illinois, October 10, 2018(2018-L-011008)

2) 재래식 전쟁면책 적용의 문제점

전쟁면책에 대한 구체적인 문구는 증권마다 상이할 수 있으나, P&C 증권에서는 대체로 광범위하게 작성된다. 전쟁면책은 그 원인이 무엇이든 전시 또는 평화 시 적대행위 또는 전쟁행위로 인해 발생한 모든 직간접적 손실을 면책한다. 낫페트야 공격으로 보험회사를 상대로 소송을 제기한 머크와 몬델레즈의 보험약관상 전쟁면책은 면책 대상 적대행위 및 전쟁행위를 ① 정부 또는 (법상 또는 사실상) 주권을 가진 조직, ② 군대·해군·공군, ③ ① 또는 ②의 대리인 등에 의해 실제 발생한, 임박한, 또는 향후 예상되는 공격을 저지·전투·방어하는 것으로 정의한다(〈표 Ⅱ-11〉 참조).

사이버공격에 재래식 전쟁면책이 적용되기 위해서는 기본적으로 두 가지 조건이 충족되어야한다. 먼저, 사이버공격이 국가 또는 그와 유사한 조직에 의해 이루어져야 한다. 보험회사는 사이버사고의 공격자를 특정해야 하고, 공격자의 배후에 국가가 있음을 입증해야 한다. 다음으로, 문제의 사이버공격이 적대행위 또는 전쟁행위여야 한다. 전술한 두 가지 조건은 재래식 전쟁면책을 사이버공간에 적용하는 데 어려움을 초래한다.

〈표 Ⅱ-11〉 Merck의 보험증권상 전쟁면책 문구

This Policy excludes loss or damage directly or indirectly caused by or resulting from any of the following regardless of any other cause or event, whether or not insured under this Policy, contributing concurrently or in any other sequence to the loss:
2) (a) hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any:
① government or sovereign power (de jure or de facto);
② military, naval, or air force; or
③ agent or authority of any party specified in ① or ② above.
동 보험증권은 그 원인이 무엇이든 다음의 사고로 인해 직간접적으로 발생한 손실을 면책한다: 전시 또는 평화 시 적대적 또는 전쟁 행위로서, ① 정부 또는 (법상 또는 사실상) 주권을 가진 조직, ② 육군·해군·공군, ③ ① 또는 ②의 대리인 등에 의해 실제 발생한, 임박한, 또는 향후 예상되는 공격을 저지·전투·방어하는 것을 포함한다.

주: Mondelez의 보험증권상 전쟁면책 문구도 배열만 다를 뿐 내용은 동일함
자료: Merck & Co., Inc. v. Ace American Insurance Co., No. UNN-L-002682-18; MONDELEZ INTERNATIONAL, INC. v. ZURICH AMERICAN INSURANCE COMPANY, Illinois court(2018-L-011008)

가) 사이버 귀책 문제

무엇보다도, 사이버공간에서는 공격자를 특정하기 어렵다. 사이버 공격자를 추적하여 실체를 특정하는 것을 사이버 귀책(Attribution)이라 한다. 국가 정보기관이나 이들의 지원을 받는 공격자들은 대개 최상위 공격자이다. 인터넷을 형성하는 통신망 아키텍처는 공격자가 흔적을 숨길 수 있는 다양한 방법을 제공하기 때문에, 사이버 귀책은 매우 어려운 일이다. 공격으로 생겨난 로그와 이벤트 정보를 통해 광범위한 디지털 증거 수집 및 분석(Digital forensic)을 하지만, 공격자는 자신이 특정될 만한 흔적을 남기지 않도록, 자신의 컴퓨터에서 공격을 수행하는 것이 아니라, 사전에 해킹해서 장악한 어떤 희생자 컴퓨터·기기에서 공격을 수행하고, IP 주소를 변조(Spoof)하거나 익명 프락시(Proxy) 서버를 이용하기도 한다. 또한 국경을 넘는 범죄 조사의 경우에는 해당국의 사법 당국 협조를 얻어야하기 때문에 신속한 증거 수집 등의 조사작업이 지연·방해되는 등의 어려움이 있다.

다음으로, 공격자를 특정했더라도, 공격자와 특정 국가 간의 관계를 규명하기 어렵다. 공격자(개인이나 단말기)를 특정했다고 해도 공격자와 책임 있는 국가나 조직과의 관계를 단정하기는 어렵다. 사이버공격의 행위자와 책임 있는 주권국가의 관계를 입증하지 못하면 보험약관상 전쟁면책을 적용할 수 없다. 각국 정부는 사이버전과 관련된 중요한 사료를 보안상의 이유로 공개하지 않고 있다. 공격이 노출된다 해도 애국적 민병대의 소행으로, 국가와의 연관성이 없음을 주장한다. 예를 들어, 보안 솔루션 업체인 Mandiant는 APT-1의 배후로 중국 인민해방군 총참3부 2국 산하 61398부대를 꼽았다. 오랜 조사를 통해 사무실 위치, 관련 중국 정부 문서, 천 명 이상 일하는 건물, 해킹 방식, 훔쳐간 정보, 공격에 동원된 IP의 주소지가 상하이 푸동에 있는 사이버 부대와 같은 점 등을 알아냈지만 혐의자를 망신주기(Naming and shaming)하는 데 그쳤다. 언론 매체와 미국 NSA의 내부 고발자 에드워드 스노든(Edward Snowden)의 주장에도 이란의 핵발전소를 공격한 악성코드 스턱스넷의 개발자에 대해서 이스라엘과 미국 당국이 스스로 진실을 밝히지 않는 한, 공격자의 특정은 영원히 해결되지 않는다. 특히나 글로벌 보안 회사들이 분석 추적하여 특정 국가 소속 단체(군 또는 정보기관)로 귀책한 그 어떤 사이버공격 사건에도 해당 국가가 사고 조사에 협조하거나 진실을 밝히는 데 협력한 바 없다(김흥근 2020).

셋째, 공격자를 특정하고 특정 국가의 배후를 확인하는 과정을 정부에 의존하는 것은 매우 단편적인 접근이다. 타국 정부가 사이버공격의 배후에 있음을 확인했더라도, 안보 또는 외교상의 이유로 이를 모두 공표하는 것은 아니다. 또한 정부조차도 결정적인 증거를

확보하지 못한 채 특정 국가 배후설을 공표하기도 한다. 나아가, 전쟁면책 적용을 위해 사이버 귀책에 대한 규명을 정부에 의존하는 것은 정부와 보험산업 간 피드백 고리를 왜곡시킬 여지가 있다. 사이버공격에 대한 전쟁면책 적용 여부를 두고 보험회사와 피보험자 간 법적 다툼이 빈번해지면, 귀책에 대한 정부의 공표 여부와 용어선택은 신중해질 수밖에 없다. 예를 들어, 오바마 대통령은 2014년 북한의 소니 픽처스 해킹사건을 사이버전쟁이 아닌 사이버반달리즘(Cybervandalism)으로 표현하였다.[33]

나) 사이버공격의 속성 문제

공격자를 특정하고 공격자의 배후에 특정 국가가 있다는 것이 성공적으로 확인되면, 전쟁면책 적용을 위해 보험회사는 문제의 국가 연루 사이버사고가 '적대 또는 전쟁(Hostile or warlike) 행위'인지 여부를 규명해야 한다.

국가 연루 사이버사고가 모두 적대 또는 전쟁 행위인가? 사이버공간에서 '적대 및 전쟁 행위'란 무엇일까? 재래식 전쟁면책에서 규정한 공격의 속성을 사이버공격에 적용하기는 쉽지 않다. '적대 또는 전쟁 행위'는 국가 연루 사이버사고를 모두 포괄할 정도로 광범위하게 해석될 수도 있고, 재래식 전쟁면책이 재래식 전쟁에 대응한 것이었다는 점에서 매우 제한적으로 해석될 수도 있다.

국가 배후 사이버공격의 표적은 국방 관련 기술 및 기밀, 사회기반시설, 산업정보 등 다양하다. 표적이 다르다고 하더라도 궁극적인 의도는 같을 수 있다. 예를 들어, 국가 배후 산업 스파이는 그 자체로 적대 및 전쟁 행위로 보기는 어렵다. 그러나 국가 배후 경제스파이가 경제적· 군사적·기술적으로 타 국가들을 군림하려는 궁극적인 의도하에 기획된 하나의 거대한 캠페인에 속해 있다면, 국가 배후 경제스파이 행위를 단순히 경제적 의도로만 보기는 어렵다. 소련이 미국의 물리력이 아닌 군비경쟁을 하던 와중에 스스로 붕괴되었다는 점을 감안하면, 현대전은 경제패권 전쟁이다. 미국 정부는 중국의 경제 스파이 전략을 '강탈하고(Rob), 복제하고(Replicate), 대체하기(Replace)'로 표현하고 이를 경제전쟁으로 보고 있다. 타국 기업의 지식재산을 훔쳐 기술을 모방하여 글로벌 시장에서 타국 기업을 대체하고 있다는 것이다. 세계 빅3 통신장비업체인 캐나다 노르텔(Nortel)의 시스템은 2000년부터 약 10년 동안 전면적인 해킹공격에 노출되어 2009년 1월 도산 신청을 했고

33) 관련 동영상은 다음을 참조하기 바람(CNN(2014. 12. 24), "Obama: North Korea's hack not war, but 'cybervandalism'")

동 기간 중국의 화웨이(Huawei)는 급성장하였다. 중국 정부의 개입이 공식적으로 확인된 바는 없지만, 해킹공격에 중국 정부가 배후에 있다는 주장이 지속적으로 제기되었다. 러시아와 북한처럼 주요 기반시설을 공격하여 물리적 타격을 가하는 요란한 사이버공격 대신, 중국은 경제스파이와 같은 '조용한' 사이버공격을 감행한다.[34] 그러나 경제스파이의 경우 재래식 전쟁약관의 '적대 또는 전쟁 행위'로 포섭되기 어려울 수 있다.

다) 사이버보험의 가치 저하

국가가 연루된 모든 사이버공격에 대해 재래식 전쟁면책이 적용된다면, 국가 연루 사이버공격이 빈번한 상황에서, 기업이 사이버보험을 구입할 이유는 무엇인가? 단독 사이버보험이 본래 포괄위험 담보방식의 영업배상책임보험에서 사이버사고로 인한 배상책임을 일부 면책하자, 그로 인한 기업의 보장공백을 해소하기 위해 도입·확산된 상품이라는 점에서, 사이버보험이 국가연루 사이버공격으로 인한 손실을 면책한다면, 단독 사이버보험의 존재 가치가 심각하게 훼손될 수 있다.

라) 집합리스크 잔존

국가 연루 사이버공격에 재래식 전쟁면책을 적용하는 것만으로 보험회사가 사이버사고로 인한 대재해리스크를 피할 수 있는 것은 아니다. 기존 전쟁약관은 포괄적이지만, 사이버공간상의 모든 집합리스크의 가능성을 제거한 것은 아니다. 여전히 사이버공간에서는 보험회사의 건전성을 훼손하는 집합리스크가 존재한다. 러시아 소행으로 알려진 낫페트야와 같은 또는 그보다 더 파괴적인 공격을 비국가 행위자가 저지를 수도 있다. 또는 대규모 피해를 초래한 사이버사고가 악의를 가진 공격자 없이 우연히 발생할 수도 있다.

3) 사이버 대재해 및 전쟁면책 마련 움직임[35]

전술한 바와 같이 국가 연루 사이버공격에 재래식 전쟁면책을 적용하는 것은 현실적으로

34) 2000년 이후 미국을 상대로 수행된 중국의 스파이 행위에 대한 CSIS(Center for Strategic and International Studies)의 보고서에 따르면, 42%가 중국 군 또는 정부에 의해 수행되었으며, 34%가 군사정보를, 51%가 상업정보를 빼냄

35) Bateman(2020)

여러 가지 한계에 이른다. 국가 연루 사이버사고가 급증하는 가운데 2017년 낫페트야 공격으로 인해 피보험기업과 보험회사 간 전쟁면책 적용 여부를 두고 소송이 진행되자, 보험업계는 재래식 전쟁면책을 국가 연루 사이버사고에 확대 적용할 수 있는지에 대해 다소 회의적인 시각을 보이며, 사이버사고에 부합한 면책조항과 부보범위를 논의하기 시작하였다. 보험업계가 국가 연루 사이버사고에 부합한 신규 면책 문구를 검토하고 있다는 자체가, 재래식 전쟁면책을 낫페트야로 인한 기업의 손실에 적용하는 것이 적절치 않을 수도 있다는 보험업계의 시각을 방증한다.

The Geneva Association과 IFTRIP(International Forum of Terrorism Risk Reinsurance and Insurance Pools, 국제 테러리즘 리스크 (재)보험풀 포럼)은 2019년 태스크포스를 구성하여 사이버 테러리즘과 사이버전쟁에 대한 연구를 진행 중이다. GA·IFTRIP은 2020년 7월과 2021년 3월 연구결과를 공개하였다(Carter&Enoizi 2020, 2021). 이들은 사이버리스크의 부보가능성을 촉진하기 위해서는 사이버사고를 규정할 공통의 용어가 필요하다고 보았다. 보고서에서는 사이버사고를 비악의적 사고, 사이버범죄, 사이버 테러리즘, 적대적 사이버행위(HCA), 사이버전쟁 등 5가지로 구분하였다. 사이버 테러리즘과 사이버전쟁 사이에 HCA를 추가하여 사이버전쟁의 개념을 보다 명확히 하고자 하였다. 국가 배후 사이버공격 중 전쟁으로 선포되었거나, 누가 보더라도 전쟁으로 볼만한 공격을 사이버전쟁으로, 국가 배후 사이버공격 중 전쟁행위에는 미치지 않은 행위를 HCA로 규정하였다. 이로써, 보험회사가 보험약관에 재래식 전쟁면책 조항을 일괄 삽입하는 대신, 자사의 역량에 따라 부보가능한 사이버공격의 유형을 선택하도록 하고자 함이다.

국가 연루 사이버공격에 재래식 전쟁면책 적용 시 가장 문제가 되는 것은 바로 공격자 특정과 공격자와 특정 국가 간의 관계 규명, 즉 사이버귀책이다. 또한 재래식 전쟁면책이 적용된다 하더라도, 보험회사는 국가가 연루되지 않은 대규모 사이버공격 또는 비악의적 대규모 사이버사고에 여전히 노출된다. 이에 Bateman(2020)은 국가 연루 여부나 사고의 악의성 여부에 상관없이, 사이버 대재해에 부합한 사이버 대재해 면책(Cyber catastrophe exclusion)을 다음과 같이 제안하였다.

This insurance does not cover any loss, damage, liability, cost, or expense of any kind directly or indirectly arising out of, resulting from, or in consequence of **catastrophic cyber-induced impacts.**

Catastrophic cyber-induced impacts mean degradation of the confidentiality,

---

integrity, or availability of computer hardware, software, or data, or their communications, which: causes serious or enduring disruptions of an essential service, or otherwise causes serious or enduring harms to public safety, public health, or societal functioning on an international, national, or regional (sub-national) scale.

Essential service means a service whose uninterrupted and reliable operations are critical for public safety, public health, or societal functioning—to include electricity, water, sewage, emergency services, the food supply, the transportation system, short-term financial services, and core telecommunications infrastructure, among others.

이 보험은 재난적 사이버사고의 결과로 발생한 어떠한 직간접적 손실도 보장하지 않는다. 재난적 사이버사고란 컴퓨터 하드웨어, 소프트웨어, 데이터, 통신의 기밀성, 무결성, 가용성 저하를 통해 필수서비스의 심각한 또는 지속적 훼손을 초래하거나 국제적, 국가적, 지역적 규모로 사회기능, 공중보건, 치안에 심각한 또는 지속적인 해를 초래하는 사고를 의미한다. 필수서비스란 치안, 공중보건, 사회기능을 위해 지속적이고 안정적인 작동이 중요한 서비스를 의미한다. 무엇보다도 전기, 상수도, 응급서비스, 식량공급, 운송시스템, 단기 금융서비스, 핵심 정보통신 인프라 등을 포함한다.

사이버 대재해 면책은 전쟁에 대해서는 언급하지 않는다. 규명이 어려운 국가 연루 여부를 따지지 않기 위함이다. 사이버 대재해 면책은 귀책에 대한 소송의 가능성을 줄인다는 점에서 의미를 가진다.

그러나 보험산업 입장에서는 사이버 대재해 면책에 더해 전쟁 관련 또는 국가 배후 사이버사고에 대한 면책이 추가되어야 할 이유가 여전히 존재한다. 그 논리를 살펴보면, 첫째, 전쟁면책은 사이버보복에 나선 정부의 도덕적 해이로부터 보험회사를 보호할 수 있다. 보험회사가 전시 또는 국가 연루 사이버공격을 보장한다면, 동 사고가 전술한 사이버 대재해 면책에 해당하지 않는 한, 정부는 사이버보복의 비용을 보험회사가 부담한다는 것을 알고 더 공격적으로 대응할 수 있기 때문이다. 전쟁면책은 이러한 도덕적 해이를 줄일 수 있다. 둘째, 전쟁면책 적용 여부를 사이버전과 키네틱전에 대해 달리할 경우, 사이버-키네틱전(Cyber-kinetic warfare)에 대한 보상에 혼란이 발생할 수 있다. 미래전은 사이버전

과 재래전을 결합한 형태의 융·복합전이 될 것이다. 초기 정보화가 인간의 정보능력을 확장시켜 통신망 지휘통제를 가능케 하는 작전 개념을 이끌어냈다면, 4차 산업혁명은 새로운 데이터 환경에서 인공지능과 로봇을 활용한, 이른바 사이버-키네틱전의 출현을 이끈다. 재래식 무기와 방법을 통해 이뤄지는 키네틱전(Kinetic war)은 높은 집합리스크와 불확실성으로 인해 대부분의 표준 보험종목에서 면책이다. 그러나 사이버전에 대해서 보상이 이뤄질 경우, 동일 전쟁에서 발생한 사이버공격과 키네틱공격에 대해 보험취급이 달라진다. 셋째, 전시는 개별적으로는 대재해 면책의 기준에 이르지 않지만 모두 합쳐 대규모 집합손실로 귀결되는 일련의 사이버사고를 초래할 수 있다.

앞서 살펴본 바와 같이 키네틱전에 적용되던 재래식 전쟁면책은 사이버전에 적합한 모형이 아니다. Bateman(2020)은 사이버전쟁 면책(Cyber war exclusion)을 다음과 같이 제안하였다.

This insurance does not cover any loss, damage, liability, cost, or expense of any kind directly or indirectly arising out of, resulting from, or in consequence of **wartime cyber-induced impacts.**

Wartime cyber-induced impacts mean degradation of the confidentiality, integrity, or availability of computer software or data, or their communications, where such software, data, or communications is stored or processed on hardware physically located within an area of hostilities.

Area of hostilities means the entire sovereign territory of a state, provided that anywhere within such territory, major combat operations are taking place at the time of the wartime cyber induced impacts or are initiated, in whole or in part, by the wartime cyber-induced impacts.

Major combat operations mean regularly recurring or large-scale military operations between at least two states or statelike entities, including any forces under their direct control, which result in significant loss of life or widespread destructionof physical property.

Statelike entity means a nonstate organization that exercises enduring, de facto political authority in a definable physical area and controls substantial conventional military capability. Examples include Hamas in Gaza, Hezbollah in parts of Lebanon,

---

and formerly the socalled Islamic State in parts of Iraq and Syria

이 보험은 전시 사이버사고의 결과로 발생한 어떠한 직간접적 손실도 보장하지 않는다. 전시 사이버사고란 물리적으로 교전지역 내 위치한 하드웨어에 저장 또는 처리되는 컴퓨터 소프트웨어, 데이터, 통신의 기밀성, 무결성, 가용성 저하를 의미한다. 교전지역이란 전체 주권국가의 영토를 의미한다. 단, 영토 내 어디에서라도 전시 사이버 유도 영향 시 전투작전이 일어나거나 전투작전이 전체적으로 또는 부분적으로 전시 사이버 유도 영향에 의해 발생한다. 주요 전투작전이란 적어도 두 개 이상의 국가 또는 유사 국가기관 간에 규칙적으로 되풀이하여 일어나는 또는 대규모 군사작전으로, 그들의 직접적인 통제하에 상당한 인명손실 또는 물리적 재산의 광범위한 파괴를 초래하는 것이다. 유사 국가기관이란 비국가 조직으로서 정의 가능한 물리적 지역에서 사실상 정치적 권한을 지속적으로 행사하고 상당한 전통적인 군사력을 통제한다. 예를 들어, 가자지역의 하마스, 레바논의 헤즈볼라, 이란 및 시리아 지역에서 IS(이슬람국가)를 포함한다.

상기 사이버전쟁 약관은 기존 전쟁약관에서 요구되었던 사이버 귀책의 문제, 즉 공격자 특정과 공격자와 특정 국가 간의 관계 규명의 문제를 해소한다. 사이버전쟁 면책은 공격자 정체 및 특정 국가 배후 여부와 상관없이, 파손된 컴퓨터 소프트웨어, 데이터, 통신이 물리적으로 교전지역 소재 하드웨어에 저장·처리된 경우 효력이 발생한다. 또한 재래식 전쟁면책과 달리, 공격의 속성을 요구하지 않는다. 재래식 전쟁면책은 적대 및 전쟁 행위로 인해 발생한 손실(Loss or damage caused by hostile or warlike action)을 면책하였다.

향후 사이버 대재해 및 전쟁면책에 대한 최종 문구는 추가 논의를 통해 보다 정교해질 것으로 보인다. 분명한 것은, 보험산업이 사이버 대재해 및 전쟁에 대해서는 어떤 방식으로든 자율적 담보 공급을 중단 또는 축소할 것이라는 점이다.

마. 벌금 및 랜섬담보의 반공익성

Berliner(1982)는 부보가능성 판단 기준을 크게 계리적 측면, 시장 측면, 공익적 측면 등 세 가지로 구분한다. 공익적 측면에서, 보험상품은 공공정책 및 법규에 반해서는 안 된다. 미국 시장에서 판매되는 단독 사이버보험은 개인정보 침해 관련 법규 위반에 따른 벌금에 담보를 제공한다. 그리고 미국, 유럽, 호주 등에서 판매되는 대부분의 단독 사이버보험은

랜섬에 대한 담보를 제공해 왔다. 개인정보보호에 대한 규제가 강화되고, 랜섬웨어 공격이 급증함에 따라, 동 담보에 대한 기업의 수요가 증가하였고 이에 보험회사가 담보 제공으로 부응한 것이다. 사이버사고와 사이버보험 시장의 급격한 변화가 단기간에 일어남에 따라, 담보 제공의 적절성에 대한 충분한 논의가 선제되지 못하였다. 최근 벌금과 랜섬에 대한 담보 제공의 반공익성에 대한 논의가 전개되고 있다.

1) 벌금담보

벌금에 대한 보험담보 제공은 2018년 EU의 GDPR(일반개인정보보호법) 시행과 함께 세계 보험업계의 주요 관심사항이 되었으며, 기업들의 요청으로 2020년 OECD가 동 논의에 개입하였다(OECD 2020a). GDPR은 EU 회원국에 일괄적으로 적용되는 개인정보보호법으로, 2016년 제정되어 2018년 5월 시행되었다. GDPR은 위반 시 과징금 부과를 규정하고 있으며, 최대 과징금은 일반적 위반사항인 경우 전 세계 매출액의 2% 혹은 1천만 유로(약 125억 원) 중 높은 금액이며, 중요한 위반 사항인 경우 전 세계 매출액의 4% 혹은 2천만 유로(약 250억 원) 중 높은 금액이다. 국내외 기업의 역차별 해소를 위해 우리나라(위반 행위 관련 매출의 3% 이하 → 전체 매출의 3% 이하)뿐만 아니라 미국, 캐나다, 호주, 중국 등도 국제적 흐름에 맞춰 벌금 부과기준을 상향하고 있어 기업의 벌금에 대한 부담이 현저히 증가하였다.

노르웨이, 슬로바키아, 스웨덴을 제외한 대부분의 유럽국가에서는 개인정보보호법 위반에 따른 벌금을 보험담보로 제공하는 것을 금지한다. 영국의 금융행위감독청(Financial Conduct Authority; FCA)은 불법원인급여 법리(Ex turpi causa)에 따라 벌금에 대한 보험제공을 명시적으로 금지한다.[36] 미국은 주마다 상이한 입장을 보인다.

개인정보보호법 강화 기조에 따라, 벌금에 대한 기업의 부담이 과도해지자, 불법행위의 고의성의 정도(고의 vs. 과실 vs. 부주의), 제재의 목적(불법행위 억제 vs. 처벌) 등에 따라 부보가능성을 달리 판단해야 한다는 논의가 없지는 않다(OECD 2020a). 그러나 유럽 대부분의 국가는 벌금에 대한 보험제공이 공익에 반한다는 점에서 기존의 입장을 강경하게 견지하고 있다. 지금까지 논의에서 합의에 이른 것이라면, 국가 간 동일한 기준이 필요하다는 점이다.

36) FCA Handbook GEN 6.1.5(Insurance against financial penalties) No firm may enter into, arrange, claim on or make a payment under a contract of insurance that is intended to have, or has or would have, the effect of indemnifying any person against all or part of a financial penalty

2) 랜섬담보

대규모 피해를 초래하는 랜섬웨어 공격이 급증함에 따라, 보험회사의 랜섬담보 제공에 대한 각국 정부와 OECD와 EIOPA 등 국제기구의 검토가 이어지고 있다. 〈그림 Ⅱ-13〉에서 보는 바와 같이, 미국·유럽·호주 시장에서 판매되는 단독 사이버보험은 대부분 랜섬을 담보한다. 그러나 사이버리스크와 사이버보험 시장이 확대됨에 따라 사이버보험에 대한 관리 감독의 기준이 정립되면서, 최근 보험회사의 랜섬담보에 대해 미국과 프랑스 등 주요 랜섬웨어 피해국 정부는 부정적인 입장을 밝히고 있다(〈표 Ⅱ-12〉 참조).

미국 재무부 OFAC(Office of Foreign Assets Control, 해외자산통제국)는 2020년 10월, 랜섬웨어에 감염됐을 경우 공격자에게 랜섬을 지급하기 전 OFAC 허락을 받아야 한다는 내용을 담은 가이드라인을 발표하였다.[37] OFAC는 제재 대상과 연관 단체에 몸값을 지불하는 것을 '국가안보 이익을 위협'하는 행위로 규정하고, 보험회사 등 랜섬지급을 용이하게 하는 회사는 공격자의 랜섬웨어 공격을 촉진시킬 뿐만 아니라 OFAC 규제를 위반할 가능성이 있음을 경고하였다(U.S. Department of Treasury 2020a). 이는 지난 몇 년간 미국 재무부가 제재해온 해커 그룹에 피해를 입은 경우에 한해 적용된다. 국제긴급경제권한법(International Emergency Economic Powers Act; IEEPA)과 적성국교역법(Trading with the Enemy Act; TWEA)에 의거, 미국인과 단체들은 제재 대상자와 포괄적 제재를 받고 있는 북한 등과의 직간접적인 거래가 금지된다. OFAC의 허가 없이 복호화 비용을 지불할 경우 해당 기업에 대한 법적 조사가 이뤄진다. 복호화 비용 지불을 처리하는 금융기관과 사이버보험을 제공하는 보험회사, 디지털 포렌식 및 침해사고 대응 관련 기업이 조사 대상으로 포함될 수 있다. 아울러 OFAC에 따르면, 제재 및 규제로 금지된 거래에 개입된 사실을 인지하지 못하고 있더라도 제재 위반 행위에 대해 민사 책임을 물을 수 있다. OFAC는 제재대상자와 북한 등 포괄적 제재대상국이 개입한 랜섬웨어 지불금 지급에 연루될 수 있는 기관들이 위험 기반 접근법을 적용한 제재 이행 프로그램을 실행해 제재 위반에 노출될 수 있는 위험성을 줄여야 한다고 권고하였다.

범죄리스크에 대한 보장이 가능한 스위스·네덜란드·영국을 제외한 대부분 유럽국가에서는 랜섬담보에 대해 미국과 유사한 입장을 견지한다.[38] 2020년 프랑스 사법부와 국가정

37) 북한 정부 지원을 받는 해커 그룹 Lazarus Group, Bluenoroff, Andariel, 러시아 해커 그룹인 Evil Corp와 리더인 Maksim Yakubet, Cryptolocker 개발자 Evgeniy Mikhailovich Bogachev, SamSam을 개발한 두 이란인을 OFAC 허가 대상 사이버 공격자로 지정함

보시스템보안국(Agence Nationale de la Sécurité des Systèmes d'Informatio; ANSSI)은 보험회사의 랜섬담보가 자금세탁금지[39]와 테러리즘 자금 지원[40] 관련 법을 위반할 소지가 있음을 경고하였다. 보험회사의 랜섬담보를 법규에서 명시적으로 금지하지는 않는다. 그러나 일부 랜섬공격이 테러리스트 조직 또는 국제제재대상으로 지정된 개인의 소행이라는 점을 감안하면, 보험회사의 사이버담보는 법규위반의 소지가 크다. ANSSI는 랜섬웨어 공격자들이 사이버보험을 구입한 기업을 표적으로 삼는다는 점에서, 보험회사의 랜섬담보 제공이 랜섬웨어 공격을 지속시키고, 그로 인한 피해를 확대시킨다고 경고하였다(ANSSI 2021). 이에 프랑스 손해보험회사 AXA는 2021년 5월 프랑스 현지에서 랜섬담보 제공 중단을 발표하였다.

〈표 Ⅱ-12〉 국가별 랜섬웨어 비용과 다운타임 비용(개인유저 제외)

구분	총 접수건수(Submission)	최소비용(억 USD)	추정비용(억 USD)
미국	15,672	48.9	195.7
프랑스	4,476	13.9	55.5
스페인	4,088	12.7	50.9
이탈리아	3,835	12.0	48.0
독일	3,747	11.6	46.4
캐나다	3,236	10.1	40.4
영국	2,718	8.4	33.6
호주	2,072	6.5	25.9
오스트리아	819	2.6	10.3
뉴질랜드	265	0.8	3.3

주: EMSISOFT는 보안업체로, EMSISOFT의 상기 추정은 랜섬웨어 식별 서비스 ID Ransomware를 이용하는 공공·민간 부문 기관의 랜섬웨어 감염 접수자료에 근거하여 산출되었으며, 전체 랜섬웨어 피해기업의 약 25%가 ID Ransomware를 이용 중인 것으로 추정함

자료: EMSISOFT

38) 일반적인 인질 및 납치 범죄에서는 범죄리스크에 대한 방어수단으로 보험회사의 몸값담보 제공에 대해 논쟁의 여지가 크지 않았을 것으로 보이나, 미국과 프랑스의 주장대로, 사이버공격에서 랜섬담보가 테러리스트의 자금 지원에 해당하고 랜섬웨어 공격을 도리어 자극하는 기제로 사용된다면, 이들 국가에서도 향후 랜섬담보에 대한 기조 변화가 있을 것으로 보임

39) French Criminal Code Article 324-1

40) French Criminal Code Article 421-2-2

3. 사이버리스크에 대한 보장공백 확대

2017년 낫페트야로 인한 총 피해액은 100억 달러로 추정된다. 보험에 가입되어 보험회사에서 지급하는 손실액, 즉, 피보험손실은 30억 달러로,[41] 이 중 90%는 암묵적 사이버보험, 나머지는 명시적 사이버보험의 보장대상이다. 낫페트야로 인한 기업의 직접적인 손해는 랩탑·데이터·시스템 파손 등 재물손해뿐만 아니라, 그로 인한 영업중단손해이다. 이는 기존 포괄위험 담보방식의 재물 및 배상책임보험에서 암묵적으로 담보하는 유형의 손해로, 단독 사이버보험에서는 주로 면책이다. 2017년 낫페트야 공격 이전까지는, 암묵적 사이버담보의 언더라이팅 리스크에 대해 보험업계가 적극적으로 대응했다고 보기는 어렵다. 그럼에도 불구하고, 한 건의 성공한 랜섬웨어에 대한 보장공백이 총 손실액의 70%에 이른다. 암묵적 사이버담보의 언더라이팅 리스크를 우려한 보험업계가 포괄위험 담보방식의 재물 및 배상책임보험에서 사이버사고에 대한 면책을 확대하고 있다는 점을 감안하면, 낫페트야 공격이 2017년이 아닌 2021년에 발생했을 경우 보장공백이 이보다 컸을 것임을 유추할 수 있다.

〈그림 Ⅱ-14〉 낫페트야로 인한 피보험손실액

주: 단위는 1억 달러임
자료: Bateman(2020)

향후에는 사이버리스크에 대한 보장공백이 이보다 커질 것으로 예상된다. 구체적으로 먼저, 사이버사고로 인한 재물 및 신체 손해에 대한 보장공백이 불가피하다. 2010년대 들어 사이버공격의 진화로 인해 사이버사고의 빈도 및 심도가 급격히 증가하면서, 보험회사의 사이버담보에 대한 언더라이팅 및 보유 리스크도 증가하였다. 이에 보험산업은 보험요율 인상, 보상한도 축소, 엄격한 인수심사 등의 전형적인 대응에서 벗어나 전통적인 포괄위험 담보방식의 재물 및 배상책임보험에서 암묵적으로 보장하던 사이버리스크에 대해서는 사이버 면책을 적극적으로 추가하고, 단독 사이버보험에서는 재물손해 또는 무형자산 손

41) 피보험손실액에 전쟁면책이 적용된 것인지 여부는 확인되지 않음

해보다는 개인정보 침해 등의 배상책임담보에 집중한다. 세계 사이버보험 시장의 주 공급자인 영국이 감독당국의 지침에 따라 2020~2021년 기간 동안 암묵적 사이버보험의 보장 및 면책 명확화 작업이 어느 정도 마무리될 것으로 보인다.

둘째, 사이버사고로 초래된 NDBI(Non-physical Damage Business Interruption)에 대한 보장공백이 존재한다. NDBI는 물리적 재물손해를 동반하지 않은 영업중단손해를 의미한다. 사이버공격은 재물에 물리적 손해를 발생시키지 않은 채, 서비스 거부 또는 중단으로 영업중단손해를 초래할 가능성이 높다. 워너크라이 감염사례에서 보듯이 랜섬웨어는 몸값 지불 시까지 시스템이 마비되기 때문에 그로 인한 영업중단손해는 심각한 수준이다. OT 및 ICS 공격도 결국은 시스템을 마비시켜 영업중단손실을 초래한다.

셋째, 국가 배후 사이버공격과 재난적 사이버사고에 대한 보장공백이 불가피하다. 현재 재래식 전쟁면책 적용 논쟁으로 국가 배후 사이버공격에 대한 보장이 불확실한 가운데, 국가 배후 사이버공격과 사이버 대재해에 대한 보험산업의 면책 움직임이 본격화되었다.

넷째, 사이버보험에 대한 제도적 논의가 진행될수록, 기업의 보장수요가 높은 벌금과 랜섬에 대한 보장공백이 커질 것으로 예상된다. 개인정보보호법 위반에 따른 수위 높은 벌금이 사실상 위반행위에 대한 사후 처벌보다는 위반행위의 사전적 억제에 방점이 있다는 점에서 향후 보험회사의 벌금담보 제공이 법 목적을 훼손할 수 있다는 결론에 도달할 수 있다. 또한 2020년에 들어서야 랜섬담보가 랜섬웨어 공격을 촉진하고 테러리즘 자금 지원 행위로 간주될 수 있다는 미국 및 프랑스 정부의 발표가 있었다. 현재 사이버보험에서 벌금담보와 랜섬담보 제공 여부는 국가마다 상이하지만, 정합성 제고를 위한 국제적 논의가 진행 중에 있으며, 긍정적이지는 않다.

〈그림 Ⅱ-15〉 사이버리스크에 대한 보장공백

사이버사고의 진화		사이버보험 공급 축소 기조	보장공백
공격자	개인, 범죄조직 → 국가, 준정부	사이버리스크 인수에 대한 불안 고조	재물 및 신체 손실
공격동기	호기심, 과시, 금전 → 정치·군사적	재물배상책임보험의 사이버손해 보장 배제	NDBI
공격표적	개인, 중소기업 → 대기업, 정부기관, 국가기반시설	단독 사이버보험의 비포괄성	국가 배후 사이버공격
피해유형	정보유출 → 물적·인적, 랜섬	사이버 대재해 및 전쟁에 대한 면책 시도	사이버 대재해
피해규모	통제가능 → 재난적	벌금 및 랜섬 담보의 반공익성	벌금 및 랜섬

자료: 저자가 작성함

4. 소결

이 장에서는 최근 기업이 직면한 사이버리스크의 양적·질적 변화, 그로 인한 사이버보험 시장 내 수요 및 공급의 변화와 보장공백을 분석하였다. 먼저, 2010년대 들어 ① 사이버사고의 공격자는 개인 또는 범죄조직에서 국가·준정부조직·테러조직으로, ② 공격동기는 호기심·금전·과시욕에서 정치적·군사적 동기로, ③ 공격표적은 개인 또는 보안이 취약한 중소기업에서 공급망 공격을 통한 대기업과 국가기반시설로, ④ 피해 유형은 정보 유출 및 개인정보 침해에서 재물, 신체, 영업중단손해, NDBI 등으로, ⑤ 피해심도는 통제 가능한 수준에서 파괴적인 수준으로 확대·진화하였다.

파괴적 사이버공격의 빈도 및 심도 증가와 기업의 사이버 관련 규제리스크 증가에 따라, 사이버보험에 대한 수요도 급격히 증가할 것으로 예상된다. 사이버리스크의 양적·질적 변화에 대응해 보험업계는 사이버보험 공급에 보수적 기조를 취할 것으로 보인다. 구체적으로, ① 사이버사고의 빈도 및 심도 증가, 대재해 가능성 등에 따른 공급 기조 변화, ② 암묵적 사이버담보의 언더라이팅 리스크 가시화와 그에 따른 보험업계의 포괄위험 담보방식의 재물·배상책임보험에서 사이버면책 확대 움직임, ③ 정보 유출 피해 등 배상책임과 비용보장에 집중된 단독 사이버보험의 비포괄성, ④ 2017년 낫페트야 공격으로 촉발된 국가 배후 사이버공격에 대한 재래식 전쟁면책 적용 논란과 그로 인한 보험업계의 사이버 대재해 및 전쟁면책 움직임, 그리고 ⑤ 보험회사의 벌금 및 랜섬담보의 반공익성 논쟁 및 규제에 따른 담보 제공 중단 움직임 등이 있다. 이에 따라 사이버사고로 인한 재물 및 영업중단손해, NDBI, 신체손해, 국가 배후 사이버공격, 사이버 대재해, 그리고 벌금 및 랜섬담보에 대한 보장공백이 커질 것으로 보인다.

사이버사고에 대한 정책적 대응은 사전적 보안강화와 사후적 피해회복으로 구분 가능한데, 우리나라의 경우 주로 전자에 집중해 왔다. 사후적 피해회복에 대한 정책적 접근은 개인정보보호 관련법 위반에 따른 법률상 손해배상금의 보험가입 의무화 등 개인정보유출과 제3자 배상책임으로 국한되고, 기업의 재물 및 영업활동중단손해 등에 대해서는 유의미한 논의가 전개되지 않았다.[42] 그러나 사이버사고의 경우 방어보다는 공격이 용이하다는 점에서, 보안강화 일변도의 정책 대응으로는 한계가 존재한다. 더욱이 테러조직 및 국

42) 신용정보의 이용 및 보호에 관한 법률 제43조의3, 전자금융거래법 제9조 제4호, 개인정보보호법 제39조의9 등은 관련 서비스 제공자가 손해배상책임의 이행을 위하여 금융위원회가 정하는 기준에 따라 보험 또는 공제에 가입하거나 준비금을 적립하도록 정함

가 배후 사이버공격이 증가하고 있는 가운데, 그 피해를 민간기업과 보험회사가 온전히 책임지는 것이 정당한지, 국가 배후 사이버공격의 책임에서 정부가 자유로운지에 대한 문제 제기가 가능하다. 우리나라에서는 상법 제660조에서 보험사고가 전쟁으로 인하여 생긴 때에는 계약당사자 간 다른 약정이 없으면 보험회사의 면책을 규정한다.[43] 전쟁과 같은 비상사태에 대하여는 사고발생의 개연성 또는 손해의 정도를 예측하기 어려워 적절한 보험료를 산정하기 어려울 뿐 아니라 경우에 따라서는 일시적으로 막대한 보험금을 지급하게 되어 통상의 보험료에 의한 보험회사의 위험인수능력을 초과하게 된다는 점 등을 고려함 때문이다.[44] 테러조직 및 국가 배후 사이버공격이 증가하고 있는 가운데, 그 피해를 민간기업과 보험회사가 온전히 책임지는 것이 정당한 지에 대한 문제 제기는 사후적 피해 회복수단으로써 보험 공급에 정부가 적극적으로 개입해야 할 당위성을 제공한다.

다음 장에서는 세계 사이버보험시장을 선도하는 주요국 정부의 사이버보험 공급 지원 동향을 자본 투입 측면에서 살펴보기로 한다. 정부 차원의 사이버보험 공급 지원은 정부가 보험시장에 자본을 투입하는 방식과, 데이터 공유·리스크 모델링·전문인력 양성 등 보험 공급 인프라 조성을 지원하는 방식으로 구분 가능하다. 전자는 정부가 보장공백이 발생한 사이버사고에 대해 직접 보험을 제공하거나 재보험담보·지급보증·유동성 제공을 통해 보험회사의 자본력을 제고하는 방식으로 구체화될 수 있다.

〈그림 Ⅱ-16〉 사이버리스크에 대한 정부의 딜레마

<table>
<tr><td>환경</td><td colspan="2">사이버사고 빈도 및 심도 증가</td><td>국가배후 공격</td></tr>
<tr><td>시장</td><td>사이버보험 공급 축소</td><td>사이버보험 수요 증가</td><td rowspan="2">• 정부는 국가배후 공격의 책임에서 자유로운가?
• 정부가 국가배후 공격을 책임질 경우, 문제의 공격이 "국가배후"임을 규명할 수 있는가?</td></tr>
<tr><td>정부 역할</td><td>① 보험회사의 건전성 감독: 사이버보험 언더라이팅 리스크 관리
② 반공익적 담보 제외</td><td>사이버리스크에 대한 보장공백 해소</td></tr>
</table>

자료: 저자가 작성함

43) 다만, 생명보험의 경우 표준약관에 전쟁면책 약관조항이 2010년 4월 1일부로 폐지되어 우리나라 생명보험계약은 '지진 등 천재지변, 핵이나 방사선사고, 전쟁 등의 경우'에도 사망과 상해 등에 대해 보장하도록 하고 있음

44) 전주지법 1990. 5. 31., 선고, 90나632, 제1민사부판결: 상고

Ⅲ 주요국 정부의 사이버보험 시장 참여 동향

사이버공격의 피해가 사이버공간에서 물리적 공간으로 확장되고, 정보 유출 피해에 그치지 않고 재물 및 신체손해를 초래하는 상황에 이르렀다. 그러나 기존 기업보험에서는 사이버사고로 인한 재물·신체·배상책임담보를 면책하는 추세인데다, 단독 사이버보험은 정보 침해 관련 배상책임 또는 랜섬 및 비용 보장에 집중한 채 재물 및 신체 손해 담보 제공에는 소극적이다. 국가 배후 사이버공격은 재래식 전쟁약관 적용 여부를 두고 소송 중에 있다. 이처럼 보험산업은 진화하는 사이버공격을 보장하는데 명백한 한계를 보인다. 반면, 2010년대 들어 사이버공격의 진화로 인해 사이버사고의 빈도 및 심도가 급격히 증가하면서, 기업의 사이버보험에 대한 수요가 증가하고 있다.

이에 세계 사이버보험 시장을 선도하는 미국, 영국, 프랑스, 독일, 호주 등에서는 자국에서 이미 운영 중인 공사협력 테러보험 프로그램을 통해 '일부 사이버공격'으로 인한 손해에 대해 재보험담보 및 유동성을 제공하는 방식을 취하고 있거나 논의 중이다(〈표 Ⅲ-1〉 참조). 아마도 공사 테러보험 프로그램이 이미 존재하는 상황에서는 사이버사고를 동 프로그램의 손인으로 추가하는 것이 정책적으로 가장 용이한 접근이었기 때문으로 사료된다. 또한 사이버리스크에 대응한 공사협력 보험 프로그램을 새로이 구성하기에는 사이버리스크와 사이버보험 시장이 너무도 짧은 시간에 급격하게 변하였다. 지금까지 저자가 살펴본 바로는, 별도의 공사협력 테러보험 프로그램이 존재하지 않는 국가에서 사이버공격에 대해 정부가 시장에 공급자 또는 공급지원자로 참여한 사례는 없다. 사이버리스크와 사이버보험 시장이 단기간에 급격한 변화를 보였기 때문에 우리나라를 비롯하여 일부 국가에서는 앞으로 전개될 사이버리스크에 대한 보장공백의 심각성을 파악할 겨를조차 없었을 것으로 보인다.

이하에서는 미국, 호주, 영국, 프랑스 등 보험선도국 정부의 사이버보험 시장 참여 동향을 살펴본다. 구체적으로, 각국 정부의 사이버리스크에 대한 보장공백 해소 방법 및 범위, 기저논리와 근거, 의사결정의 과정, 고려사항 및 한계, 보장범위 확대 여지 등을 살펴본다. 미국과 호주는 현재 정부의 사이버보험 시장 개입을 가장 적극적으로 논의하고 있는 국가이면서, 주요 논의 내용이 상이하다는 점에서 검토의 실익이 크다. 이미 정부가 사이버 테

러리즘에 대해 재보험담보를 제공하고 있는 미국의 경우, 정부의 재보험담보 제공 범위 확대를 다각도에서 검토하고 있는 반면, 사이버사고에 대해 정부가 어떠한 보장도 제공하고 있지 않은 호주에서는 사이버 테러리즘으로 인한 재물손해에 대해 정부가 재보험담보 및 지급보증을 제공하는 방안을 5년여에 걸쳐 신중히 검토하고 있다. 미국은 사이버보험 시장의 주 수요자이기도 하지만, 최근 진화된 사이버공격의 주요 표적이기도 한 만큼, 정부의 사이버보험 시장 개입에 대한 논의가 가장 적극적이다. 영국은 다른 서방국가들과 달리 9·11 테러리즘 이전인 1993년에 테러리즘 프로그램을 만들었고, 프랑스는 1986년부터 테러보험 담보 제공 및 가입을 법적으로 의무화하였다. 그만큼 테러리즘에 민감한 국가들이다. 이 두 국가는 테러리스트의 공격수법이 물리적 공간에서 사이버공간으로 이동하는 것에 대응하여 그에 상응한 보장을 제공한다.

다만, 전술한 바와 같이 미국, 영국, 프랑스 등은 기존 공사협력 테러보험 프로그램에 사이버공격을 보장손인으로서 추가했을 뿐이다. 기존 공사협력 테러보험 프로그램은 물리적 테러리즘을 계기로 설계·도입되었다는 점에서 현재 사이버리스크의 보장공백을 모두 포함하는 데에 명백한 한계를 보인다. 무엇보다도 문제의 사이버행위가 테러리즘 요건을 충족해야 하므로, '테러리스트'에 의한 사이버공격이 아닌 경우, 인간의 실수에 의한 대규모 사이버사고, 범죄조직의 대규모 금전 목적 랜섬웨어 공격, 또는 국가 배후 사이버공격은 정작 프로그램 적용대상에서 배제될 수 있다. 주요국은 이러한 한계를 이미 인지하고 있으며, 현 시점에서는 미국이 기존 테러보험 프로그램에 매몰되지 않고 동 프로그램의 범위를 벗어나 사이버리스크에 대한 보장공백을 메우는 방법을 적극적으로 탐색 중이다. 이하에서 살펴볼 보험선도국들의 이러한 논의는 물리적 공격과 대조되는 사이버공격의 이질적 특성을 선명화함으로써 향후 사이버리스크에 부합한 프로그램 설계 시 도움이 될 것으로 보인다.

〈표 Ⅲ-1〉 주요국 정부의 사이버보험 시장 참여 동향

국가	테러보험 프로그램		사이버사고 보장		보장 확대 논의 중
	정부 역할	보장손해	여부	손해	
미국	재보험자	PD·BI·배상책임·신체손해	2017년부터 테러보험 프로그램 적격보험에 단독 사이버보험을 포함	PD·BI·배상책임·신체손해	○
영국(GB)	유동성 제공자	PD·BI·NDBI	2018년부터 RDI담보를 제공, 사이버공격으로 인한 손해도 프로그램 적용	PD·BI (무형자산 제외)	○
프랑스	재보험자 (지급보증)	PD·BI	법상 테러리즘 정의에 Computer Offense를 명시적으로 포함	PD·BI	-
독일	재보험자	PD·BI	문제의 사이버공격이 프로그램에서 정한 테러리즘 정의에 부합하다고 Extremus AG가 인정하는 경우 적용	-	-
호주	재보험자 (지급보증)	PD·BI	현재 사이버 테러리즘은 테러보험 프로그램 적용이 배제되나, 적용을 긍정적으로 논의 중	-	○
스페인	원보험자 (지급보증)	PD·BI·신체손해	문제의 사이버공격이 법상 테러리즘 정의에 부합하다고 CCS(국영 재보험회사)가 판단하는 경우 적용	PD·BI·신체손해	-

주: PD(Property Damage)는 재물손해, BI(Business Interruption)은 재물손해로 인한 영업중단손해를, NDBI(Non-physical Damage Business Interruption)는 물리적 재물손해를 동반하지 않은 영업중단손해를 의미함
자료: 저자가 작성함

1. 미국

가. 사이버보험 시장

1) 보험가입

2002년 세계 최초로 캘리포니아에서 보안위반통지법(California Security Breach Notification Act 2002, California SB 1386)이 제정되었다. 이를 시작으로, 미국 내 개인정보 침해에 따른 기업의 통지의무, 위반 시 처벌, 민사소송 제기 근거 등을 규정한 입법

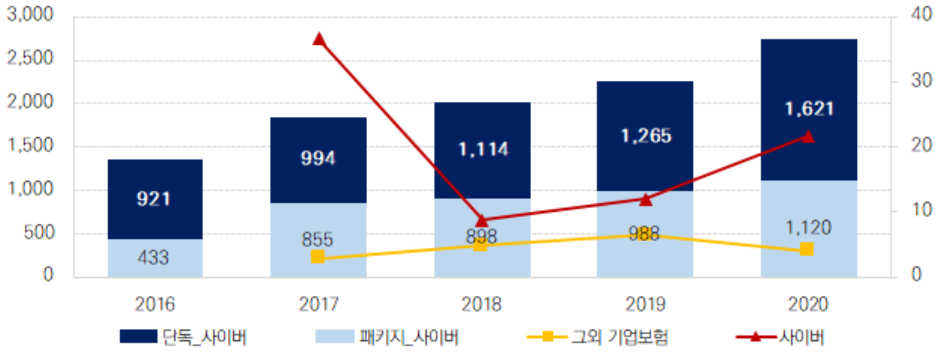
례가 증가하였다. 통지 비용, 벌금, 개인정보 유출에 따른 배상책임 등 전통적인 재물 및 배상책임보험에서 보장하지 않는 손해가 발생함에 따라 이를 별도로 보장하는 단독 사이버보험이 판매되기 시작하였다. 나아가 2006년을 시작으로 ISO가 표준 영업배상책임보험의 신체상해 및 재물손해 배상책임담보(담보 A)에 전자적 데이터 면책을 추가하는 등 기존 기업보험에서 사이버사고 관련 면책이 추가됨에 따라 미국에서는 단독 사이버보험에 대한 의존도가 커졌다. 미국은 원수보험료 기준 세계 단독 사이버보험 시장의 약 90%를 차지한다.

미국 기업은 사이버보험 시장의 주 수요자로, 전 세계 사이버보험 원수보험료의 약 90%를 차지한다는 점에서 미국 시장의 보험금 청구빈도나 청구내용은 사이버보험 시장의 현재를 이해하고 미래를 예상 가능하게 한다. 미국 시장에 대한 상세한 분석이 필요한 이유이다. 다행스럽게도, 미국에서는 재부무 내 FIO(Federal Insurance Office, 연방보험국)에서 2017년부터 명시적 사이버보험 시장 현황을 연차보고서를 통해 발표하고 있다. 현재 FIO 자료는 2019년까지만 공개되어, 이하에서는 보다 최근의 자료를 포함한 AM Best(2021)의 자료를 이용하여 사이버보험 시장 현황을 살펴보도록 한다.

명시적 사이버보험 원수보험료는 전년 대비 22% 증가하여 27억 달러에 이른다(〈그림 Ⅲ-1〉 참조). 이는 동기간 급격한 요율 인상뿐만 아니라 사이버공격을 통해 기업의 사이버리스크에 대한 우려가 반영된 것으로 보인다(〈그림 Ⅲ-2〉 참조). 대형 보험중개사 고객의 명시적 사이버보험 가입률은 2020년 47%로, 2016년 26%에서 지속적으로 증가하고 있다(〈그림 Ⅲ-3〉 참조). 그러나 명시적 사이버보험의 원수보험료는 재물보험의 1%에 미치지 못하며, 2020년 기준 전년 대비 증가율은 21.7%로, 2018년(8.8%)에 비해 증가한 수치이나 2015~2016년 27.4%, 2016~2017년 36.6%에 비해서는 다소 낮은 증가율이다. 사이버보험 원수보험료의 전년 대비 증가율은 2016~2020년 기간 동안 8.8~36.6%에 분포하여 신흥시장의 불안정한 상황을 여실히 드러내는 반면, 이미 성숙단계에 진입한 타 기업보험은 2.9~6.4%에 분포하여 상대적으로 안정적이다. 명시적 사이버보험에서 단독 사이버보험의 비율은 2020년 기준 약 60%로 2017년(54%) 이후 증가세를 보인다.

사이버보험을 제공하는 보험회사는 2015년 322개사에서 2017년 507개, 2019년 580개사로 증가하였다(FIO 2020a). 그러나 미국 사이버보험 시장은 상위 5개사가 2020년 기준 시장점유율 48.1%, 상위 10개사가 68.3%를 차지할 정도로 집중된 시장이다(〈표 Ⅲ-2〉 참조).

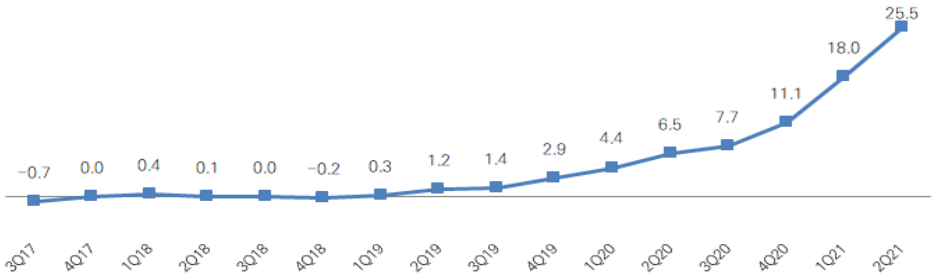
〈그림 Ⅲ-1〉 미국 명시적 사이버보험 원수보험료



주: 좌축은 원수보험료(USD 1,000), 우축은 원수보험료 연간변화율(%)임
자료: AM Best(2021)

〈그림 Ⅲ-2〉 미국 손해보험회사의 사이버보험 분기별 요율 변화율

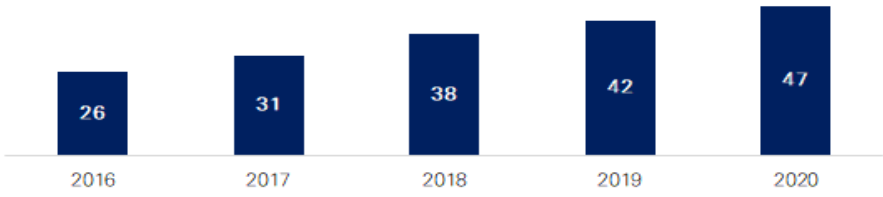
(단위: %)



주: 맥락상 명시적 사이버보험의 요율 변화로 추정됨
자료: Council of Insurance Agents&Brokers(2021)

〈그림 Ⅲ-3〉 대형 보험중개사 고객의 명시적 사이버보험 가입률

(단위: %)



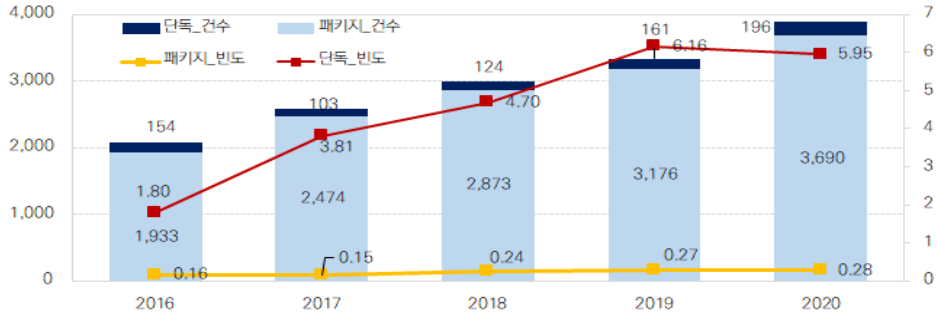
자료: GAO(2021)

2) 보험사고

요율 인상과 리스크 기반 수요 증가에 따른 사이버보험 시장의 급격한 성장은 보험산업의 언더라이팅 및 보유 리스크를 의미한다. 급격한 요율 인상에도 불구하고 사이버보험 가입률이 늘었다는 것은, 그만큼 사이버리스크가 증가했다는 것으로, 보험산업 관점에서는 사이버사고 언더라이팅 및 보유 리스크 증가를 우려해야 할 시점이다.

명시적 사이버보험의 보험금 청구빈도(보유계약 100건당 청구 건수)가 단독·패키지 여부에 상관없이 2016년 이후 증가하는 추세이며, 단독형이 2020년 기준 6%로 패키지형(0.3%)보다 현저히 높다(〈그림 Ⅲ-4〉 참조). 단독형의 보험금 청구빈도는 2016년 1.8%에서 점차 증가하여 2019년 6.2%로 정점을 찍은 이후 소폭 감소하고, 패키지형은 동기간 0.16~0.28%에 분포한다.

〈그림 Ⅲ-4〉 미국 명시적 사이버보험 계약 건수 및 사고 빈도



주: 좌축은 보유계약 건수(100건), 우축은 보유계약 건수 대비 보험금 청구 건수의 비율(%)임
자료: AM Best(2021)

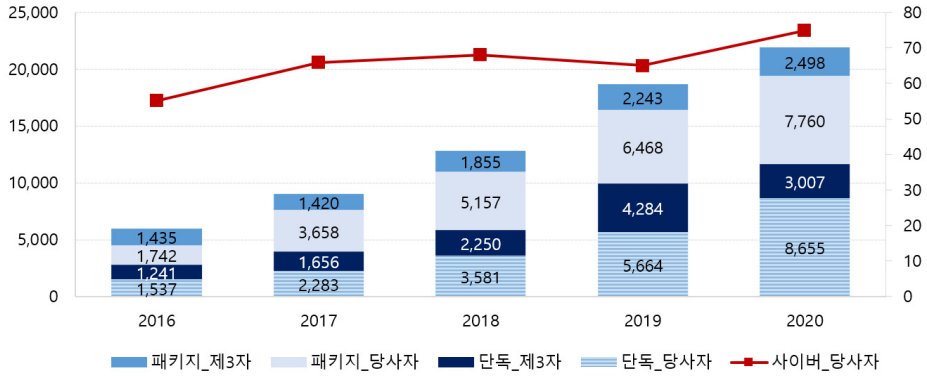
지난 5년간 사이버보험의 원수보험료는 연평균 19% 증가하였다. 동기간 사이버보험 청구건수는 2016년 5,955건에서 2020년 21,920건으로 연평균 38.5% 증가하였다(〈그림 Ⅲ-5〉 참조). 증권 유형별로는 단독형이 43%, 패키지형이 34%로 단독형에서 보험금 청구가 보다 빠르게 증가하였다.

사이버공격으로 인한 피해양상의 변화를 보험금 청구내용을 통해 관찰할 수 있다. 사이버보험 청구건을 담보 유형별로 살펴보면, 관찰기간 동안 당사자(1st-party) 담보가 배상책임(3rd-party)에 비해 높다(〈그림 Ⅲ-5〉 참조). 전체 청구건수 대비 당사자 담보 청구건수

의 비율은 2016년 55%에서 2020년 75%로 급격히 증가하였다. 2020년의 경우 보험금 청구건의 대부분이 당사자담보인 것으로 나타났다. 예상과 달리, 사이버보험 청구건의 대부분이 개인정보 유출에 따른 배상책임이 아니라는 의미이다. 이는 2016~2020년 기간 동안 집중적으로 발생한 대규모 랜섬웨어 공격 증가에 기인한 것으로 보인다. 랜섬웨어 공격으로 인해 기업활동중단에 따른 손해, 데이터 및 시스템 손상 등을 회복하기 위한 보험금 청구가 보다 빈번하게 이뤄지고 있음을 유추해 볼 수 있다.

요율 인상에도 불구하고 보험금 청구가 증가함에 따라 산업의 손해율이 빠른 속도로 증가하고 있다. 사이버보험 시장 내 상위 5개사의 2020년 기준 손해율은 78.3%로 전년 대비 33%p 증가하였다(〈표 Ⅲ-2〉 참조). 산업 전체 손해율은 2020년 67.8%로 전년 대비 23%p 증가하였다. 시장점유율이 높은 상위사가 비교적 높은 손해율을 보인다. 또한 단독형의 손해율은 73%로, 패키지형(59%)에 비해 14%p 높다.

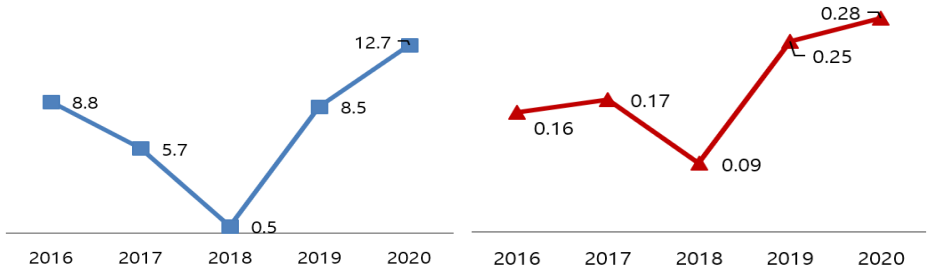
〈그림 Ⅲ-5〉 미국 명시적 사이버보험의 증권 및 담보 유형별 청구 건수



주: 좌축은 청구 건수, 우축은 전체 청구 건수 대비 당사자담보 청구 건수의 비율(%)임
자료: AM Best(2021)

사이버보험의 경우 물가상승률보다 높은 DCC(Defense and Cost Containment, 방어 및 비용절감 비용)에 주목할 필요가 있다. DCC는 법률 비용, 법원 비용, 전문가 증인 비용(Expert witnesses), 조사 비용, 기록보존 비용(Records duplications), 재판준비 비용 등을 포함한다. 2016~2020년 기간 동안 발생손실액 대비 DCC의 비율은 0.5~12.7%에 분포하며, 지급보험금 대비 DCC의 비율은 0.09~0.28%에 분포한다(〈그림 Ⅲ-6〉 참조). AM Best(2021)는 사이버보험의 높은 DCC 비율이 사이버담보의 모호성에 기인한 것으로 풀이한다.

〈그림 Ⅲ-6〉 미국 사이버보험의 방어비용



주: 1) 좌측은 발생손실액 대비 DCC 비율(%), 우측은 지급보험금 대비 DCC 비율(%)임
2) DCC(Defense and Cost Containment, 방어 및 비용절감 비용)는 법률 비용, 법원 비용, 전문가 증인 비용 (Expert witnesses), 조사 비용, 기록보존 비용(Records duplications), 재판준비 비용 등을 포함함

자료: AM Best(2021)

〈표 Ⅲ-2〉 미국 주요 보험회사별 원수보험료 및 손해율

(단위: %)

보험회사	2020 원수 보험료[1)]	원수 보험료 변화율	시장 점유율	단독 비율	2019 손해율	2020 손해율	2020 합산 비율
Chubb INA Group	404.1	13.3	14.8	0.0	31.8	61.0	84.8
XL Reinsurance America Group	293.0	27.6	10.8	100.0	68.5	98.2	123.0
American International Group	228.4	0.5	8.4	99.2	55.7	100.6	125.8
Travelers Group	206.8	15.8	7.6	81.2	34.5	85.5	117.2
Beazley USA Insurance Group	177.7	17.8	6.5	95.0	30.0	47.9	75.1
AXIS US Operations	133.6	37.2	4.9	67.3	29.3	46.2	73.1
CNA Insurance Companies	119.6	26.3	4.4	15.2	56.5	106.1	133.5
Fairfax Financial (USA) Group	108.5	66.7	4.0	99.9	54.8	55.7	80.7
Hartford Insurance Group	102.9	78.8	3.8	10.7	34.7	29.4	59.9
BCS Financial Group	86.6	13.8	3.2	57.7	54.9	59.1	85.8
Sompo Holdings US Group	72.6	46.0	2.7	100.0	43.5	114.1	136.4
Tokio Marine US PC Group	65.7	24.9	2.4	48.1	32.9	48.8	75.6
Zurich Insurance US PC Group	64.4	30.9	2.4	89.2	89.3	40.4	63.1
Liberty Mutual Insurance Companies	41.9	-38.8	1.5	41.7	56.0	30.0	64.9
Aspen US Insurance Group	39.3	101.0	1.4	99.6	4.2	29.6	56.9
Berkshire Hathaway Insurance Group	37.4	19.9	1.4	29.8	129.6	25.8	42.7
Markel Corporation Group	29.7	52.2	1.1	74.9	33.9	38.0	68.4
Everest Re U.S. Group	28.2	151.8	1.0	100.0	15.2	48.0	74.8
The Cincinnati Insurance Companies	24.9	14.9	0.9	0.0	15.4	24.6	56.0
Swiss Reinsurance Group	23.7	72.6	0.9	100.0	99.3	42.6	70.5
Top 5	1,310.2	14.6	48.1	66.0	44.6	78.3	104.1
Top 10	1,861.3	20.5	68.3	60.8	45.4	74.5	100.7
Top 20	2,289.0	21.2	84.0	59.0	47.4	70.2	96.1
Total Standalone	1,605.3	26.9	58.9	-	-	73.0	99.5
Total Package	1,117.3	13.5	41.0	-	-	59.0	85.4
Total P/C Industry	2,724.7	21.2	100.0	58.9	44.8	67.8	94.2

주: 1) 원수보험료 단위는 1,000달러임

자료: AM Best(2021)

나. 정부개입

1) 테러보험 프로그램

2001년 9·11 테러리즘으로 인한 보험손해액은 약 230억 달러로, 역대 테러공격 중 최대 보험손해액을 기록하였다. 손실을 입은 보험회사들과 재보험회사들이 기존의 포괄위험 담보방식의 보험상품들의 보장범위에서 테러리즘으로 인한 손해를 제외하거나 테러보험 시장에서 사업을 철수하였다. 9·11 테러리즘 이후 보험회사는 기업보험 약관에 테러면책조항을 명시적으로 추가할 수 있도록 주보험당국에 승인을 요청하였고, 그 결과 2002년까지 45개주가 이를 승인하였다. 9·11 테러리즘으로 인해 막대한 손실을 입은 보험회사가 기업보험에 테러면책조항을 추가하자, 진행 중이거나 계획되었던 건설 프로젝트, 부동산 거래들이 취소·지연되고 임대료가 급격하게 인상되었다.

이에 2002년 6월 의회는 Terrorism Risk Insurance Act of 2002(테러위험보험법, S.B. 2600)을 제정하여, 모든 기업보험에 테러리즘 담보 제공을 의무화하고 정부가 재보험회사로 시장에 참여하여 보험회사에 비례방식의 재보험담보를 제공하는 테러보험 프로그램 TRIP(Terrorism Risk Insurance Program)을 만들었다. 정부는 테러리즘으로 인한 지급보험금이 기준금액을 초과하면 보험산업 20%, 정부 80% 비율로 손실을 분담한다.

TRIP 적용대상 보험은 기업용 P&C보험(Property and Casualty insurance)으로 제한된다. 화재보험, 기업종합보험(배상책임 포함), 산재보험, 해상보험, 생산자배상책임보험, 항공보험, 보일러 및 기계보험 등 대부분의 기업성 재물보험이 TRIP 적격 보험종목에 해당한다. 테러리즘으로 인해 원 보험계약에서 담보한 손해가 발생한 경우 이를 보장하기 때문에, 계약내용에 따라 재물손해, 영업중단손해, CBI, NDBI, 배상책임 등을 보장한다. 산재보험의 경우 테러리즘으로 인한 인적피해도 보장한다. 다만, NAIC가 분류한 P&C보험 중에서 연방농작물보험, 민영모기지보험, 권원보험, 모노라인 금융보증보험회사가 발행한 금융보증보험(Financial guarantee), 의료과실보험, 건강 및 생명보험(단체 생명보험 포함), 국가홍수보험법(National Flood Insurance Act of 1968)에 의거한 홍수보험, 재보험 또는 재재보험, 상업용 자동차보험, 도난 및 강도 보험, 보증보험(Surety insurance), 임원배상책임보험(Directors&Officers liability)을 제외한 전문인배상책임보험(Professional liability), 농장주 다중위험보험(Farm-owners multiple peril insurance) 등은 TRIP의 적용을 받지 않는다.[45]

45) TRIA Section 102(11)(xi)(excluding "professional liability insurance"); 31 Code of Federal Regulations Part 50.4(w)

TRIP 적격 테러리즘 사고는 재무부장관, 국토안보부 장관(Secretary of Homeland Security), 그리고 검찰(Attorney General) 간 협의와 재무부장관의 승인을 요한다. TRIP 적용대상 테러리즘은 '미국 시민을 협박하거나, 협박 또는 강요를 통하여 정부 정책에 영향을 미치기 위해 미국의 영토 내 혹은 미국 국적의 항공기나 선박 내에서의 인명·재물·기간산업에 해를 가할 수 있는 폭력적인 행위'로 정의된다.[46] 테러리즘이라 할지라도 동 행위가 의회가 전쟁으로 승인한 과정에서 발생한 행위이거나[47] 테러리즘으로 인한 재물보험 피보험손실 총계가 5백만 달러를 초과하지 않으면 TRIP 발동 조건의 테러리즘에 해당하지 않는다.[48] 2002년 도입된 이후 TRIP이 실행된 적은 없다. 미국 정부는 2013년 보스턴 마라톤 폭발을 테러리즘으로 규정하였지만, 관련 재물보험 피보험손실액이 500만 달러에 미치지 않아 TRIP이 실행되지 않았다.

재무부는 의회의 권고에 따라 TRIP 발동 요건을 구체화하는 방안을 검토하였다(U.S. Department of Treasury 2015). 2015년 TRIA 재승인법의 일부로서 의회는 재무부가 DTI 승인을 위한 합리적인 타임라인 설정을 분석·도입하도록 권고하였다. 재무부는 TRIP 적용대상 테러행위인지 여부를 판단함에 있어 불확실성이 존재하는 바, 소요기간을 일괄적으로 확정하기가 어렵다고 응답하였다.

2) 사이버공격의 테러보험 적용

2016년 이전까지 보험회사는 사이버배상책임보험 상품을 NAIC의 P&C보험 분류표(Uniform Property&Casualty Product Coding Matrix)에서 일반배상책임보험 또는 전문인배상책임보험(Professional liability) 등의 항목으로 분류하여 신고하였다. 별도의 사이버배상책

46) TRIA Section 102(1)(A): The term "act of terrorism"' means any act that is certified by the Secretary, in concurrence with the Secretary of State, and the Attorney General of the United States (i) to be an act of terrorism; (ii) to be a violent act or an act that is dangerous to (I) human life; (II) property; or (III) infrastructure; (iii) to have resulted in damage within the United States, or outside of the United States in the case of (I) an air carrier or vessel described in paragraph (5)(B); or (II) the premises of a United States mission; and (iv) to have been committed by an individual or individuals ~~acting on behalf of any foreign person or foreign interest~~(국내 테러리즘을 보장범위에 포함하기 위해 Terrorism Risk Insurance Program Reauthorization Act of 2015 에서 동 문구를 삭제함), as part of an effort to coerce the civilian population of the United States or to influence the policy or affect the conduct of the United States Government by coercion.

47) 1942년 이후 미국은 전쟁 중에 있었지만, 미국 의회가 마지막으로 전쟁을 승인한 것은 1942년임

48) TRIA Section 102(1)(B)

임보험이 없었기 때문이다. 그러나 전술한 바와 같이 전문인배상책임보험은 명시적으로 TRIP 적용대상에서 제외되기 때문에, 사이버배상책임보험은 TRIP의 적용을 받지 않는 것으로 간주되었다.

2016년에 주 보험감독당국은 NAIC의 P&C보험 분류표에 전문인배상책임보험과 별도로 사이버배상책임(Cyber liability) 보험상품을 추가하였다.[49] 이로 인해 사이버 배상책임 라인의 보험상품이 TRIP 적용대상에 해당하는지 또는 TRIP에서 명시적으로 면책하는 전문인배상책임보험(Professional liability)에 해당하여 TRIP의 적용을 받지 않는지에 대한 의문이 제기되었다.[50]

이에 재무부는 2016년 12월 27일, 2016년 주 감독당국에 의해 소개된 사이버 배상책임(Cyber-liability) 라인의 보험상품이 TRIP 적용대상 P&C보험에 포함된다는 지침을 발표하였다(U.S. Department of Treasury 2016). 사이버배상책임 라인으로 신고된 단독 사이버보험이 TRIA의 P&C보험 정의에 포함된다고 보았다. 이에 따라 2017년 4월 1일부터 테러리즘으로 인해 사이버배상책임보험에서 보장하는 손해가 발생한 경우 이는 TRIP의 적용을 받게 된다. 또한 2017년 4월 1일부터 보험회사가 단독 사이버배상책임보험(Stand-along cyber liability insurance)으로 신고된 상품을 갱신 또는 신규 판매 시에는 TRIA를 준수해야 한다. TRIP 적격 보험상품 판매 시 보험회사는 테러리즘 담보를 의무적으로 권유해야 한다. 즉, 단독 사이버배상책임보험 판매 시, 보험회사는 테러담보를 의무적으로 권유해야 한다. 2020년 11월 재무부는 2016년 재무부지침을 관련 법령에 반영하기 위해 31 Code of Federal Regulations Part 50 개정안을 예고하였다(U.S. Department of Treasury 2020b).

사이버보험이 TRIP 적용대상에 포함됨에 따라 보험회사는 P&C보험에서 사이버 테러리즘 면책조항을 제거하였으나, 체계적 누적 리스크에 대한 우려로, 단일 사고에 대한 사이

49) NAIC Uniform Property&Casualty Product Coding Matrix에 따르면, 사이버배상책임보험(Cyber liability)에 대한 NAIC의 정의는 다음과 같음(Stand-alone comprehensive coverage for liability arising out of claims related to unauthorized access to or use of personally identifiable or sensitive information due to events including but not limited to viruses, malicious attacks or system errors or omissions. This coverage could also include expense coverage for business interruption, breach management and/or mitigation services. When cyber liability is provided as an endorsement or as part of a multi-peril policy, as opposed to a stand-alone policy, use the appropriate Sub-TOI of the product to which the coverage will be attached.)

50) NAIC, Uniform Property&Casualty Product Coding Matrix(effective Jan. 1. 2020), 10, https://www.naic.org/documents/industry_pcm_p_c_2020.pdf

버리스크 보상한도를 3억~5억 달러로 제한하는 경향이 있다.

3) 한계 및 추가논의

가) 테러보험 적용 사이버공격의 불확실성

사이버배상책임보험이 TRIP 적용대상이 되면서 이후 논쟁의 핵심은 구체적으로 어떤 유형의 사이버공격이 테러리즘으로 인정되는지, 즉 DTI(Declared Terrorism Incidents) 요건이다. 2002년 TRIP 도입 이후 DTI 요건이 충족되어 TRIP이 작동된 적이 없다. 따라서 DTI 요건에 대한 사회적 검토가 충분히 이루어질 기회가 없었다. 다만, 2013년 보스턴 마라톤 폭발 사고를 계기로 2015년 TRIP 갱신 시 의회는 재무부에 DTI 요건에 대해 분석하도록 권고하였다. 당시만 하더라도 사이버 테러리즘이 TRIP 적용대상이 아니었기 때문에, DTI에 대한 심도 있는 논의가 이뤄지기 시작한 것은 2016년 12월 재무부의 지침에 따라 사이버보험이 TRIP 적용대상이 된 이후이다. 재무부의 구체적이고 명확한 DTI 요건은 보험회사의 계리적 또는 언더라이팅에 중요한 고려요소이다. 따라서 보험업계는 재무부가 TRIP이 적용되는 사이버공격을 명확히 할 것을 요구하였다.

악의적인 사이버사고로 인한 손해가 TRIP 적용을 받기 위해서는 TRIA의 테러리즘 행위 구성요건을 충족해야 한다. Terrorism Risk Insurance Program Reauthorization Act of 2015에 따르면, TRIP 적용대상 테러리즘은 ① 테러리즘 행위이어야 하고, ② 인명·재물(Property)·기간산업에 위협이 되는 행위 또는 폭력적인 행위이어야 하고, ③ 미국의 영토 내 혹은 미국 국적의 항공기나 선박 내, 또는 미국 관할 내에 피해를 초래해야 하고, ④ 개인 또는 개인들이 저지른 행위이어야 한다. 테러리즘이라 할지라도 동 행위가 의회가 전쟁으로 승인한 과정에서 발생한 행위이거나 테러리즘으로 인한 재물보험 피보험손실 총계가 5백만 달러를 초과하지 않으면 TRIP 발동 조건의 테러리즘에 해당하지 않는다. 사이버공격으로 인한 피보험손실이 500만 달러를 초과하는지 여부는 구체적이고 명확하지만 나머지 요건은 그렇지 않다.

이처럼 사이버리스크에 대한 보장공백을 기존 테러보험 프로그램 체계 내에서 해결하려다 보니, 이를 실행함에 있어 여러 문제점이 제기되었다. 재무부는 거론되는 문제점들에 대해 이해관계자들의 의견을 조회·청취해오고 있다(Patel 2021). 구체적으로 먼저, 사이버공간에서 인명·재물·기간산업에 위협적 행위 또는 폭력적 행위가 무엇인지 구체화되지

않았다. TRIP 적용을 위해서는 재무부장관은 사이버공격이 폭력적이거나, 또는 적어도 인간생활·재물·주요 기반시설에 위협이 되는 행위인지를 판단해야 한다.

둘째, TRIA는 재물(Property)을 구체적으로 정의하지 않는다. 재무부장관은 재물을 어떻게 정의할 것인지에 대한 단독의 권한을 가진다. TRIA가 9·11 공격 이후 보험회사의 테러리즘 리스크 면책에 대한 의회의 대응이었고 동법이 특정 유형의 재물에 국한되지 않으며 테러리즘 리스크에 대한 P&C보험의 원활한 공급을 목적으로 한다는 점에 비추어,[51] 재물이 P&C보험의 보험목적물일 것으로 유추가능하다. TRIP 적용대상 재물이 유형의 재물에 국한되는지, 데이터, 컴퓨터 네트워크 등 무형의 재물을 포함하는지 명확히 할 필요가 있다.

셋째, 공격자 및 공격동기 요건을 입증하기 쉽지 않다. 모든 테러리스트 집단이 그들의 소행임을 밝히지도 않고 역사적으로 거짓 주장을 하는 경우도 있었다. 특히 사이버공격의 경우 공격자를 특정하기가 더 어렵다. 공격자가 특정되더라도 그러한 행위가 미국 시민 및 정부의 협박(Coercion)으로 작용하는지 여부, 일반적인 사이버범죄인지 협박을 위한 테러리즘 행위인지 여부를 구분하기 쉽지 않다. 또한 신속한 DTI는 피해보상 및 복구에 있어 매우 중요한 사안이나, 공격자 및 공격동기를 밝히는 데 많은 시간이 소요될 수 있다. 2017년 5월 12일 워너크라이의 경우 6개월이 지난 12월에 공격자가 밝혀졌다. 사이버공격이 명백하게 테러리스트에 의한 것이 아니라면 전쟁면책을 들어 보험회사는 보험금 청구를 거절할 수도 있다.

넷째, TRIP의 피해범위에 대한 지리적 제한은 사이버공격에 부합하지 않다. TRIP은 사이버공격의 피해가 미국 내에 발생할 것으로 요구한다. 그러나 외국 소재 외국 기업이 관리하는 네트워크에 사이버공격이 있어 미국 소재기업의 중요한 금융정보 또는 데이터가 파손되어 손실이 발생할 수 있다. 물리적 공격과 달리 데이터 손실은 지리적으로 식별불가하다. 데이터는 서버에 저장되고 서버는 미국에 위치하지 않을 수 있다.

마지막으로, 사이버공격의 피해는 상당 부분 TRIP 적용대상 P&C보험에서 면책대상으로, TRIP 적용만으로는 보장공백 해소에 한계가 있다. 통상 사이버보험 증권은 지적재산의 도난·위반·누출 또는 침해 등에 대해 면책을 가진다. 또한 일반 기업재물보험은 전원 서지(Power surge), 전기장애, 온도 변화, 기계적 결함에 의한 손해를 면책한다. 그런데 이러한 면책은 낫페트야, 워너크라이와 같이 컴퓨터를 파손하는 전형적인 악성소프트웨어 기법이다.

51) TRIA Section 101(b)

나) 사이버보장 확대 기조의 전면적 변화 예고

미국 정부는 사이버보험을 테러보험 프로그램의 적용을 받는 보험상품으로 포함시키는 데 그치지 않고, 사이버리스크에 대한 보장공백 해소를 위해 기존 테러보험 프로그램의 한계와 적합성을 다각도로 검토하고 있다. 의회 산하 GAO(Government Accountability Office, 회계감사원)는 2019년 테러보험 재승인법(Terrorism Risk Insurance Program Reauthorization Act of 2019, P.L. 116-94)에 의거하여, ① 물리적 또는 디지털 손해를 초래할 수 있는 미국 공공 또는 민간 기반시설에 대한 사이버공격의 잠재적 비용과 취약성, ② P&C 라인 보험상품 중 사이버배상책임이 사이버 테러리즘 행위에 대한 적정한 담보인지 여부, ③ 보험산업이 사이버리스크에 대한 요율산출 역량이 있는지 여부, ④ 현행 TRIA의 위험보유구조가 사이버 테러리즘에 적합한지 여부에 대한 연구를 수행 중에 있다.[52] 또한 동 법에 따라 GAO는 분석에 근거하여 차세대 사이버위협에 대응하기 위해서 의회가 TRIA를 어떻게 개정할 것인지에 대한 의견을 제시해야 한다. 동 연구는 2021년 말에 발표될 예정이다.[53] 테러리즘 행위가 물리적 공간에서 사이버공간으로 이동하고, 잠재적 테러리스트 조직의 사이버공격 역량이 강화됨에 따라 기존 테러리즘 프로그램(TRIP)을 대폭 개선할 수 있음을 시사한다.

나아가, CSC(Cyberspace Solarium Commission, 사이버공간 솔라리움 위원회)를 중심으로 사이버보장 확대를 위한 전면적인 변화를 시전하고 있다. 2016년 대선 당시 러시아 해커의 개입과 북한 및 중국 등 국가의 지원을 받는 해커들의 활동이 미국의 중요 기반시설과 경제에 영향을 미치면서, 미국은 자국의 사이버 영역에 중대한 영향을 미칠 수 있는 사이버공격에 대한 방어 전략을 수립하고 공감대를 형성하기 위해, 2019년 미 국방수권법(National Defense Authorization Act)에 따라 CSC를 설립하였다. CSC는 국무부, 국방부, 법무부, FBI, 국토안보부, 상무부, 국가정보국 등 국가 핵심기관으로 구성된 임시기구로, 사이버공격에 대한 미국의 전략적 접근방안을 개발하는 업무를 수행한다.

2020년 3월, CSC는 결과 보고서(CSC Final Report)를 발표하였다. CSC가 제안한 사이버 억지력 전략은 ① 사이버공간을 위한 미국 정부의 구조와 조직 재편 전략, ② 규범과 비군사적 도구 강화 전략, ③ 국가의 복원력 증진 전략, ④ 보안강화를 위한 사이버 생태계 재구성 전략, ⑤ 민간부문과 사이버 보안협력 운영 전략, ⑥ 군사 기기의 보존과 도입 전략으

52) TRIP의 위험보유구조는 송윤아·홍보배(2021)을 참고하기 바람

53) Public Law 116-94 Section 502 (d)

로 크게 6개 부문, 80개의 권고안으로 구성된다.

2020년 3월 CSC의 80개 권고사항이 발표된 후 2020년 12월 상원과 하원은 CSC 권고사항 중 25개(31%)를 국가수권법에 반영하였으며(National Defense Authorization Act for Fiscal Year 2021, FY2021 NDAA), 나머지 권고안도 향후 입법화될 것으로 예상된다(CSC 2021). CSC의 권고안 중 4개가 사이버보험과 밀접한 관련이 있다. 이는 모두 '④ 보안강화를 위한 사이버 생태계 재구성 전략'의 일부로 구체화되었으며 다음과 같다. ① 국토안보부 내 사이버통계국 설치(권고안 4.3), ② 연방정부의 사이버보험 전문가 양성 및 보험상품 개발 지원(권고안 4.4), ③ 사이버리스크 모델링을 위한 공사 파트너쉽 구축(권고안 4.4.1), ④ 재난적 사이버사고에 대한 정부의 재보험지원에 대한 GAO의 연구 수행(권고안 4.4.2) 등이다.

구체적으로, 권고안 4.3은 정부가 보다 효과적인 사이버안보정책을 구상하고 보험산업이 보다 정확하게 사이버리스크를 평가할 수 있도록 국토안보부(Department of Homeland Security; DHS) 내에 사이버 통계국(Bureau of Cyber Statistics) 설치를 제안하였다. 이와 관련하여 현재 법안이 발의된 상태이다.

권고안 4.4는 주 감독당국이 사이버보험의 발전 및 성숙을 위해 연방정부의 지원하에 사이버보험 인증 프로그램을 설치하는 법안을 제안하였다. CSC는 보험시장이 효율적으로 작동할 수만 있다면 이는 기업의 리스크관리 및 사이버보안 행태에 대한 규제적 개입과 같은 긍정적인 효과를 가져올 수 있다고 보았다. 그러나 현재까지는 민영보험시장 내 전문성 있는 언더라이터나 손해사정사가 부족하고, 사이버리스크에 대한 요율산출 기준 및 역량이 갖춰지지 않아 정책목적 달성에 부합한 수준의 담보 제공이 이루어지지 않는다고 보았다. 보험산업에 대한 감독관할은 주정부이므로 연방정부는 보험시장에 직접적인 영향을 미칠 수는 없는 바, 사이버보험 전문 언더라이터와 손해사정사 교육 및 인증 프로그램을 개설하고 주정부와 협의하여 사이버보험상품을 개발할 수 있도록 연방정부의 자금지원을 제안하였다. 이는 FY2021 NDAA 9005조(GAO의 사이버보험 연구)에 일부 반영되었다.[54]

권고안 4.4.1은 국가안보부 내에 공사협력 작업반을 만들어 보험회사와 리스크 모델링 업체가 사이버리스크 모델링을 개선할 데이터와 이용 가능한 통계를 공동으로 작업하도록 제안하였다. 보험시장이 충분히 효율적이라면 보험료 및 보상한도는 피보험기업의 리스

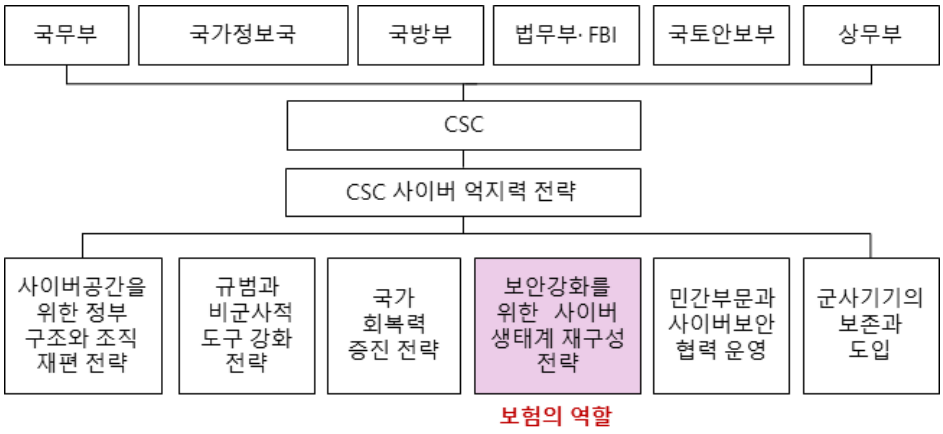
54) FY2021 NDAA Section 9005.(GAO Study of Cybersecurity Insurance)

크 수준을 나타내는 지표로서, 피보험기업으로 하여금 자발적으로 사이버리스크를 줄이도록, 즉 사이버 보안을 강화토록 하는 기제로 작용할 수 있다. 이처럼 보험산업이 사실상 기업행태의 규제자로 역할하기 위해서는 실제 리스크를 반영한 요율 산출이 전제되어야 하고 정확한 요율 산출을 위해서는 양질의 경험데이터가 있어야 한다. 따라서 국토안보부 내에 사이버 통계국을 설치하여 사이버사고에 대한 통계를 구축하고, 국토안보부 내에 보험회사와 리스크 모델링 업체로 구성된 작업반을 설치하여 양질의 데이터로 리스크 모델링을 개선할 필요가 있다고 보았다.

권고안 4.4.2는 재난적 사이버사고에 대한 정부의 재보험지원에 대한 연구를 GAO가 상무부(Department of Commerce)·국토안보부·재무부와 협의하여 수행하도록 제안하였다. 이는 FY2021 NDAA에서 통과된 법률에 부분적으로 반영되었다. 연구내용은 구체적으로 ① TRIP이 전쟁면책과 같은 현행 P&C 보험의 면책을 보장할 경우 어떠한 문제가 있는지, ② TRIP이 국가 연루 사이버사고를 보장하기에 충분한지 여부, ③ 테러보험 프로그램 발동 기준손해액(2020년 기준 2억 달러)이 재난적 사이버사고에 대해 적절한 규모인지 여부, ④ 연방정부 분담 비율에 대한 비교 모델, ⑤ 어떤 유형의 사이버사고가 TRIP 발동 요건인 '테러리즘 인정행위'에 해당하는지, ⑥ 대부분의 사이버 테러리즘이 TRIP 발동 요건인 '테러리즘 인정행위'에 포함되는지 여부, '테러리즘 인정행위'에 부합하지 않아 TRIP이 적용되지 않는 사이버공격이 어느 정도인지, ⑦ 물리적 테러리즘은 대개 지리적으로 제한된 지역에서 발생하고 피해도 지리적으로 국한되지만, 사이버사고는 공격지점과 피해가 지리적으로 제한되지 않는데, 어떤 사고가 그리고 어떤 개체가 TRIP의 보장범위에 포함되어야 하는지, 예를 들어, 미국 기업에 대한 사이버공격이 타국 소재 자산에만 피해를 준 경우 TRIA 적용대상인지 여부를 연구해야 한다.

이처럼 CSC가 주문한 연구내용만 보더라도, 미국 정부의 주요 의사결정기구에서 향후 사이버공격에 대한 폭넓은 보장을 얼마나 개혁적으로 추진할지 예상할 수 있다.

〈그림 Ⅲ-7〉 CSC의 사이버 억지력 전략



자료: CSC(2020)를 참고하여 저자가 작성함

〈표 Ⅲ-3〉 CSC의 사이버보험 관련 권고의 법규화 진행상태

전략	세부제안	경과
4. 보안 강화를 위한 사이버 생태계 재구성 전략	4.3 Bureau of Cyber Statistics 설치	입법 제안
	4.4 사이버보험 전문가 양성을 위한 연방정부출자연구기관 지원	FY2021 NDAA 통과된 법률을 통해 부분적 이행 완료
	4.4.1 사이버리스크 모델링에 대한 공사 파트너쉽 구축	행정명령 제안
	4.4.2 사이버 대재해에 대한 정부의 재보험프로그램 제공 필요성 검토	행정명령 제안, FY2021 NDAA 통과된 법률을 통해 부분적 이행 완료

자료: CSC(2021)

〈표 Ⅲ-4〉 테러보험 프로그램의 DTI 요건

국가	테러리즘 정의	근거	DTI 주체
미국	① 폭력적인 행위, 또는 생명·재물·주요 기반시설에 위험한 행위이어야 하며, ② 미국 내, 항공, 미국 선박, 또는 미국 관할 내 손해를 초래해야 하며, ③ 미국 시민을 협박하거나 협박 또는 강요를 통해 미국정부의 행동 및 정책에 영향을 미치기 위한 노력의 일환으로서 개인 또는 개인들에 의해 행해지는 행위	법률 (Terrorism Risk Insurance Act of 2002)	재무부의 테러리즘 인정
영국 (GB)	조직을 위하여 또는 조직과 관련된 개인들이 영국 정부를 전복시키거나 영향을 주기 위하여 사용하는 폭력적 또는 강압적 행위	법률 (Reinsurance (Acts of Terrorism) Act 1993)	재무부의 테러리즘 인정
프랑스	개인 또는 집단의 획책 아래 의도적으로 위협 또는 공포에 의하여 공공질서를 현저하게 방해할 목적으로 행해지는 다음 각 호의 범죄 ① 고의에 의한 생명 및 사람의 완전성에 대한 침해, 약취, 감금 및 항공기, 선박 기타 모든 수송수단의 탈취 ② 절도, 강요, 손괴, 훼손, 효용상실 및 컴퓨터 공격(이하 생략)	법률 (Code Pénal-Article 421-1)	프로그램 규정 및 보험약관에 따름
독일	개인 또는 개인으로 이루어진 단체가 정치, 종교, 인종 또는 이념적 이유로 정부 또는 공공단체에 영향을 주기 위해 민중에게 위협을 가하는 모든 행동	프로그램 자체 규정	프로그램 규정 및 보험약관에 따름
호주	정치적, 종교적, 이념적 명분을 이루기 위해 정부 또는 대중을 협박하여 영향을 미치거나 강압하는 행위로서, 타인에 심각한 물리적 피해, 심각한 재물손해, 사망, 인명 위협, 공공의 안전 및 보건 위협, 전자시스템(예를 들어, 정보시스템, 정보통신시스템, 금융시스템, 주요 국가기반시설 시스템 등)의 심각한 방해 및 파괴를 초래하는 행위	법률 (Criminal Code Act 1995 Part 5.3 Section 101.1~101.2)	총리의 테러리즘 선언
스페인	기존 정치질서를 불안정하게 하고 사회 환경에 불안과 공포를 조장할 목적으로 행해지는 모든 폭력적인 행위	규정 (Reglamento del seguro de riesgos extraordinarios)	프로그램 규정 및 보험약관에 따름

주: DTI(Declared Terrorist Incident)는 특정 사고의 테러리즘 인정 여부로서, 테러리즘 프로그램 작동 여부를 결정함
자료: 저자가 작성함

2. 호주

가. 사이버보험 시장

호주 기업들은 사이버사고에 대한 보장을 전통적인 재물보험 및 배상책임보험과 단독 사이버보험을 통해 얻고 있다. 호주에서는 재물보험과 배상책임보험 모두 사이버사고로 인한 재물손해, 영업중단손해, 배상책임손해를 암묵적으로 보장한다. 호주의 대표적인 기업보험인 ISR(Industrial Special Risk)은 재물손해와 영업중단손해를 보장하며, 포괄위험 담보방식으로 사이버담보를 암묵적으로 보장한다. 제2장에서 설명한 바와 같이 미국에서는 2006년부터 배상책임보험에 전자데이터 면책을 시작으로 사이버사고에 대한 면책을 확대하였고, 영국 로이드 시장에서도 LMA 5274 등 사이버사고 면책이 배상책임보험에 추가되었다. 그러나 호주에서는 배상책임보험 약관에 사이버사고에 대한 보장 또는 면책을 명시적으로 규정하지 않아, 사이버사고로 인한 배상책임손해가 기업배상책임보험에서 보장되는 것으로 해석한다(OECD 2020b).

2018년 단독 사이버보험 시장규모는 2018년 원수보험료 기준 약 1억 달러(USD)로 추정된다(OECD 2020b). 동기간 기업용 재물보험과 배상책임보험 원수보험료가 각각 100억 달러, 44억 달러인 것에 비하면 단독 사이버보험 시장규모는 상당히 작은 편이다. 호주의 경우 사이버보험 시장이 발전 초기 단계이니 만큼 사이버보험 가입현황에 대한 정확한 수치가 집계되지 않고, 설문조사 등에 의존한다. 조사마다 차이를 보이나, OECD와 University of Cambridge의 공동조사에 따르면, 기업들의 단독 사이버보험 가입률은 20% 수준으로, 대기업(35%)이 보다 적극적으로 가입하는 경향이 있다.

사이버사고 증가 및 사이버리스크에 대한 기업의 인식 제고와 함께, 보안 및 개인정보 침해에 대한 정부의 태세 전환도 기업의 보험수요 증가에 영향을 미친 것으로 보인다. 사이버보안에 대한 정부의 대응이 인식제고와 교육에서 규제 강화로 전환되었다. 2018년 데이터 침해에 대한 통지의무가 강화되면서 단독 사이버보험에 대한 수요가 높아지고 있는 추세이다. 뿐만 아니라, 호주 정부는 개인정보보호법(Privacy Act of 1988) 중대 위반 시, 최대벌금을 현행 210만 호주 달러에서 '1천만 호주 달러, 법 위반으로 인한 부당이득의 3배, 또는 매출액의 10% 중 큰 금액'으로 상향조정하는 것을 논의 중이다(Australian Government 2020).

Aon 또는 Marsh와 같은 보험중개업체에 따르면, 최근 호주 사이버보험 시장은 높은 사고빈도 및 손해율로 인해 요율 인상과 함께 보장한도 축소가 관찰된다. Aon은 당사 고객 기준 2021년 2/4분기 보험요율이 전년 대비 최대 80% 인상되고 보험금 지급 건수는 50% 증가한 것으로 보고하였다.

나. 정부개입

1) 테러보험 프로그램

9·11 테러리즘 이전에는 일반 기업보험에서 테러위험을 보장하였다. 그러나 9·11 테러리즘 이후 테러리즘에 대한 재보험담보를 얻을 수 없게 되자 보험회사는 테러담보 제공을 중단하기에 이르렀다. 테러리즘에 대한 안전장치가 확보되지 않자 투자 및 자금 조달이 원활하지 않아, 진행 중이거나 계획되었던 건설 프로젝트, 부동산 거래들이 취소·지연되었다. 이에 정부는 2003년 Terrorism Insurance Act 2003(테러보험법)을 제정하여, 총리가 테러리즘을 선언하면, 원 보험계약에 명기된 테러면책조항이 무효화되도록 하였다. 약관상 테러면책 여부에 상관없이, 특정 사고가 테러리즘으로 선언되면 보험회사는 테러리즘으로 인한 손해를 보장해야 한다. 대신 정부는 재무부 산하에 테러리즘 전용 재보험기구, ARPC(Australian Reinsurance Pool Corporation, 호주 재보험풀)을 설립하여, 총리의 테러리즘 선언 시 보험회사에 테러담보에 대한 재보험을 제공하고, 100억 호주 달러 한도 내에서 지급을 보증한다.

총리가 테러리즘으로 공식 발표한 건에 한해 테러보험 프로그램이 실행된다. Insurance Terrorism Act 2013에서 테러리즘을 별도로 정의하지 않아 형법상의 정의에 따라 보상이 이루어진다. 형법에서는 테러리스트 행위(Terrorist act)를 정치적, 종교적, 이념적 명분을 이루기 위해 정부 또는 대중을 협박하여 영향을 미치거나 강압하는 행위로서, ① 타인에 심각한 물리적인 위해, ② 심각한 재물손해, ③ 사망, ④ 인명 위협, ⑤ 공공의 안전 및 보건 위협, ⑥ 전자시스템(예를 들어, 정보시스템, 정보통신시스템, 금융시스템, 주요 국가기반 시설시스템 등)의 심각한 방해 및 파괴를 초래하는 행위로 정의한다.[55] 단, 지지(Advocacy)·항의(Protest)·반대(Dissent)·노동쟁위 행위(Industrial action)로서, 타인에게 심각한 물리적 위해를 가하거나, 사망을 초래하거나, 생명을 위협하거나, 공중 안전 또

55) Criminal Code Act 1995 Part 5.3 Section 100.1~101.2

는 보건에 심각한 위협을 가할 의도가 아닌 경우에는 테러리스트 행위에 해당하지 않는다. 종합하면, 심각한 재물손해 또는 전자시스템의 심각한 방해 및 파괴를 초래하였더라도 그 행위의 목적이 정치적·종교적·이념적 명분이 아닌 지지·항의·반대·노동쟁위인 경우에는 형법상 테러리스트 행위에 해당하지 않는다.

ARPC의 재보험담보가 제공되는 손해는 재물손해, 영업중단손해, 배상책임손해이다. ARPC의 보장대상 재물은 상업, 산업, 건설, 농업(농장을 보험목적물로 하는 BI 담보를 가진 경우)용 건물 및 시설이다. 선박, 항공, 주거용 빌딩, 자동차 등에 대한 공격은 면책이다. 현재 테러보험은 전쟁, 핵폭발, 방사선 장해(Dirty bomb 포함), 컴퓨터범죄(Computer crime)로 인한 재물손해를 보장하지 않는다.[56] 사이버공격은 컴퓨터범죄에 해당하여 ARPC 보장대상에서 배제된다.

2) 사이버공격의 테러보험 적용

테러보험법과 ARPC를 통한 테러리즘 재보험제도는 임시적인 조치로, 3년 주기로 연장 여부 및 운영방식을 검토한다. 주로 정부의 개입 없이는 테러리즘 담보가 시장에서 자율적으로 공급되기 어려운 상황인지, 그리고 테러리즘 관련 추가적인 보장공백은 없는지를 살펴본다. 2006년 1차 검토(Triennial review)를 시작으로 2021년 6차 검토를 진행 중이다. 2018년 5차 검사부터 사이버 테러리즘으로 인한 재물손해의 테러보험 적용 여부를 핵심의제로 검토하였으나 아직은 시기상조이며 지속적인 검토를 예고하였다. 2021년 6차 검사에서도 핵심의제로 재검토 중에 있다.

호주에서는 2016년부터 사이버공격에 대한 보장공백이 정부 차원에서 검토되었다. 사이버공격의 파괴적 특성이 가시화되고 테러리스트의 공격도 물리적 공간에서 사이버공간으로 이동할 것이라는 우려가 현실화되었다. 이에 ARPC는 2016년 3월, 사이버 테러리즘으로 인한 재물손해가 테러보험 프로그램에서 보장되는 손인인지를 검토하였다(ARPC, 2016). Terrorism Insurance Regulations 2003의 Schedule 1에서는 ARPC에서 면책되는 40개 항목을 열거하는데, 컴퓨터공격이 그 중 하나이다. 사이버공격은 Criminal Code Act 1995에서 규정한 컴퓨터범죄에 해당하여 ARPC 보장대상에서 배제된다. 따라서 보험회사가 판매하는 원 보험증권에서 설령 원격 컴퓨터 접근으로 인한 물리적 재물 손해를

56) ARPC의 테러보험 면책은 40가지로, Terrorism Insurance Regulations 2003의 Schedule 1에서 상세히 기술함

보장해준다고 하더라도, 동 증권의 테러담보에 대한 재보험을 제공하는 ARPC는 컴퓨터 범죄를 면책으로 규정하여, 동 손해를 보장하지 않는다. ARPC는 기존 테러보험 프로그램이 사이버 테러리즘 리스크에 대한 보장공백을 초래한다고 보았다. ARPC가 사이버공격에 의한 재물손해를 재보험자로서 보장해주지 않게 되면 결국 동 손해에 대한 재보험담보를 구하지 못한 보험회사들이 해당 담보를 기업에 공급하지 않을 것이기에 보장공백이 발생하게 되는 것이다.

2018년 제5차 검사에서 사이버 테러리즘에 따른 재물손해를 테러보험 보장항목에 포함해야 하는지를 검토하였다(Australian Government 2018). 그러나 2018년 당시 시장상황으로는, 사이버 테러리즘에 따른 재물손실 보장에 대한 시장공백은 존재하지만 정부가 개입해야 할 만큼의 명확한 시장실패가 존재하지 않다고 보고 사이버 테러리즘으로 인한 재물손해를 보장항목에 포함하지 않기로 결론지었다. 구체적으로, ① 호주 사이버보안센터(Australian Cyber Security Centre)에 따르면 테러리스트 조직의 사이버공격 역량이 아직 우려할 정도로 파괴적이지 않다는 점, ② 민영 사이버보험 시장이 빠르게 성장하고 있다는 점, ③ 시장에 보장공백이 존재하기는 하지만, 보험회사가 공백을 메우기 위해 적극적으로 인수하고 있는 점을 보아 현재의 보장공백은 시장실패로 보기는 어렵다는 점을 들었다.

2018년 말, ARPC는 OECD, University of Cambridge와 공동으로 호주 사이버 테러리즘에 대한 보험리스크를 평가하였고, 그 결과는 2020년 OECD보고서를 통해 공개되었다(ARPC et al. 2020). 구체적으로, 가상 시나리오를 구성하여 사이버 테러리즘으로 인한 재물손해와 영업중단손해를 추정하고, 사이버 테러리즘을 테러보험 보장대상에 포함할 경우 현실적으로 어떠한 문제들이 있는지를 검토하였다. 구체적으로, 연구진은 발생 가능한 사이버 테러리즘 시나리오로 다음을 가정하였다. ① 공격자가 펌웨어 업데이트 등을 통해 정보통신장비에 내장된 인화성이 높은 리튬이온의 과열을 유도하여 호주 상업지구에서 대규모 폭발이 일어나는 시나리오, ② 호주 내 빌딩관리시스템을 공격하여 재물손실이 발생하는 시나리오이다. ①의 최대손실은 833억 달러, 평균손실은 20억 달러, ②의 최대손실은 418억 달러, 평균손실은 13억 달러로 추정되었다. 사이버공격에 따른 평균손실은 기존에 ARPC가 보장하던 유형의 사고(예를 들어, 시드니에 대규모 폭발이 발생)와 유사하나, 최대손실은 생화학공격(920억 달러)과 유사하다. 연구진은 비록 발생 가능성은 낮지만 거대손실 가능성이 존재하므로, 사이버 테러리즘에 따른 재물 손실을 ARPC 개입 없이 민영 시장에서 단독으로 인수·보장하기에는 어려울 것이라고 강조하였다. 또한 동 연구에서는 국가 배후 사이버공격의 경우 ISR 또는 단독 사이버보험 등 원 보험계약의 전쟁면

책 적용 가능성으로 인해 보장공백이 존재할 수 있다고 보았다. 따라서 국가 배후 사이버 공격으로 인한 재물손해와 영업중단손해를 Insurance Terrorism Act 2013와 그 하위규정을 개정하여 테러보험 프로그램의 보장대상에 포함할 것을 제안하였다. 즉, ARPC의 재보험담보 제공 범위를 사이버 테러리즘이 아니라, 공격자에 상관없이 정치적·종교적·이념적 목적을 가진 악의적 사이버공격으로 확대할 것을 제안한 것이다.

2020년 12월, ARPC는 University of Queensland와 공동으로 호주 내 테러리즘 행위로 인한 손실과 잠재적인 보장공백을 분석하였다. 이 연구에서는 보장공백의 근원을 ① 문제의 손해를 보험회사가 기업에 판매하는 원 보험계약에서 담보하지 않기 때문에 재보험자인 ARPC가 동 손해에 대해 재보험담보를 제공하지 않는 경우, ② 원 보험증권에서 담보하는지 여부에 상관없이 ARPC에서 면책하는 경우 등 두 가지로 구분하였다. 사이버공격으로 인한 재물손해는 ①과 ② 모두에서 보장공백이 존재하며, 예상가능한 모든 테러수법 중 보장공백이 가장 심각한 항목으로 평가되었다. 사이버공격의 재물손해로 인한 영업중단손해와 랜섬웨어로 인한 영업중단손해는, 비록 ARPC 재보험담보에는 포함되지 않지만, 낮은 보장한도, 조건부 보장 등 제한적이나마 민영시장에서 거래되고 있기 때문에 사이버공격으로 인한 재물손해보다는 보장공백이 낮다고 보았다. 그 외 테러리스트의 생화학공격이나 폭발로 인한 건물붕괴, 외로운 공격자(Lone actor) 등으로 인한 재물손해는 원 보험계약과 재보험계약에서 대부분 보장되나, 그로 인한 영업중단손해는 원 보험계약에서 보장되지 않아 보장공백이 심각한 수준으로 파악되었다.

2021년 7월, 재무부는 제6차 검토의 일환으로, ① 테러보험 프로그램을 지속할 것인지 여부, ② ARPC 보장대상에 물리적 재물 손실을 초래하는 사이버 테러리즘을 포함할 것인지 여부, ③ ARPC가 보장하는 타 리스크와 어떻게 상호작용할 것인지[57] 등 세 가지 핵심의제에 대한 자문보고서를 발표하고 이해관계자의 의견을 요청하였다(Australian Government: The Treasury 2021). 민영시장에서 사이버 테러리즘으로 인한 재물손해를 어느 정도로 보장하고 있는지, 사이버 테러리즘으로 인한 재물손해 담보가 충분치 않다면, 그 요인은 무엇이며, 정부가 ARPC를 통해 시장에 개입할 경우 시장에 어떠한 변화가 생길 것이며, 호주 사례에 적용할 만한 해외사례가 있는지에 대한 의견을 조회하였다.

이에 2021년 8월, 호주 보험중개인협회(The National Insurance Brokers Association,

57) 2022년 7월부터 ARPC는 기업용 테러담보뿐만 아니라 사이클론 및 홍수로 인한 가계와 소기업의 재물손해를 보장하는 재보험 프로그램을 운영함

NIBA)는 테러리스트의 사이버공격으로 인한 재물손해와 영업중단손해를 정부의 테러보험 프로그램 보장대상에 포함시켜 줄 것을 제안하였다.[58] 보험회사가 기업에 판매하는 원보험계약에서 사이버공격에 의한 재물손해 및 영업중단손해를 일부 보장하고 있지만, 테러리스트에 의한 사이버공격은 보장항목에서 제외됨에 따라 시장에 보장공백이 존재한다고 주장하였다. 또한 시장의 인수능력이 부족하여 사이버 테러리즘으로 인한 재물손해를 보장하기 어려우므로, 사이버 테러리즘으로 인한 재물손해에 대해 ARPC가 재보험담보를 제공해줄 것을 요청하였다. 이는 바꿔 말하면, 호주 보험업계도 사이버 테러리즘에 대한 재보험담보만 있다면, 보험회사가 사이버 테러리즘으로 인한 재물손해를 기꺼이 보장하고 이에 대한 손실의 일부를 인수하겠다는 의미이다.

〈표 Ⅲ-5〉 가상 사이버 테러리즘에 대한 보험 담보

가상손실	랩탑 배터리 폭발 공격 및 빌딩관리시스템 공격
재물보험(ISR)	테러리즘 면책에 따른 PD와 BI 면책, CBI 제한적 보상
배상책임	테러리즘 면책에 따라 보상 불가
사이버보험	PD 보장 불가, BI 잠재적으로 보장 가능, CBI 일부 제한적 보상 가능
단독 테러보험	사이버면책에 따른 PD와 BI 면책, CBI는 통상 제공 않음
ARPC 재보험	컴퓨터 범죄 면책에 따라 보장 불가

주: PD(Property Damage)는 재물손해를, BI(Business Interruption)는 재물손해로 인한 영업중단손해를, CBI(Contingent BI)는 거래상대방의 재물손해 등으로 인한 피보험자의 영업중단손해를 의미함
자료: OECD(2020b)

3) 한계 및 추가논의

2020년 공개된 ARPC, OECD, University of Cambridge의 공동연구는 사이버 테러리즘과 국가 배후 사이버공격을 테러보험 프로그램의 보장대상에 포함하는 방안을 제안하고, 이를 실행할 시 현실적으로 어떠한 문제들이 있는지를 검토하였다. ARPC의 재보험담보 범위를 확대하여 공격자에 상관없이 정치적 목적을 가진 악의적 사이버공격을 포함할 경우, ARPC와 정부는 다음과 같은 운영상 문제에 직면할 수 있다고 지적하였다.

첫째, 전통적인 테러리즘 행위와 달리, 사이버공격의 경우 적시에 공격자를 특정하기가

58) The National Insurance Brokers Association(2021. 8)

어렵고, 설령 공격자를 특정하였다 하더라도 공격자를 정치적·종교적·이념적 목적을 가진 테러리스트로 식별하기는 더 어렵다. 사이버공격의 속성상 신속한 공격자 특정의 어려움에 대해서는 너무나 자명하여 군말을 더 보탤 여지가 없다. 문제의 사이버공격을 테러리즘으로 선언하기 위해서는 행위의 목적과 결과가 형법상 테러리즘 정의에 부합해야 한다. 형법에서 규정한 바에 따르면, 심각한 재물손해 또는 전자시스템의 심각한 방해 및 파괴를 초래하였더라도 그 행위의 목적이 정치적, 종교적, 이념적 명분이 아닌 지지·항의·반대·노동쟁위인 경우에는 형법상 테러리스트 행위에 해당하지 않는다. 문제의 사이버공격이 정치적·종교적·이념적 명분의 발로인지, 지지·항의·반대의 발로인지, 혹은 단순히 과시욕구 또는 경제적 목적인지 어떻게 구분할 것인가?

둘째, 국가 주도 및 지원 사이버공격은 기존 전쟁면책과의 정합성 문제, 그리고 테러리즘 정의와의 정합성 문제 등을 가지고 있어 기존 테러보험 프로그램의 전면개편이 불가피하다. 현재 ARPC는 사이버공격뿐만 아니라 전쟁으로 인한 재물손해 및 영업중단손해에 대해서는 재보험담보를 제공하지 않는다. 국가 주도 및 지원 사이버공격의 재래식 전쟁면책 적용에 대한 논쟁이 한창 진행 중이다. 국가 주도 및 지원 사이버공격은 공격 주체가 국가라는 점에서 형법상 테러리즘의 범위를 벗어난다.

셋째, ARPC의 재보험담보 범위를 사이버 테러리즘 및 국가 배후 사이버공격으로 확대할 경우, ARPC의 위험노출도를 급격히 증가시키고 이는 재재보험료, 재보험료, 원보험료의 연쇄적인 인상을 초래할 것이다. 테러리스트 조직의 사이버 역량이 빠르게 발전하고 있으며, 근래 여러 사례에서 보았듯이 공격자로서 국가는 파괴적 사이버공격을 실행할 수 있는 역량을 보유하고 있다.

호주 정부의 사이버리스크에 대한 접근은 매우 논리적이고 신중하면서도 파괴적이다. 사이버공격으로 인한 기업의 보장공백을 정확히 읽어내고 기존 테러보험 프로그램의 정체성을 뛰어넘어서까지 보장공백 해소 방안을 검토해 왔다. 논의의 시작은 테러리스트의 사이버공격으로 인한 재물손해 및 영업중단손해에 대한 보장공백이었으나, 이에 국한하지 않고, 국가 배후 사이버공격에 대한 보장 가능성을 다각도에서 검토하고 있다. 즉, 기존 테러보험 프로그램의 정체성에 매몰되지 않겠다는 것이다.

3. 영국

가. 사이버보험 시장

영국 보험시장에서 사이버담보는 단독 사이버보험,[59] 기업책임보험에 사이버위험을 특약으로 포함하는 패키지보험, 그리고 포괄위험 담보방식 재물 및 배상책임보험 등을 통해 제공된다. 사이버보험에 가입한 영국 소재 기업의 원수보험료 규모에 대해서는 공식적으로 알려진 바가 없다. 그나마도 암묵적 사이버보험을 포함한 것인지 여부가 분명하지 않아 현황 파악에 한계가 있다.[60] 일찍이 단독 사이버보험이 등장한 미국과 달리, 영국에서는 암묵적 사이버담보에 대한 의존도가 높았기 때문으로 풀이된다. 그러나 분명한 것은 영국이 세계 사이버보험 수입보험료의 약 25~33%를 부보한다는 점이다. 미국이 세계 사이버보험 원수보험료의 약 90%를 차지하는 주 수요자라면, 영국은 주 공급자라 할 수 있다(AM Best 2020).

영국에서는 디지털·문화·미디어·스포츠부(Department for digital, Culture, Media and Sport)가 디지털 정책을 관장하면서, 2017년부터 기업을 대상으로 사이버보안 침해조사(Cyber security breaches survey)를 매년 수행하고 있다. 2020년 조사에 따르면, 대상 기업의 46%가 지난 1년간 사이버공격을 경험한 것으로 나타났으며, 이는 기업규모에 따라 43~75%에 분포하여 대기업일수록 사고발생 가능성이 높은 것으로 나타났다(〈표 Ⅲ-7〉 참조). 특히, 영국에서는 2017년 국민보건서비스제도(National Health Service; NHS)가 워너크라이 랜섬웨어 공격을 받아 의료분야가 1억 2천만 달러 상당의 피해를 입는 상황에 이르렀다(U. K. Department of Health&Social Care 2018).

응답 기업의 4%는 단독 사이버보험에, 28%는 암묵적 사이버보험에 가입하는 등 응답기업의 32%가 사이버담보를 가지는 것으로 나타난다. 보험가입률은 기업규모에 따라 단독은 4~21%, 암묵적 담보는 28~32%에 분포한다. 즉, 담보방식에 상관없이 기업규모가 커질수록 보험가입률도 증가한다. 상대적으로 보안이 취약한 공급망을 통한 사이버공격이 빈번해짐에 따라, 대기업이 계약조건의 일부로서 공급기업에 사이버보험 가입을 요구하

59) 구체적으로 사이버책임보험(Cyber liability insurance cover), 기술 E&O 배상책임(Technology errors and omissions, technology E&O liability insurance)의 형태로 판매됨

60) U.K. HM government&Marsh(2015)에서는 세계 사이버보험 시장에서 영국이 차지하는 비율을 2014년 원수보험료 기준 약 10%로 추정하였으며, EIOPA(2018)는 2016년 기준 EU가 차지하는 비율을 5~9%로 추정함

는 경향이 있다. 또한 2018년 GDPR 시행 등 개인정보 관련 규제 강화로 인해 적극적인 보험가입이 이뤄지고 있는 것으로 파악된다.

〈표 Ⅲ-6〉 2017년 워너크라이 공격

워너크라이(WannaCry) 또는 워너크립트(WannaCrypt), WanaCrypt0r 2.0는 2017년 5월 12일부터 등장한 랜섬웨어 멀웨어 툴이다. 2017년 5월 12일부터 대규모 사이버공격을 통해 널리 배포되었으며, 전 세계 150개국의 컴퓨터 30만 대 이상을 감염시켰다. 감염된 컴퓨터에 20개의 언어로 워너크라이는 암호화된 파일을 푸는 대가로 300달러(약 34만 원)의 비트코인을 요구하고, 사흘 내 지불하지 않으면 요구액을 배로 올린다는 메시지를 띄웠다.

워너크라이 랜섬웨어는 일부 기업·개인을 타겟으로 한 것이 아니라 전 세계적으로 불특정 다수를 공격해 피해가 컸다. 워너크라이 사이버공격으로 영국에서는 국민건강서비스(National Health System; NHS) 산하 40여 개 병원이 환자 기록 파일을 열지 못하는 등 진료에 차질을 빚거나 예약을 취소했다. 영국 정부는 사이버공격이 있었던 2017년 5월 12일부터 18일까지 환자들이 병원 예약 취소 등으로 제대로 치료를 받지 못하며 초래된 비용을 2,500만 달러, 사이버공격 후 6월과 7월 사이에 병원 컴퓨터 시스템 복구에 들어간 비용을 9,600만 달러로 추산해, 총 1억 2천만 달러의 피해를 입은 것으로 추정하였다. 페덱스, 도이체반, 스페인의 텔레포니카 등의 대기업, 러시아 내무부, 러시아 방위부, 러시아 통신사 메가폰 역시 감염 피해를 보았다.

2017년 6월 영국 정부는 워너크라이 랜섬웨어 공격은 북한의 소행이라고 공식 확인했다. 북한 정부가 배후에 있는 것으로 알려진 해커집단 라자루스(Lazarus)가 이번 공격을 감행한 것으로 확인하였다.

자료: U. K. Department of Health&Social Care(2018)

〈표 Ⅲ-7〉 영국 기업의 사이버리스크 및 사이버보험 가입 실태

(단위: %)

구분		전체 기업	소상공인	소기업	중기업	대기업
보험 가입	단독 사이버보험	4	2	14	20	21
	재물·배상책임보험 (암묵적 사이버보험)	28	27	30	32	32
사이버공격 경험		46	43	62	68	75

주: 사이버공격 경험은 지난 1년간 사이버피해를 당한 경험이 있는지 여부임

자료: U. K. Department for Digital, Culture, Media and Sport(2020)

나. 정부개입

1) 테러보험 프로그램

1990년 이전에도 영국에서는 아일랜드 민족주의자에 의한 테러리즘이 빈번하게 발생하였으나, 손실규모가 그리 크지 않아 보험회사는 NBCR을 면책으로 하는 테러리즘 담보를 가계 및 기업에 제공하였다. 그러나 1990년대 초 12건의 테러리즘이 연속으로 발생하자 테러위험에 대한 담보력 제공이 불가능해졌다. 이에 1993년 영국은 테러보험 전용 상호재보험회사 Pool Re(Pool Reinsurance Company Limited)를 설립하여 테러리즘으로 인해 발생한 기업의 재물손해 및 영업중단손해를 보험회사로부터 수재하도록 하고 정부가 상환조건부로 무제한 지급보증을 제공하기로 하였다. 2020년 기준 영국 내 기업보험 판매 보험회사의 95%(Lloyd's syndicate 포함 150여 개)가 Pool Re 회원사로 참여하고 있다. Pool Re 참여 보험회사는 자사의 모든 테러위험을 Pool Re에 출재해야 한다. Pool Re는 재무부(HM Treasury)와 재재보험 협정을 체결하여 Pool Re의 기금이 소진되어 보험금을 지급할 수 없게 되면 상환조건부로 정부가 보험금을 지급하도록 한다.[61]

테러보험은 기업의 재물보험 및 영업중단보험에만 적용되며, Reinsurance (Act of Terrorism) Act 1993에서 테러리즘으로 규정한 행위로 인해 발생한 재물손해와 영업중단손해를 보장한다. 표준 기업보험증권에 테러리즘이 부보위험으로 포함되는 형식이다. Reinsurance (Act of Terrorism) Act 1993에서는 테러리즘을 '조직을 위하여 또는 조직과 관련된 개인들이 영국 정부를 전복시키거나 영향을 주기 위하여 사용하는 폭력적 또는 강압적 행위'로 정의한다.[62] 다만, 북아일랜드를 제외한 잉글랜드·스코틀랜드·웨일즈 지역에서 발생한 테러리즘에 한하여 보장하며, 북아일랜드에서 발생한 테러리즘 손해에 대해서는 정부가 직접 보상한다.

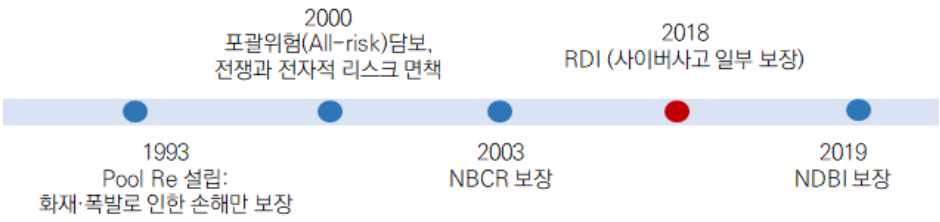
Pool Re는 테러리즘 수법 및 양상의 변화에 대응하여 보장범위를 지속적으로 확대해왔다. 1993년 설립 당시 Pool Re는 화재 및 폭발로 인한 기업의 재물손해와 영업중단손해

61) Pool Re 참여 보험회사, Pool Re, 정부의 위험보유구조는 송윤아·홍보배(2020)를 참고하기 바람

62) Reinsurance (Acts of Terrorism) Act 1993 Section 2 (2) In this section "acts of terrorism" means acts of persons acting on behalf of, or in connection with, any organisation which carries out activities directed towards the overthrowing or influencing, by force or violence, of Her Majesty's government in the United Kingdom or any other government de jure or de facto

를 담보해왔다. 2000년에는 전쟁과 전자적 리스크(Electronic risk)를[63] 면책으로 규정하고 나머지 리스크에 대해서는 포괄적으로 보장하는 포괄위험 담보방식을 채택하였다(〈그림 Ⅲ-8〉 참조). 2001년 9·11 테러리즘을 기점으로 세계 보험시장의 담보력이 불안정해지고 테러수법 및 피해양상이 다양해지자 2003년부터 NBCR로 인한 재물손해와 영업중단 손해를 보장하였다. 2018년에는 사이버 테러리즘이 사업장 내 전자기기를 파손하는 등 물적 손해를 동반한다는 점을 감안하여 사이버 트리거로 인한 직접적인 물적 손해와 영업중단손해를 보장하기로 하였다(Pool Re 2019). 이 담보를 RDI(Remote Digital Interference, 원격 디지털장애) 담보라 한다. 나아가 2019년에는 테러리즘 발생 시 사업장접근금지 등 행정명령으로 인해 영업을 중단해야 하는 경우가 발생함에 따라, 사업장 내 물적 손해를 동반하지 않는 영업중단손해를 보장할 수 있도록 Reinsurance (Acts of Terrorism) Act 1993을 개정하였다.

〈그림 Ⅲ-8〉 Pool Re의 보장 확대



주: NBCR(Nuclear, Biological, Chemical and Radiological)은 핵·생화학·방사능 사고를, RDI(Remote Digital Interference)는 사이버사고의 일부를, NDBI(Non-physical Damage Business Interruption)는 물리적 손실을 동반하지 않은 영업중단손해를 의미함
자료: Pool Re의 각 연도 연차보고서 등을 참고하여 저자가 작성함

2) 사이버공격의 테러보험 적용

2014년 독일 제철소 공격, 2015년 우크라이나 공격 등 2010년대 들어 사이버공격으로 인한 피해 유형 및 규모가 확대되고, 사이버공격이 극단적 피해를 노리는 테러리스트 조직의 공격수단으로 활용될 가능성이 높아짐에 따라, Pool Re는 그로 인한 보장공백 검토에 착수하였다. 2017년 11월, Pool Re는 University of Cambridge와의 공동 연구에서 기존

63) 컴퓨터 해킹·바이러스·서비스거부(Denial of Service) 공격으로 인한 손해를 의미함

사이버공격 시나리오에 근거하여 영국의 사이버위협 취약성을 분석하고 주요 테러리스트 조직의 사이버역량을 추정하였다(Pool Re&University of Cambridge 2017). 건물, 항공, 유통, 건설, 에너지, 제약, 우주, 화학, 교통 등 10개 산업에 사이버공격이 있을 가능성과 예상되는 피해규모를 추정하였다. 연구에 따르면 향후 3년 내 영국에서 가장 치명적인 피해를 줄 수 있는 사이버공격은 항공기, 철도 인프라, 화학반응기, 무기에 대한 공격으로, 이는 모두 물적·인적 피해를 수반한다(〈표 Ⅲ-8〉 참조).

동 연구에 근거하여, Pool Re는 영국 재무부의 동의하에, 사이버공격과 관련한 보장항목의 면책사항을 개정하였다. 2018년 4월 1일부터 원격 장애로 인한 재물 손실과 이로 인한 영업중단손실은 Pool Re의 면책항목에서 제외하기로 하였다. 사이버 테러리즘이 사업장 내 전자기기를 파손하는 등 물적 손해를 동반한다는 점을 감안하여 사이버 트리거로 인한 직접적인 물적 손해와 영업중단손해를 보장한 것이다. 다만, 통상의 사이버보험에서 보장하는 데이터 및 지적재산과 같은 무형자산 손실과 그로 인한 영업중단손해는 보장하지 않는다. 또한 RDI 보장은 공격근원지에 상관없이 기존의 Pool Re 테러리즘 보장과 동일하게 잉글랜드·스코틀랜드·웨일즈 지역에 소재한 재물에 손실이 발생한 경우에만 재물손해와 영업중단손해를 보장한다.

〈표 Ⅲ-8〉 사이버공격 리스크 상위 4개 시나리오

표적	사망률	재물손해	가능성
항공기	8	10	6
철도 인프라	7	10	7
화학 반응기	10	10	9
무기(Ordnance)	8	10	5

주: 표 안 수치는 0~10 척도임
자료: Pool Re & University of Cambridge(2017)

3) 한계 및 추가논의

Pool Re의 RDI 담보는 매우 제한적이어서, 급격히 진화하는 사이버공격의 손실을 보장하기에는 명백한 한계를 지닌다.

먼저, RDI 담보는 사이버공격으로 데이터 및 시스템 마비로 인한 영업중단손해를 보장하

지 않음으로써 시스템 마비를 초래하는 사이버공격에 대해서는 심각한 보장공백을 가진다. 워너크라이 감염사례에서 보듯이 랜섬웨어는 몸값 지불 시까지 시스템이 마비되기 때문에 그로 인한 영업중단손해가 심각한 수준이다. OT 및 ICS 공격도 결국은 시스템을 마비시켜 영업중단손실을 초래한다. 사이버 테러리즘과는 달리 물리적 테러리즘 발생 시 Pool Re는 재물손해, 영업중단손해, 물리적 손실을 동반하지 않은 영업중단손해(NDBI) 등 테러리즘으로 인해 발생한 모든 손실을 보장한다. 그러나 RDI는 사이버 트리거로 인한 재물손실과 동 재물손실로 인한 직접적인 영업중단손해만 보장한다. 즉, 데이터 및 지적재산과 같은 무형자산 손실은 보장하지 않고, 데이터 및 시스템 훼손으로 인한 영업중단손실은 보장되지 않는다.

둘째, RDI 보장을 위해서는 문제의 사이버공격이 Reinsurance (Act of Terrorism) Act 1993에서 정의한 테러리즘 정의에 부합해야 하는데, 근래의 사이버공격은 여러 측면에서 동 정의에 부합하지 않다. 동 법에서는 테러리즘을 '조직을 위하여 또는 조직과 관련된 개인들이 영국 정부를 전복시키거나 영향을 주기 위하여 사용하는 폭력적 또는 강압적 행위'로 정의한다. 동 정의에서는 사이버공격의 귀책이 조직 또는 개인이고 공격의 동기가 확인될 것을 요구한다. 사이버공격은 전통적인 테러리즘과 달리 공격자를 특정하기 어려울 뿐만 아니라 공격동기가 정치적인 이유임을 입증하기도 어렵다.

셋째, Pool Re의 테러보험은 전쟁면책을 가지고 있어, 국가 주도 및 지원 사이버공격에 대한 보장공백이 발생할 수 있다. Pool Re의 테러보험은 제도 도입 당시부터 전쟁면책을 가진다. 전쟁면책에 의거, 국가 주도 및 지원 사이버공격으로 인한 재물손해와 영업중단손해는 면책가능성이 존재한다. 2010년대 이후 국가가 적극적인 사이버 공격자로 등극한 상황에서, 전쟁면책은 피보험기업의 보장공백을 확대시킨다. 아울러, 전쟁면책은 앞서 이 보고서 2장 2절 라.에서 다루었던 전쟁면책 적용 여부에 대한 지리한 논쟁이 불가피하다.

영국의 경우 2001년 9·11 테러리즘 이전에 이미 테러보험 프로그램을 갖추고 있었고, 〈그림 Ⅲ-8〉에 보는 바와 같이 테러리즘 수법 및 피해양상에 맞춰 그에 상응한 보장담보를 추가로 제공함으로써 기업의 보장공백을 적극적으로 해소해왔다. 영국 재무부의 민첩한 대응에 비추어볼 때, 2018년 RDI 담보에 이어 향후 추가적인 사이버담보가 공급될 것으로 예상된다.

4. 프랑스

가. 사이버보험 시장

프랑스 기업은 전통적인 포괄위험 담보방식 재물보험 및 배상책임보험(민사책임보험, 임원배상책임보험 등), 그리고 단독 사이버보험을 통해 사이버리스크에 대한 담보를 얻을 수 있다. 포괄위험 담보방식 재물보험은 사이버사고로 인한 직접적인 재물손해와 그로 인한 영업중단손해를 암묵적으로 보장하지만, 사이버사고로 재물손해를 동반하지 않은 운영손실은 보장하지 않는다. 또한 대부분의 기업용 재물보험은 국가의 테러보험 프로그램에 의해 사이버 테러리즘으로 인한 재물손해와 영업중단손해도 보장한다. 다음으로, 민사책임보험(Civil liability)은 손인에 상관없이 기본적으로 제3자에 가해진 신체 및 재물 손해뿐만 아니라 비물리적 손해까지도 보장한다. 임원배상책임보험은 임원이 업무를 수행함에 있어 주주 및 제3자에게 입힌 경제적 손해에 대한 법률상 배상책임을 폭넓게 보장한다. 배상책임보험은 악의성 여부에 상관없이, 사이버사고로 인해 발생한 배상책임을 보장한다. 단, 형법상 테러리즘에 해당하는 사이버공격으로 인한 배상책임은 원 보험계약에 명시된 테러면책에 의해 보장되지 않는다. 단독 사이버보험은 기존 재물 및 배상책임보험에서 보장하지 않던 개인정보 침해 통지비용, 랜섬, 포렌식 비용 등을 별도로 보장한다.

단독 사이버보험 시장의 규모는 2020년 원수보험료 기준 약 1억 3천만 유로로, 2019년의 8,700만 유로 대비 약 48% 증가하였다. 이는 기업의 사이버보험 수요 증가 및 요율 인상에 기인한다. 단독 사이버보험 시장은 가입률, 손해율 및 요율 측면에서 기업규모별로 뚜렷한 층화를 보인다. 대기업(연매출 15억 유로 초과)은 원수보험료의 약 82%(1억 5백만 유로), 중기업(연매출 5천만~15억 유로)은 11%(15백만 유로)를 차지한다. 대기업의 87%는 하나 이상의 사이버보험에 가입되어 있는 반면, 중기업은 약 8%만이 사이버보험에 가입되어 있으며, 소규모 기업(연매출 약 1천만~5천만 유로)은 사이버보험에 거의 가입되어 있지 않은 것으로 나타난다(Le Club des Justices 2018).

단독 사이버보험의 지급보험금은 2019년 7,300만 유로에서 2020년 2억 1,700만 유로로 약 3배 증가하였다.[64] 이와 함께 손해율이 2019년 84%에서 2020년 167%로 증가하

64) L'Association pour le Management des Risques et des Assurances de l'Entreprise(AMRAE)(2021)을 바탕으로 작성됨. AMRAE는 The National Information System Security Agency, Institute of Actuaries, The French Insurance Federation(FFA)와 논의하여, 8개 주요 보험중개사(Aon, Marsh, Gras

면서 보험회사의 수익성이 악화되었다. 이는 각 1천만~4천만 유로에 해당하는 4건의 대규모 지급보험금 청구에 기인한다. 지급보험금을 기업규모별로 살펴보면, 대기업은 2019년 3,100만 유로에서 2020년 2억 유로로 약 533% 증가한 반면, 중기업은 2019년 3,900만 유로에서 2020년 1,300만 유로로 약 67% 감소하였다. 이에 따라 보험요율도 기업규모별로 차이를 보인다. 대기업의 사이버보험 요율은 2019년 0.93%에서 2020년 1.03%로, 중기업은 2019년 0.34%에서 2020년 0.45%로 증가하였다. 대기업의 사이버보험 요율이 중기업 대비 약 3배 정도 높게 나타난다.

사이버보험 시장은 최근 빠르게 성장했지만, 보장 수준 및 한도는 위험 대비 상당히 낮은 수준이다. 보장한도는 대기업이 평균 3,800만 유로, 중소기업이 평균 800만 유로이다. 사이버공격에 따른 손실추정액이 수억 유로 이상이며, 연매출 15억 유로 이상의 대기업의 1일 평균 영업중단손실만 해도 수백만 유로에 달한다는 점을 감안하면, 보장한도가 위험노출도 대비 상당히 낮은 수준임을 알 수 있다.

나. 정부개입

1) 테러리즘 프로그램

프랑스에서는 1986년 9월부터 해양·항공·사이버위험·제3자 배상을 제외한 대부분의 손해보험에서 테러리즘 담보의 제공 및 가입이 법적으로 의무화되었다.[65] 법상 의무화된 테러리즘 담보는 프랑스 영토 내 또는 프랑스가 관할하는 해외 지역에서 발생한 테러리즘에 의한 손해를 보상하였다. 그러나 2001년 9·11 테러리즘 이후, 테러위험 담보 인수에 대한 보험회사들의 부담이 커졌다. 보험회사가 재물보험 인수 시 테러담보만을 선택적으로 거절할 수 없기 때문에 재물보험 갱신 자체를 거절하는 상황이 발생하였다. 이에 정부와 보험업계는 보험회사로 구성된 비영리 공동재보험 풀인 GAREAT을 설립하여 테러담보에 대한 공동재보험을 운영하도록 하고, 정부는 국영재보험회사인 CCR(Caisse Centrale de Réassurance)을 통해 GAREAT에 재보험과 무제한 지급보증을 제공하기로 하였다.

Savoye-Willis Towers Watson 등)와 총 1,879개 프랑스 기업, 328건의 보험 청구건 분석을 토대로 보고서를 작성함

65) Insurance Code Article L 126-2

전술한 테러리즘 프로그램이 실행되는 테러리즘 행위는 형법의 정의를 따른다.[66] 프랑스 형법(Code penale) 제421-1조는 테러리즘을 '개인 또는 집단의 획책 아래 의도적으로 위협 또는 공포에 의하여 공공질서를 현저하게 방해할 목적으로 행해지는 다음 각 호의 범죄로 규정한다. ① 고의에 의한 생명 및 사람의 완전성에 대한 침해, 약취, 감금 및 항공기, 선박 기타 모든 수송수단의 탈취, ② 절도, 강요, 손괴, 훼손, 효용상실, 정보처리에 관한 범죄(Computer offences, as defined under Book III of the present Code), ③ 해산된 무장단체에 관련한 범죄와 동법 제434-6조와 제441-2조부터 제441-5조까지 규정된 범인은닉 등의 원조행위, 공문서 위조, 위조한 공문서 소지 및 행사, 공문서 부정발급, ④ 무기·폭발물·핵물질에 관련된 범죄, ⑤ 상기 본조 제1호부터 제4호까지 열거된 범죄행위들 중에서 비롯된 산출물의 은닉, ⑥ 자금세탁범죄, ⑦ 자신의 금융시장과 관련한 업무·지위·특수정보를 이용하여 투자자의 이익과 금융시장의 투명성을 해치는 행위로 정의한다. 테러리스트에 대한 조력 행위(형법 제421-2-1)와 테러리즘에 자금을 지원하는 행위(형법 제421-2-2)도 테러리즘 행위에 해당한다.

테러보험 프로그램은 재물화재보험(Property fire damage), 자동차보험(Motor hull), 백만 유로 미만의 비상업용 항공보험(Aircraft hull), 백만 유로 미만의 레저용 선박보험(Vessel hull)에 적용되며, 건설배상책임보험, 해상항공보험, 화물 및 철도차량보험, 상해보험, 배상책임보험 등에는 적용되지 않는다. 테러리즘으로 인한 재물 및 금전적 손실과 피보험기업의 사업장 내 물적 손실로 인한 영업중단손해를 보장한다. 형법 Article 421-2에 따라 NBCR 공격도 보장대상에 포함된다.

2) 사이버공격의 테러보험 적용

문제의 사이버공격이 형법의 테러리즘에 부합할 경우, 테러보험 프로그램은 테러리스트에 의한 사이버공격을 보장한다. 즉, 사이버 테러리즘을 일괄 면책하지 않는다. 테러리즘 프로그램은 형법 Article 421-1.2와 Article 323-1~8로 인한 직접적인 재물손해와 그로 인한 영업중단손해를 보장한다. 형법 Article 421-1.2와 Article 323-1~8에 해당하는 사이버 테러리즘 행위로 인한 비물리적 손해, 직접적인 재물손실을 동반하지 않은 운영손실은 보장되지 않는다. 예를 들어, 악성 소프트웨어가 산업안전시스템을 감염시켜 화재와 운영손실이 발생한 경우 이를 보장한다. 그러나 컴퓨터 네크워크에 대한 DDOS공격의 경

66) Criminal Code Articles 421-1 and 421-2

우 직접적인 재물손해는 없지만 기업활동중단으로 인한 운영손실이 발생한 경우, 이에 대한 손실은 보장하지 않는다. 또한 데이터 손상이나 가용성 훼손, 정보매개체(하드웨어, 메모리, 하드디스크, USB, 스틱 등)의 기술적으로 복구 불가능한 손상 등은 보장되지 않는다.

형법 Article 421-1.2에서는 형법 제3장에 정의한 컴퓨터 공격(Computer offences, as defined under Book III of the present Code), 즉 정보처리에 관한 범죄를 테러리즘 행위로 규정한다. 형법 제323-1~7에서는 '비인가자의 자동화된 정보처리시스템에 대한 접근(Unauthorised Access to Automated Data Processing System)'에 해당하는 행위를 열거하고 그에 상응한 처벌을 규정한다. ① 자동화된 정보처리시스템에 악의적으로 접속하거나 이를 유지하는 자는 처벌한다. 정보의 삭제나 변경, 또는 운영체계의 변경도 처벌한다(Article 323-1). ② 자동화된 정보처리시스템의 작동을 방해하거나 변조하는 행위는 5년의 구금형 또는 7만 5천 유로의 벌금형에 처한다(Article 323-2). ③ 자동화된 정보처리시스템에 악의적으로 정보를 집어넣거나 정보처리시스템에 들어있는 정보를 악의적으로 삭제 또는 변경하는 행위를 처벌한다(Article 323-3). ④ 형법 제323-1 이하의 범죄를 행하기 위해 개발되거나 특히 그에 적합하게 조작된 장치나 컴퓨터프로그램, 정보를 적법하지 않게 수입·소유·제공·증여·대여하는 행위는 그 범죄를 행한 것과 동일하게 처벌한다(Article 323-1). ⑤ 형법 제323-1 내지 제323-3-1의 범행을 예비하기 위해 단체나 집단에 가입한 자는 가장 중하게 처벌되는 행위에 대한 형벌로 처벌한다(Article 323-4). ⑥ 자동화된 정보처리시스템에 대한 공격의 미수도 처벌한다(Article 323-7).

3) 한계 및 추가논의

사이버 테러리즘으로 인한 기업의 재물손해와 영업중단손해에 대한 국가의 재보험담보 및 무제한 지급보증에도 불구하고, 프랑스의 경우 인간의 실수 또는 시스템 오류로 인한 대규모 사이버사고, 국가 주도·지원 사이버공격으로 인한 재물손해 및 영업중단손해와 신체손해, 물리적 손해를 동반하지 않은 영업중단손해(사이버사고로 인한 NDBI) 등에 대한 보장공백이 존재한다. CCR 등 관련 정부기관의 영문 문서를 확인하였으나 이러한 공백에 대해 프랑스 정부에서 어떠한 논의가 추가적으로 진행되고 있는지 확인되지 않는다.

5. 소결

사이버보험 시장을 선도하는 미국, 영국, 프랑스, 호주 등에서는 자국에서 이미 운영 중인 공사협력 테러보험 프로그램을 통해 '일부 사이버공격'으로 인한 손해에 대해 재보험담보 및 유동성을 제공하는 방식을 취하고 있거나 논의 중이다. 기존 테러보험 프로그램이 있는 상황에서는 사이버사고를 동 프로그램의 손인으로 추가하는 것이 정책적으로 가장 용이한 접근일 뿐만 아니라, 사이버리스크에 대응한 공사협력 보험 프로그램을 새로이 구성하기에는 사이버리스크와 사이버보험 시장이 단기간에 급격하게 변하였기 때문으로 사료된다.

그러나 기존 테러보험 프로그램은 물리적 테러리즘과는 이질적인 사이버테러리즘의 특성을 반영하고 심각한 보장공백이 예상되는 사이버공격을 포섭하는 데 있어 여러 난관에 직면한다. 무엇보다도 문제의 사이버행위가 테러리즘 요건을 충족해야 하므로, '테러리스트'에 의한 사이버공격이 아닌 경우, 인간의 실수에 의한 대규모 사이버사고, 범죄조직의 대규모 금전 목적 랜섬웨어 공격, 또는 국가 배후 사이버공격은 정작 프로그램 적용대상에서 배제될 수 있다. 또한 국가 배후 사이버공격, 경제적 목적의 사이버공격 등은 기존 '테러리즘'의 정의에 부합하지 않을 뿐만 아니라, 사이버공격은 공격주체를 특정하기 쉽지 않아 특정 사이버공격을 '테러리즘'으로 인정하는 것에도 불확실성이 존재한다. 주요국은 이러한 한계를 이미 인지하고 있으며, 현 시점에서는 미국이 기존 테러보험 프로그램에 매몰되지 않고 동 프로그램의 범위를 벗어나 사이버리스크에 대한 보장공백을 메우는 방법을 적극적으로 탐색 중이다. 미국에서는 재난적 규모의 사이버사고, 국가 배후 사이버공격, 사이버공격으로 인한 NDBI(물적 손해를 동반하지 않은 영업중단손해) 등에 대한 정부의 재보험담보 제공을 심도 있게 검토하고 있다. 호주에서도 테러리스트의 사이버공격으로 인한 기업의 재물손해 및 영업중단손해에 대해 정부가 재보험담보 및 지급보증을 제공하는 방안이 현재 긍정적으로 논의 중인 가운데, 국가 배후 사이버공격을 포함할 수 있도록 '공격자에 상관없이 정치적·종교적·이념적 목적을 가진 악의적 사이버공격'으로 논의 범위를 확대하고 있다.

Ⅳ 결론

이 보고서는 최근 기업이 직면한 사이버리스크의 양적·질적 변화, 그로 인한 사이버보험 시장 내 수요 및 공급상의 변화와 보장공백을 분석하고, 동 보장공백에 대한 미국, 호주, 영국, 프랑스 등 사이버보험 시장을 선도하는 주요국의 대응을 검토하였다.

분석 결과, 2010년대 들어 사이버사고의 공격자는 개인 또는 범죄조직에서 국가·준정부 조직·테러조직으로, 공격동기는 호기심·금전·과시욕에서 정치적·군사적 동기로, 공격표적은 개인 또는 보안이 취약한 중소기업에서 공급망 및 산업제어시스템 공격을 통해 대기업과 국가기반시설로, 피해 유형은 정보 유출 및 개인정보 침해에서 재물·신체·영업중단 손해 등으로 확대되고, 피해 심도는 통제가능한 수준에서 파괴적인 수준으로 진화하였다. 파괴적 사이버공격의 빈도 및 심도 증가와 기업의 사이버 관련 규제리스크 증가에 따라, 사이버보험에 대한 수요도 급격히 증가할 것으로 예상된다. 사이버리스크의 양적·질적 변화에 대응해 보험업계는 사이버보험 공급에 보수적 기조를 취할 것으로 보인다. 구체적으로, ① 사이버사고의 빈도 및 심도 증가, 대재해 가능성 등에 따른 보험업계의 공급 기조 변화, ② 암묵적 사이버담보의 언더라이팅 리스크 가시화와 그에 따른 포괄위험 담보 방식 재물·배상책임보험의 사이버면책 확대 움직임, ③ 정보 유출 피해 등 배상책임과 비용보장에 집중된 단독 사이버보험의 비포괄성, ④ 2017년 낫페트야 공격으로 촉발된 국가 배후 사이버공격에 대한 재래식 전쟁면책 적용 논란과 그로 인한 보험업계의 사이버 대재해 및 전쟁면책 움직임, 그리고 ⑤ 벌금 및 랜섬담보의 반공익성에 따른 규제 강화와 동 담보 제공 자제의 움직임 등이 관찰된다. 이에 따라 사이버사고로 인한 재물 및 영업중단손해, NDBI, 신체손해, 국가 배후 사이버공격, 사이버 대재해, 그리고 벌금 및 랜섬담보에 대한 보장공백이 커질 것으로 예상된다.

이에 세계 사이버보험 시장을 선도하는 미국, 영국, 프랑스, 호주 등에서는 자국에서 이미 운영 중인 공사협력 테러보험 프로그램을 통해 '일부 사이버공격'으로 인한 손해에 대해 재보험담보 및 유동성을 제공하는 방식을 취하고 있거나 논의 중이다. 이미 테러보험 프로그램이 존재하는 상황에서는 사이버사고를 동 프로그램의 손인으로 추가하는 것이 정책적으로 가장 용이한 접근일 뿐만 아니라, 사이버리스크에 대응한 공사협력 보험 프로그

램을 새로이 구성하기에는 사이버리스크와 사이버보험 시장이 단기간에 급격하게 변하였기 때문으로 사료된다. 그러나 기존 테러보험 프로그램은 물리적 테러리즘과는 이질적인 사이버테러리즘의 특성을 반영하고 심각한 보장공백이 예상되는 사이버공격을 포섭하는데 있어 여러 난관에 직면한다. 무엇보다도 문제의 사이버사고가 테러리즘 요건을 충족해야 하므로, 인간의 실수에 의한 대규모 사이버사고, 범죄조직의 대규모 금전 목적 랜섬웨어 공격, 또는 국가 배후 사이버공격은 프로그램 적용대상에서 배제될 수 있다. 또한 국가 배후 사이버공격, 경제적 목적의 사이버공격 등은 기존 '테러리즘'의 정의에 부합하지 않을 뿐만 아니라, 공격주체를 특정하기 쉽지 않아 특정 사이버공격을 '테러리즘'으로 인정하는 것에도 불확실성이 존재한다. 주요국은 이러한 한계를 이미 인지하고 있으며, 현 시점에서는 미국이 기존 테러보험 프로그램에 매몰되지 않고 사이버리스크에 대한 보장공백 해소방안을 적극적으로 탐색 중이다. 미국에서는 재난적 규모의 사이버사고, 국가 배후 사이버공격, 사이버공격으로 인한 NDBI(물적 손해를 동반하지 않은 영업중단손해) 등에 대한 정부의 재보험담보 제공을 심도 있게 검토하고 있다. 호주에서도 테러리스트의 사이버공격으로 인한 기업의 재물손해 및 영업중단손해에 대해 정부가 재보험담보 및 지급보증을 제공하는 방안이 현재 긍정적으로 논의 중인 가운데, 보장범위에 국가 배후 사이버공격이 포함될 수 있도록 '공격자에 상관없이 정치적·종교적·이념적 목적을 가진 악의적 사이버공격'으로 논의 범위를 확대하고 있다.

자연재해나 물리적 테러리즘과 달리, 사이버사고로 인한 피해는 국경이 없고, 손해보험은 업의 속성상 활발한 국경 간 거래가 불가피한 산업이라는 점에서, 전술한 사이버보험 시장 상황이 특정 국가에 국한된 것은 아니다. 특히, 국내 사이버보험은 세계 보험시장을 선도하는 주요 국가의 보험제도 변화, 손해율, 보험요율, 인수전략 등에 상당한 영향을 받기 때문에 사이버리스크에 대한 보장공백의 문제가 특정 국가에 국한된 이슈는 아니다. 그동안 우리나라의 사후적 피해회복에 대한 정책적 접근은 개인정보유출 및 제3자에 대한 배상책임으로 국한되고, 기업의 재물 및 영업중단손해 등에 대해서는 어떠한 논의도 이뤄지지 못하였다. 사이버리스크의 양적·질적 변화에 대응하여 정부는 사전적 보안강화뿐만 아니라 사후적 피해회복을 위한 정책 방안을 선제적으로 수립해야 한다. 국내 사이버보험 시장 내 시장실패 및 보장공백에 대한 검토와 함께 국가 배후 사이버공격, 사이버 대재해 등 보장공백이 예상되는 사이버사고에 대해 정부가 직접 보험을 제공하거나 재보험·지급보증·유동성 제공을 통해 보험회사의 자본력을 제고하는 방안을 고려할 수 있다. 정부가 공급자로서 보험시장에 참여하는 구체적인 방법은 우리나라 보험산업의 인수역량에 따라

달라질 수 있으며, 보험이 정책수단으로 활용되기 위해서는 효과성뿐만 아니라, 타 정책수단 대비 비용효율성 우위 입증이 선제되어야 한다.

참고문헌

김홍근(2020),「사이버 공격자는 누구인가」,『KISA Report』, 9, 한국인터넷진흥원

송윤아·홍보배(2021),「공사협력 재난보험 프로그램 연구」,『이슈보고서』, 21-4, 보험연구원

신영웅(2020),「북한 사이버공격의 남북한 합의사항 위반 여부의 분석에 관한 연구」,『한국공안행정학회보』, 29(4), pp. 91~126

유성민(2016),「4차 산업혁명과 사이버 보안대책」,『지능화 연구 시리즈 2016』, 한국정보화진흥원

임준·이상우·이소양(2018),「디지털 경제 활성화를 위한 사이버보험 역할제고 방안」,『연구보고서』, 18-21, 보험연구원

채재병(2019),「국제 사이버공격 전개 양상 및 주요국 대응전략」,『INSS연구보고서』, 2019-18, 국가안보전략연구원

최윤성(2021),「스마트제조 및 산업제어시스템 융합보안 동향」,『주간기술동향』, 1980호, 정보통신기획평가원

AM Best(2020), "Scrutiny of Management Approach Increases as London Cyber Insurance Market Grows", *Best's Market Segment Report*, A.M. Best Company, Inc.

_____(2021), "Ransomware and Aggregation Issues Call for New Approaches to Cyber Risk", *Best's Market Segment Report*, A.M. Best Company, Inc.

AMRAE: L'Association pour le Management des Risques et des Assurances de l'Entreprise(2021), "Lumière sur la Cybersecurity"

ANSSI: Agence nationale de la sécurité des systèmes d'information(2021), "Etat de la menace rançongiciel"

Australian Government: The Treasury(2018), *Terrorism Insurance Act Review 2018*

_____(2021), "2021 Triennial Review of the Terrorism Insurance Act 2003: Consultation Paper"

Australian Government: The Attorney-General' Department(2020), "Privacy Act Review: Issues Paper"

ARPC: Australian Reinsurance Pool Corporation(2016), "Cyber Terrorism and Australia's Terrorism Insurance Scheme: Physically Destructive Cyber Terrorism Is A Gap In Current Insurance Coverage"

ARPC: Australian Reinsurance Pool Corporation and University of Queensland Australia(2020), "Analysis of Identified Gaps in Australia's Terrorism Insurance Environment"

ARPC, OECD and University of Cambridge(2020), "Insurance risk assessment of cyber terrorism in Australia"

Bateman, J.(2020), "War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions. Carnegie Endowment for International Peace"

Berliner, B.(1982), "Limits of Insurability of Risks", Englewood Cliffs, NJ: Prentice Hall Professional Technical Reference

Cartagena, S., Gosrani, V., Grewal, J. and Pikinska, J.(2020), "Silent cyber assessment framework", *British Actuarial Journal*, 25(2), pp. 1~19

Carter, R. and Enoizi, J.(2020), "Cyber War and Terrorism: Towards a Common Language to Promote Insurability", The Geneva Association

_____(2021), "Mapping a Path to Cyber Attribution Consensus", The Geneva Association

CIAB: Council of Insurance Agents and Brokers(2021), "Commercial Property/Casualty", Market Index Q2/2021

Crosignani, M., Macchiavelli, M. and Silva, A.(2020), "Pirates without Borders: the Propagation of Cyberattacks through Firms' Supply Chains", Federal Reserve Bank of New York

CSC: Cyberspace Solarium Commission(2020), "Final Report: A Warning from Tomorrow"

_____(2021), "2021 Annual Report on Implementation"

Cybersecurity and Infrastructure Security Agency(2020. 6. 23), "Guidance on the North Korean Cyber Threat"

Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., Welburn, J.W. and Winkelman, Z.(2018). "Estimating the Global Cost of Cyber Risk: Methodology and Examples", Rand Corporation

EIOPA: European Insurance and Occupational Pensions Authority(2018), "Understanding Cyber Insurance-A Structured Dialogue with Insurance Companies"

FIO: Federal Insurance Office(2020), "Annual Report on the Insurance Industry", U.S. Department of the Treasury

G7(2017), "G7 Declaration on Responsible States Behavior in Cyberspace", Group of Seven

General Secretariat of the Council of the European Union(2017), "Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities", Council of the European Union

GAO: Government Accountability Office(2021), "Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market", Report to Congressional Committee, GAO-21-477

ISO: Insurance Services Office(2013), "Commercial General Liability, Exclusion-Access or Disclosure of Confidential or Personal Information and Data-Related Liability-with Limited Bodily Injury Exception"

IAIS: International Association of Insurance Supervisors(2020), "Cyber Risk Underwriting: Identified Challenges and Supervisory Considerations for Sustainable Market Development"

L'Association pour le Management des Risques et des Assurances de l'Entreprise(AMRAE)(2021), "Lumière sur la Cybersecurity"

Le Club des Juristes(2018), “Insuring Cyber Risk”, Cyber Risk Commission Report

LLoyd’s(2018), “Cloud Down: Impacts on the US Economy”, Emerging Risk Report

Lloyd’s and University of Cambridge(2015), “Business Blackout: The insurance implications of a cyber attack on the US power grid”, Lloyd’s

OECD(2017), “Enhancing the Role of Insurance in Cyber Risk Management”, OECD, Paris

_____(2020a), “Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation”, OECD, Paris

_____(2020b), “Insurance Coverage for Cyber Terrorism in Australia”, OECD, Paris

Patel, N.(2021), “Cyber and TRIA: Expanding the Definition of an ‘Act of Terrorism’ to Include Cyber Attacks”, *19 Duke Law & Technology Review*, pp. 23~42

Plotnek, J. and Slay, J.(2021), “Cyber Terrorism-A Homogenized Taxonomy and Definition”, Computers&Security, p. 102

Pool Re(2019), “Pool Re Terrorism 2019”, Pool Reinsurance Company Ltd.

Pool Re and University of Cambridge(2017), “Cyber Terrorism: Assessment of the Threat to Insurance”, Pool Reinsurance Company Ltd.

PRA: Prudential Regulation Authority(2016), “Consultation Paper: Cyber insurance underwriting risk(CP 39/16)”, Bank of England

_____(2017a), “Cyber insurance underwriting risk: Policy Statement PS15/17 (July)”, Bank of England

_____(2017b), “Cyber insurance underwriting risk: Supervisory Statement SS4/17 (July)”, Bank of England

_____(2019), “Cyber underwriting risk: follow-up survey results(Dear CEO letter)”, Bank of England

Romanosky, S., Ablon, L., Kuehn, A., and Jones, T.(2019), “Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?”, *Journal of Cybersecurity*, 5(1), pp. 1~19

SolarWinds Corp.(2020), “United States Securities and Exchange Commission Form 8-K”

The National Insurance Brokers Association(2021. 8), “NIBA Submission Treasury ARPC Review”

U. K. Department for Digital, Culture, Media and Sport(2020), “Cyber Security Breaches Survey 2020”

U. K. Department of Health and Social Care(2018), “Securing cyber resilience in health and care”

U.K. HM Government and Marsh(2015), “UK Cyber Security: The Role of Insurance in Managing and mitigating the Risk”, Marsh LLC, Marsh

University of Cambridge(2016), “Managing Cyber Insurance Accumulation Risk Reforming Exclusions”, Carnegie Endowment for International Peace

U. S. Department of Treasury(2015), “The Process for Certifying an ‘Act of Terrorism’ under the Terrorism Risk Insurance Act of 2002”

_____(2016), “Guidance Concerning Stand-Alone Cyber Liability Insurance Policies Under the Terrorism Risk Insurance Program”, Federal Register, Vol. 81, No. 248

_____(2020a), “Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments”

_____(2020b), “Terrorism Risk Insurance Program; Updated Regulations in Light of the Terrorism Risk Insurance Program Reauthorization Act of 2019, and for Other Purposes”, Federal Register, Vol. 85, No. 218

Wrede, D., Tino Stegen and Johann-Matthias Graf von der Schulenburg(2020), “Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market”, *The Geneva Papers on Risk and Insurance-Issues and Practice*, 45, pp. 657~689

CSIS: Center for Strategic and International Studies, Significant Cyber Incidents,https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

EMSISOFT, The cost of ransomware in 2021: A country-by-country analysis, https://blog.emsisoft.com/en/38426/the-cost-of-ransomware-in-2021-a-country-by-country-analysis/

ISO: Insurance Services Office(2006), Commercial General Liability Coverage Form (CG 00 01 12 07), Insurance Services Office (ISO), http://www.tmsic.com/pdfs/CommercialGeneralLiabilityCoverageForm_OccurrenceBasis.pdf

NAIC, Uniform Property and Casualty Product Coding Matrix(effective Jan. 1. 2020), 10, https://www.naic.org/documents/industry_pcm_p_c_2020.pdf

NATO(2014), Wales Summit Declaration: issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, North Atlantic Treaty Organization, https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en

U. K. Attorney General's Office(2018), Cyber and International Law in the 21st Century, Government of the United Kingdom, https://www.gov.uk/government/speeches/cyber-and-international-law-inthe-21st-century

도서회원 가입안내

회원	연회비	제공자료	
법인 회원	₩300,000원	- 연구보고서 - 기타보고서 - 연속간행물 · 보험금융연구 · 보험동향 · 해외 보험동향 · KOREA INSURANCE INDUSTRY	영문 연차보고서 추가 제공
특별 회원	₩150,000원		
개인 회원	₩150,000원		

* 특별회원 가입대상 : 도서관 및 독서진흥법에 의하여 설립된 공공도서관 및 대학도서관

가입 문의

보험연구원 도서회원 담당
전화 : (02)3775-9113 | 팩스 : (02)3775-9102

회비 납입 방법

무통장입금
- 계좌번호 : 국민은행 (400401-01-125198) | 예금주: 보험연구원

자료 구입처

서울 : 보험연구원 자료실(02-3775-9113 | lsy@kiri.or.kr)

저자약력

송윤아 Indiana University 경제학 박사 / 연구위원
E-mail : knuckleball@kiri.or.kr

홍보배 Claremont Graduate University 경제학 박사 수료 / 연구원
E-mail : bobae.hong@kiri.or.kr

이슈보고서 2021-19

주요국 정부의 사이버보험 시장 참여 배경 및 동향

발 행 일 2021년 12월
발 행 인 안 철 경
발 행 처 보험연구원
주 소 서울특별시 영등포구 국제금융로 6길 38 화재보험협회빌딩
인 쇄 소 고려씨엔피

ISBN 979-11-89741-69-3
979-11-89741-37-2(세트)