민간항공의 사이버위협 대응을 위한 국제협약 적용에 관한 연구

A Study on the Application of International Conventions to Respond to Cyber Threats in Civil Aviation

박 만 희*

Park, Man-Hui

요 약

항공편과 승객의 흐름을 효율적으로 처리하기 위한 디지털 시스템에 대한 의존도 증가와 승객용 기내 와이파이 서비스 등으로 인해 민간항공의 사이버 보안 취약성은 매년 증가하고 있는데 비해 공항에 대한 무장 공격, 항공기에 폭발물 설치 및 납치와 같은 전통적인 테러에 맞춰 마련된 항공보안 관련 국제협약은 사이버 위협에 직접적으로 적용하기 어렵다는 문제를 갖고 있다.

본 연구는 민간항공에 대한 사이버 공격의 예방 및 기소와 관련된 국제협약의 적정성을 검토한 후, 사이버 위협 대응을 위한 기존 국제협약 체계, 잠재적 차이 해석 등을 중점적으로 분석하여 민간항공의 안전을 위협하는 불법방해행위로부터 중요정보 및 시스템을 보호하는 항공 사이버 보안 국제표준 마련 및 이행 촉진을 강조하고자 한다.

Keywords : 사이버 위협, 사이버 보안, 국제협약, 항공보안, 불법방해행위

1. 서 론

민간항공 분야에 대한 사이버 위협은 공항, 항공사, 항공기, 항공교통관제 및 항행안전시설의 시스템 및 정보 등을 목표로 운항 중인 항공기에 장애를 발생시키거나 손상을 입힐 수 있으며 인명 손실을 초래할 수 있다. 이러한 항공 시스템에 대한 사이버 공격은 기내에서 물리적으로 비행경로를 변경하는 등의 작업 없이 항공기를 납치하는 것이 가능하다는 특징이 있다.

항공분야의 사이버 공격은 다른 인프라와 다르게 많은 국가에 동시에 영향을 미칠 수 있기 때문에 국가별로 서로 다른 법체계 적용으로 관할권 문제와 국제협약 적용 차이 등 문제점을 유발하고 있다. 또한 민간항공 분야에 적용할 수 있는 많은 규제 및 법률이 존재하지만 사이버 보안에 대해서는 명확하게 다루고 있지 않은 실정이다. 이러한 민간항공 인프라의 특수성으로 인한 사이버 위험을 예방하기 위해 항공 사이버 보안에 대한 국제협약 적용의 중요성과 국제표준 마련의 시사점을 찾아보고자 하였다.

2. 항공 사이버 보안 관련 국제협약 적용

사이버 공격은 동기, 유발하고자 하는 효과, 기존의 완화 조치를 회피할 수 있는 능력 등에 따라 다양하다. 또한 새로운 능력과 기술이 개발됨에 따라 공격 방법은 시간이 지남에 따라 달라질 것이기 때문에 구체적인 사이버 위협 행위에 대한 분석과 국제협약의 적용 가능성은 민간항공의 안전에 대한 영향, 가해자의 위치, 공격 시점, 이러한 공격의 효과와 관련된 모든 요소를 확인·분석할 필요가 있다.

2.1 1963년 도쿄협약 및 2014년 몬트리올 의정서

1963년 도쿄협약은 사이버 공격이 범죄(국내 형법에 따라)이든 아니든 항공기의 안전 또는 항공기에 탑승한 사람이나 재산을 위태롭게 하거나 위험을 초래할 수 있는 행위로 간주되는 경우 적용된다. 2014년 몬트리올 의정서는 착륙국을 유효한 관할권으로 포함하도록 협약의 적용 범위를 확대하여 1963년 도쿄협약과 비교하여 사이버 공격에 대한 기소 가능성을 높임으로써 항공기에 탑승한 사이버 공격의 가해자를 기소하는 데 도움이 된다는 점에 그 특징이 있다. 그러나 적용 기준 중 하나로 가해자가 항공기에 탑승해야 한다는 점에서 사이버 공격은 원격으로 수행될 수 있다는 점을 고려할 때, 사이버 위협을 해결하기 위한 1963년 도쿄협약과 2014년 몬트리올 의정서의 적용 가능성은 제한적일 수 밖에 없는 시사점을 주고 있다.

* 평생회원 · 국토교통부 항공보안감독관 oditimes@naver.com

2.2 1970년 헤이그협약 및 2010년 베이징 의정서

1970년 헤이그협약은 탑승자가 사이버 공격을 통해 항공기를 조종하는 사이버 보안 사례에 적용될 수 있다. 다만, 실제로 헤이그협약을 적용하기 위해서는 항공기 탑승자에 의한 사이버 공격이 효과적으로 항공기의 통제로 이어졌다는 것이 입증되어야 한다. 2010년 베이징 의정서는 헤이그협약 하에서 고려되는 불법방해행위의 범위를 확대하고 사이버 공격을 보다 직접적으로 다룰 수 있는 보다 광범위한 적용을 하고 있지만, 사이버 공격이 비행 중인 항공기에 대한 불법적인 납치 또는 통제권 행사를 위한 기술적 수단이 추가되어야 한다는 것을 입증하는 것이 필요하다.

2.3 1971년 몬트리올협약, 1988년 몬트리올 보충의정서 및 2010년 베이징협약

항공기에 가해자가 탑승할 필요가 없고, 항행안전시설, 중요 비행정보 제공자 또는 공항시설에 영향을 미칠 때에도 사이버 공격이 적용될 수 있다는 특징이 있다. 2010년 베이징협약은 미수, 참여, 공모 등을 포함한 형사책임의 범위를 확대하고 있으며, 해당 국가의 영토 또는 해당 국가의 국민이 범하는 범죄를 포함하여 보다 광범위한 관할권을 포함함으로써 각 국가에 해당 범죄에 대해 범죄인 인도 아니면 소추하도록 하여 엄중한 처벌을 부과하도록 요구하고 있다.

3. 결 론

사이버 공격은 사이버 구성요소로만 이루어진 공격과 사이버 공격이 접근통제 위반으로 연결되어 물리적 구성요소와 사이버 구성요소가 결합된 사이버 공격이 존재한다. 이러한 사이버 위협에 대한 국제협약의 적용은 조항의 세부적인 적용과 관할권 문제 등 복잡하며, 사이버 공격의 행위자, 공격 및 효과는 서로 다른 국제협약의 여러 관할권을 포함할 수 있기 때문에 기소가 어렵거나 불가능한 상황을 초래할 수 있다는 특징이 있다.

항공보안 국제협약을 분석해 보면, 사이버 위협이 모든 협약에 명시적으로 언급되지는 않지만, 국제협약은 민간항공을 보호하는 것을 목적으로 하고 있기 때문에 사이버 위협을 개선하기 위한 유용한 근거를 제공하고 있는 것은 분명해 보인다. 이에 따라 ICAO는 민간항공의 중요 인프라 시스템과 정보를 사이버 공격으로부터 보호하고 사이버 보안을 협력적이고 체계적으로 개선하기 위해 항공 사이버 보안 전략을 채택함으로써 사이버 보안 법규 및 규정의 일관되고 일관성 있는 이행을 위한 기반을 마련하고 사이버 공격의 예방, 기소 및 적시 대응을 위해 지속적으로 사이버 보안을 보장하는 역할을 하고 있다.

참고문헌

Dalit Ken-Dror Feldman & Emanuel Gross (2020) Cyber Terrorism and Civil Aviation: Threats, Standards and Regulations, Journal of Transnational Law & Policy Vol. 29, pp.132~164.

U.S. Government Accountability Office (2015) Information Security FAA Needs to Address Weaknesses in Air Traffic Control Systems, GAO-15-221, pp.7~21.