Cyber-Kinetic Hijacking and International Aviation Law: Bridging the Legal Gaps in the Digital Age

Asfiya Bathul[1]

ABSTRACT

The rapid digitalization of civil aviation has exposed aircraft operations, navigation, airport infrastructure as well as air traffic management to complex cyber threats that are capable of causing physical harm. This phenomenon, described as the cyber-kinetic hijacking, challenges the adequacy of existing international aviation security conventions, which were largely developed in response to the traditional, physically executed acts of unlawful interference. This paper examines whether the current international aviation security conventions, particularly the Tokyo Convention, Hague Convention, Montreal Convention, and the Beijing Convention efficiently address cyber-kinetic hijacking. Using a doctrinal and analytical methodology, the paper analyses treaty provisions, ICAO standards, and relevant institutional practices to assess the extent to which cyber-enabled acts may be accommodated through interpretation. It argues that while certain provisions can be expansively constructed to include cyber-kinetic conduct, substantial legal gaps persist with respect to definitional clarity, jurisdiction, attribution, state responsibility, and enforcement. Addressing these issues requires a targeted four-pillar reform which is redefining unlawful seizure to encompass cyber-kinetic control, expanding universal jurisdiction over cyber-kinetic attacks on aviation, integrating cybersecurity obligations into the core aviation treaties, and establishing harmonised global standards for cyber resilience in civil aviation. Only through such a comprehensive normative recalibration can international aviation law effectively deter and respond to cyber-kinetic hijacking in the digital age.

Keywords: Cyber-kinetic hijacking, International Aviation law, Aviation cybersecurity, International Aviation Security Conventions, Unlawful interference, State responsibility.

INTRODUCTION

Civil aviation has long been considered as one of the most extensively regulated sectors of international activity, owing to its inherent transboundary nature and the potentially catastrophic consequences of security failures. Traditionally, threats to aviation security

[1] 3rd Year Law Student, School of Law, CHRIST (Deemed to be University), Bangalore.

manifested through physically executed acts such as the aircraft hijacking, sabotage, and violence on board aircraft. In response, the global community enacted a comprehensive legal framework under the supervision of the International Civil Aviation Organization (ICAO), thereby criminalizing the unlawful acts against civil aviation and establishing jurisdictional and enforcement mechanisms through conventions such as the Tokyo Convention, the Hague Convention, the Montreal Convention and the Beijing Convention.

In the last few decades, however, civil aviation has undergone a drastic digital transformation. Contemporary aircraft are no longer isolated mechanical systems but highly integrated cyber-physical platforms dependent on software-driven avionics, satellite navigation, data transfer, and automated flight control systems.[2] Air traffic management and airport infrastructure have now become increasingly dependent on the digital communication networks and information-intensive technologies. Within this constantly changing technological word, the problem of cyber-kinetic hijacking has come up as one of the major security risks. Unlike that of the traditional hijacking, which involves physical seizure of an aircraft, cyber-kinetic hijacking involves the unlawful interference through cyber means that results in tangible kinetic consequences, such as physical intrusion or conventional weapons.

This development raises a loss of aircraft control, navigation disruption, collision, or forced crashes. Even the Beijing Convention of 2010, although its broader approach to unlawful acts against civil aviation, does not expressly address cyber-enabled attacks that lack pressing legal question as to whether the current international aviation security regime is capable of effectively regulating and responding to cyber-kinetic hijacking. The prevailing conventions are still based on a twentieth-century perspective of kinetic violence, which leads to significant doctrinal ambiguities in relation to the actus reus and mens rea of cyber-enabled crimes, a fragmentation of jurisdictional and enforcement processes, and a lack of common preventive cybersecurity obligations. Although ICAO has started to address the issue of aviation cybersecurity by means of standards, guidance material, and policy initiatives, these measures have been largely viewed as soft law and hence, lacking any binding normative force.[3]

This paper examines the adequacy of international aviation law in addressing cyber-kinetic hijacking. The research is methodologically doctrinal and analytical based on the interpretation

[2] Ruwantissa Abeyratne, Strategic Issues in Air Transport 45 (Springer 2011).
[3] Id.

of treaties, institutional practice, and scholarly commentary. The paper identifies continuing legal and structural gaps in the existing aviation security framework and evaluates the extent to which the current international conventions can be interpreted in order to address cyber-based risks. It argues that while these instruments provide a solid foundation to deal with unlawful interference, they fall short of adequately addressing the unique challenges posed by cyber-kinetic hijacking. The paper ends by proposing a reform agenda in order to recognize cyber-physical threats within the definition of unlawful seizure, strengthen jurisdictional mechanisms, and develop a mandatory, ICAO-led cybersecurity regime capable of effectively responding to aviation security threats in the digital age.

CONCEPTUALISING CYBER-KINETIC HIJACKING IN CIVIL AVIATION

Cyber-kinetic hijacking refers to the unlawful seizure, manipulation, or interference with an aircraft or its safety-critical systems through cyber means that result in the tangible physical or kinetic effects.[4] The term "cyber-kinetic" depicts the dual nature of the threat: the attack originates in cyberspace but manifests in the physical domain, producing consequences functionally equivalent to that of the traditional aircraft hijacking.

In the aviation context, cyber-kinetic hijacking involves the deliberate cyber operations that remotely compromise aircraft systems or their supporting infrastructure such as air traffic control, satellite navigation, or ground operations in a manner that enables an attacker to seize control, divert, disable, or endanger an aircraft that is in service. The methods available for such attacks are varied and include, among others, hacking into flight management systems or avionics software, GPS spoofing that alters navigational data, data links manipulation, and air traffic management networks interference through the injection of false or misleading information. Moreover, cyberattacks might target terrestrial systems that are associated with the maintenance of the aircraft, the schedules of the flights, or the security of the airport, thereby extending the range and impact of the threats.

In layman's terms, cyber-kinetic hijacking is an attack on a cyber-physical system, which leads to physical changes, for instance, the aircraft deviating from its intended course, changing altitude, shutting down the engine, and even losing complete control by the pilot through the

[4] Jan Klenka, Aviation Cyber Security: Legal Aspects of Cyber Threats, 14 J. TRANSP. SEC. 89, 92 (2021).

use of attacks on information systems like avionics software or satellite navigation signals. The functional result is similar to that of a cockpit takeover but without the physical presence of an intruder.

Civil aviation has become exposed to such acts of terrorism because of its increasing dependence on networked technologies and data-driven systems. Contemporary aircrafts, air traffic control systems, and airport operations are all so tightly interconnected that besides the added benefit of efficiency, there is also a large area opened up for cyber exploitation. A successful hijacking involving cyber-kinetic capabilities could result in a whole spectrum of different negative consequences, including but not limited to the interruptions of flight operations, large-scale financial loses, people's lives, and real estate being damaged hugely. Among the things that could cause such attacks are the goals of terrorists, cyber wars that are meant to destroy a nation's aviation infrastructure, or even ordinary crime like extortion and stealing cargo.

The technological intricacy of the cyber-kinetic hijacking is only one of its aspects; another is the legal uncertainty that it raises. The primary response of the international aviation security conventions were acts of violence, seizure, and sabotage through physical means, almost always through the presence of a hijacker on board an aircraft or the use of conventional weapons. Decoupling the physical presence of control, Cyber-kinetic hijacking challenges these basic assumptions. The disconnect between the two physical controls creates a new area of marshalling and legal ambiguity and also puts forth the very basic questions if the concepts of “hijacking” and “unlawful seizure” can be given such interpretation in the case of digital activities that yield similar physical results. Cyber-kinetic hijacking, therefore, becomes a new area of law and of security where the old traditional aviation law conflicts with the new need of digital world.

HISTORICAL FOUNDATIONS OF INTERNATIONAL AVIATION SECURITY CONVENTIONS

The global legal framework for aviation security describes “Chicago architecture” and is mainly built on the Convention on International Civil Aviation (1944) (Chicago Convention) and a group of various treaties recognized by the International Civil Aviation Organization (ICAO) with the help of multilateral agreements. The Chicago Convention, which regulates

international civil aviation, sets out key principles such as State sovereignty over the airspace above their territory (Article 1).[5] Furthermore, it requires ICAO to create Standards and Recommended Practices (SARPs) for the safe, secure, and orderly growth of international civil aviation. The Chicago Convention is not primarily a security treaty; however, it still provides the institutional and normative frameworks within which aviation security law has been developing.

The substantive international regime addressing unlawful acts against civil aviation is primarily contained in the so-called quadrilateral aviation security conventions: the Tokyo Convention (1963), the Hague Convention (1970), the Montreal Convention (1971), and the Beijing Convention and Protocol (2010). Each instrument reflects the dominant security threats of its time and collectively illustrates the gradual expansion of international concern from in-flight misconduct to sophisticated forms of unlawful interference.

The Tokyo Convention (1963) was the first international instrument to address offences committed on board aircraft.[6] It gives priority to the actions that put people's or property's safety at risk during the flight and it confirms the power of the aircraft commander to restrain the troublemakers. The jurisdiction under the Convention is mainly given to the State of registration, with only minor duties imposed on the State of landing and the State of the offender's nationality. The scope of the Convention, however, is basically on the behavior of the people on board and does not directly imply any of the matters related to the hijacking of the aircraft or the use of aircrafts as weapons.

This limitation underwent a change with the Hague Convention (1970), which, in its very first Article, categorically pronounced the unlawful takeover of an aircraft in flight as a separate international crime. Article 1 comes with a definition of hijacking as the illegal taking over or control of an aircraft by using force, threat, or any other means of intimidation by someone aboard the aircraft.[7] The Convention is clearly written in such a way as to consider the case of an actual hijacker being physically present who takes over the plane by using force against the flight crew. In terms of jurisdiction, it follows the aut dedere aut judicare principle requiring

[5] Convention on International Civil Aviation art. 1, Dec. 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295.
[6] Convention on Offences and Certain Other Acts Committed on Board Aircraft, Sept. 14, 1963, 20 U.S.T. 2941, 704 U.N.T.S. 219.
[7] Convention for the Suppression of Unlawful Seizure of Aircraft art. 1, Dec. 16, 1970, 22 U.S.T. 1641, 860 U.N.T.S. 105.

States to either prosecute or deport the alleged offenders to their home country if they have committed an offense in the territory of that State.[8] Although it was a landmark change in the area of aviation security law, the definition of hijacking still very much depends on physical presence and coercion.

The Montreal Convention (1971) continued to broaden the definition of acts which, though not directly related to aviation, might still endanger the safety of international civil aviation.[9] These include the destruction of an aircraft in flight, damage making an aircraft incapable of flight, and blocking the air navigation facilities. Among other things, the Convention also prohibits the use of the aircraft in order to commit murder, seriously injure or cause the loss of property or damage to the environment, even if the crime is not happening on board the plane. Although not drafted with cyber threats in mind, the Montreal Convention offers limited scope for analogical extension to cyber-enabled interference with aviation infrastructure.

The Beijing Convention and Protocol of 2010 represent the most comprehensive attempt to modernise the international aviation security regime.[10] The new regulations combat the dangers by making the use of planes as weapons, dropping poisonous or radioactive materials from airplanes, and telling lies about the safety of an airplane in the air, all their respective crimes. Among this, the inclusion of false information offenses is particularly significant as it recognizes that the modification of data and information systems can indeed compromise aviation safety.[11] The Beijing instruments do not directly cover cyber-attacks but they do create a conceptual basis for the interpretation of certain cyber-enabled acts, like the sending of false navigational data or the manipulation of air traffic control systems, as falling under the existing treaty framework.

Despite this gradual expansion, none of the core aviation security conventions expressly define or address cyber-attacks against aircraft or aviation infrastructure. Any attempt to bring cyber-kinetic hijacking within their scope relies on interpretive extensions that remain uncertain and uneven across States. In parallel, ICAO has sought to address aviation cybersecurity through

[8] Cheryl Esquerra-Abella, The Extradition Of Aircraft Hijackers 12-15 (2010).
[9] Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, Sept. 23, 1971, 24 U.S.T. 565, 974 U.N.T.S. 177.
[10] Ruwantissa Abeyratne, The Beijing Convention of 2010 on the Suppression of Unlawful Acts Relating to International Civil Aviation, 4 J. TRANSP. SEC. 131, 133 (2011).
[11] Jiefang Huang, Aviation Safety through the Rule of Law: ICAO's Mechanisms and Practices, 22 KLUWER LAW INT'L 101 (2009).

Annex 17 to the Chicago Convention and policy instruments such as the ICAO Cybersecurity Strategy.[12] Consequently, while the historical framework of international aviation law provides a foundational response to unlawful interference, it remains ill-equipped to comprehensively address cyber-kinetic threats in an increasingly digitalised aviation enironment.

DOCTRINAL AND STRUCTURAL GAPS IN INTERNATIONAL AVIATION LAW

Cyber-kinetic hijacking brings to light some very basic doctrinal and structural weaknesses in the present international aviation security system. The aviation security treaties have changed to some extent according to the new threats but their relevance to the cyber-enabled disruption of aircraft and aviation facilities is still unclear and uneven. The above-mentioned weaknesses result from the non-existence of cyber-related definitions, unclear interpretation of treaties, problems regarding the allocation of judicial power and identification of the offenders, and the current system's limited ability to prevent and enforce.

Absence of Cyber-Specific Definitions and Conceptual Ambiguity

One of the main drawbacks of the current structure is the lack of a universally accepted definition of cyber-hijacking or cyber-enabled unlawful interference with civil aviation. Cyber intrusion, digital seizure, and remote manipulation of aircraft systems are not mentioned in any of the key aviation security conventions. This vagueness in the law has led to different interpretations in different States regarding the classification of cyber-kinetic hijacking under existing treaty provisions, thereby sowing confusion and hindering consistent application.

According to the Hague Convention (1970), “unlawful seizure” refers to the force, threat, or intimidation that a person on board the aircraft uses to take control of an aircraft in flight or to seize the aircraft. A cyber-kinetic attacker who operates remotely and does not physically present on board does not match this definition very well.[13] A teleologic interpretation could possibly view the term “control” to encompass the digital domination that is effective over aircraft systems, but the clear stipulation of the offender being “on board” reveals a physical paradigm that makes the application of the Hague Convention to such a case of cyber-kinetic hijacking legally precarious.

[12] ICAO, Annex 17 to the Convention on International Civil Aviation: Security (12th ed. 2022).
[13] Brian F. Havel & John Q. Mulligan, The Future of International Civil Aviation Law, 24 WM. & MARY BILL RTS. J. 75, 78 (2015).

The Montreal Convention (1971) lends a somewhat broader interpretation that is more easily applied to the aspect of illegal aircraft seizure involving computer methods. Article 1 criminalises the destruction of an aircraft in service, damage rendering it incapable of flight, and interference with air navigation facilities that endanger aircraft safety. Importantly, Article 1(2) criminalises the use of an aircraft in service to cause death, serious injury, or significant damage, whether the act is committed "on board" or "otherwise". In this way, remote attacks can be included and it is also possible to consider the cyber-kinetic hijacking as such, which would cause devastating physical destruction. Likewise, the deliberate cyber disruption of satellite positioning systems or air traffic control networks might not be regarded as interference with the means of air navigation. Nevertheless, the Montreal Convention's applicability is still dependent on the presence of manifest damage or injury.[14]

The Beijing Convention and Protocol (2010) take the modernization of the legal framework a step further by including among the criminalized acts the use of an aircraft as a weapon, the releasing of dangerous materials, and the informing about aircraft safety that constitutes further risk, thereby causing an airline to be misled. The including of wrong information-related offenses is very significant with regard to the online world, as it to a certain extent, admits the dangers due to the manipulation of information. Yet, even the Beijing instruments do not go so far as to include the act of computer hacking into avionics and air traffic systems or the like as an independent offense, thus there are major gaps in the case of cyber-seizure that does not result in immediate physical injury.

Regulatory Blind Spots for High-Risk Non-Kinetic Cyber Intrusions

One of the main drawbacks of the current treaty system is that it only deals with crimes that have resulted in death, injury, or major damages. But, in the case of cyber-kinetic hijacking, it could be the scenario that there are high-risk cyber intrusions where the offender is able to take full or partial control of the airplane through digital means with no physical consequences. For instance, breaking into a flight management system or feeding incorrect navigational data that is later corrected by pilots or automated systems may not cause the levels of destruction, damage, or injury necessary for the conventions' application. So, even though the situation is very dangerous, such acts might not be punished under the law which indicates a significant gap in aviation security law.

[14] Paul Stephen Dempsey, Public International Air Law 612 (McGill-Queen's Univ. Press 2008).

Mens Rea Limitations and Misalignment with Cyber Threat Motivations

Aircraft security related international treaties have generally adapted the mens rea prerequisites to consist of and be limited to the traditional unlawful acts of hijacking, sabotage or terrorism, often inferring the intention to take control, destroy the plane or cause a large number of casualties. On the other hand, cyber-kinetic assaults could be motivated by several purposes like spying, interfering, forceful measures, ransomware, or destabilization of the opponent's strategy and among others. Oftentimes, such intentions are not in absolute alignment with the mental state conditions of the existing treaty offences which leads to complex cases and less prevention.

Jurisdiction, Attribution, and Enforcement Gaps in a Borderless Domain

The cyber-kinetic hijacking has revealed the enormous inadequacies of jurisdiction and enforcement in the international aviation security system that is in place today. The problem comes from the borderless, decentralized nature of cyberspace that is not compatible with the aviations law model based on territorial jurisdictions. The main air security treaties, the Tokyo, Hague, Montreal, and Beijing instruments give the right to judge mainly to the country where the aircraft is registered, the country of landing, the country of the offender's nationality, and the territory where the crime took place. This arrangement works well for the physically carried out unlawful interferences but its use in cyber-attacks is very questionably effective.

In the case of a cyber-kinetic hijacking, the attacker can be in one country, the airplane that is the target can be registered in a different country, the flight might be in the airspace of several countries, and the cyber intrusion might be going through different servers and networks in various jurisdictions. The harmful effects of the attack as a loss of control, navigational disruption, or forced diversion may occur in the airspace of the country that has not either hosted the attacker or provided the technological infrastructure used for the attack. Thus, it is a legal question that has to be solved when it comes to where a cyber-kinetic offence is "committed" for jurisdictional purposes.

Jurisdiction might be asserted by both the registration State and the State where the aircraft lands according to the Hague and Montreal Conventions. However, On the other hand, the state where the cyber-attack originates or the intermediate states involved in the technical routing of the attack may not have a clear jurisdictional tie-up under the existing treaty provisions. This

fragmentation results in a scenario where the law is not applied and practically speaking it may be possible for cyber-kinetic hijackers to be operating from jurisdictions that are not willing or able to exercise their criminal jurisdiction effectively giving rise to safe havens for cyber-enabled unlawful interference with civil aviation.

The State of registration plus the State where the aircraft lands could claim their jurisdiction rights under the Hague and Montreal Conventions however, the State where the cyber-attack comes from together with the intermediate States where the attack is technically routed might not have any jurisdictional connection at all according to the existing treaties. This fragmentation is the cause of enforcement gaps and may even in reality let those who are behind cyber-kinetic hijacking acts to operate from the jurisdictions that are not willing or able to exercise criminal jurisdiction thus effectively giving rise to cyber-enabled unlawful interference with civil aviation being conducted in safe havens.

Attribution difficulties are among the reasons why these jurisdictional challenges arise. Cyber-attacks are frequently anonymous, executed remotely, and hidden behind several layers of digital infrastructure, thus making it hard to point out individual wrongdoers or draw a sufficient connection between the action and a State.[15] Attribution, while being a requirement for both criminal prosecution and the claiming of state responsibility under general international law, is not addressed by the aviation security conventions which therefore do not provide any standards for attribution or any thresholds for evidence in case of cyber scenarios.[16] This lack of guidance contributes to the weakening of both accountability and enforcement.

The enforcement mechanisms under the aviation security conventions are also limited in the same way. The Hague Convention's aut dedere aut judicare requirement obliges States to either carry out a trial or surrender to another jurisdiction the suspected criminals found in their territory. Nevertheless, this principle's potency is solely contingent upon the concurrence of the State where the culprit is present. If the cyber-kinetic hijacking case is associated with or has taken refuge in the territory of a State that is lacking in domestic cybercrime legislation, technical capacity, or political willingness to cooperate, then effectively, neither trial nor

[15] David E. Graham, Cyber Threats and the Law of War, 4 J. NAT'L SEC. L. & POL'Y 87, 91 (2010).
[16] Eric Talbot Jensen, Cyberattack Attribution Matters Under Article 51 of the U.N. Charter, 36 BROOK. J. INT'L L. 1, 5 (2010).

extradition can happen.[17] No forceful means of enforcement through conventions exist to deal with such situations of non-cooperation.

The jurisdictional and enforcement situation of international civil aviation law, therefore, is based on a thinking of the twentieth century that wrongly assumed that civil aviation unlawful acts would be bound by territory and would be physically observable. Cyber-kinetic hijacking totally contradicts this assumption as it cuts off the traditional connection between the physical location of the crime, its commission and control of the aircraft. The legal fragmentation that arises as a result significantly reduces the deterrence of transnational cyber-kinetic threats.

One potential response to this enforcement deficit lies in the clarification or expansion of universal jurisdiction for core cyber-kinetic acts against civil aviation. In both customary international law and existing aviation security treaties, offences such as aircraft hijacking and the destruction of aircraft in service are treated as crimes of international concern, permitting prosecution by any State regardless of where the offence occurred. Explicitly recognising cyber-kinetic hijacking that results in the unlawful seizure or use of an aircraft in service as a basis for universal jurisdiction would close jurisdictional loopholes, eliminate safe havens, and strengthen deterrence.[18] However, such an approach would require clear treaty-based recognition, which is currently absent from the international aviation security regime.

Reliance on Soft Law and the Absence of Preventive Cyber Obligations

Finally, the existing aviation security regime remains overwhelmingly reactive, prioritising offence and punishment over prevention, resilience, and shared responsibility. None of the aviation security conventions impose explicit obligations on States to maintain cyber-security standards for aircraft systems, air traffic management networks, or aviation infrastructure. They also do not set up any compulsory information sharing, technical co-operation, or joint reaction to cyber-kinetic incidents mechanisms.

Although ICAO has tried to tackle the issue of cybersecurity in aviation through the interpretation of the Convention and policy measures like the ICAO Cybersecurity Strategy, these actions mainly function as soft law. The lack of bindingness naturally affects the manner

[17] Stephan Hobe, Air Law 145 (Columbia Univ. Press 2019).
[18] Eugene Kontorovich, The Piracy Analogy: Modern Universal Jurisdiction's Hollow Foundation, 45 HARV. INT'L L.J. 183, 186 (2004).

in which they are enforced and leads to varying levels of implementation among States that, in turn, contributes to the problem of regulatory fragmentation that the aviation industry is already facing.

Interim Assessment

The combination of these factors reveals that the present-day international aviation security framework, while being fundamental, was not intended to cater to the realities of cyber-kinetic hijacking. The lack of cyber-specific terms, the confusion over interpretation of treaties, jurisdiction and attribution problems, and no compulsory preventive measures taken together weaken the international aviation law's ability to counteract the cyber-enabled threat effectively. This structural inadequacy emphasizes the necessity of bringing about legal reforms that are specially aimed at when the aviation security laws would be considered unfit due to the digital age.

ICAO SOFT-LAW GOVERNANCE AND THE LIMITS OF CYBER-CRIME FRAMEWORKS

The International Civil Aviation Organization (ICAO) has increasingly viewed the troubled civil aviation industry suffering from cybersecurity weaknesses as a challenge. Consequently, ICAO has enacted a variety of policies, adopted standards, and provided guidance materials to enhance the security of aviation against cyberattacks, especially by the introduction of these measures under Annex 17 to the Chicago Convention and the ICAO Cybersecurity Strategy.[19] The mentioned initiatives highlight a considerable change in institutional awareness of cyber-enabled threats to aviation safety as they go through risk management, information sharing, capacity building, and protection of critical aviation systems.

Nonetheless, the cybersecurity measures of the organization remain to be soft-law-regulated predominantly. While Annex 17 gives States binding obligations concerning aviation security, their implementation is mainly left to the States because the provisions concerning cybersecurity are of vague and adaptable nature. The ICAO Cybersecurity Strategy and related guidance documents are made explicit as being non-binding and they depend on voluntary compliance.[20] Therefore, these instruments have no enforcement mechanisms and do not

[19] ICAO, Annex 17 to the Convention on International Civil Aviation: Security (12th ed. 2022).
[20] ICAO, Aviation Cybersecurity Strategy (Doc 10118) (2019).

impose a uniform legally binding obligation on the parties to prevent, detect, and respond to Cyber-kinetic hijacking. Hence, this makes the effectiveness of the ICAO, Cybersecurity approach heavily reliant on the technical capacity, political will, and regulatory maturity of the individual countries, thus resulting in uneven and fragmented regulation.

In parallel, international cyber-crime conventions provide a complementary legal framework for addressing the cyber means employed in cyber-kinetic hijacking. Instruments such as the Council of Europe Convention on Cybercrime (2001) and the forthcoming United Nations Convention against Cybercrime (2024) criminalise core cyber offences, including illegal access, illegal interception, data interference, and system interference.[21] These provisions may be invoked to prosecute the technical components of cyber-kinetic attacks against aircraft avionics, flight management systems, or air traffic management networks. For instance, a hacker who gains unauthorised access to an aircraft's Flight Management System or interferes with air traffic control data in a manner that endangers flight safety may fall within the scope of "system interference" or "serious damage" under cyber-crime law.

Besides, the aforementioned essential international cooperation methods of mutual legal assistance, extradition, and evidence sharing, the cyber-crime conventions provide important procedural tools to the law enforcement agencies. They are very much needed when it comes to investigating the transnational cyber-kinetic incidents. In this connection, the treaties against cyber-crime provide the means to overcome some of the difficulties associated with the enforcement and collection of evidence that are caused by the borderless nature of cyberspace. However, it would be a mistake to think that the international agreements regarding cyber-crime would be the only or the best solution to the problem of cyber-kinetic hijacking.

First, traditional cyber-crime law is primarily concerned with protecting the confidentiality, integrity, and availability of information systems, rather than with the kinetic consequences of cyber operations.[22]

Second, cyber-crime conventions lack aviation-specific norms tailored to the unique risks of cyber-kinetic hijacking. They do not define or prioritise the protection of critical aviation

[21] Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185 [Budapest Convention].
[22] Orin S. Kerr, Cybercrime's Scope: Interpreting 'Access' and 'Authorization', 78 N.Y.U. L. REV. 1596, 1602 (2003).

systems, allocate responsibilities among States for safeguarding such systems, or impose obligations to prevent and respond to cyber-attacks that threaten the safety of international civil aviation.

There is a risk that cyber-kinetic hijacking could be treated merely as a case of cybercrime by the States, thus failing to consider its significant effects on aviation safety, international transport security, and international peace and security, if the aviation security law and cyber-crime law were not integrated.

On the other hand, the global reach of cyber-crime conventions is still not fully uniform worldwide. The Council of Europe Convention on Cybercrime, for example, is considered to be a regional treaty since it was not universally ratified, while the UN Convention against Cybercrime, which was supposed to provide a global comprehensive framework, is still far from being widely adopted and effectively implemented.[23] The situation is not only fragmented but also prolongs the inconsistency and unpredictability of legal responses to cyber-kinetic hijacking.

The trend towards reliance on ICAO soft-law mechanisms and general cyber-crime conventions taken together reflects a regulatory gap at the junction of aviation security and cybersecurity. Although these instruments support the process and are very important in their own right, they cannot replace the need for a dedicated and binding international legal framework that is capable of addressing the peculiar cyber-physical character of cyber-kinetic hijacking. Thus, the gap intensifies the need for normative reform that marries aviation-specific security obligations with strong cyber-law principles.

TOWARDS A REFORMED INTERNATIONAL FRAMEWORK FOR AVIATION CYBERSECURITY

The previous analysis has clearly shown that the current international aviation security system, although it is the basis, is not able to cope with the new and different difficulties that cyber-kinetic hijacking presents. The cyber-physical character of such attacks reveals gaps between the doctrines, jurisdictions, and enforcement which cannot be solved by merely increasing the

[23] Jonathan Clough, Principles of Cybercrime 31 (Cambridge Univ. Press 2015).

existing interpretations. A mix of interpretative changes, institutional support, and reforms in the law will be necessary to overcome these shortcomings.[24]

To begin with, until a comprehensive reform is accomplished, the interpretations of the existing aviation security conventions should be such that they would include cyber-physical interference that leads to either the effective possession of an airplane or its safety risk. Words like "unlawful seizure," "exercise of control," and "interference with air navigation facilities" should be defined in a functional manner rather than in just physical terms, so that cyber-kinetic actions that have kinetic effects can be covered by the existing treaties. Though this interpretation will not clear all the uncertainties, it still provides a temporary way of improving the legal system's responsiveness.

Second, the ICAO's institutional mandate concerning aviation cybersecurity should be made more powerful. The danger created by cyber-kinetic hijacking is systemic and global, which is why the International Civil Aviation Organization (ICAO) should be allowed to issue laws regarding the protection of critically important aviation systems, incident reporting, information sharing, and coordinated response mechanisms, which would be considered as binding standards and practices (SARPs) for cyber security specifically for these areas. Binding standards would promote harmonisation, reduce regulatory fragmentation, and enhance collective resilience.

Third, and most importantly, the international community should consider the adoption of a dedicated protocol or convention on aviation cybersecurity. The definition of cyber-kinetic hijacking, along with the description of other cyber-enabled unlawful acts, should be included in such an instrument together with jurisdictional bases in cyber contexts, standards for attribution and state responsibility, and the extension of universal jurisdiction to the most serious cyber-kinetic offences against civil aviation. A new treaty would link the two different domains of law, that is, aviation security law and cyber law, and this would mean that the cyber-physical threats would be tackled in a coherent and comprehensive way.

[24] Ruwantissa Abeyratne, The Digitalized Aircraft: Safety and Security Issues, 12 J. TRANSP. SEC. 55, 59 (2019).

INDIA'S AVIATION CYBERSECURITY FRAMEWORK: A DOMESTIC PERSPECTIVE

From a domestic perspective, security measures for aviation in India are still mostly focused on traditional and physically executed threats. The Aircraft Act of 1934 along with DGCA's directions and rules basically cover the topics of airworthiness, safety, and physical security.[25] Although the mentioned acts create a very strong rule-making environment for the usual aviation activities they do not include cybersecurity concerns very well and that's besides the fact that these concerns can be aircraft systems, air traffic management, or aviation infrastructure.

India has been successful in the creation of a national cybersecurity framework through the establishment of policies and institutions dedicated to the protection of critical information infrastructures.[26] Nevertheless, aviation-related cybersecurity regulation remains scattered and lacking development, with only a little integration made between general cyber law and aviation regulation specific to the sector.[27] This results in regulatory blind spots in the handling of cyber-kinetic threats whose nature is closely linked to flight safety and international obligations of aviation.

The Indian experience highlights the need for wider synchronization between domestic aviation law and international cybersecurity standards which are starting to emerge. India, being one of the fastest-growing aviation markets in the world, is in a strategic position to both support the development of universal norms and at the same time, keep its domestic law up to date with the threats posed by cyber-physical attacks.[28] Finally, the action of synchronizing national laws with the changing international aviation security standards would not only make India's aviation more resilient but also help in a global way through coordinated and legally strong measures against the cyber-kinetic hijacking issue.

CONCLUSION

Cyber-kinetic hijacking is a new and major hazard to civil aviation, as it has the potential to take control of safety-critical aviation systems through a digitally enabled and remote act

[25] Aircraft Act, 1934, No. 22, Acts of Parliament, 1934 (India).
[26] National Cyber Security Policy, 2013 (India).
[27] K.V.K. Santhy, Cyber Security Challenges in the Aviation Sector, 3 INT'L J. PUB. L. & POL'Y 1, 4 (2020).
[28] DGCA, Annual Report 2024-25, 12-15 (2025).

instead of a physically executed one.[29] Thus, it unveils the weaknesses of international aviation security law that was developed based on physical presence, kinetic violence, and territorial enforcement methods.

According to the existing framework of the Tokyo, Hague, and Montreal Conventions, even if one takes into account the Beijing Protocol and the Chicago Convention regime, one can only find fragmented and incidental coverage of cyber-enabled attacks. While some cyber-kinetic incidents might be treated as cyber-enabled attacks, the existing legal instruments lack the capability to address key characteristics of such attacks like the absence of offenders on board, the potential of harm without physical destruction, and the existence of cyber-specific intent. Jurisdictional rules further compound these deficiencies, as territorially anchored enforcement mechanisms struggle to respond to borderless and anonymised cyber operations. If the cyber-kinetic hijacking is treated only within the scope of general cyber-crime frameworks, it would be a case of underestimating the gravity of the threat to the safety of international aviation.

Dealing with these issues means an international aviation law that all countries will use to gradually evolve together. The unlawful seizure situation must be clearly stated and there is to be no doubt that it includes the remote digital control over the planes and the aviation infrastructure. Serious cyber-kinetic attacks should be subjected to universal jurisdiction so that the courts where the perpetrators can escape prosecution will not exist, and ICAO has to go further than simply promoting the idea of developing binding, harmonised cybersecurity standards that will be applicable not just to the aircraft but also to air traffic management and ground-based systems, across the world.[30]

In the end, protecting civil aviation during the digital era is going to be a hard task that cannot be accomplished by merely a legal interpretation of the old treaties.[31] It is of necessity the explicit acknowledgment of cyber-kinetic hijacking as a separate security threat that would be accompanied by legal reform, institutional enforcement, and international cooperation which lasts. If not, then the international aviation law will be in danger of being very much out of touch with the technical reality that it wants to control.

[29] Supra *note* 3.
[30] ICAO, Res. A41-19: Consolidated Statement of Continuing ICAO Policies Related to Aviation Security (2022).
[31] Supra *note* 1.