International Civil Aviation Organization

LC/39-WP/2-5[1]
10/5/24

WORKING PAPER

LEGAL COMMITTEE – 39TH SESSION

(Montréal, 25 – 28 June 2024)

Agenda item 2: Consideration of the General Work Programme of the Legal Committee

ACTS OR INFRINGEMENTS OF CONCERN TO THE INTERNATIONAL CIVIL AVIATION COMMUNITY, INCLUDING CYBER THREATS, FOR WHICH PROVISION IN THE CURRENT INSTRUMENTS OF AIR LAW MAY BE INADEQUATE

(Presented by the Dominican Republic)

1. BACKGROUND

1.1 The 41st Session of the ICAO Assembly determined that certain acts or crimes of concern to the international civil aviation community, including cyber threats, may not be adequately covered by the existing instruments of air law; the approach to those threats has therefore focused on legal work on cybersecurity. It is our understanding that the efforts made in this regard in recent decades have always involved adapting to current problems. In 2022, the Secretariat presented a report of the Research Subgroup on Legal Aspects to the 38th Session of the Legal Committee, meeting in Montreal, in which it was stated that the existing framework of international air law was partially adequate to address cyber threats against civil aviation.

1.2 Subsequently, in the Proceedings of the Civil Aviation Legal Advisers Forum (16 and 17 May 2019), Singapore presented findings and recommendations to the effect that the "challenges and vulnerabilities related to cybersecurity and cyber safety are side products of the digital era. This is an issue that is not limited to aviation activities, but to all activities in our society. Consequently, also from the legal perspective, aviation can be addressed in the same manner as other sectors". No resources should be spared in addressing the cyber challenges facing civil aviation security. The focus must be holistic, so that measures are deployed in all sector-related fields. Failing that, more legal gaps will emerge.

1.3 We agree with the 2019 ICAO Aviation Cybersecurity Strategy: "The principal aim of international, regional and national legislation and regulation on cybersecurity for civil aviation is to support the implementation of a comprehensive Cybersecurity Strategy to protect civil aviation and the travelling public from the effects of cyber-attacks." The Strategy further provides that States "must ensure that appropriate legislation and regulations are formulated and applied, in accordance with ICAO provisions, prior to implementing a national cybersecurity policy for civil aviation". Noteworthy progress has obviously been made in technology and therefore in aviation. It therefore follows that every State has taken measures related to digital transformation, cyber attacks, cyber threats, privacy and data protection; it also follows that in some cases it may not be necessary to amend the national and international guidance, guidelines, policies and regulations covering the inclusion of cybersecurity-related aspects, specifically in operational and aviation safety.

[1] Spanish version provided by Dominican Republic.

1.4 Under the 2022 ICAO Cybersecurity Action Plan, for its part, "States are encouraged to evaluate their existing national legal frameworks in the field of cybersecurity and civil aviation in order to determine existing gaps, as well as to ensure appropriate legislation and regulations are in place for specific civil aviation cybersecurity elements. Another key component is the enforcement mechanism that States are encouraged to implement, if it does not already exist in their national legal frameworks, for the criminalization and prosecution of unlawful acts against civil aviation committed using cyber means."

2. ANALYSIS

2.1 In 2019, through the ICAO Cybersecurity Strategy, States were directed to consider whether their respective national legislation should be updated and therefore whether they should adopt new national legislation to enable the prosecution of terror-related cyber attacks and attacks adversely affecting civil aviation. Relevant laws and regulations undoubtedly exist. However, given that, in law, it is crucial to define offences if the relevant sanctions are to be correctly implemented, there is an urgent need for States to have clear and uniform guidelines. It is not enough simply to recognize the importance of cybersecurity in international civil aviation. Guidelines have been issued, but technology evolves faster than we do and we are still trying to catch up with current developments. The time has come to establish the legal obligations and responsibilities of States in this area.

2.2 Although there are voluntary, non-binding standards and non-voluntary, binding standards, such as those provided in Annex 17; it is necessary to establish how to apply the principles of international law in this regard and at the same time be more thorough in the nation's norms. The current limitations, whether legislative or technological of each nation, do not allow us to see beyond the probabilities of threats to situations considered to be remedied.

2.3 In the Dominican Republic, legislation such as Law No. 53-07 (2007) covers high-tech crimes and offences. However, we consider that the cyber threats to civil aviation that arise or may arise in the future are not necessarily covered or defined in the Law or in our Penal Code. We refer here to cyber terrorism and cyber espionage, and to attacks on critical infrastructure. In addition, most of the cases taken up by the Public Prosecutor's Office involve public enforcement of private complaints, i.e. the person affected has to file a complaint and work with the Public Prosecutor's Office throughout the proceedings, which can mean that the accused goes unpunished. The definitions must be such that any case taken up is purely and simply public.

2.4 Regulatory bodies tend to classify threats and/or flaws in information and communication (ICT) or operational technologies. Certainly, there has been an obvious focus in recent decades on ICT security in all administrative and technical matters. However, this is not the case for operational technologies, given that the implementation of certain safeguards comes at the cost of their efficient operation in areas such as air navigation and flight rules; the question of effectiveness versus safety is a matter of constant debate.

2.5 The Dominican Republic took measures in line with its Constitution, specifically Article 260, to ensure that technological developments and their impact on civil aviation do not put security at risk, indicating that "high priority national objectives are: to combat transnational criminal activities that put the interests of the Republic and its inhabitants in danger; to organize and sustain effective systems that prevent or mitigate damages caused by natural and technological disasters."

2.6 Subsequently, Decree No. 230-18, published on 19 June 2018, established the National Cybersecurity Strategy 2018–2021 and created the National Cybersecurity Centre. The Cyber Incident Response Team (CSIRT-RD) serves as a nationwide point of contact for the prevention, detection and management of incidents affecting government information systems and critical infrastructure.

2.7 In 2024, a bill on the comprehensive management of cybersecurity in the Dominican Republic, currently before the Congress of the Republic, aims to strengthen the regulatory framework for the cybersecurity management of public administration ICT infrastructure and critical infrastructure across the country. Once the bill has been approved, the National Cybersecurity Council will be formed as the collegiate body and highest authority of the National Cybersecurity Centre, in charge of establishing and directing policies for the management of cyber issues relating to public administration ICT infrastructure and critical infrastructure.

2.8 This bill recognizes the principles set out on 12 November 2018 in the Paris Call for Trust and Security in Cyberspace and in the November 2019 final report of the Global Commission on the Stability of Cyberspace. It covers, without distinction, the principles of mutual assistance, prevention of illicit activities, exchange of information, protection of human rights and protection of critical infrastructure, among others.

2.9 It is important to specify that, although the National Cybersecurity Centre has existed since 2018, under the bill it would be attached to the Ministry of the Presidency as a public law entity with legal personality and functional, budgetary, administrative, technical and fiscal autonomy; the aim is to give the Centre greater independence in the execution of its functions.

2.10 Likewise, the bill discusses critical infrastructure and information on cybersecurity incidents, namely how they are to be recognized, the framework according to which they will be designated, the corresponding administrative procedures and a risk analysis. It defines significant cyber impacts and the system of penalties. The bill endeavours to cover points that have so far not been considered.

3. CONCLUSION

3.1 Obviously, successful action in the face of cybersecurity threats and incidents must be predicated on a framework that regulates the adoption of preventive measures, the management of effective responses and the regulation of the respective infrastructure. We face a situation that will affect everyone and everything – this is how it must be confronted. The Dominican Republic sees cybersecurity as a matter of national security and has therefore taken the corresponding measures.

3.2 We encourage other States that have yet to take such action to do so with similar enthusiasm. We recommend that all States that have not reflected on the matter evaluate their penal, criminal and procedural legislation, considering this type of crime as a public act against national security. We also urge that criminal offences such as cyber terrorism and cyber espionage be updated and included, so that they can be prosecuted and properly defined for the protection of aviation security, both nationally and internationally. The terminology should also be broadened to include the new types of cyber attack and cyber threat that have arisen in the past decade.

— END —