Politeja
No. 4(79), 2022, pp. 55-71
https://doi.org/10.12797/Politeja.19.2022.79.04

Briony CALLANDER
University of South Wales
briony.callander@southwales.ac.uk

Christian KAUNERT
Dublin City University, University of South Wales
christian.kaunert@dcu.ie, christian.kaunert@southwales.ac.uk

TECHNOLOGICAL INNOVATION IN AVIATION SECURITY

FROM INDUSTRIES AS POLICY ENTREPRENEURS

ABSTRACT Aviation is a highly technical sector, but conversely policy regarding the security of it has historically been reactive and driven by human factors. Governance of aviation security is regulated and controlled by national governments, yet policy is primarily developed by international organisations. This article is concerned with what impact technological innovation has had on aviation security with particular focus on the effect of the developments in the cyber-sphere on the policy process. It will consider how cyber innovations have changed the aviation security threat picture and thus the policy process. Technology has become a critical enabler of those looking to subvert aviation. Yet until 9/11, an exogeneous shock to the policy area, the changing threat picture only impacted the content of aviation security policy rather than the policy process or the roles of those involved. This article will argue the industry is acting as a driving force for this legislative agenda nowadays indicating a clear role reversal. To analyse the response to the rise of the cyber threat as a determinant of the contemporary aviation security policy process, this article will use John Kingdon's concept of policy entrepreneurs. It will argue that the industry has acted as a policy entrepreneur driving legislation due to its technical expertise in response to cyber-attacks becoming the primary threat.

Keywords: technological innovation, aviation security, policy entrepreneurship

INTRODUCTION

Aviation is a highly technical sector. From the Wright brothers to unmanned aerial vehicles and spacecraft, aviation has always been *at the forefront of technological innovation*.[1] The UK's regulatory body for aviation – the Civil Aviation Authority (CAA) argues that the *pace of innovation in aviation is relentless*.[2] This article will adapt and expand the definition of innovation provided by Veland Ramadani and Shqipe Greguri, in line with approach of the aviation industry, to define technological innovation as: the process in which methods generated by new ideas and knowledge result in new products or technological systems or the enhanced efficiency of existing ones.[3] Aviation security can be summarised as the safeguarding of aviation by preventing acts of unlawful interference such as seizure, sabotage or acts of violence directed against aircraft, persons, or facilities. In practice aviation security is a multi-faceted concept which is extremely different depending on the specific area of operations or the particular method of application. It is a multi-layered system of measures: a system of systems. It should be noted that when this article refers to aviation security, it is civil aviation security not military, and commercial aviation not general aviation or cargo. The organisational structure of the aviation sector is complex, it is comprised of many international bodies, sovereign states, trade associations and commercial organisations and functions as a result of the interactions between these various entities. As such, any evaluation of technological innovation in aviation security must consider the various actors involved. For the purposes of examining the regulation of aviation security, this article will simplify the organisational structure of the aviation security landscape into five representative levels. These will be considered as: *local* – the national civil aviation authorities and stakeholders such as airports, airlines and aviation manufacturing or technology companies; *national* – sovereign states; *regional* – international networks or organisations and trade associations whose membership is not global but refined to a particular content, geographical region or other sub-section of membership; *international* – international organisations and trade associations whose global membership are not sovereign states; and *supranational* – the intergovernmental organisation with global membership consisting of sovereign states. It should be noted that where this article refers to the 'industry' this is the local, regional, and international level.

This article is concerned with what impact technological innovation has had on aviation security with particular focus on the effect of the developments in the cybersphere on the policy process. It will consider how cyber innovations have changed the aviation security threat picture and thus the policy process. Technology has become

[1] Civil Aviation Authority, "About the Innovation Team", at https://www.caa.co.uk/Our-work/Innovation/About-the-Innovation-Team/, 10 April 2022.

[2] Civil Aviation Authority, "Aviation Futures: Exploring the Future of Aviation", at https://www.caa.co.uk/Our-work/Innovation/Aviation-futures/, 10 April 2022.

[3] V. Ramadani, S. Gerguri, "Theoretical Framework of Innovation: Competitiveness and Innovation Program in Macedonia, *European Journal of Social Sciences*, vol. 23, no. 2 (2011), pp. 268-276.

a critical enabler of those looking to subvert aviation. Yet until 9/11, an exogeneous shock to the policy area, the changing threat picture only impacted the content of aviation security policy rather than the policy process or the roles of those involved. This article will argue the industry is acting as a driving force for this legislative agenda nowadays, indicating a clear role reversal. To analyse the response to the rise of the cyber threat as a determinant of the contemporary aviation security policy process, this article will use John Kingdon's concept of policy entrepreneurs. It will argue that the industry has acted as a policy entrepreneur driving legislation due to its technical expertise in response to cyber-attacks becoming the primary threat.

Kingdon identified three process streams: problem, policy and politics. He claims that a policy window occurs when a focusing event causes these three streams to come together or 'couple'.[4] Policy windows are the window of opportunity in which a particular issue is prominent facilitating action to be taken in the form of policy. Policy windows provide *an opportunity for advocates to push for their solutions*.[5] Kingdon describes the defining characteristic of policy entrepreneurs as *advocates who are willing to invest their resources —time, energy, reputation, money—to promote a position*.[6] On this, Michael Mintrom builds identifying seven key skills of policy entrepreneurs: strategic thinking, team building, networking, negotiating, evidence collection, making arguments and engaging multiple audiences. Mintrom further defines policy entrepreneurs as *actors who engage in collaborative efforts in and around government to promote policy innovations*.[7] The opening of policy windows can be both predictable, for example in the case of a particular program reaching its renewal date or unpredictable, for example when an issue unexpectedly gains prominence. It is further argued by Kingdon that policy windows do not remain open for any significant length of time, and that the opportunity for action is in fact short lived. Kaunert supports this, paying note to the fact that policy entrepreneurs often will have prepared their solutions before an issue becomes prominent, and that in fact they *lie in wait for a window to open and therefore seize the right moment*.[8] This, however, requires policy entrepreneurs to if not pre-empt the opening of policy windows, at least to have solutions prepared just in case, so they can be ready when they do. A policy entrepreneur must be an actor who is in a position to have the solution they propose heard, the power to have it considered for legislating and the persistence to see it through. It is argued that policy entrepreneurs are generally not solely responsible for an issue gaining prominence on the agenda or any resulting policy, as this requires multiple actors rather that they are the central figures in bringing this about.

[4] J.W. Kingdon, *Agendas, Alternatives and Public Policies*, Boston 2011.

[5] C. Kaunert, "Conclusion: Assessing the External Dimension of EU Counter-Terrorism: Ten Years On", *European Security*, vol. 21, no. 4 (2012), p. 36.

[6] J.W. Kingdon, *Agendas, Alternatives...*

[7] M. Mintrom, P. Norman, "Policy Entrepreneurship and Policy Change", *Policy Studies Journal*, vol. 37, no. 4 (2009), pp. 649-667.

[8] C. Kaunert, "Conclusion: Assessing the External...", p. 37.

THE REGULATION OF AVIATION SECURITY

Regulation of aviation originated due to the major air powers of the Second World War recognising the need for international cooperation in civil aviation. At the subsequent International Aviation Conference in Chicago in 1944, the fifty-three sovereign states present discussed those matters deemed pertinent to the development of international civil aviation which led to the passing of the Convention on International Civil Aviation (the Chicago Convention) on 7 December 1944. The most significant result of this was the creation of the International Civil Aviation Organisation (ICAO). ICAO, which is now a specialised agency of the United Nations, was predominantly focused on air navigation and safety.[9] Matters relating to unlawful interference – or security were not covered by the Chicago Convention, as the issue was not foreseen and would not be addressed until the escalating surge of aerial piracy in the 1960s and other forms of terrorism directed against aviation in the 1970s. ICAO was established with the mandate *to ensure the safe, efficient and orderly evolution of international civil aviation*.[10] This is achieved through ICAO's governing bodies: the Assembly which consists of all Contracting States, and the Council which is comprised of thirty-six Contracting States elected by the Assembly. In addition to the supranational level of the Council and through it the Assembly, ICAO also operates on the international level through the Secretariat. The Secretariat is the *administrative and expert bureaucracy* which is charged with supporting the diplomacy of the Assembly and the Council, and *to research new air transport policy and standardization* [sic] *innovations as directed and endorsed by governments through the ICAO Assembly or by the Council*.[11] The Secretariat is aided in this by Invited Organisations which are [i]*ndustry and civil society groups, and other concerned regional and international organizations* [sic].[12] Since the creation of ICAO and subsequent international level industry bodies such as the International Air Transport Association (IATA) – the trade association of the worlds scheduled airlines, and the Airports Council International (ACI World), the aviation policy process could be expressed simply as: aviation is regulated by governments and implemented, audited and enforced by the industry. In practice however, this is far more complex. At the supranational level discussion and negotiation among the sovereign states that make up the membership of ICAO's Assembly results in agreement on the specific scope and details of a particular issue. At the international level the ICAO Secretariat and Invited Organisations set the standards necessary to achieve this focus and build consensus on the best practices to enact this provision. At the national level governments then legislate this and at the local, regional, and international levels the industry provides

[9] D. MacKenzie, *ICAO: A History of the International Civil Aviation Organization*, Toronto 2010.

[10] International Civil Aviation Organization, "ICAO Aviation Security Programme", at http://www2.icao.int/e_n/AVSEC/Pages/default.aspx, 25 March 2022.

[11] Idem, "About ICAO", at https://www.icao.int/about-icao/Pages/default.aspx, 25 March 2022.

[12] Ibid.

solutions to make this possible. This is audited at the local and international levels and enforced at the local level.

Since the development of security as a policy area, it has followed the same structure. Governments drive the legislative agenda for aviation security operating at the supranational, regional and national levels. They are responsible for that state's involvement in international aviation security matters through membership of the ICAO Assembly which sets the focus of aviation security agreements, at the regional level through networks such as the European Civil Aviation Conference (ECAC) and for the national aviation security strategy and policy including legislating security standards to meet or surpass the international agreements. The industry facilitates this operating at the local, regional and international levels. At the local level, this is through national civil aviation authorities, airports, airlines and individual technology, supply or manufacturing companies and service providers. The national civil aviation authority is responsible for monitoring compliance with and enforcing the national legislation. In addition, the civil aviation authorities provide guidance to support the government in international negotiations, and to airports, aircraft operators and other entities regarding the implementation of national security policy. At the regional level this is through organisations such as Airports Council International – Europe (ACI-Europe), IATA-Europe, European Regions Airline Association (ERAA), European Business Aviation Association (EBAA), and the European Cockpit Association (ECA) who share best practices and implementation efforts. At the international level this is through the ICAO Secretariat and Invited Organisations, as well as trade associations such as IATA and ACI World.

There has been much scholarly attention paid to the regulatory structure of international aviation security and the roles of the various organisations involved, a central theme of which is the immeasurable strength of having the technical aspects of policy informed by cooperation with and between practitioners from across the entire community whilst cautioning against the historic tendency of operators to allow the issue of profit to be a determining factor.[13] It has been postulated that among the various reasons why a technology can be changed are *an active attempt by its users or creators to change it* [...] *the characteristics of its use or by changes in the physical and social setting within which the technology exists*.[14] This is true for the use of technology in aviation security where these are not mutually exclusive. One such area of technological innovation is x-ray screening and methods of detecting explosives, and people screening

[13] G. Easterbrook, "The All Too Friendly Skies: Security as an Afterthought", in J.F. Hoge Jr., G. Rose (eds), *How Did This Happen? Terrorism and the New War*, New York 2001; D. MacKenzie. *ICAO...*; O. St. John, *Air Piracy, Airport Security and International Terrorism*, New York 1991; idem, "The Politics of Aviation Terrorism", in P. Wilkinson, B.M. Jenkins (eds), *Aviation Terrorism and Security*, London 1999; R. Wallis, *Combating Air Terrorism*, Washington 1993; idem, "The Role of International Aviation Organisations in Enhancing Security", in P. Wilkinson, B.M. Jenkins (eds), *Aviation Terrorism...*; idem, *Lockerbie: The Story and the Lessons*, Westport 2001; P. Wilkinson, "Enhancing Global Security?", in: P. Wilkinson, B.M. Jenkins (eds), *Aviation Terrorism...*; idem, *Terrorism versus Democracy: The Liberal State Response*, London 2006; idem (ed.), *Homeland Security in the UK*, London 2007.

[14] B. Bozeman, "Technology Transfer and Public Policy: A Review of Research and Theory", *Research Policy*, vol. 29, no. 4-5 (2000), p. 69.

technologies. Xiana Barros' examination of the impact on aviation security policy of new screening technologies reinforces the commonly held truism that developments in aviation security have historically been in response to innovation on the part of those acting against the industry rather those within.[15] Despite the diverse focus, a prevalent common theme in the literature is the opportunity for technological innovation to counter what has historically been perceived as the single biggest risk of failure: human error.[16] There is a vibrant discourse on how this can be facilitated through innovation in Artificial Intelligence (AI) and Machine Learning (ML).[17] Information technology will allow for better connectedness, making aviation security more seamless yet it also prevents the biggest threat thus making cyber security a primary area of concern.[18]

AVIATION SECURITY, TECHNOLOGICAL INNOVATION AND THE RISE OF THE CYBER THREAT

A significant criticism of aviation security prior to 9/11 was that since its inception in the 1970s, it was reactive in nature – policy developments occurred only in response to the weaknesses or shortcomings highlighted by terrorist success with a new method or target of attack, rather than resulting from the continual proactive identification of potential vulnerabilities and establishing of measures to prevent these being exploited. Aviation Security has always been predominantly driven by human factors. From the earliest recorded instance of aerial piracy in 1930 through to the foiled 2006 liquids plot – which planned the coordinated sabotage of multiple trans-Atlantic flights using liquid explosives disguised as innocuous soft drinks – the threat to aviation posed by terrorism centred around the actions of individuals or groups.[19] Aerial piracy, regardless of its form or intent, required a human actor to commandeer the aircraft. Attacks or incursions against aircraft, airports or other property or assets belonging to aviation entities were also carried out by human actors. Even sabotage as the most technical of historical threats still required a human actor to smuggle the explosive device onboard,

[15] X. Barros, "EU Counterterrorism and Aviation Security: Supranational Rules but Intergovernmental Politics?", *European Foreign Affairs Review*, vol. 17 (2012), pp. 53-69.

[16] P. McFarlane, "Linking Aviation Security Failures to Human-Mediated Error: A Review of the Related Literatures with Directions for Policy and Research", *Journal of Transportation Security*, vol. 13 (2020), pp. 33-51.

[17] P. Benda, "Commentary: Harnessing Advanced Technology and Process Innovations to Enhance Aviation Security", *Journal of Air Transport Management*, vol. 48 (2015), pp. 23-25; G. Lohmann, B.A. Pereira, "Air Transport Innovations: A Perspective Article", *Tourism Review*, vol. 75, no. 1 (2020), pp. 96-101; P. McFarlane, "Linking Aviation Security Failures…".

[18] G. Lohmann, B.A. Pereira, "Air Transport Innovations…"; P. McFarlane, "Linking Aviation Security…".

[19] O. St. John, *Air Piracy…*; D. Campbell, "El Al Guards Kill US Airport Gunman", *The Guardian*, 5 July 2002, at http://www.theguardian.com/world/2002/jul/05/usgunviolence.usa, 20 March 2022; TSA, "UK 2006 Liquid Explosives Plot Trial Overview", at https://www.tsa.gov/press/releases/2008/09/08/uk-2006-liquid-explosives-plot-trial-overview, 20 March 2022; R. Wallis, *Combating Air…*; idem, *Lockerbie…*

either directly in person – which could be detonated manually or hidden onboard to be triggered by a timer after they have deplaned – or remotely through linked systems such as baggage, cargo, or in-flight supply chains.[20] The measures aviation security programmes consist of have evolved in-line with regulatory efforts to counter the threat, most notably the 1974 amendment to the Chicago Convention to incorporate the newly created "Annex 17 – Security". Throughout the early decades of aviation security, the standards and recommended practices (SaRPs) contained within regulatory developments were primarily concerned with the physical actions that security staff of airports and airlines should take – such as the IATA-developed security standard of full passenger and baggage reconciliation, and recommendation of lifting seat cushions during searches at transit stops to counter sabotage attempts.[21] As technological advances occurred throughout the latter half of the twentieth century the resulting improved capabilities were incorporated into SaRPs to bolster aviation security efforts.

Technology is not however a panacea, but should rather be viewed as a double-edged sword. Just as the strength of aviation security benefits from the technological development of the actors involved, it is at increasing risk from the technological development of those actors who would seek to undermine it. Furthermore, not only is aviation security dependant on technological innovation to counter would-be perpetrators of acts of unlawful interference devising novel ways to carry-out traditional threats such as sabotage, but it is also increasingly subject to risk from these technological innovations themselves. The most prominent example of this is the cyber-sphere. The technological revolution of the twenty-first century, especially that referred to as the fourth industrial revolution regarding digital technologies and cyber systems, has brought undeniable benefits for aviation such as increasing data exchange, interconnectedness, and inter-operability.[22] As aviation becomes increasingly digitised and more dependent on cyber technologies it becomes more vulnerable to the cyber threat. As well as the traditional threats, aviation security must now counter the risk of cyber-attack.

As with previous forms of threats that aviation security has and continues to face, cyber-attacks can be driven by a variety of methods and utilise many attack vectors including phishing, fraudulent websites, malware, ransomware, distributed denial-of-service (DDoS), and exploitation of cloud-based infrastructure.[23] There have been several data theft cyber-attacks targeting aircraft manufacturers aiming to monetarise

[20] B.M. Jenkins, "Aircraft Sabotage", in P. Wilkinson, B.M. Jenkins (eds), *Aviation Terrorism...*; R. Wallis, *Combating Air...*; idem, "The Role of International..."; idem, *Lockerbie...*; P. Wilkinson, "Enhancing Global...".

[21] B.M. Jenkins, "Aircraft Sabotage"; R. Wallis, *Lockerbie...*

[22] World Economic Forum, "Advancing Cyber Resilience in Aviation: An Industry Analysis", January 2020, at https://www3.weforum.org/docs/WEF_Cyber_Resilience_in_Aviation_An_Industry_Analysis.pdf, 20 March 2022.

[23] Eurocontrol, "Aviation under Attack: Faced with a Rising Tide of Cybercrime, Is Our Industry Resilient Enough To Cope?", *Eurocontrol EATM-CERT Services Think Paper*, no. 12, 5 VII 2021, at https://www.eurocontrol.int/sites/default/files/2021-07/eurocontrol-think-paper-12-aviation-under-cyber-attack.pdf, 25 March 2022.

intellectual property, for example the 2014 malware attack on Safran by Chinese Intelligence and their subsequent attack on GE Aviation.[24] Airlines are also increasingly subject to financially motivated cyber-attacks targeting customers personal data.[25] In 2018, Air Canada, British Airways (BA) and Cathay Pacific airlines were subject to cyber security attacks within four months of each other that caused the personal data of over nine million people to be breached.[26] In 2020, Easyjet suffered a cyber-attack in which the contact details and travel information of nine million customers had been breached, the airline however only revealed it four months after the event resulting in a class-action lawsuit by more than ten thousand customers seeking billions of pounds in damages.[27] In 2015, a purported 'white hat hacker' posted videos on YouTube explaining his hack on Norwich Airport's website which affected bookings and digital information boards requiring the website to be shut down and replaced.[28] A significant issue regarding the regulation of aviation security is that the economic and technical disparity amongst the member states of the international organisations spans the entire global scale in terms of both wealth and development. The SaRPs must therefore be set at the level of the lowest common denominator (LCD). One cyber-attack that clearly demonstrates the risk of the interconnected nature of aviation, which can be summed up by the adage 'a chain is only as strong as its weakest link' is the 2021 attack on SITA, a telecommunications and IT services provider used by the airline industry, which compromised passenger processing systems and the personal data of customers of the Star Alliance Network which includes; Air Canada, Air India, Air New Zealand, Cathay Pacific, Finnair, Lufthansa, Scandinavian Airlines, Singapore Airlines, Swiss Air, and

[24] Centre for Strategic and International Studies, "Significant Cyber Incidents", at https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents, 25 March 2022; M.K. Whitehead, "Safe Cyber: GE Aviation's Cybersecurity Leader Talks Data Protection and STEM", *GE Aerospace. The Blog*, 7 June 2019, at https://blog.geaviation.com/technology/safe-cyber-ge-aviations-cybersecurity-leader-talks-data-protection-and-stem/, 25 March 2022; The United States Department of Justice, "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research", 19 July 2021, at https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion, 25 March 2022; W. Bellamy III, "New Eurocontrol Data Shows Airlines Increasingly Becoming Targets for Cyber Attacks", *Aviation Today*, 12 July 2021, at https://www.aviationtoday.com/2021/07/12/new-eurocontrol-data-shows-airlines-increasingly-becoming-targets-cyber-attacks, 25 March 2022.

[25] Centre for Strategic and International Studies, "Significant Cyber…"; Eurocontrol, "Aviation under Attack…".

[26] Avlaw Aviation Consulting, "Cyberattacks in the Aviation Industry", 10 March 2020, at https://avlaw.com.au/cyberattacks-aviation-industry/, 25 March 2022; Eurocontrol, "Aviation under Attack…".

[27] S. Hosalikar, "Top Most Common Type Cyber Attacks in Aviation Industry", Great Learning, 9 November 2021, at https://www.mygreatlearning.com/blog/top-most-common-type-cyber-attacks-in-aviation-industry/#:~:text=%20Here%E2%80%99s%20a%20list%20of%20the%20topmost%20severe,Airways%3A%20The%20British%20Airways%20breach%20is…%20More%20, 25 March 2022.

[28] "Norwich Airport and Hospital Cyber-Attack: Man Admits Guilt", *BBC News*, 25 May 2017, at https://www.bbc.co.uk/news/uk-england-norfolk-40047908, 25 March 2022.

United among others.[29] The reduced technological capabilities of economically and technological weaker (developing) states increases the risk to the rest of the membership despite their own cyber strengths or technological capabilities.

The World Economic Forum (WEF) considers the potential impact of cyber-attacks to go beyond data loss and reputational damage resulting from breaches motivated by financial gain, which could *quickly result in serious loss of life and utter catastrophe* [...] *and have cascading dire effects on the entire industry*.[30] The civil aviation authority of the U.S., the Federal Aviation Administration (FAA), experienced a cyberattack in 2006 that exploited a lack of security protocols preventing unauthorised access arising from the use of commercial software and Internet Protocol-technologies, which necessitated a partial shut-down of national Air Traffic Control systems.[31] In 2011, a former BA software engineer was convicted of terrorism offences for passing sensitive information to al-Qaeda to target BA flights for sabotage, as well as planning to crash the airline's computer systems.[32] Furthermore, the technological innovations which have resulted from the niches of increasingly digital airplanes combined with in-flight connectivity (IFC) and fifth generation (5G) air-to-ground (ATG) networks present new hazards that if subjected to a cyber-attack could negate the established protections of physical aviation security processes. A cyber-attack that was successful in breaching such an aircraft could result in digitally, and potentially even remotely, committed piracy or sabotage – ultimately resulting in physical destruction and loss of life such as occurred on 9/11, or from the 1985 Air India's *Kanishka* and the 1988 Pan American Airways (PanAm) *The Maid of the Seas* tragedies. The drastic evolution of the threat posed by such technological innovations requires an equally momentous redefining of the landscape to embed aviation cyber security as a policy priority.

A prominent criticism of aviation security often centres on the lack of international uniformity. It must be noted however, that until the moment when a supreme organisation that can eradicate sovereignty comes into being, it is highly unlikely there will ever be true uniformity of aviation security standards. States will always have differing histories, political outlooks, and threat levels that will influence national perceptions of the risk posed by terrorism and thus the relative importance of aviation security as a legislative issue. Furthermore, given the sheer range of capabilities among the member states of the international organisations, those who are capable are likely to exercise

[29] I. Arghire, "Researchers Attribute Airline Cyberattack to Chinese Hackers", *Security Week*, 14 June 2021, at https://www.securityweek.com/researchers-attribute-sita-cyberattack-chinese-hackers, 25 March 2022; Centre for Strategic and International Studies, "Significant Cyber..."; CyberPeace Foundation, "#Incident_Report: The Air India and SITA PSS Data Leak", 1 June 2022, at https://www.cyberpeace.org/incident_report-the-air-india-and-sita-pss-data-leak/, 25 March 2022.

[30] World Economic Forum, "Cybersecurity in Aviation: Building a Resilient Future", 2 June 2021, at https://www.weforum.org/impact/we-are-building-a-cyber-resilient-future-for-the-aviation-sector, 25 March 2022.

[31] Avlaw Aviation Consulting, "Cyberattacks in the Aviation...".

[32] "Terror Plot BA Man Rajib Karim Gets 30 Years", *BBC News*, 11 March 2011, at https://www.bbc.co.uk/news/uk-12788224, 25 March 2022.

their right to go over and above the required minimum. This does not, however, mean that the aforementioned status quo of setting the LCD of SaRPs at the lowest level possible should be the de facto approach towards technological innovation. Conversely, one of the greatest opportunities that cyber developments offers for aviation security is the provision of possible solutions to this historic weakness. Open architecture allows for information technology processes and software programs, or parts thereof, to be changed without having to replace whole operating systems.[33] This will potentially reduce the economic impact of implementing changes thus making it more achievable for the developing states. The increased connectivity and interconnectedness further aided by innovations such as 5G have to potential to remove obstacles to burden sharing as the more technologically capable states would be able to provide remote assistance, support and even oversight to developing states. The WEF shares the view of the importance of greater harmonisation and has called upon the aviation industry to adopt a unified approach to cyber security as [a]*irlines, airports and aircraft manufacturers comprise a complex infrastructure that must be protected holistically and in each of its individual parts*.[34] To encourage this, it launched the Cyber Resilience in the Aviation Industry initiative in collaboration with governments and regulators, international organisations, and stakeholders from across the aviation industry.

THE AVIATION INDUSTRY'S CYBER SECURITY RESPONSE – CASE OF POLICY ENTREPRENEURSHIP

The emergence of cyber security as a policy priority for aviation security has been recognised and acted upon by the industry. IATA defines aviation cybersecurity as *the convergence of people, processes, and technology that come together to protect civil aviation organizations, operations and passengers from digital attacks*.[35] IATA has argued that its *global leadership role* [places it] *in a strong position to drive the harmonization of aviation cyber security regulations, approaches and risk management*.[36] As such it has developed an *industry-wide Aviation Cyber Security Strategy to coordinate and calibrate through advocacy, standards and services, the most appropriate level of holistic cyber protection for the industry*.[37] In doing so, IATA has demonstrated behaviours and skills associated with policy entrepreneurship – strategic thinking, fostering networks, engaging multiple audiences, arguing their proposed policy solution to the identified problem and working

[33] Airport Council International, "ACI Webinar – Transforming Aviation Security through Artificial Intelligence, 20 January 2022, at https://store.aci.aero/form/webinar-transforming-aviation-security-through-artificial-intelligence/, 25 March 2022.

[34] World Economic Forum, "Cybersecurity in Aviation…".

[35] International Air Transport Association, "Aviation Cyber Security – Effective July 2015 Version 3 (May 2020)", at https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/aviation-cyber-security-position.pdf, 25 March 2022.

[36] Ibid.

[37] Ibid.

collaboratively with governments to promote policy innovation. IATA's position paper on aviation cyber security emphasises the role of those at the international level to encourage, coordinate and facilitate cooperation among and between local, regional, national/supranational levels. It also recognises that global dialogue, cooperation, and action on aviation cyber security can be best achieved if driven by ICAO.[38] This demonstrates a role reversal from the established norm of policy innovations originating from ICAO and radiating out to the industry.

ICAO's Cybersecurity Strategy for Civil Aviation outlines a central strategic vision that international civil aviation *is resilient to cyber-attacks and remains safe and trusted globally, whilst continuing to innovate and grow*.[39] The operationalisation of this includes: the requirement that the national level consider aviation cyber security as part of their obligations under the Chicago Convention; the coordination of aviation cyber security at the international and supranational levels; and the commitment at the local, regional and international levels to focus on the development of cyber resilience to protect against cyber-attacks. To aid implementation of the Cybersecurity Strategy, ICAO adopted the Cybersecurity Action Plan which outlines the aviation cyber security SaRPs.[40] The rise of cyber threats has not only changed the aviation security policy process in terms of the actors involved but also the nature of it. In contradiction to the historic tendency of aviation security to be reactive, ICAO's Cybersecurity Strategy emphasises the importance of aviation cyber security being future-focused, recommending that cyber security policies include, among other elements, *promotion of security by design,* […] *pro-active vulnerability management, improving agility in security updates without compromising safety*.[41]

The aviation sector in general, and specifically those involved in aviation security, in recognition of the risks posed by the interconnected nature of aviation puts great significance on the benefit and necessity of capacity building initiatives. The pre-eminent example is ICAO's No Country Left Behind (NCLB) initiative. The NCLB applies to all aspects of international aviation, not just security, and has the main goal of ensuring greater global harmonization of implementation of SaRPs to better enable developing states to *have access to the significant socio-economic benefits of safe and reliable air transport*.[42] The NCLB considers the ICAO's role at the supranational and international levels to be that of coordination and encouraging the more developed countries to pool resources to aid the developing states.[43] In remarks made during the ICAO

[38] Ibid.

[39] International Civil Aviation Organization, "Aviation Cybersecurity Strategy", October 2019, p. 5, at https://www.icao.int/aviationcybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.EN.pdf, 28 March 2022.

[40] Idem, "Cybersecurity Action Plan", at https://www.icao.int/cybersecurity/Pages/Cybersecurity-Action-Plan.aspx, 28 March 2022.

[41] Idem, "Aviation Cybersecurity Strategy", p. 7.

[42] Idem, "No Country Left Behind", at https://www.icao.int/about-icao/nclb/pages/default.aspx, 28 March 2022.

[43] Ibid.

Year of Security Culture Inauguration, the European Commission Director-General for Mobility and Transport, Henrik Hololei spoke of EU commitment to NCLB and the willingness to seek out opportunities to share experience and work with the international community to elevate standards in international aviation security culture through capacity building initiatives.[44] Given the global membership of ICAO and the extent of the disparity of technical capabilities among the Contracting States, in line with the NCLB initiative one of the seven pillars the ICAO Cybersecurity framework is built on is capacity building, training, and cyber security culture. One clear focus under this pillar is the human element – the cyber security skills and knowledge of aviation security personnel, and a cyber security culture where security is seen as the responsibility of all. This is absolutely imperative. Government acknowledgement of both the immediacy and the increasing and evolving nature of the cyber security threat due to aviation's increasing dependency on digital technologies was evidenced at the Inauguration of ICAO's Year of Security Culture. In his remarks, Director-General Hololei spoke of a cyber security toolkit currently in development to strengthen awareness of the cyber threat and the cyber security skills and hygiene of staff and decision makers.[45] Across the entire aviation sector, the future aviation security landscape is being perceived as radically altered by technological innovation. The scale, pace and scope of cyber innovations has already significantly changed the content of aviation security policy and will continue to do so as further innovation occurs and these are applied either to strengthen or subvert aviation security. New policy initiatives and best practices for aviation security were typically formulated and agreed by ICAO and legislated by governments. As technological innovations, especially cyber, are further incorporated causing the aviation security landscape to change, the importance of technical expertise increases exponentially. As the problems become more technically complex so must the proposed policy solutions. The technical expertise of the industry as a whole provides the requisite knowledge to achieve this.

As previously illustrated, aviation security, including aviation cyber security, does not operate on an immutable hierarchical structure, but rather results from interactions between the many organisations within and across the various levels of the industry and governments. These can be in the form of dialogue and cooperation but also consortiums and partnerships that transcend the boundaries of the defined levels. One such that operates internationally, is formed of aviation companies from across the various areas of the industry is the Aviation Information Sharing and Analysis Centre (A-IASC) which works in partnership with both industry organisations such as ACI World and national governments.[46] Research published by EUROCONTROL

[44] H. Hololei, "ICAO Year of Security Culture: Inauguration", January 2021, at https://www.icao.tv/year-of-security-culture-2021/videos/avsec2020-year-of-security-culture-inauguration, 28 March 2022.

[45] Ibid.

[46] Airports Council International, "Airports Council International and The Aviation Information Sharing and Analysis Center Enter Cooperative Agreement", 23 January 2020, at https://aci.aero/2020/01/23/airports-council-international-and-the-aviation-information-sharing-and-analysis-center-enter-cooperative-agreement/, 28 March 2022; Aviation ISAC, *A-ISAC Aviation Information Sharing*

using data collected by the European Air Traffic Management Computer Emergency Response Team (EATM-CERT) found a 530% year on year increase in reported aviation cyber-attacks from 2019 to 2020.[47] In response to this the A-ISAC in cooperation with EATM-CERT launched an awareness campaign to increase understanding of the threat posed by ransomware and recommend best practices to reduce risks.[48] By recognising and responding to the policy window resulting from EUROCONTROL's research to focus attention on a specific problem the A-ISAC was able to use the resulting opportunity to push their solution. ACI World then further demonstrated the ability of the industry to act as a policy entrepreneur by expanding the solution proposed by the A-IASC. In an attempt to counter potential weaknesses resulting from insufficient cyber knowledge among stakeholders, ACI World produced a handbook for cyber security implementation using knowledge and experience drawn from across the industry.[49] This increased inter-linking and interchangeability in terms of the roles and purviews of the various organisations of the industry especially in aviation cyber security – is not only beneficial for the content of aviation cyber security policy but is also demonstrating how the policy process is changing.

CONCLUSION

Technological innovation has significantly changed the processes and practices that aviation security is comprised of, and provides many benefits in terms of both more efficient and effective security. The increasing digitisation of aviation security also offers a multitude of opportunities, especially through increased connectivity which facilitates data sharing and systems integration. The increased interconnectedness also provides an opportunity to increase capacity building and burden sharing, reducing and potentially in the future negating a fundamental hindrance to uniformity of standards resulting from those national governments and civil aviation authorities of economically stronger and technologically more capable states enacting standards over and above the internationally agreed SaRPs. Conversely, cyber innovation also poses increased risk. The increased digitisation and connectivity has been accompanied by the increased threat of cyber-attack. The volume of attempted cyber-attacks against aviation for financial and malicious reasons that have occurred to date, and the potential devasting consequences of a successful attack motivated by more nefarious intent than mere disruption has led to an industry-wide focus on aviation cyber security.

and Analysis Center, at https://www.icao.int/cybersecurity/SiteAssets/A-ISAC/04_14_15_A-ISAC_Brochure_FINAL.pdf, 28 March 2022.

[47] Eurocontrol, "Aviation under Attack...".

[48] W. Bellamy III, "New Eurocontrol Data...".

[49] Airports Council International, "ACI Launches New Guidance for Addressing Cybersecurity Threats", 11 February 2020, at https://aci.aero/2020/02/11/aci-launches-new-guidance-for-addressing-cybersecurity-threats/, 28 March 2022.

This article analysed the impact technological innovation has had on aviation security, with particular focus on the effect of the developments in the cyber-sphere on the policy process. It has shown how technology has become a critical enabler of those looking to subvert aviation. Initially, until 9/11, the changing threat picture only impacted the content of aviation security policy rather than the policy process or the roles of those involved. This article has shown the industry to be a driving force for this legislative agenda – indicating a role reversal. The article used John Kingdon's concept of policy entrepreneurs, with the industry acting as a policy entrepreneur driving legislation due to its technical expertise. Aviation efforts in cyber security have fundamentally resulted in a paradigm shift in aviation security policy. The article has shown a deviation from the norm regarding the roles and precedence of those involved in the policy-making process; from governments as the regulators of aviation security to industry. Due to the technical expertise necessary to provide solutions to increasingly more complex problems, the industry representatives are now acting as policy entrepreneurs. As technological innovation continues, these changes to the aviation security policy process will likely continue to evolve.

BIBLIOGRAPHY

Airports Council International, "ACI Launches New Guidance for Addressing Cybersecurity Threats", 11 February 2020, at https://aci.aero/2020/02/11/aci-launches-new-guidance-for-addressing-cybersecurity-threats/.

Airport Council International, "ACI Webinar – Transforming Aviation Security Through Artificial Intelligence", 20 January 2022, at https://store.aci.aero/form/webinar-transforming-aviation-security-through-artificial-intelligence/.

Airports Council International, "Airports Council International and The Aviation Information Sharing and Analysis Center Enter Cooperative Agreement", 23 January 2020, at https://aci.aero/2020/01/23/airports-council-international-and-the-aviation-information-sharing-and-analysis-center-enter-cooperative-agreement/.

Arghire I., "Researchers Attribute Airline Cyberattack to Chinese Hackers", *Security Week*, 14 June 2021, at https://www.securityweek.com/researchers-attribute-sita-cyberattack-chinese-hackers.

Aviation ISAC, *A-ISAC Aviation Information Sharing and Analysis Center.* https://www.icao.int/cybersecurity/SiteAssets/A-ISAC/04_14_15_A-ISAC_Brochure_FINAL.pdf.

Avlaw Aviation Consulting, "Cyberattacks in the Aviation Industry", 10 March 2020, at https://avlaw.com.au/cyberattacks-aviation-industry/.

Barros X., "EU Counterterrorism and Aviation Security: Supranational Rules but Intergovernmental Politics?", *European Foreign Affairs Review*, vol. 17 (2012), pp. 53-69, https://doi.org/10.54648/EERR2012014.

Bellamy W., III, "New Eurocontrol Data Shows Airlines Increasingly Becoming Targets for Cyber Attacks", *Aviation Today*, 12 July 2021, at https://www.aviationtoday.com/2021/07/12/new-eurocontrol-data-shows-airlines-increasingly-becoming-targets-cyber-attacks.

Benda P., "Commentary: Harnessing Advanced Technology and Process Innovations to Enhance Aviation Security", *Journal of Air Transport Management*, vol. 48 (2015), pp. 23-25, http://dx.doi.org/10.1016/j.jairtraman.2015.06.008.

Bozeman B., "Technology Transfer and Public Policy: A Review of Research and Theory", *Research Policy*, vol. 29, no. 4-5 (2000), pp. 627-655, https://doi.org/10.1016/S0048-7333(99)00093-1.

Campbell D., "El Al Guards Kill US Airport Gunman", *The Guardian*, 5 July 2002, at http://www.theguardian.com/world/2002/jul/05/usgunviolence.usa.

Civil Aviation Authority, "About the Innovation Team", at https://www.caa.co.uk/Our-work/Innovation/About-the-Innovation-Team/.

Civil Aviation Authority, "Aviation Futures: Exploring the Future of Aviation", at https://www.caa.co.uk/Our-work/Innovation/Aviation-futures/.

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

CyberPeace Foundation, "#Incident_Report: The Air India and SITA PSS Data Leak", 1 June 2022, at https://www.cyberpeace.org/incident_report-the-air-india-and-sita-pss-data-leak/.

Easterbrook G., "The All Too Friendly Skies: Security as an Afterthought", in J.F. Hoge Jr., G. Rose (eds), *How Did This Happen? Terrorism and the New War*, New York 2001.

Eurocontrol, "Aviation under Attack: Faced with a Rising Tide of Cybercrime, Is Our Industry Resilient Enough to Cope?", *Eurocontrol EATM-CERT Services Think Paper*, vol. 12, 5 July 2021, at https://www.eurocontrol.int/sites/default/files/2021-07/eurocontrol-think-paper-12-aviation-under-cyber-attack.pdf.

Hololei H., "ICAO Year of Security Culture: Inauguration", January 2021, at https://www.icao.tv/year-of-security-culture-2021/videos/avsec2020-year-of-security-culture-inaugu ration.

Hosalikar S., "Top Most Common Type Cyber Attacks in Aviation Industry", *Great Learning Blog*, 9 November 2021, at https://www.mygreatlearning.com/blog/top-most-common-type-cyber-attacks-in-aviation-industry/#:~:text=%20Here%E2%80%99s%20a%20list%20of%20the%20topmost%20severe,Airways%3A%20The%20British%20Airways%20breach%20is...%20More%20.

International Air Transport Association, "Aviation Cyber Security – Effective July 2015 Version 3 (May 2020)", at https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/aviation-cyber-security-position.pdf.

International Civil Aviation Organization, "About ICAO", at https://www.icao.int/about-icao/Pages/default.aspx.

International Civil Aviation Organization, "Aviation Cybersecurity Strategy", October 2019, at https://www.icao.int/aviationcybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.EN.pdf.

International Civil Aviation Organization, "Cybersecurity Action Plan", at https://www.icao.int/cybersecurity/Pages/Cybersecurity-Action-Plan.aspx.

International Civil Aviation Organization, "ICAO Aviation Security Programme", at http://www2.icao.int/e_n/AVSEC/Pages/default.aspx.

International Civil Aviation Organization, "ICAO Regional USAP-CMA Seminar Auditing Annex 17 Standards", at https://www.icao.int/MID/Documents/2018/USAP-CMA%20Seminar/Module%202%20-%20Auditing%20Annex%2017%20Standards.pdf.

International Civil Aviation Organization, "No Country Left Behind", at https://www.icao.int/about-icao/nclb/pages/default.aspx.

Jenkins B.M., "Aircraft Sabotage", in P. Wilkinson, B.M. Jenkins (eds), *Aviation Terrorism and Security*, London 1999.

Kaunert Ch., "Conclusion: Assessing the External Dimension of EU Counter-Terrorism – Ten Years On", *European Security*, vol. 21, no. 4 (2012), pp. 578-587, https://doi.org/10.1080/09662839.2012.688810.

Kingdon J.W., *Agendas, Alternatives and Public Policies*, Boston 2011.

Lohmann G.M., Pereira B.A., "Air Transport Innovations: A Perspective Article", *Tourism Review*, vol. 75, no. 1 (2020), pp. 95-101, https://doi.org/10.1108/TR-07-2019-0294.

MacKenzie D., *ICAO: A History of the International Civil Aviation Organization*, Toronto 2010, https://doi.org/10.3138/9781442670143.

McFarlane P., "Linking Aviation Security Failures to Human-Mediated Error: A Review of the Related Literatures with Directions for Policy and Research", *Journal of Transportation Security*, vol. 13 (2020), pp. 33-51, https://doi.org/10.1007/s12198-020-00209-z.

Mintrom M., Norman P., "Policy Entrepreneurship and Policy Change", *Policy Studies Journal*, vol. 37, no. 4 (2009), pp. 649-667, http://dx.doi.org/10.1111/j.1541-0072.2009.00329.x.

Mintrom M., "So You Want To Be a Policy Entrepreneur?", *Policy Design and Practice*, vol. 2, no. 4 (2019), pp. 307-323, https://doi.org/10.1080/25741292.2019.1675989

"Norwich Airport and Hospital Cyber-Attack: Man Admits Guilt", *BBC News*, 25 May 2017, at https://www.bbc.co.uk/news/uk-england-norfolk-40047908.

Pereira B.A., Lohman G., Houghton L., "Innovation and Value Creation in the Context of Aviation: A Systemic Literature Review", *Journal of Air Transport Management*, vol. 94 (2021), art. 102076, https://doi.org/10.1016/j.jairtraman.2021.102076.

Ramadani V., Gerguri S., "Theoretical Framework of Innovation: Competitiveness and Innovation Program in Macedonia", *European Journal of Social Sciences*, vol. 23, no. 2 (2011), pp. 268-276.

St. John P., *Air Piracy, Airport Security and International Terrorism*, New York 1991.

St. John P., "The Politics of Aviation Terrorism", in P. Wilkinson, B.M. Jenkins (eds), *Aviation Terrorism and Security*, London 1999.

"Terror Plot BA Man Rajib Khan Gets 30 years", *BBC News*, 11 March 2011, at https://www.bbc.co.uk/news/uk-12788224.

The United States Department of Justice, "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research", 19 July 2021, at https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion.

TSA. "UK 2006 Liquid Explosives Plot Trial Overview", at https://www.tsa.gov/press/releases/2008/09/08/uk-2006-liquid-explosives-plot-trial-overview.

Wallis R., *Combating Air Terrorism*, Washington 1993.

Wallis R., *Lockerbie: The Story and the Lessons*, Westport 2001.

Wallis R., "The Role of International Aviation Organisations in Enhancing Security", in P. Wilkinson, B.M. Jenkins (eds), *Aviation Terrorism and Security*, London 1999.

Whitehead M.K., "Safe Cyber: GE Aviation's Cybersecurity Leader Talks Data Protection and STEM", *GE Aerospace. The Blog*, 7 June 2019, at https://blog.geaviation.com/technology/safe-cyber-ge-aviations-cybersecurity-leader-talks-data-protection-and-stem/.

Wilkinson P., "Enhancing Global Security?", in P. Wilkinson, B.M. Jenkins (eds), *Aviation Terrorism and Security*, London 1999.

Wilkinson P. (ed.), *Homeland Security in the UK*, London 2007, https://doi.org/10.4324/9780203087459.

Wilkinson P., *Terrorism versus Democracy: The Liberal State Response*, London 2006, https://doi.org/10.4324/9780203087336.

World Economic Forum, "Advancing Cyber Resilience in Aviation: An Industry Analysis", January 2020, at https://www3.weforum.org/docs/WEF_Cyber_Resilience_in_Aviation_An_Industry_Analysis.pdf.

World Economic Forum, "Cybersecurity in Aviation: Building a Resilient Future", 2 June 2021, at https://www.weforum.org/impact/we-are-building-a-cyber-resilient-future-for-the-aviation-sector.

World Economic Forum, "Pathways Towards a Cyber Resilient Aviation Industry", 14 April 2021, at https://www.weforum.org/reports/pathways-towards-a-cyber-resilient-aviation-industry.

Briony CALLANDER is a visiting research fellow at the University of South Wales. Dr Callander obtained a BSc in Aerospace Business Systems and an MA in Intelligence and Security Studies from the University of Salford and a PhD in EU Politics from the University of Dundee. Dr Callander worked as a Lecturer in International Studies at the University of Salford. As a PhD researcher Dr Callander has had success in achieving significant research funding including securing a prestigious UACES Scholarship and the Lord Cockfield Scholarship.

Christian KAUNERT is Professor of International Security at Dublin City University, Ireland. He is also Professor of Policing and Security, as well as Director of the International Centre for Policing and Security at the University of South Wales. In addition, he is Jean Monnet Chair, Director of the Jean Monnet Centre of Excellence and Director of the Jean Monnet Network on EU Counter-Terrorism (www.eucter.net). He has recently been awarded a Jean Monnet Teaching Training Grant EUACADEMY, as well as a research grant by the Swedish Research Council.