sciendo

Land Forces Academy Review
Vol. XXVII, No. 1(105), 2022

THE NEED FOR A GLOBAL AVIATION CYBERSECURITY DEFENSE POLICY

Calvin NOBLES
Illinois Institute of Technology, Chicago, USA
cnobles1@iit.edu

Darrell BURRELL
The Florida Institute of Technology, Melbourne, Florida, USA
darrell.burrell@yahoo.com

Tyrone WALLER
Capitol Technology University, Laurel, USA
waller.t9@gmail.com

ABSTRACT

Commercial aviation is vital to the economic health of the global economy. Commercial aviation as a global entity should be an international critical infrastructure that constantly safeguards and protects from malicious threats, including cybersecurity threat actors (Nobles, 2019). The international aviation industry needs a comprehensive cybersecurity defense plan to prevent cyber-based threats from negatively impacting civil aviation. Critical components of the global aviation systems consist of airport operations, air traffic management, ground operations, airline operations, unmanned systems, operations (Kessler, Craiger, & Haass, 2018), aviation maintenance, airport security (physical security), and cargo and logistics. The existing aviation infrastructure was designed, engineered, and implemented without forbearance on cybersecurity (Kessler, Craiger, & Haass, 2018). The lack of international cyber governance impedes the enforcement of cybersecurity policies; therefore, requiring a global-based alliance to create standards and best practices for evaluating and managing cybersecurity risks (Urban, 2017), especially in commercial aviation.

KEYWORDS: aviation, civil aviation, cybersecurity, globalization, hyperconnectivity, policy, technology

1. Introduction

The global economic value of civil aviation is 3.5 percent of the gross domestic product, equating to $2.7 trillion and 62.7 million jobs (Aviation Benefits, 2017). Civil aviation has direct and indirect economic and employment implications on other industries as a vector for global trade and electronic commerce by quickly transporting products to markets (Aviation Benefits, 2017). Eighty-seven percent of business-to-business transactions are conducted via civil aviation, highlighting a dependency on aviation as a transport platform (Aviation Benefits, 2017). Researchers are forecasting that passenger volume and air freight will double by 2034 (Aviation Benefits, 2017); thus, making the protection of civil aviation a top priority.

DOI: 10.2478/raft-2022-0003

Governments worldwide recognize the need for increased vigilance to protect civil aviation from cyber-attacks; however, the low cost of malicious cyber payloads and the opportunity to remain anonymous makes such attacks feasible (Nobles, 2019). A cyber-attack on civil aviation will have economic, diplomatic, political, security, and social implications (Nobles, 2019). Integrating digital technologies in civil aviation increased usability, optimization, and safety (Nobles, 2019). Given the diverse nature of airports ranging from smart airports to rudimentary infrastructure, the challenge is creating a cybersecurity culture, awareness, and practices in less developed countries to prevent a pervasive cybersecurity threat from wreaking havoc on a significant portion of the commercial aviation in the region. Therefore, a Global Aviation Cybersecurity Defense Plan in which stakeholders implement standardized practices is necessary. A global cyber defense plan could enforce domestic regulations, policies, and procedures; however, the intent is not to upend existing security postures but to create a cyber defense umbrella to reinforce prevailing defensive postures and fill the gaps in countries that struggle with cybersecurity. This research aims to instigate discourse and scholarly research to support a global aviation cybersecurity defense.

2. Implications of System of Systems in Civil Aviation

Information, communication, and navigation systems within an aviation architecture are hyperconnected and provide essential services throughout the aviation traffic management network. Architecturally, aviation systems' hyperconnected and interconnected nature at the national, regional, and international levels are ideal for cybersecurity attacks. Thus far, cybersecurity attacks have occurred transoceanically, consequently inflicting security and financial devastation across the globe. Hyperconnected networks and systems continuously communicate to support critical infrastructure, such as global aviation systems (Nobles, 2019). Today's aviation infrastructure is hyperconnected, highly integrated, and dependent on individual systems within the more extensive network (Nobles, 2019). Another concern regarding the system of systems framework at the international level is the lack of standardization of certification and accreditation because each country uses different criteria for assessing the security robustness of its aviation infrastructure. For example, the U.S. aviation infrastructure is uniquely different from the U.K.; yet, commercial airlines transition both countries' airspace as necessary without any global cybersecurity defense standards. A Global Aviation Cybersecurity Defense Plan can provide the framework to address the negated and overlooked security concerns.

The vastness of the aviation operations and security systems is one of the largest in the world, McFarlane and Hill (2014) classified the aviation infrastructure as the *"mother of all socio-technical problems"* (p. 225). Aviation organizations are constantly integrating advanced technologies to reduce risks; hence, the repeated shuffling of people, processes, and technology in a system of systems is inherently risky. Malicious actors are aware of these gaps and will exploit them, requiring the rapid integration of global cybersecurity defense strategies.

The absence of international aviation cybersecurity policies threatens the financial and security freedom relished by businesses, governments, and consumers. At issue is the growing dependency on autonomous and intricate designs of aviation systems and technologies that manage complicated issues in international aviation (McFarlane & Hills, 2013) in which national, regional, and global systems operate without any underlying

international aviation cybersecurity regulations or policies. This oversight could be the vector that malicious actors exploit due to the foundational weaknesses from geopolitical, diplomatic, and multipolar variability. In addition, the latency of laws, regulations, and policies stemming from technological advances in the cyber domain (Dombrowski & Demchak, 2014) is a significant challenge.

3. Synchronizing International Efforts

Aviation organizations, including commercial airlines, should demand a global aviation cybersecurity defense policy from a business perspective. Many nations rely on commercial aviation, free from political, security, and economic disruptions compounded by an insalubrious dependency on technological systems (McFarlane & Hills, 2013). Organizations such as the (a) Association of Southeast Asian Nations (ASEAN), (b) the Collective Security Treaty Organization (CSTO), (c) Shanghai Cooperation Organization (SCO), (d) the North Atlantic Treaty Organization (NATO), (e) the Organization of American States (OAS), (f) the European Union, (g) the International Telecommunication Union, (h) Organization for Security and (i) Co-operation in Europe (OSCE), and (j) the United Nations (McFarlane & Hills, 2013) are critical entities for promoting the need for a global-based cybersecurity plan in aviation. An influential juggernaut at the nexus of global aviation accompanies the ICAO to serve as the international body to lead efforts in garnering support for a global aviation cybersecurity plan.

4. Economic Underpinning of Civil Aviation

Civil aviation is a growing concern in the continuous integration of technology, progressive innovation, and easiness to acquire malicious cyber payloads from the dark web, outdated regulations, and policies in numerous areas within the aviation ecosystem (Cooper, 2017). The need for overarching national and international policies regarding cybersecurity defense in global aviation is to ensure the safety of civil aviation from cyber threats and prevent any potential disruptions that might inflict economic implications on the international economy. The U.S. and the U.K. list civil aviation as critical infrastructure (Copper, 2017); however, this is not enough and calls for every nation to list civil aviation as critical infrastructure. The dependency on civil aviation demonstrates the global populace's affinity for air travel and transport.

5. Global Cybersecurity Issues in Aviation

Aviation-based businesses continue to struggle with the inevitable changes in technology compelled by the cybersecurity threat landscape. Given the multidisciplinary and interdisciplinary complexity associated with developing an international cybersecurity defense policy, many challenges could impede the development of a global cybersecurity defense plan. In addition, the interplay between business, security, and geopolitics are significant factors in securing aviation from cybersecurity threats. The sections below provide in-depth perspectives on challenges with developing an international aviation cybersecurity defense plan.

5.1. Lack of International Cybersecurity Policies in Aviation

Cooper (2017) emphasized that the practicality of innovation, technological change, and adversary capability advancement averts policy and regulation development in the global aviation ecosystem. International aviation cybersecurity policies are required to address the technology risks (Cooper, 2017); the U.S. and U.K. are critical stakeholders in driving global policies in

aviation. The International Civil Aviation Organization (ICAO), an entity of the United Nations, is positioned to serve as the governing body and lead agency to bring other international governing bodies, governments, states, and aviation organizations together to develop frameworks, policies, and regulations which will be a slow and deliberate process (Cooper, 2017). This existing foundation needs to be leveraged in discussing policy solutions centric to the U.S. and the U.K. but all nations seeking to become partners and contributors.

The AeroSpace and Defence Industries Association of Europe (ASD) contended that the international orientation of aviation cybersecurity is paramount as a diplomatic matter throughout the European Union because unbalanced regulatory advances can be problematic across the globe (ASD, 2017). Therefore, regulatory alignment of civil aviation cybersecurity policies and requirements should be an elevated diplomatic matter and a top priority for all nations with commercial aviation activity. According to ASD (2017), commercial aviation is the safest form of transportation; however, with increasing cybersecurity threats to the aviation industry, all industries and organizations are prone to more sophisticated cyber-attacks.

5.2. The Global Aviation Ecosystem as an International Critical Infrastructure

A reputable consulting firm indicated that 85 % of Chief Executive Officers (CEO) are concerned with risk compared to 71% of CEOs in other industries (Urban, 2017). Cyber-attacks on Spanair and the Malaysian Civil Aviation Department, the blocking of 2.9 million cyber hacks from July 2010 to July 2011, and numerous other malware attacks throughout the international aviation community (Urban, 2017) call for swift action to safeguard international aviation travel. With global aviation increasingly relying on information communication technologies (De Gramatica, Massacci, Shim, Tedeschi, & Williams, 2015), coupled with the unsustainable pace and cost of rapid changes to upgrade software, hardware, internet of things, and information technology infrastructure, is indicative of the forecasted $1T cybersecurity spending between 2017 to 2021 (Morgan, 2016). The interconnected nature of cybertechnologies in national, regional, and international aviation systems is susceptible to cyber-attacks as airports throughout the world are continually mitigating cyber threats, internet misuse, and setbacks from malware infecting operational systems (Haas, Sampigethaya, & Capezzuto, 2016). Undoubtedly, aviation is inherently dangerous, especially with the added perils of cybersecurity, requiring global aviation entities to take aggressive actions to protect critical aviation systems. Cybertechnologies in aviation are interconnected systems beyond national and regional dimensions.

Establishing the global aviation ecosystem as an international infrastructure would increase security prioritization. Urban (2017) argued that the lack of global standardization is a significant problem as a cyber-attack at one location can cascade through the networks and impact other international aviation organizations due to the hyperconnected state of the information technology infrastructure. The global aviation community can collectively leverage resources and security practices to avert cybersecurity attacks as an international infrastructure. Classifying the global aviation ecosystem as an international infrastructure can provide the means of proactively prioritizing the security protection of critical systems (Haas, Sampigethaya, & Capezzuto, 2016). Aviation is too vital for the international community. Therefore, aviation inherently deserves protection as a global critical infrastructure to safeguard the technologies and infrastructure to protect the passenger.

Another issue impacting global aviation is the lack of international cyber governance (Urban, 2017). With global aviation as an international critical infrastructure, countries could work collaboratively in a joint and federated orientation to design and implement regulations, rules, and governance oversight practices analogous to how International Civil Aviation Organization (ICAO) directs guidance on international aviation operations. The scope of these regulations, policies, and governance oversight will only apply to the jurisdiction of global aviation. This approach could increase international discourse on agreeing to global internet practices. Global aviation entities, governments, and international bodies like ICAO should consider global aviation an international infrastructure. A Global Aviation Cybersecurity Defense Plan is acceptable if international aviation is deemed a critical infrastructure.

5.3. International Norms to Protect Global Aviation

Cyberspace continues to evolve as a new frontier for businesses, organizations, and governments for (a) advancing economic growth and maturity, (b) capital development, (c) information sharing, (d) global connectivity, and (e) improved international relations (Demchak, 2013). Cyberspace serves as a platform for state and non-state actors to conduct offensive and coercive behavior that impedes the aforementioned purposes (Demchak, 2013). The growing dependence on civil aviation and the necessity to protect the international populace, businesses, governments, and other organizations need to advocate for an international norm signed by all countries to safeguard global commercial aviation and its associated ecosystems from any directed or unintentional offensive cyber-attacks. The norm should call for states to work collaboratively to safeguard civil aviation at all causes given the need to protect the populace, global economic implications, and disruption to international air travel. The lack of standardized law, practices, and interpretation between countries regarding cybersecurity is indicative of this critical covenant in support of global aviation, which is good business, international security, and public safety.

5.4. International Cybersecurity Standardization in Aviation

The lack of standardized cybersecurity practices in global aviation could increase the organization's susceptibility to cybersecurity incidents. Urban (2017) postulated the likelihood of attaining cybersecurity standardization on an international level, given that the different perspective on norms and laws is challenging. It is worth exploring the standardization from a practical level to understand the challenge holistically. For example, Jaatun and Koelle (2016) questioned the necessity of a European Computer Security Incident Response Team during a cybersecurity incident. A Cybersecurity Event Response Team (CERT) is applicable in many variants, including scale and scope; therefore, it depends on the country's practices. Standardizing cybersecurity practices is paramount in global aviation because each country has a different way of executing cybersecurity functions. Using ICAO as a global example of developing international regulations and policies is a similar approach that cybersecurity will need to imitate, especially if the global aviation ecosystem becomes an international infrastructure.

In the book, *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, the author discussed the significance of international norms in cyberspace as a method to reduce variability and increase predictability (Hurwitz, 2016). Standardizing cybersecurity practices in

global aviation is beneficial in dealing with threats, security incidents, policies, and jurisdiction; however, it is not beyond reach. Global aviation is a significant business multiplier for the international community; yet, cybersecurity in all aviation sectors is an immense vulnerability. Through standardization, countries can improve security, exchange information, and enhance cybersecurity resiliency by implementing best practices (Urban, 2017). The standardization will be narrowly applied to global aviation to ensure that cyber threats are minimized and mitigated and that the international populace is protected during global aviation operations.

6. A Global Aviation Cybersecurity Defense Policy

Regarding the development of a global cyber defense plan with international implications, it is imperative to highlight that cyberspace is cluttered with a vigorous and diverse array of norms, national and regional regulations, international laws, standards, political concords, and technical controls that impact cybersecurity (Finnemore & Hollis, 2016). At this time, there is no lawfully binding international regulation enforcing cybersecurity defense in aviation due to cyberspace being a contestable area (Fox, 2016) or a central cyber authority (CCA) (Matania, Yoffe, & Goldstein, 2017). Researchers highlight the significance of a CCA; undoubtedly, the international community needs a leading cyber authority to enforce cyber defense preparation (Matania, Yoffe, & Goldstein, 2017). The ICAO is a central authority entity yet does not have any sovereign mandates in which Articles 54 and 37 are not enforceable internationally (Emanuilov, 2019).

The American Institute of Aeronautics and Astronautics (2013) Decision Paper titled, *Framework for Aviation Cybersecurity* cited the need for (a) established universal cyber standards for aviation systems, (b) establish a cybersecurity culture, (c) identify threats and risks, (d) disseminate the threat information to enhance situational awareness, (e) build an incident response capability, (f) strengthened cybersecurity defenses, and (g) establish partnerships with academia, industry, and government. In 2014, the International Air Transportation Association (IATA), the International Civil Aviation Organization (ICAO), the Civil Air Navigation Service Organization (CANSO), and the International Coordinating Council of Aerospace Industry Associations agreed to synchronized initiatives and actions to combat cybersecurity threats ("Cyber Security", n.d.). There are existing unified international cohesive platforms to address critical issues in civil aviation; however, a global effort to articulate cybersecurity defense efforts is imminent as cybersecurity threats continue to plague organizations worldwide. Developing a cybersecurity defense plan mandates governments, organizations, and aviation industry stakeholders as critical elements to creating a cybersecurity umbrella to protect all aspects of civil aviation from cyber threats and vulnerabilities.

The Decision Paper listed above identified the following imperatives for the global aviation community in developing a roadmap (AIAA, 2013):

1. Cultivate a cybersecurity culture;
2. Know the threat;
3. Identify the risk;
4. Discuss the threat and increase situational awareness;
5. Conduct incident response;
6. Increase the defensive posture and systems;
7. Define design principles;
8. Define operational principles;
9. Engage in research and development;
10. Build partnerships between government and industry.

There is no shortage of national or regional level organizations and state sponsorship to promote a global defense policy. A significant hurdle is creating standardization and a shared understanding of cybersecurity (AIAA, 2013), akin to ICAO providing flight operations regulation to govern flights in international airspace. A global cybersecurity defense plan could provide a strategic approach for promulgating guidance to international civil aviation stakeholders. The salient objective is to protect global commercial airlines from the perils of increasing and persistent cybersecurity threats by ameliorating cybersecurity defenses.

7. Conclusion

Global commercial aviation is too economically vital for cybersecurity defense gaps to exist. Global aviation is susceptible to cybersecurity vulnerabilities that threatens the international aviation industry. A comprehensive international aviation cybersecurity policy can reduce the gaps, solidify defensive postures, and increase information sharing and communication. The interconnected technological infrastructure and ecosystems in aviation connect business and flight operations worldwide. As the threat landscape evolves and creates vulnerabilities, malicious actors will continue to capitalize on weaknesses in the infrastructure and systems. A global cybersecurity defense policy could mitigate gaps and prevent nefarious activity within the aviation industry and associated business community.

REFERENCES

Aerospace and Defense Industries Association of Europe. (2017). *Position Paper on of the ASD Civil Aviation Cybersecurity Task Force*. Available at: https://www.asd-europe.org/position-paper-of-the-asd-civil-aviation-cybersecurity-task-force.

Aviation Benefits. (2017). *Aviation Benefits 2017 Report: The importance of aviation on supporting the global economy*. Available at: https://etradeforall.org/aviation-benefits-2017-report-importance-aviation-supporting-global-economy/.

Cooper, P. (2017, November). *Aviation cybersecurity: Finding lift, minimizing drag*. Available at: https://www.atlanticcouncil.org/publications/reports/aviation-cybersecurity-finding-lift-minimizing-drag.

Cyber Security. (n.d.) Fact sheet. Available at: https://www.iata.org/pressroom/facts_figures/fact_sheets/Documents/fact-sheet-cyber-security.pdf.

Demchak, C.C. (2013). Economic and political coercion and a rising cyber Westphalia. *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, 595-620.

De Gramatica, M., Massacci, F., Shim, W., Tedeschi, A., & Williams, J. (2015). IT interdependence and the economic fairness of cybersecurity regulations for civil aviation. *IEEE Security & Privacy, Vol. 13, Issue 5*, 52-61.

Dombrowski, P., & Demchak, C. (2014). Cyber War, cyber conflict, and the maritime domain. *Naval War College Review*, *Vol. 67, Issue 2,* 70.

Emanuilov, I. (2019). *International (Cyber) security of the Global Aviation Critical Infrastructure as a Community Interest*.

Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *American Journal of International Law*, *Vol. 110, Issue* 3, 425-479.

Haass, J., Sampigethaya, R., & Capezzuto, V. (2016). Aviation and cybersecurity: opportunities for applied research. *TR News*, *No. 304*, 39.

Hurwitz, R. (2016). A New normal? The cultivation of global norms as part of a cybersecurity strategy. *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, 233-64.

Jaatun, M.G., & Koelle, R. (2016, August). Cyber Security Incident Management in the Aviation Domain. *11th International Conference on Availability, Reliability and Security (ARES)*, 510-516. IEEE.

Kessler, G.C., Craiger, J.P., & Haass, J.C. (2018). A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identification system. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, Vol. 12, Issue 3*, 429.

Matania, E., Yoffe, L., & Goldstein, T. (2017). Structuring the national cyber defence: In evolution towards a Central Cyber Authority. *Journal of Cyber Policy*, *Vol. 2, Issue 1*, 16-25.

McFarlane, P., & Hills, M. (2013). Developing immunity to flight security risk: prospective benefits from considering aviation security as a socio-technical ecosystem. *Journal of Transportation Security, Vol. 6, Issue 3*, 221-234.

Morgan, S. (2016). *Cybersecurity spending outlook: $1 trillion from 2017 to 2021*. CSOOnline. Available at: https://www.csoonline.com/article/3083798/cybersecurity-spending-outlook-1-trillion-from-2017-to-2021.html.

Nobles, C. (2019). Cyber threats in civil aviation. In *Emergency and Disaster Management: Concepts, Methodologies, Tools, and Applications* (pp. 119-141). IGI Global.

Urban, J.A. (2017). Not your granddaddy's aviation industry: The need to implement cybersecurity standards and best practices within the international aviation industry. *Albany Law Journal Science and Technology, Vol. 27*, 62.