



Intelligence and Airport Security: A SWOT Analysis of the Brazilian Scenario

David Medeiros Oliveira^{1,*} , Donizeti de Andrade¹ , Arthur Maximus Monteiro² 

1. Departamento de Ciência e Tecnologia Aeroespacial  – Instituto Tecnológico de Aeronáutica – Divisão de Engenharia Aeronáutica – São José dos Campos (SP), Brazil. **2.** Universidade de Lisboa  – Faculdade de Direito – Centro de Estudos Jurídico-Políticos – Lisboa, Portugal.

*Correspondence author: medeirosoliveira@gmail.com

ABSTRACT

The Brazilian airport infrastructure arises under the government management, through a public company created especially for it: the Brazilian Airports Infrastructure Company (Infraero). This management model thrived until the early 2000s, when the concessions of Brazilian airports to the private sector started. Since the Brazilian Intelligence System (SISBIN) was created in 1999, Infraero has been under a federal government's cabinet with a seat at the system. After the concessions' processes started, though, some of the main airports in the country are not under SISBIN's formal umbrella anymore. This paper uses a SWOT matrix to analyze the scenario that comes out after of the migration of the airport management to the private sector under the Intelligence activity's scope.

Keywords: Intelligence; Airport security; Critical infrastructure concessions; SWOT matrix.

INTRODUCTION

The Brazilian aeronautical tradition was sided by the formation of the necessary infrastructure for the conditioning, maintenance and operation of aircraft: the airfields. Brazil is worldly ranked in second regarding to the number of airfields—only behind the United States of America (USA). The quantity of airfields in Brazilian territory exceeds China by approximately 8 times (CIA 2020).

Of the more than 4,000 aerodromes in the country, around 580 are approved by the National Civil Aviation Agency (ANAC). Among the approved ones are those of which interruption or destruction, in whole or in part, has the potential to cause a serious social, environmental, economic, political, international impact or to the security of the State and society. These airfields are considered critical infrastructures by the Brazilian law and demand special attention from the government agencies.

In the history of commercial aviation around the world have been more than 600 hijackings and more than 100 aircraft explosions attributed to terrorism. Although many rules, policies and operational procedures have been introduced over the years to mitigate risks, terrorism and other threats are still active in the 21st century (Young and Wells 2014).

According to Maleiner (2020), the probabilities of accidents and the severity of their consequences are the object of coordinated efforts to control and reduce them, through various actions, practiced by various actors, such as national and international organizations, both public and private, regulators, operators and various service providers. The articulation of these actions is guided by the fundamental pillars of aviation security, which are written in norms, from the most diverse hierarchies, from constitutional provisions to normative instructions (Fig. 1).

Received: May 29, 2022 | Accepted: Aug 19, 2022

Peer Review History: Single-Blind Peer Review.

Section editor: Ana Morais



This is an open access article distributed under the terms of the Creative Commons license.

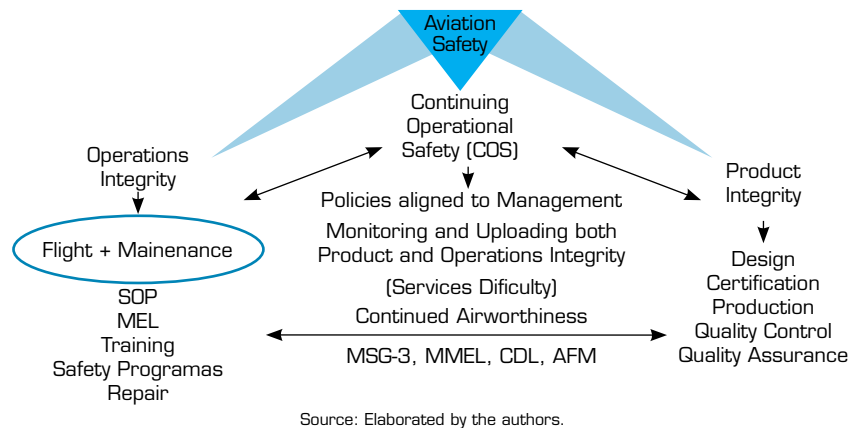


Figure 1. Aviation security pillars.

In Brazil, the complex environment of Civil Aviation is under a wide spectrum of norms that regulate the relationship between the government and other actors, with different degrees of cooperation and intensity. Airport security is the object of several public policies. As examples, could be mentioned the National Civil Aviation Security Plan against Acts of Illicit Interference (Brazil 2010) and the National Intelligence Policy (Brazil 2016), the latter also known as PNI.

In the context of the security of critical national infrastructures, including the airports, the sharing of Intelligence with the Brazilian Intelligence System (SISBIN) has the potential to be a tool for improving situational awareness. Such integration is essential for implementing the principles of prevention and precaution, in order to improve the resilience and guarantee the continuity of the operation of the airport.

Infraero (a federal public company) has always been under a cabinet with a seat at SISBIN. Since 2011, however, some of the country's main airports have gone or are going to be under private control—some of which under foreign management.

If towards the airports that remain under the administration of Infraero the sharing of Intelligence occurs through SISBIN, in relation to the airports operated by private entities the law requires previous accreditation for the treatment of classified information.

Sharing intelligence with government agencies has the potential to allow the operator of critical national infrastructure—including airports—to increase awareness towards identified and identifiable threats. Although most of the works published after 9/11, especially Anglo-Saxon ones, have terrorism as their main factual basis, threats are not restricted to this phenomenon. The PNI (Brazil 2016) provides, for example, eleven threats, including organized crime and cyber-attacks.

The airport's concession processes in Brazil were not accompanied by policies regarding accreditation for handling classified information by private airport administrations. The situation apparently creates a legal vacuum concerning the intelligence sharing process. To analyze how this scenario emerges after the concessions of Brazilian airports, this paper uses a SWOT matrix as a situational analysis tool.

Given the fact that national intelligence is guided by threats and opportunities, the SWOT matrix seems to be timely and adequate for analyzing a country's Intelligence System and its subsystems.

METHODS

The SWOT Analysis

The SWOT analysis was born at the Harvard Business School (HBS), in the early 1950s, when the comparison of a company's organizational strategies with the external environment began (Panagiotou 2013). The formation of the matrix then becomes a tool for the analysis of case studies. The acronym SWOT stands for strengths, weaknesses, opportunities and threats.

In the 1980s, Weihrich (1982) published a case study on Volkswagen and introduced the SWOT matrix as a situational analysis tool. Since then, his work is considered the most important reference on the subject.

The matrix, as it does not have a predefined structure and allows the combination with other methodologies, demonstrates a resilience that allows it to be used, until the present day, in the formulation of policies (public and corporate), as well as in decision-making and strategic planning.

According to Lambert (2021), although the SWOT analysis has historically been used by the corporate world as a tool to identify factors that promote or inhibit the implementation of business policies, there are several points of communion with intelligence agencies: while business entities seek to maximizing profit to remain operational and competitive, an intelligence agency seeks to maximize national security in order to continue receiving state resources and remain competitive with other intelligence agencies, inside and outside its country. It is based on the reasons above that it is believed, therefore, to be the matrix adequate for the analysis of a national intelligence system.

The perception of threats and opportunities serves as an azimuth for intelligence services all over the world. PNI (Brazil 2016) is the main framework for the Intelligence activity in the country.

For the purpose of the matrix object of this paper, the following will be considered as: i) threats, those foreseen in the PNI; ii) opportunities, the guidelines provided by the PNI. The analysis of the internal environment, however, will be based on a certain subjectivity on the part of the author (a limitation that coexists with secrecy, always conditioning papers about Intelligence).

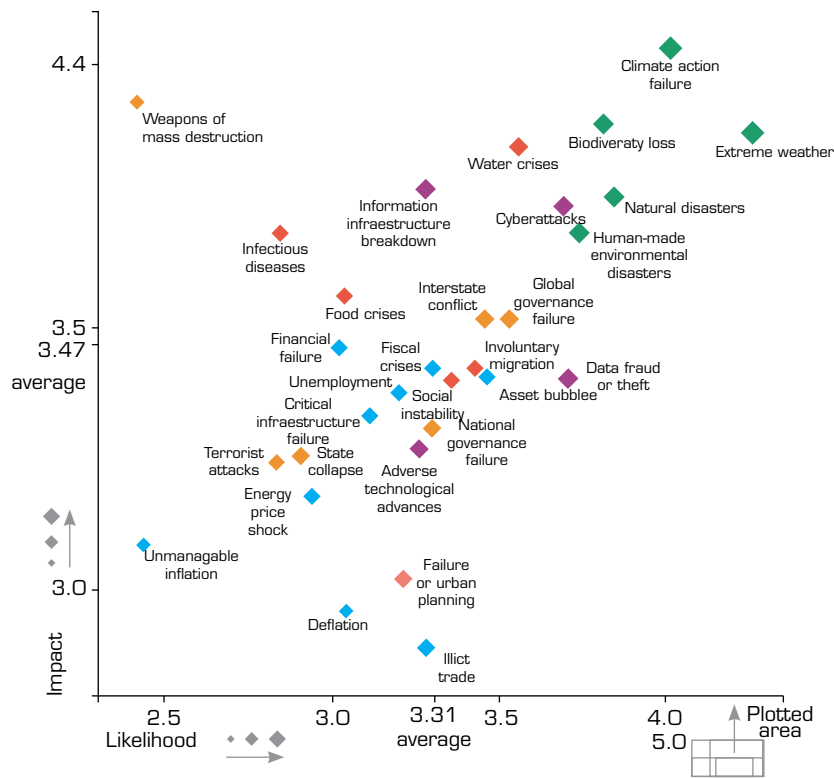
According to Weihrich (1982), the process can become complex when many factors are identified. Thus, it is necessary to reduce the factors so that the matrix becomes intelligible.

Thus, for the purpose of forming an intelligible SWOT matrix, the parameters of the classic SWOT matrix—applied to Volkswagen—will be followed. The Volkswagen matrix is composed by three threats, three opportunities, three strengths and three weaknesses.

Threats

The first mission is to establish criteria for choosing three among ten threats foreseen in the PNI. Annually, the World Economic Forum (WEF) publishes a Global Risks Report, a document prepared in partnership with academia (National University of Singapore, University of Oxford and University of Pennsylvania). Thus, the threats foreseen in the PNI are crossed with those foreseen by the WEF’s Global Risk Report.

When comparing the threats foreseen in the PNI with the WEF’s Global Risk Report matrix (Fig. 2), the most severe ones are weapons of mass destruction; and the most likely are cyberattacks.



Source: Retrieved from WEF (2020).

Figure 2. Risk matrix.

According to Miranda Filho (2016), the discourse created in the USA after the 9/11 attacks has spread the notion that terrorism was the new global threat and that all countries should join the USA in this crusade. Speeches were launched through academic articles, mainly on Political Science, Defense and Intelligence topics, in the massive and generalized press, in official speeches by authorities and in any communication that dealt with security issues. For Miranda Filho (2016), the avalanche of speeches was so great that it became embarrassing for any security analyst, whether civilian or military, linked to the government or the private sector, to express the opinion that terrorism was not the greatest global threat. There were virtually no dissenting voices.

Brazil felt the impact of this narrative when the Department of Counterterrorism was created in 2008 within the Brazilian Intelligence Agency (ABIN)'s structure. It should be noted that this narrative remains present even in countries that do not share the terrorism reality and among the main examples are the security procedures used in Civil Aviation.

Thus, despite the fact that much of the papers about Intelligence and airport security have terrorism as a background, the phenomenon in the quadrant of low impact and probability of the WEF's Global Risk Report. On the other hand, although it is not listed as an isolated phenomenon in the WEF's Global Risk Report matrix, organized crime, due to its impacts on the formulation of public policies by the Brazilian Government, should be chosen to compose the matrix.

The theme is present in the WEF's matrix in a diffuse way, under other names: illegal trade, fraud and data theft. In Brazil, these modalities are often under the control of a couple of criminal organizations, often commanded and born within prison institutions (state collapse).

Weapons of Mass Destruction

According to the PNI, weapons of mass destruction are a threat that affects all countries. The mere existence of weapons of mass destruction (chemical, biological and nuclear) is a potential source of proliferation. In addition, it represents a risk to world peace and to the countries that have abdicate the option of these weapons for their defense. To counter the threat, two imperatives stand out: non-proliferation and elimination of existing stocks.

Intelligence actions in this area contributes to the protection of the Brazilian population and critical infrastructure against possible effects of the use of weapons or artifacts produced from these goods or technologies.

Despite the low probability, among the threats foreseen in the PNI, it is the one with the greatest impact on the WEF matrix. For Soares (2020), the reduced history of incidents related to weapons of mass destruction and dual-use goods in Brazil should not serve as an excuse for the relaxation of preventive measures, especially in such a complex, dynamic and vulnerable sector as Civil Aviation.

Cyber-attacks

According to the PNI, cyber-attacks are deliberate actions, with the use of information and communications technology resources, aimed at interrupting, penetrating, tampering with or destroying networks used by public and private sectors essential to society and the State, such as those part of the national critical infrastructure, as airports.

The losses resulting from actions in cyberspace do not come only from the commitment of information and communications resources. They also result from the manipulation of opinions through actions of propaganda and disinformation.

There are countries that openly seek to develop the capacity to act in the so-called cyber war, even though attacks of this nature can be carried out not only by government agencies, but also by criminal groups, sympathizers of specific causes or even by nationals who come to support actions that are antagonistic to the interests of their country.

Of all the threats predicted in the PNI, cyber-attacks are located in the quadrant of greatest impact versus greatest risk by the analysis of the WEF.

According to Valor Econômico (2021), Eletrobrás, a Brazilian company that is responsible for generating 28% of the countries' energy, reported that its subsidiary responsible for the nuclear plants at the Angra dos Reis complex was a target of cyber-attack. The attack on Eletrobras' nuclear power unit follows other incidents that have recently hit companies in various sectors in Brazil, including electric power companies (such as Copel, from the state of Paraná), which are also critical infrastructures.

Organized Crime

Organized crime is a threat to all countries and deserves special attention from national and international intelligence and law enforcement agencies. Its transnational aspect reinforces the need to deepen cooperation.

Increasingly integrated action in the preventive (Intelligence) and reactive (Police) aspects of the organized crime appear to be the most effective way to face the phenomenon, especially when Intelligence sharing subsidizes procedures for identifying and interrupting the financial flows that support it.

In 2017, 60 rifles (AK-47, G3 and AR-15) were seized at the cargo terminal at the Rio de Janeiro/Galeão International Airport; in 2018, men armed with rifles subtracted USD 5 million from a Lufthansa plane, in Campinas, São Paulo state; in 2019, in an action that ended with three suspects dead and involved a 10-month-old child as hostage, a heavily armed group entered, in trucks characterized as Brazilian Air Force's vehicles in the yard of the cargo terminal at Viracopos Airport; also in 2019, criminals entered the cargo terminal at Guarulhos International Airport and stole 720 kg of gold. The situation involved hostages, the use of rifles and the use of cars characterized as if they belonged to the Brazilian Federal Police.

The Port of Santos, as widely publicized, is a critical national infrastructure under the influence of a criminal faction whose tentacles reach also the security structure of the Guarulhos Airport, the largest in Latin America.

In Brazil, in addition to repression actions, the fight against organized crime is the object of a specific Intelligence Task Force, created by the Decree N. 9527 (Brazil 2018) which aims to analyze, share and produce intelligence reports aimed at subsidizing the elaboration of public policies and government action.

Opportunities

Increase the Reliability of the SISBIN

Access to intelligence is valuable since it is reliable, as well as the professionals who are part of SISBIN. The dissemination of falsified or inaccurate Intelligence can compromise the decision-making chain. Unauthorized disclosure of classified documents also harms intelligence agencies, directly affecting their credibility. In this context, SISBIN's reliability must be continually increased by improving the process of selecting human resources for the Intelligence area.

Training programs and effective implementation of corporate security countermeasures are essential for the security and the development of the intelligence activity.

Strengthen the Culture of Knowledge Protection

Unauthorized access to techniques, innovation processes, research, plans and strategies, as well as genetic heritage and associated traditional knowledge, can compromise the achievement of national objectives and result in significant losses in the socioeconomic field.

The protection of sensitive knowledge is an essential factor for a country's development. Results that arise from scientific and technological research require continuous improvement of protection mechanisms, both in academic and business circles.

It is, therefore, essential and urgent to strengthen the culture of protection, with a view to establishing practices to safeguard knowledge on the part of those who hold it. Intelligence agencies must contribute to the dissemination of this culture as a way to avoid or minimize damages to the country.

Cooperate in the Protection of Critical National Infrastructures

Threats such as terrorism, transnational criminal and groups linked to acts of sabotage must be monitored as a way of minimizing the chances of actions aimed at interrupting or even compromising the functioning of national critical infrastructures.

Therefore, Intelligence agencies must participate in the process of evaluating risks and vulnerabilities related to potential targets of those threats.

Strengths

National and International operation

ABIN has branches in all of the state capitals in Brazil, as well as two subunits (Tabatinga and Foz do Iguaçu). The national scope (Fig. 3) contributes to provide the Agency with a unique capillarity and wide vision.



Source: Retrieved from ABIN (2021).

Figure 3. ABIN's offices in Brazil. Blue icon: Headquarters in Brasília; Orange icons: State Superintendencies; Yellow icons: Subunits.

In addition to representations in Brazil, ABIN has offices in 19 countries (Fig. 4), where Intelligence officers work as civilian attachés, exchanging information and producing knowledge on topics of interest.



Source: Retrieved from ABIN (2021).

Figure 4. ABIN's branches overseas.

As a comparison, the Brazilian agency that oversees Civil Aviation in Brazil (ANAC) is headquartered in Brasília and has some units throughout the country, but with less capillarity (Fig. 5). In addition to regional representations in Rio de Janeiro, São Paulo and São José dos Campos, ANAC is present in some states through the Regional Civil Aviation Centers.



Source: Retrieved from ANAC (2022).

Figure 5. ANAC's units in Brazil.

The scope of ABIN's activities, not to mention several other SISBIN bodies, has the potential to promote diversified situational awareness, contextualizing national and international topics of interest to Civil Aviation security.

Infraero also does not have the same number of branches that it is used to have in the recent past. Currently, there are states where the company is no longer present (Fig. 6).



Source: Retrieved from Infraero (2019).

Figure 6. Brazilian airports under Infraero.

Thus, ABIN's capillarity is perceived as positive. The ability to identify threats and opportunities has the potential to provide intelligence to airports all over the country.

Specialized Training

One of ABIN's responsibilities is to develop its human resources, in addition to carrying out studies and research for the improvement of the Intelligence activity.

The School of Intelligence (ESINT) is responsible for planning and executing training activities in Intelligence and in transversal and complementary competences, both for the Agency's intelligence officers and for those appointed by other SISBIN agencies. Also, entities that are partners of ABIN, even if they are not part of SISBIN, are currently eligible to have its personal trained by ESINT.

ESINT also cooperates with schools, teaching centers, libraries and other national and foreign training organizations.

Thus, the possibility of specialized training that is before airport operators, not only the professionals involved in security, but also managers and those who participate in the decision-making process, is a valuable asset to the country.

Culture of Protection

According to the National Doctrine of the Intelligence Activity (Brazil 2016), the Intelligence Activity, unlike the other apparatuses that are part of the State's core, is not based on force, but on knowledge and secrecy.

According to the aforementioned Doctrine, certain knowledge generated by the state bureaucratic apparatus, due to its strategic value from a political, military and economic point of view, imposes the use of state secrecy.

Although in a Republic the principle of publicity prevails, the policy of secrecy is admitted, especially by the provision of punishment for those who publicize reserved acts and documents. State secrecy, therefore, is legitimized by law.

ABIN's acts whose publicity may compromise the success of its confidential activities must be published in an extract. As an Intelligence agency, the care in dealing with secrets contributed to the creation of a culture that values the protection of knowledge.

The expertise in implementing measures of access control, protection of areas, accreditation, communication, among others, allowed ABIN a know-how that could be shared with public and private institutions.

Weaknesses

Absence of Data Sharing Culture Towards the Private Sector

In August 2020, two Brazilian political parties (Rede Sustentabilidade and Partido Socialista Brasileiro) filed a petition of which purpose was to question the provision of data to ABIN by the other SISBIN agencies.

According to the political parties, a sole request by the director of the agency would be enough for having access to confidential information and, despite the law has been published over 20 years ago, the way it has been interpreted compromises fundamental rights.

The Attorney General's Office, defending the constitutionality of the Law, highlighted that the rule has been in force for more than 20 years without questioning and that ABIN is subject to internal, judicial and parliamentary controls.

The Federal Supreme Court, in a plenary session held on August 13, 2020, partially granted a precautionary measure to establish that the component agencies of the SISBIN can only provide specific data and knowledge to the ABIN when the public interest is proven, ruling out any possibility of these data to serve any personal or private interests. According to the Court, all decisions that request data must be duly motivated, for possible legality control by the Judiciary.

The Court has decided that, even if there is public interest, Intelligence obtained through the interception of communications cannot be shared due to limitation of fundamental rights. The Federal Supreme Court also declared that, in the appropriate cases of providing information and data to ABIN, it is essential to establish a formal procedure and the sharing must be through a safe and secure electronic system, with access registration.

Although the judgment was not final, the decision has effects on the sharing of data within the scope of SISBIN since its publication. Therefore, data sharing under SISBIN must be under these circumstances: i) Evident public interest; ii) Motivation; iii) Formal procedure; iv) Electronic security systems with access records.

If Intelligence sharing within SISBIN faces limitations, formal sharing with private entities is a challenge. Only in the specific case would be possible to assess whether the public interest in promoting a safer Civil Aviation should prevail over the operator's interest in offering safety as an asset in order to, in the end, obtain profit.

The classification of the airport as a national critical infrastructure, however, serves as a guideline in the sense of generating the presumption of public interest when sharing Intelligence.

Limited operation in Aviation Security

Although it is believed that data sharing has a much broader spectrum than Aviation Security (AVSEC), with the potential to be an instrument for creating situational awareness on the part of the airport operator in the face of a variety of themes, there is this formal limitation.

There is nothing in the National Program for Civil Aviation Security against Acts of Unlawful Interference (PNAVSEC) about intelligence sharing under SISBIN. The System is only remembered when the Program gives the Federal Police the responsibility of “establishing threat levels to Civil Aviation security, in interface with ANAC, the airport administration and the bodies that are part of SISBIN” (Brazil 2010).

The PNAVSEC also provides that, after processing and classifying the threats, the Federal Police is responsible for the immediate dissemination of data and information to those bodies and systems, public and private, endowed with some competence in AVSEC, such as ANAC, COMAER, RFB, ANVISA, VIGIAGRO, public security agencies, air operators and airport administration (Brazil 2010). Once again, there is no mention of ABIN, limiting its access to the AVSEC environment in Brazil.

As explained, the legal text of PNAVSEC restricts the use of intelligence activity in AVSEC to the Federal Police and COMAER. It should be noted that ANAC, the Federal Police and the Ministry of Defense are included in SISBIN. They therefore have the legitimacy to contribute, within their competences, to State Intelligence. However, the interface of these bodies with the System does not make up for the absence of ABIN, since the Agency's main activity is to produce Intelligence; ANAC, Federal Police and Ministry of Defense have different scopes of action.

Both PNAVSEC and Brazilian Civil Aviation Regulation (RBAC) nº 107 do not provide for ABIN's participation as a permanent member of a Airport Security Commission (CSA), where facts related to AVSEC of each airport are discussed and shared. There is, though, a legal possibility for the Agency to join the meetings, depending on the approval of an invitation formalized by one of the members of the Commission.

Absence of Intelligence Mention in the Concession Notices

Completed, in 2021, 10 years of the federal program of airport concessions, 5 concession rounds were carried out and the operation of 22 airports was transferred to the private sector.

Once Infraero leaves the airport management, it automatically leaves SISBIN. None of the notices published during all the rounds—up to the time this paper was written—mentions this possibility. Often confused with a mere anticipation of safety and security issues, the Intelligence Activity loses the potential to advise the decision-making process of some of the main national critical infrastructures.

Interaction Matrixes

For Weihricht (1982), the matrix indicates four strategies that are conceptually distinct, although, of course, they can be executed in combination or independently. Once the SWOT acronyms that will form the matrix are identified, the focus should be on the potential for interaction between the four sets of variables. To this end, Weihricht suggests four interaction visualization schemes, which are:

- WT (mini-mini): aimed at minimizing weaknesses and threats;
- WO (mini-maxi): minimize weaknesses and maximize opportunities;
- ST (maxi-mini): aims to determine which forces are capable of facing threats;
- SO (maxi-maxi): aims to maximize both strengths and opportunities.

Thus, crossings are carried out in order to identify which are the preponderant factors, when they are related, and which are not related to each other. Relationships will be indicated with the character “+”; when the factors are not related to each other, the character “0” for neutrality, will be used. Note that the character “+” indicates the existence of a relationship, and the positive

or negative potentiation is not analyzed in the table. This analysis will occur after the verification of interdependence and when the strategy is formed, at the end of the matrix composition.

Initially, the interaction between weaknesses and threats will be addressed. It is the mini-mini matrix, or WT (Fig. 7). From the interaction, the absence of a culture of sharing with private institutions and the limited performance in AVSEC stand out, as they relate to all threats.

Weaknesses \ Threats	Absence of data sharing culture towards the private sector	No meeting regarding intelligence in concession notices	Limited operation on AVSEC
Cyber-attacks	+	•	+
Weapons of mass destruction	+	•	+
Organized crime	+	•	+

Source: Elaborated by the authors.

Figure 7. Matrix WT (mini-mini).

The logical strategy that emerges from the WT Matrix, therefore, is: creation of a data sharing policy with private institutions and strengthening the role of Intelligence in AVSEC. In other words, the transformation of weaknesses into strengths. Next, the interaction between forces and opportunities is analyzed (Fig. 8).

Strengths \ Opportunities	National and international operation	Specialized training	Culture of protection
Increase SISBIN's reliability	•	+	•
Strengthen the protection culture	•	+	+
Cooperate on protecting national critical infrastructure	+	+	+

Source: Elaborated by the authors.

Figure 8. Matrix SO (maxi-maxi).

In the analysis of the SO matrix (maxi-maxi), cooperation in protecting critical national infrastructure and specialized training stand out as influential factors. Thus, the strategy that logically emerges from the matrix is: specialized training in Intelligence applied to the security of critical infrastructures. Next, the interaction between forces and threats are analyzed (Fig. 9).

Strengths \ Threats	National and international operation	Specialized training	Culture of protection
Cyber-attacks	+	+	+
Weapons of mass destruction	+	+	+
Organized crime	+	+	+

Source: Elaborated by the authors.

Figure 9. Matrix ST (maxi-mini).

In the ST matrix analysis (maxi-mini), all factors influence each other. Thus, the strategy that emerges from the matrix is: specialized training, focusing on the culture of protection, on the identification of threats. Next, weaknesses with opportunities are compared (Fig. 10).

	Weaknesses	Absence of data sharing culture towards the private sector	No meeting regarding intelligence in concession notices	Limited operation on AVSEC
Opportunities				
	Cyber-attacks	+	•	•
	Weapons of mass destruction	+	•	•
	Organized crime	+	•	+

Source: Elaborated by the authors.

Figure 10. Matrix WO (mini-maxi).

Analyzing the WO matrix (mini-maxi), it can be seen that the absence of a culture of data sharing with private institutions is the main factor of influence, being, therefore, the strategy that emerges from the matrix: the creation of a sharing policy data with private institutions.

From the previous interactions (interaction matrixes) emerges the formation of the SWOT Matrix (Figure 11), which consolidates the strategies resulting from the analyzes carried out and has the power to help the proposition of strategies that allow the re-engagement of airports under private administration to a formal system of processing of intelligence documents with the State.

	STRENGTHS (S)	WEAKNESSES (W)
	<ul style="list-style-type: none"> • National and international operation • Specialized training • Culture of protection 	<ul style="list-style-type: none"> • Absence of data sharing culture towards the private sector • No mention regarding Intelligence in the concession notices • Limited Intelligence operation on AVSEC
OPPORTUNITIES (O)		
<ul style="list-style-type: none"> • Increase SISBIN's reliability • Strengthen the culture of protection • Cooperate on the protection of the national critical infrastructure 	To promote specialized Intelligence training for the critical infrastructure operators, focused on the protection culture	To create a classified information sharing policy towards the private sector
THREATS (T)		
<ul style="list-style-type: none"> • Cyber-attacks • Weapons of mass destruction • Organized crime 	To promote specialized training focused on the identification of threats	Overcome the weaknesses and turn them into strengths

Source: Elaborated by the authors.

Figure 11. The SWOT matrix.

CONCLUSION

The changes concerning the legal status of airport operators in Brazil that took place after the concession processes should not be the cause of the end the airport's relationship with the Brazilian Intelligence community.

In terms of importance for the country, it does not matter whether the administration of the airport is carried out by a public authority or by a private entity. Although the existence of a legal framework does not automatically imply the effective Intelligence sharing within SISBIN, the situation is no different when private operators, some of which are under foreign stock control, became part of the airport security environment in Brazil.

The strategic nature of the airport infrastructure, however, does not depend if its legal personality is public or private. Thus, what is needed from ABIN is working to establish the proper protocols to provide an intelligence sharing environment among the airport's operators in Brazil.

If the airports that are under the administration of Infraero, the intelligence sharing is still through SISBIN, regarding the airports currently operated by private entities under a concession regime, the Brazilian legal system provides possibilities for a private entity to have access to confidential data.

Sharing data with intelligence agencies has the potential to allow the operator of critical national infrastructure—including the airports—to increase their perception of identified and identifiable threats. Although much of the post-9/11 academic papers, especially Anglo-Saxon ones, have in terrorism their main factual ballast, threats are not restricted to this phenomenon

The SWOT matrix shows that the current scenario demands an active stance on the part of ABIN, by promoting specialized training, focused on threat identification, to the critical infrastructure operators, so that it promotes the reengagement of airports to a proper intelligence sharing environment, according to security protocols and accreditations regulated by the Brazilian law.

AUTHORS' CONTRIBUTIONS

Conceptualization: Oliveira DM; **Methodology:** de Andrade D; **Validation:** de Andrade D; **Formal analysis:** Monteiro AM; **Investigation:** Oliveira DM; **Writing - Original Draft:** Oliveira DM; **Writing - Review & Editing:** de Andrade D and Monteiro AM; **Supervision:** de Andrade D.

DATA AVAILABILITY STATEMENT

The data will be available upon request.

FUNDING

Not applicable.

ACKNOWLEDGEMENTS

Not applicable.

REFERENCES

[ABIN] Agência Brasileira de Inteligência (2021) Estrutura. [accessed Dec 01 2021]. <https://www.gov.br/abin/pt-br/acesso-a-informacao/institucional/estrutura>

[ANAC] Agência Nacional de Aviação Civil (2022) Unidades da ANAC [accessed Sept 14 2022]. <https://www.gov.br/anac/pt-br/acesso-a-informacao/institucional/unidades-da-anac>

Brazil (2010) Decreto nº 7.168, de 5 de maio de 2010. Revogado pelo Decreto nº 11.195, de 2022. Dispõe sobre o Programa Nacional de Segurança da Aviação Civil Contra Atos de Interferência Ilícita (PNAVSEC). Diário Oficial da União, Brasília, DF, May 6, 2010. [accessed Jun 10 2022]. https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/decreto/d7168.htm

Brazil (2016) Decreto nº 8.793, de 29 de junho de 2016. Fixa a Política Nacional de Inteligência. Diário Oficial da União, Brasília, DF, June 30, 2016. [accessed Dec 01 2020]. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm

Brazil (2018) Decree N. 9527, de 15 de outubro de 2018. Cria a Força-Tarefa de Inteligência para o enfrentamento ao crime organizado no Brasil. Diário Oficial da União, Brasília, DF, October 16, 2018. [accessed Jun 10 2022]. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9527.htm

- [CIA] Central Intelligence Agency (2020) The World Factbook. [accessed Jun 10 2022]. <https://www.cia.gov/library/publications/resources/the-world-factbook/fields/379rank.html>.
- [Infraero] Empresa Brasileira de Administração Aeroportuária (2019) Infraero 40 anos servindo pessoas, empresas e o Brasil. [accessed Oct 22 2019]. <http://www.infraero.gov.br/portal/images/stories/Infraero/INFRAERO40ANOS.pdf>
- Lambert M (2021) SWOT matrix of the five eyes in the worldwide intelligence community. Russian International Affairs Council. [accessed Jun 10 2021]. <https://russiancouncil.ru/en/blogs/mlambert/35457/>
- Maleiner RJ (2020) Proposta de disposições complementares sobre o trato com evidências, em face da relação entre a investigação SIPAER e a investigação criminal, de acidentes aeronáuticos (masters dissertation). São José dos Campos: Instituto Tecnológico de Aeronáutica. In Portuguese.
- Miranda Filho FN (2016) Ferramentas de interpretação de textos para uso da Inteligência. Revista Brasileira de Inteligência 11:47-66.
- Panagiotou G (2003) Bringing SWOT into focus. Bus Strateg Rev 14(2):8-10. <https://doi.org/10.1111/1467-8616.00253>
- Soares JKG (2020) Inteligência de estado e segurança da aviação civil contra atos de interferência ilícita: análise comparativa de Brasil e Estados Unidos (professional master's thesis) Segurança da Aviação e Aeronavegabilidade Continuada. São José dos Campos: Instituto Tecnológico de Aeronáutica, Programa de Pós-Graduação em Engenharia Aeronáutica e Mecânica. In Portuguese.
- Valor Econômico (2021) Setor elétrico corre atrás de segurança cibernética (<https://valor.globo.com/empresas/noticia/2021/02/08/setor-eletrico-corre-atras-de-seguranca-cibernetica.ghtml>) [accessed Mar19 2021]
- Weihrich H (1982) The TOWS matrix a tool for situational analysis. Long Range Plann 15(2):54-66. [https://doi.org/10.1016/0024-6301\(82\)90120-0](https://doi.org/10.1016/0024-6301(82)90120-0)
- [WEF] World Economic Forum (2020) The global risks report 2020. 15th edition. Geneva: World Economic Forum. [accessed Jan 10 2021]. <https://www.weforum.org/reports/the-global-risks-report-2020>
- Young S, Wells A (2014) Aeroportos: Planejamento e gestão. Menezes RS, translator. Porto Alegre: Bookman.