Revista de Relaciones Internacionales, Estrategia y Seguridad 2023 Vol. 18(1)

Editorial Neogranadina

enero-junio ▪ ISSN: 1909-3063 · ISSN-e: 1909-7743 ▪ pp. 87–109

DOI: https://doi.org/10.18359/ries.6613

Protection of the Brazilian Airspace Control System against Unmanned Aircraft System from the Perspective of the Capability-Based Planning*

Edson Atallah Monreal[a] ▪ Gills Vilar-Lopes[b]

Abstract: the Brazilian Airspace Control System against Unmanned Aircraft Systems is a strategic issue that can become a target of new 21st-century threats due to its importance for civil aviation and the Brazilian Aerospace Power. The characteristics of this new device involve its low detection rate by radars and the ineffectiveness of traditional air countermeasures systems in its confrontation. The scrutiny is performed from the perspective of Capability-Based Planning, as it provides more rationality for decision-making on future acquisitions and makes planning more responsive to uncertainties, budgetary constraints, and risks. The main objective of this article is to analyze the current perceived capability of the Brazilian Airspace Control System to face and counter the unlawful use of Unmanned Aircraft Systems against this critical national infrastructure. An exploratory-descriptive study, conducted in a qualitative research style, is carried out. However, descriptive statistics are also used to assess the results extracted from the application of questionnaires to the Brazilian Airspace Control System managers. The responses indicate that the perceived capability is 74.2% positive, showing that air navigation security operators, on average, consider the measures adopted by the Brazilian Department of Airspace Control to be sufficient and proficient to protect civil aviation and its national aerospace infrastructure against uncrewed aircraft.

Keywords: counter-unmanned aircraft systems; unmanned aircraft systems; Brazilian Airspace Control System; capability-based planning; aviation security

Recibido: 08/01/2023. **Aceptado:** 19/07/2023. **Disponible en línea:** 22/09/2023

Cómo citar: Atallah Monreal, E., & Vilar Lopes, G.(2023). Protection of the Brazilian Airspace Control System against Unmanned Aircraft System from the Perspective of the Capability-Based Planning. *Revista de Relaciones Internacionales, Estrategia y Seguridad, 18*(1), 87–109. https://doi.org/10.18359/ries.6613

* Artículo de investigación

a Master in Aerospace Sciences. Air Force University (UNIFA), Brasília, Brazil.
Correo electrónico: monrealeam@fab.mil.br ORCID: https://orcid.org/0000-0002-4438-5921

b PhD in Political Science. Air Force University (UNIFA), Rio de Janeiro, Brazil.
Correo electrónico: gillsgvl@fab.mil.br ORCID: https://orcid.org/0000-0003-3597-2152

Protección del Sistema de Control del Espacio Aéreo Brasileño contra Sistemas de Aeronaves no Tripuladas desde la perspectiva de la planificación basada en capacidades

Resumen: El Sistema de Control del Espacio Aéreo Brasileño contra Sistemas de Aeronaves No Tripuladas es un asunto estratégico que puede convertirse en un objetivo de nuevas amenazas del siglo XXI debido a su importancia para la aviación civil y el Poder Aeroespacial Brasileño. Las características de este nuevo dispositivo incluyen su baja tasa de detección por radares y la ineficacia de los sistemas tradicionales de contramedidas aéreas en su confrontación. El análisis se realiza desde la perspectiva de la Planificación Basada en Capacidades, ya que proporciona una mayor racionalidad para la toma de decisiones sobre adquisiciones futuras y hace que la planificación sea más receptiva a las incertidumbres, restricciones presupuestarias y riesgos. El principal objetivo de este artículo es analizar la capacidad percibida actual del Sistema de Control del Espacio Aéreo Brasileño para enfrentar y contrarrestar el uso ilegal de Sistemas de Aeronaves No Tripuladas contra esta infraestructura nacional crítica. Se lleva a cabo un estudio exploratorio-descriptivo, realizado en un estilo de investigación cualitativa. Sin embargo, también se utilizan estadísticas descriptivas para evaluar los resultados extraídos de la aplicación de cuestionarios a los gerentes del Sistema de Control del Espacio Aéreo Brasileño. Las respuestas indican que la capacidad percibida es del 74,2% en términos positivos, lo que muestra que los operadores de seguridad de la navegación aérea consideran, en promedio, que las medidas adoptadas por el Departamento de Control del Espacio Aéreo Brasileño son suficientes y competentes para proteger la aviación civil y su infraestructura aeroespacial nacional contra aeronaves no tripuladas.

Palabras clave: sistemas de contrarresto de aeronaves no tripuladas; sistemas de aeronaves no tripuladas; sistema de control del espacio aéreo brasileño; planificación basada en capacidades; seguridad de la aviación.

Proteção do Sistema de Controle do Espaço Aéreo Brasileiro contra Sistemas de Aeronaves Não Tripuladas na Perspectiva da Planejamento Baseado em Capacidades

Resumo: A proteção do Sistema de Controle do Espaço Aéreo Brasileiro contra Sistemas de Aeronaves Não Tripuladas é uma questão estratégica que pode se tornar alvo de novas ameaças no século XXI devido à sua importância para a aviação civil e o Poder Aeroespacial Brasileiro. As características desse novo dispositivo incluem sua baixa taxa de detecção por radares e a ineficácia dos sistemas tradicionais de contramedidas aéreas em enfrentá-lo. A análise é feita a partir da perspectiva do Planejamento Baseado em Capacidades, pois isso proporciona maior racionalidade para a tomada de decisões sobre aquisições futuras e torna o planejamento mais receptivo às incertezas, restrições orçamentárias e riscos. O principal objetivo deste artigo é analisar a capacidade percebida atual do Sistema de Controle do Espaço Aéreo Brasileiro para enfrentar e opor-se ao uso ilegal de Sistemas de Aeronaves Não Tripuladas contra essa infraestrutura nacional crítica. É realizado um estudo exploratório-descritivo, conduzido no estilo de pesquisa qualitativa. No entanto, também são utilizadas estatísticas descritivas para avaliar os resultados obtidos na aplicação de questionários aos gestores do Sistema de Controle do Espaço Aéreo Brasileiro. As respostas indicam que a capacidade percebida é de 74,2% em termos positivos, o que mostra que os operadores de segurança da navegação aérea consideram, em média, que as medidas adotadas pelo Departamento de Controle do Espaço

Aéreo Brasileiro são adequadas e competentes para proteger a aviação civil e sua infraestrutura aeroespacial nacional contra aeronaves não tripuladas.

Palavras-chave: sistemas de contramedidas de aeronaves não tripuladas; sistemas de aeronaves não tripuladas; sistema de controle do espaço aéreo brasileiro; planejamento baseado em capacidades; segurança da aviação

Introduction

The so-called swarms of drones are already a reality both in the civil and military spheres, with countries such as the United States of America (USA), China, Israel, and Russia at the forefront of their development and use on the battlefield. However, their low cost and easy access allow non-state actors to use them creatively (Sanders, 2017) to challenge public order and authorities.

To understand their unlawful use in isolation or swarm formation, we assume that Unmanned Aircraft Systems (UAS[1]) are elements that have already been incorporated into the warfare of the 21st century, not only in the specialized literature reviewed here but also in the current Russian-Ukrainian war. We bring this theme to the context of the Brazilian Airspace Control System[2] (SISCEAB), problematizing this concern for Brazil since the global strength of civil aviation appears in the statistics. To get an idea, in 2018, 4.3 billion passengers and 58 billion tons of cargo were transported, representing 35% of world trade in value (International Civil Aviation Organization, 2019, p. 5). Therefore, this sector is vital for the progress of humanity. In Brazil, its strategic importance is such that it is one of the six constitutive instruments of Brazilian Aerospace Power[3] (Brazilian Air Force Command [COMAER], 2020b, p. 29).

In Brazil, the airspace control and air defense infrastructure were designed in an integrated manner (Jasper & Nunes, 2022), with the Department of Airspace Control (DECEA) managing them. At this point, the incorporation of the civil-military organization proposed by Douhet (2019) into the Brazilian aeronautical structure has been verified. SISCEAB remains an integrated system encompassing and supporting civil and military equipment and installations for airspace defense.

In this sense, the (DECEA) – the central body of SISCEAB, responsible for air navigation safety and security[4] (Exec. Order No. 11237, 2022), was included by the Brazilian Institutional Security Office of the Presidency of the Republic (GSI) of the Presidency of the Republic of Brazil in discussions on critical infrastructures, understanding that this is a crucial component of national transport (GSI, 2019) and of the global civil aviation system (2021b). Furthermore, remember that this system was deeply impacted by the terrorist attacks of September 11, 2001 (Tamasi & Demichela, 2011), when governments and international organizations took numerous security countermeasures, completely transforming the context in which not only aviation security (AVSEC[5]) undergoes, but also international security (Monreal & Vilar-Lopes, 2021).

Concomitantly with this change in the international scenario, the reduction and scrutiny of defense spending compelled the adoption of a strategic planning system that addressed not only the hypotheses of using the military expression but also the visualization of its resources - budgetary, technological, and – in a single methodology (Da Silva, 2020). Capability-Based Planning (CBP). It provides more rationality for decision-making on

1 In line with the Brazilian Department of Airspace Control (DECEA) regulations, we use the acronym UAS for Unmanned Aircraft Systems. Unmanned aircraft are also known as Unmanned Aerial Vehicles (UAV) or Remotely Piloted Aircraft (ARP). This system consists of the Unmanned Aircraft (UA) and its hardware and software components, which can be remotely piloted or fully autonomous (COMAER, 2020a). In turn, 'drone' is also known as a small unmanned aircraft system (SUAS).

2 The Brazilian Aerospace Defense System (SISDABRA) and its central body, the Aerospace Operations Command (COMAE), were not addressed because this work is limited to threats to civil aviation rather than the sovereignty of the entire Brazilian airspace.

3 Aerospace Power consists of "[...] projection of the portion of National Power that results from the integration of the resources available to the Nation for the use of airspace and outer space, either as an instrument of political and military action or as a factor of economic and social development, with a view to achieving and maintaining national objectives" (COMAER, 2020b).

4 The term "safety" addresses dangers and threats posed by unintentional errors, and "security" concerns violations and intentional acts.

5 AVSEC (Aviation Security) is defined in Annex 17 to the Chicago Convention as safeguarding civil aviation against acts of unlawful interference. This objective is achieved by a combination of measures and human and material resources (International Civil Aviation Organization, 2020).

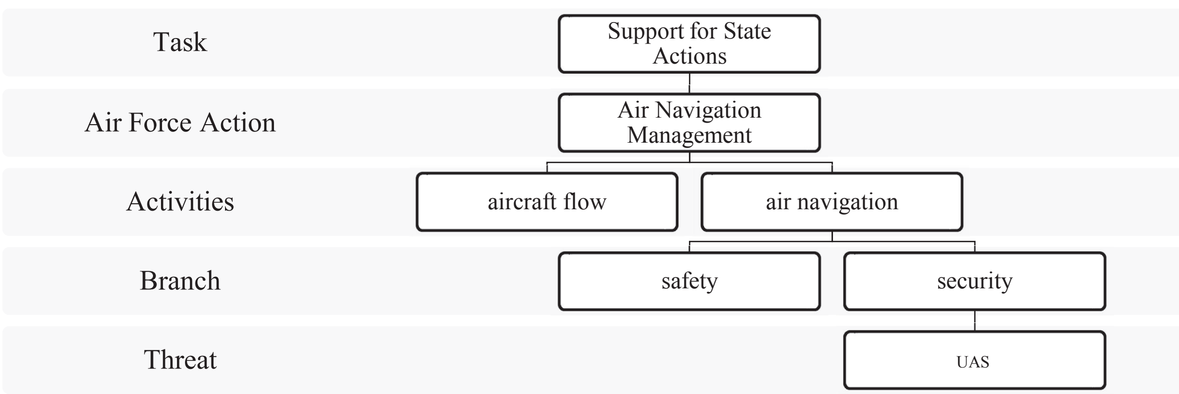
future acquisitions. It makes planning more responsive to uncertainties, economic restrictions, and risks by proposing a cultural and organizational change in qualitative and quantitative aspects for each Air Force Action[6] (COMAER, 2020d). Moreover, it focuses on goals and end states, thereby encouraging innovation and asking, "What do we need to do?" rather than "What equipment are we replacing?" (Taylor & Wood, 2005).

In Brazil, the Ministry of Defense points out that capability is obtained from a set of determining, interrelated, and inseparable factors known by the acronym DOPEMAII, that is, Doctrine, Organization, Personnel, Education, Materiel, Infrastructure, and Interoperability (Brazil, 2021a).

Regarding these considerations, the concern that motivated this work was exploring the most effective ways to protect SISCEAB from the threats represented by the unlawful use of UAS. In a context of activating capabilities, faced with an external threat – even if internally active, as is the case of terrorist groups – this fog of war, in Clausewitzian terms, can pose risks to the effective situational awareness of the aerospace authority. Thus, the present work seeks to answer the following problem: What is the perception of SISCEAB's capability to oppose the UAS from the perspective of DOPEMAII? In other words, we seek to understand how DECEA managers see their ability to use their resources effectively in the face of this threat.

Due to the scope of the subject, this study was limited to the threats posed by UAS to AVSEC and air navigation by analyzing the capability of the Air Navigation Management (COMAER, 2020c) to fulfill the Support Task for State Actions, as presented in Figure 1.

Figure 1. Delimitation of the object of this work in the light of Brazilian systematics



Source: Own elaboration.

Given this scenario, the general objective is to analyze the current perceived capability of SISCEAB to deal with the unlawful use of UAS. In doing so, an essential real-world topic is sought – the capability of critical aerospace infrastructures to deter UAS – which, at the same time, can contribute directly or indirectly to the specialized literature (King et al., 1994) on Aerospace Power.

The work is characterized as an exploratory-descriptive study with a qualitative style, given the type of data extracted and the survey of documents carried out during its execution. However, descriptive statistics are also used to complement the analysis of the results. According to this scope, the research strategy was outlined, incorporating three specific objectives, as shown in Table 1.

6 Air Force Actions are carried out through the appropriate combination of personnel, aircraft, space platforms, land vehicles, vessels, weapons, facilities, equipment and systems, to achieve the desired effects (COMAER, 2020c).

Table 1. Methodological dynamics

APA TAB	Consulted authors	Used technique
1) Identify the main threats to civil aviation related to UAS	Douhet (2019) and Carter (2020)	Literature review
2) Distinguish the main existing C-UAS	Lyu and Zhan (2022)	
3) Evaluate the perceived capability of SISCEAB to oppose the UAS from the perspective of PBC	Lessa (2016)	Questionnaire

Source: Own elaboration.

Regarding the theoretical framework, this work was based on critical authors for the creation of Brazilian documents related to the subject discussed here, namely Douhet (2019) to associate civil aviation with Aerospace Power; Carter (2020) to explain the threat posed by the use of UAS by non-state actors; Lyu and Zhan (2022) to deal with C-UAS; and, finally, Lessa (2016) to characterize the CBP.

This article has been divided into two sections to explore the research problem. First, knowledge about drones and their swarms is deepened, as is their potential threat to civil aviation security. Secondly, the CBP methodology is covered from the perspective of DOPEMAII, and the results of the Brazilian case are analyzed.

Drones and their swarms as threats to aviation security

According to Dudenhoeffer (2020), using uncrewed aerial platforms in warfare is not new. There are reports that his birth occurred in Austria in 1849, when the army launched balloon bombs to quell a significant rebellion in the Republic of Venice. During World War I, The US Navy tested UAS as aerial torpedoes [7], but they were not used in combat. In the interwar period, military interest in these aircraft grew, which fostered the development of UAS. However, when its use ceased to be exclusively military and incorporated commercial objectives, concern arose about its proliferation and use by criminals, including terrorists.

Schóber et al. (2012) point out that, in addition to the technical and legal challenges for the safe integration of non-segregated airspace, that is, shared with other aircraft, it is necessary to be prepared for the possible use of UAS by terrorists. The authors also mention that the low effectiveness of current air defenses against such small targets, combined with insufficient radar coverage at low altitudes, makes the swarm practically intrepid and invisible, often identified as a bird, cloud, or false reflection.

Dudenhoeffer (2020), in turn, indicates that UAS have the potential to carry out bellicose activities ranging from reconnaissance vehicles to even remotely guided missiles. The main targets of terrorist attacks, with this technology in hand, can include significant events, such as rallies and sports meetings, and critical infrastructure, as this work seeks to demonstrate that the increasing episodes involving UAS in airports, penitentiaries, and military installations demand emphasis and the availability of countermeasures.

According to Custer (2016), UAS can be used in practically all sectors of society, from public to private, from civil to military. However, it is in the latter that the UAS gains an offensive character. In addition to the US, UK, and Israel being the leaders in producing these aerospace assets, 19 other countries were developing or operating UAS in 2020 (Lyu & Zhan, 2022). China, Russia, and Iran's growing export of this equipment raises severe concerns about the need for effective proliferation control of armed UAS (Haider, 2020) that can be used according to the employment hypotheses in Table 2.

7 Kettering Aerial Torpedo "Bug", invented by Charles F. Kettering in Dayton, Ohio (National Museum of the United States Air Force, 2022).

Table 2. Military use of UAS

Employment hypothesis	Example
UAS itself as a weapon	flying bomb, Harop
weapons platform	MQ-9 Reaper
intelligence gathering unit, for Intelligence, Surveillance and Reconnaissance	RQ-450 Hermes
simulated target for air defense units	Pilotless Target Aircraft (PTA)

Source: Mátyás and Máté (2019, with adaptations)

However, some aeronautical technologies are being embarked on UAS, as summarised in Table 3.

Table 3. UAS Specifications

Aspect	Subdivision		Description	Example
type	fixed-wing		Combining speed with advance to generate lift on the wings; need a runway to operate	MQ-1B
	multi-rotors		Aircraft that use rotary wings to generate lift, the ability to take off and land vertically, as well as hover in the air	DJI Mavic 3
	Others		Hybrids (have characteristics of multi-rotor and fixed-wing systems), ornithopters (imitate the wings of birds and insects), or jet-powered (with operation similar to multi-rotors)	FVR-90
level of autonomy	Operation		Automatic stability, but with fully human decisions	A20W
	Delegation		Automation enabled by human delegation	Hermes 900
	Supervision		Automation initiated by sensors or humans, within the designated task, under human supervision	Lily
	Total		Performs assigned tasks without human interaction	Kargu-2
power supply	aviation fuel		Large fixed-wing UAS	RQ-4 Global Hawk
	battery cells		Smaller multi-rotors, short throw and shorter operating time (recreational use)	LiPo
	fuel cell		Electrochemical device that chemically converts fuel directly into electrical energy	SOFC
	solar cells		They are rare in the industry. It can be used on all types of UAS with an extended permanence capacity.	Solara 50
size and weight	light	Mini	Up to 2 kilograms	Black Hornet
		Small	Between 2 and 25 kilograms	S900
		Large	Between 25 and 150 kilograms	Draganfly
	Heavy		Above 150 kilograms	MQ-8B

sensor	Camera	Visible or infrared spectrum (night vision and heat detection)	DJI Mini 3 Pro
	Biological	Screening of microorganisms	EAG
	Chemical	Measurement of chemical compositions and traces of specific substances, such as radioactive	Cypher-6
	Meteorological	Measurement of wind, temperature, humidity, radiation, etc.	Black Swift S2

Source: Vergouw et al. (2016, with adaptations)

The aerodynamic performance of the UAS, determined by the characteristics mentioned in Table 2 and associated with the onboard sensors, defines its application possibilities, whether civil or military. For example, Lu et al. (2018) point out that, to navigate, UAS have a sort of situational awareness, including position, speed, direction, starting point, and target location. It is noted, at this point, that the UAS present a similarity with the rules of civil aviation[8] since the aircraft also use inertial and satellite systems to guide the overflight of oceanic areas – where electronic aids cannot be installed – as well as the visual flight when the pilot has good weather and visibility conditions. Depending on the application and available navigation sensors, UAS can be applied according to Table 4.

Table 4. Types of navigation and sensors in UAS

Navigation System	Sensor Type	Applications
inertial	accelerometers and gyroscopes	environments with degraded GNSS[9] signal
satellite	GPS, GLONASS, Galileo and BeiDou	known and open environments
visual	monocular, stereo, RGB-D, or fisheye	dynamic environments

Source: Lu et al. (2018, with adaptations)

The small size and relative speed of the UAS create significant difficulties for those defending themselves. Moreover, these vulnerabilities attract non-state actors with the capability to operate armed UAS (Patterson, 2017), with the subject being highlighted even in the 2011 Joint Operations Doctrine of the Department of Defense (DOD):

Unmanned aircraft is a new challenge to US air defenses, as many systems have smaller radar cross sections and fly at much slower speeds than manned aircraft, making them much harder to detect. (DOD, 2011).

This vulnerability was discovered in January 2015, when a commercial UAS flown by an amateur operator in the US capital area crashed on the White House lawn. Although the event was an accident without malicious intent, it demonstrated how UAS could penetrate robust defenses (Wallace & Loffi, 2015). The episode revealed the criticality of the threat and pointed to possible scenarios of unlawful use. Unlike conventional aerial threats of crewed aircraft and missiles, predominantly used in war, UAS must be considered a threat in peace, crisis, and war (Cieślak, 2021). Furthermore, once launched, drone swarms are secure from conventional Airpower and are likely to be decisive weapons in future wars (Hambling, 2018).

UAS are cheap and quickly proliferated; therefore, they are a potential weapon of choice for terrorist groups worldwide (Cook, 2007). This idea is not new. In 1995, the Japanese terrorist group Aum Shinrikyo, which attacked the Tokyo subway with sarin gas, planned to use remote-controlled helicopters to spray dangerous chemicals from the air. However, the aircraft was unsuccessful during the tests and, therefore, was discarded (Ballard et al., 2005). It is with this bias that Miasnikov (2005)

8 The rules of the air are divided into two types: instrument [IFR] and visual [VFR] flight rules. (Internacional Civil Aviation Organization, 2005).

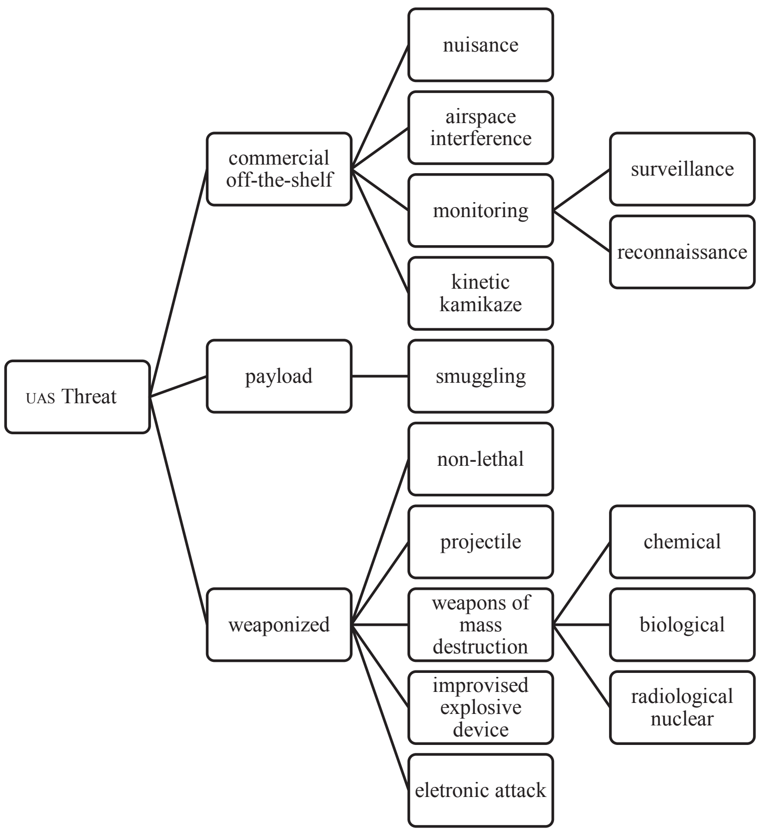
9 The GNSS (Global Navigation Satellite Systems) is composed of several navigation systems by artificial satellites. Among the systems, GPS (Global Positioning System) and GLONASS (*GLObal'naya NAvigatsionnaya Sputnikk*ovaya Sistema) are fully operational, and new systems are being developed, such as Galileo and BeiDou (Menezes, 2019).

lists some advantages of using UAS in terrorist attacks:

- ability to attack unreachable targets by land;
- possibility of carrying out an area attack intended to inflict a high mortality rate with the use of chemical or biological weapons.
- discretion in the preparation of attacks and flexibility in the launch site.
- accuracy and long range with cheap and easily accessible technology.
- better cost-effectiveness compared to ballistic missile attacks and crewed aircraft.
- strong psychological effects by terrorizing the population and putting pressure on politicians.

Wallace and Loffi (2015) argue that the threat is real. Terrorists are adept at using new technologies in their attacks and can modify UAS to carry explosives, automatic weapons, and non-lethal weapons. As can be seen, the threat is not exaggerated, with the potential unlawful use of the UAS being limited by the perpetrator's creativity, as shown in Figure 2.

Figure 2. Unlawful uses of UAS



Source: Wallace and Loffi (2015, with adaptation)

Data on the civilian UAS industry indicate that around 5 million units were purchased worldwide in 2022, with an expected reach of 7.1 million in 2025 and 9.6 million by 2030 (Statista, 2020). With the rise of commercial UAS, they will still likely incorporate more and better features, potentiating the threats posed by their unlawful use (Haider, 2020).

In this context, assets of the State's National Power are also potential targets of attack, and some incidents or attacks have already been recorded, detailed in Table 5.

Table 5. Incidents and attacks with UAS and their impact on National Power

Date	Expression of National Power	Country	Event	Description
September 15, 2013	Political	Germany	UAS crashed in front of the German Chancellor[10]	During a rally in Dresden, a small quadcopter flew within yards of German Chancellor Angela Merkel and Defense Minister Thomas de Maiziere, briefly hovering in front of them before crashing into the stage practically at Merkel's feet. Fortunately, the quadcopter was harmless.
August 12, 2017	Military	Great Britain	UAS landing on a British aircraft carrier[11]	An amateur photographer flew his DJI Phantom across Invergordon harbor to snap some images of Royal Navy aircraft carriers. When the UAS sensed a risk of strong wind, it landed on the flight deck. After taking pictures from the deck, the photographer was able to pilot the UAS back safely.
August 04, 2018	Political	Venezuela	Attempted Assassination of Venezuelan President[12]	Two DJI M600 drones, each carrying a kilogram of C-4 explosives, to carry out an attack on Venezuelan President Nicolas Maduro as he speaks at a military parade in Caracas.
December 19, 2018	Economic	Great Britain	Flight disruption at Gatwick Airport[13]	Hundreds of flights have been canceled at Gatwick Airport, near London, England, after reports of drone sightings near the runway. The reports caused major disruptions, affecting approximately 140,000 passengers and 1,000 flights. At least two UAS were used, and the offenders had detailed knowledge of the airport.
February 10, 2021	Psychosocial	Saudi Arabia	Attack on commercial aircraft at the airport[14]	The case occurred at Abha airport, 120 km from the border with Yemen. Four drones were used, with one successfully hitting one of the planes parked at the airport. After the UAS hit the plane's fuselage, the explosive charge detonated, causing severe damage to the plane's left side, near the tail.
March 22, 2022	Scientific	Ukraine	Attack on the scientific institute[15]	At least one person was killed in a drone attack on a seven-story building at the Institute for Superhard Materials in northwestern KYIV, part of the National Academy of Science of Ukraine.
June 22, 2022	Economic	Russia	Attack on Russian oil refinery[16]	A Ukrainian kamikaze drone destroyed part of a Russian oil refinery located in the city of Novoshakhtinsk, about eight kilometers from the border with Ukraine. Despite the explosion, no injuries were reported.

Source: Own elaboration.

10 German chancellor's drone "attack" shows the threat of weaponized UAVs. Retrieved from https://arstechnica.com/information-technology/2013/09/german-chancellors-drone-attack-shows-the-threat-of-weaponized-uavs/. Accessed on: December 1, 2022.

11 Tiny drone lands on the Queen Elizabeth aircraft carrier. Retrieved from https://www.bbc.com/news/uk-scotland-highlands-islands-40910087. Accessed on: December 1, 2022.

12 Venezuela makes six arrests in alleged Maduro assassination attempt. Retrieved from https://edition.cnn.com/2018/08/05/americas/venezuela-maduro/index.html. Accessed on: December 1, 2022.

13 The mystery of the Gatwick drone. Retrieved from https://www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone. Accessed on: December 1, 2022.

14 Shrapnel injures 12 at Saudi Abha airport as drone intercepted. Retrieved from https://www.reuters.com/world/middle-east/saudi-led-coalition-says-destroyed-drone-launched-towards-abha-airport-4-injured-2022-02-10/ Accessed on: December 1, 2022.

15 One Dead in Drone Attack on Kyiv Science Institute: Report. Retrieved from https://www.news18.com/news/world/one-dead-in-drone-attack-on-kyiv-science-institute-report-4898732.html. Accessed on: December 1, 2022.

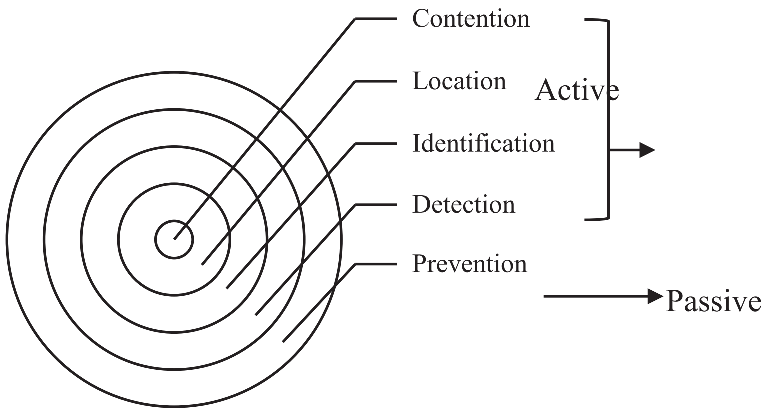
16 A drone crashes into a Russian oil refinery in a possible attack. Retrieved from https://www.theguardian.com/world/2022/jun/22/russian-novoshakhtinsk-oil-refinery-struck-drone-possible-attack-inside-borders. Accessed on: December 1, 2022.

The cases mentioned above materialize these new threats to Aerospace Power and demonstrate how UAS can be used in larger contexts if used by terrorist groups to attack high-value targets for National Power.

Not only are UAS technologies evolving rapidly, but so are those to counter them (Cole, 2019). The complexity of C-UAS depends on which component of the UAS must be fought – whether the operator, the drone, the communications between it and the remote pilot, or the navigation technologies used (Sarma & Quinn, 2018) –, their characteristics such as size, speed, and autonomy.

The level of UAS cooperation defines the type of defense to be employed. In other words, if it meets the rules for access to airspace and protection against inadvertent overflight, it is passive (safety). However, if it fails to cooperate with the regulations and adopts a non-cooperative posture, the defense against it becomes active (security), as shown in Figure 3.

Figure 3. Types of C-UAS defenses



Source: Own elaboration.

After reviewing the literature, it can be stated that the most common passive defense technology against UAS is geofencing (Lyu & Zhan, 2022), which acts in the intrusion prevention process of cooperative UAS by demarcating "no-fly zones" in pre-defined airspace volumes (Sun et al., 2020), blocking the UAS operating system. This technology plays a vital role in the operational security of airports by ensuring, for example, that inattentive UAS operators do not interfere with aircraft airspace.

On the other hand, geofencing hinders, but it does not stop operators from manually turning off this block to invade restricted areas (Lykou et al., 2020) and, therefore, use the UAS in a hostile manner. In addition, the system's security depends on continuously updating the UAS database of the operators, which compromises the integrity and reliability of the process. Therefore, active defense systems are necessary to guarantee protection against inadvertent or unlawful intrusions.

Miranda (2021), when discussing the C-UAS at SISCEAB, indicates that active defense includes detection, identification, location, and containment processes described below:

Detection happens when some sensor – radar, active or passive optical, acoustic, electromagnetic emission, radio frequency (RF), or human observation - captures the presence of a drone within the coverage area. It is the first C-UAS action and should take place as quickly and over the most significant distance as possible (Haider, 2020).

Identification: After detection, the system separates real targets from noise, analyzes the information (Birch et al., 2015), and defines the characteristics of the equipment, such as manufacturer, model, and operating frequency.

Location: In-flight ground sensors estimate UAS trajectories through models and predictive techniques (Guvenc et al., 2018). RF goniometers receive the signals and, by triangulating the signal origin sources, indicate the location and trajectory of the UAS and the Remote Piloting Station (RPS).

Contention is the chain's last and most critical link, directly determining the defense's success. It consists of blocking or electronic interference in the piloting link between the UAS and its RPS, causing the jammer signal of greater intensity, which overwhelms the UAS's signal, preventing it from receiving commands and conducting it adversely to the remote pilot's will. Containment can also occur with the emission of a blocking signal or interference in the frequency of GNSS that enables the geolocation of drones, causing them to lose their instantaneous geospatial location information. Other forms of containment are the capture or physical destruction of the drone.

Miranda (2021) asserts that containment can result in returning the drone to the RPS known as (Return to Home) –, hovering it until the end of the battery, and landing it vertically at the blocking point or in a predefined location, assuming command, forcing its downfall, capturing it or destroying it. Regarding the latter case, the author emphasizes that although Law n. 9,614/1998 included the hypothesis of aircraft destruction in the national legal framework, Decree n. 5,144/2004, regulates it, applies to aircraft suspected of trafficking in narcotic substances, and disallows the destruction measure over densely populated areas. Such conditions do not allow the legal framework for the destruction of hostile UAS, which is another barrier to be overcome for the completeness of their integration into Brazilian airspace.

Sarma and Quinn (2018) assert that containment is subject to specific aviation and telecommunications regulations, requiring careful evaluation before its use, as

There are already plans to install 'anti-drone' [C-UAS] solutions in a number of airports worldwide. However, jamming and, even more, spoofing may disturb aircraft avionics and CNS [communication, navigation, and surveillance] systems and thus impair aviation safety; installation of 'anti-drone' systems near airports needs careful consideration. (European Aviation Safety Agency, 2016, p. 20).

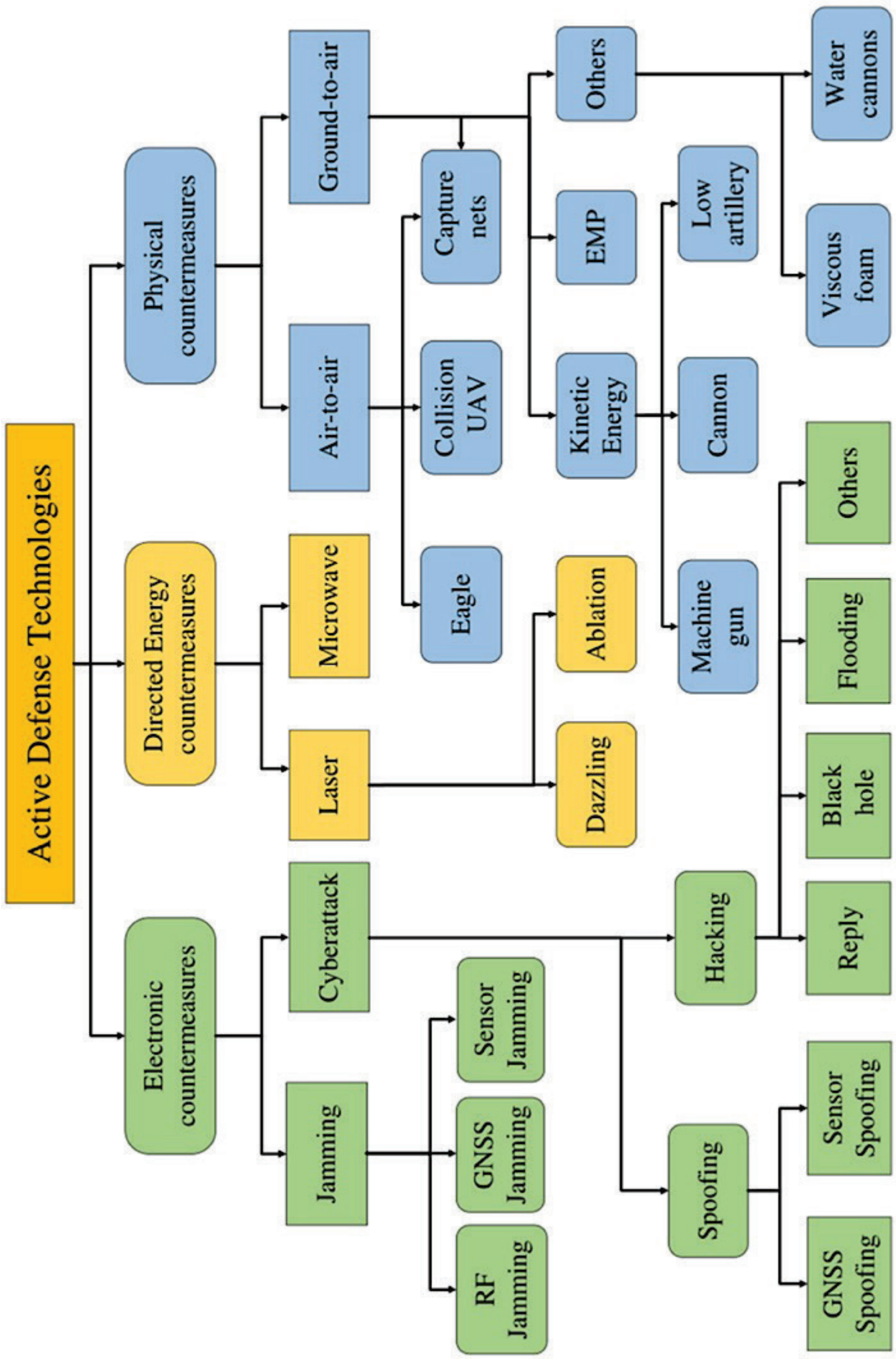
In this sense, complementing the observation of the European Aviation Safety Agency, Park, et al. (2021) point out that most C-UAS adopt military-grade components to obtain the destruction of unlawful drones. When applied in deadlock scenarios, the side effects of blocking can be ignored or managed. However, for civil applications, in addition to civil liability for the downed or captured drone, the action can paralyze existing wireless network systems in the region, such as mobile phone access or wireless sensor networks.

Different defense technologies are suitable for each tactical environment and mission requirement. Active defense countermeasures are classified into three categories (Lyu & Zhan, 2022): electronic, direct energy, and physics, as shown in Figure 4.

Electronic countermeasures can be either electromagnetic (jamming) or cybernetic. Jamming seeks to disable the UAS by disturbing its sensors (avionics), RF signals (data and command channels, radar, commercial mobile telephony), and GNSS systems, causing communication failure (Salameh et al., 2020) and, therefore, the neutralization of the UAS, as exemplified in Figure 5. This technology is a consolidated solution and one of the most used in C-UAS, and its effectiveness has been proven in military operations (Birch et al., 2015).

Lyu and Zhan (2022) also indicate that cyber-attacks are the most sophisticated type of existing active defense technology, as they allow the defender to change navigation (spoofing) or take control (hacking) of the UAS. The authors also mention that terrorists generally use commercial UAS with weak encryption and are, therefore, more susceptible to this counterattack.

Figure 4. Active Defense Technologies



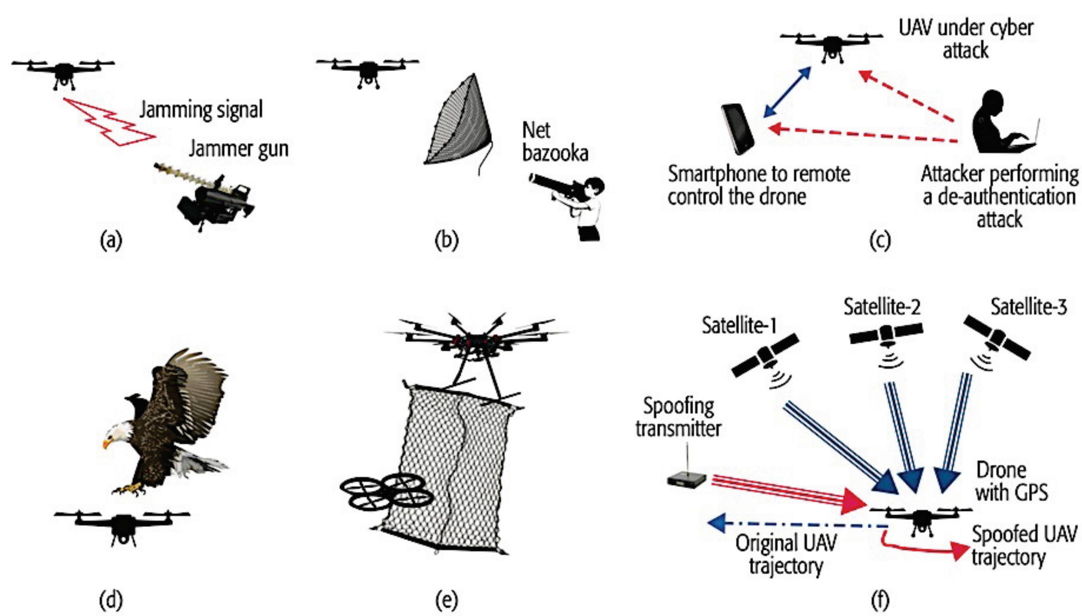
Source: Lyu and Zhan (2022)

In recent years, direct energy countermeasures – High Energy Laser Weapons (HELW) and High-Power Microwave Weapons (HPMW) – have become the most promising in the future of C-UAS technologies, possessing unrivaled advantages over conventional weapons (Zohuri, 2016). Lyu and Zhan (2022) point out that the laser characteristics give HELW absolute advantages over any other weapon in speed and accuracy, thus making it the best way to deal with future aerial threats such as hypersonic and orbital weapons. On the other hand, extreme precision undermines its effectiveness against a swarm attack, with HPMW being the best way to counter it.

HPMW is a high-power narrowband electromagnetic wave weapon with thousands of volts at a single frequency, introducing noise or signals into electrical and electronic systems, interrupting, confusing, or damaging them (Radasky et al., 2004). However, due to technical characteristics and power supply limitations, the effective range of existing HPMWs is no more than a few hundred meters (Air Force Research Laboratory, 2021).

Physical countermeasures are the more traditional C-UAS methods, including ground-to-air and air-to-air such as kinetic energy – projectiles, firearms, rockets – capture nets, electromagnetic pulse (EMP), collision UAS, high-pressure water cannons, viscous foam, and even birds of prey. On the subject, Lyu & Zhan (2022) emphasize that the use of EMP can temporarily disable or permanently destroy electronic devices (Giri, 2004) within the range of action, be they friends, enemies, or neutrals. Therefore, due to the potential risks for uninvolved parties, these countermeasures have restrictions for private or commercial use (Haider, 2020). On the other hand, capture nets have the fewest side effects, making them suitable for use in the urban environment (Lyu & Zhan, 2022).

Figure 5. Examples of Active Defense Technologies



Source: Guvenc et al. (2018)

Lyu and Zhan (2022) point out that electronic countermeasures are currently the leading active defense technologies (69%), with jamming being the second most used (60%). The authors also indicate that, although direct energy countermeasures represent a low proportion (12%) due to their high cost, they are the most promising defense technologies.

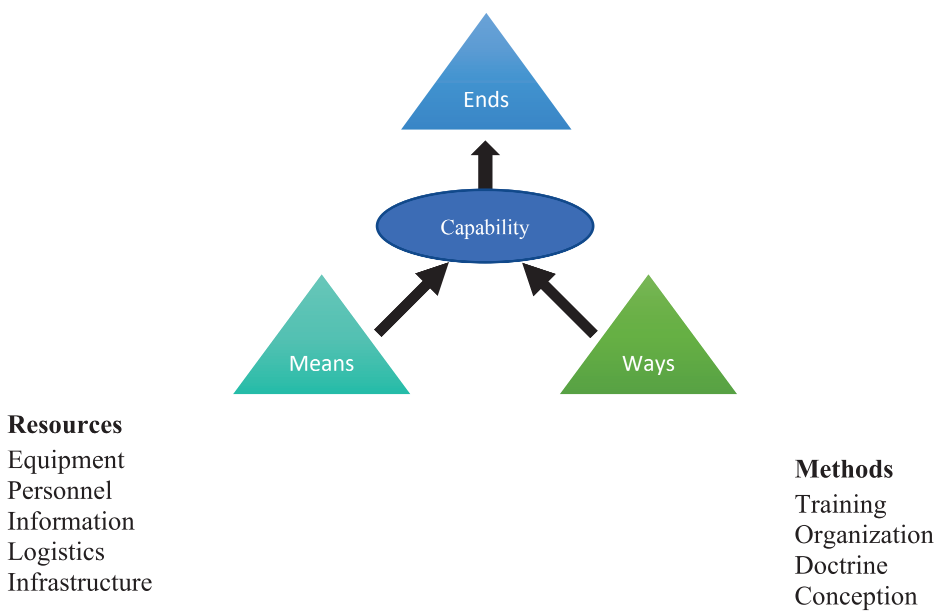
After covering the threats arising from the unlawful use of UAS and the technological alternatives for combating them, the perception of the C-UAS protection of the SISCEAB structure will be evaluated from the perspective of DOPEMAII. To do so, the origins of the methodology and its major branch within COMAER, the CBP, are explored.

CBP, DOPEMAII, and the Brazilian case

CBP differs from the traditional threat-based approach in that it focuses financial and technological resources on addressing a broad range of defense challenges rather than focusing on a specific adversary. According to Gomes et al. (2021), integrating resources and methods is necessary for the organization and use of the capability. Thus, it generates the desired final effect, as shown in Figure 6.

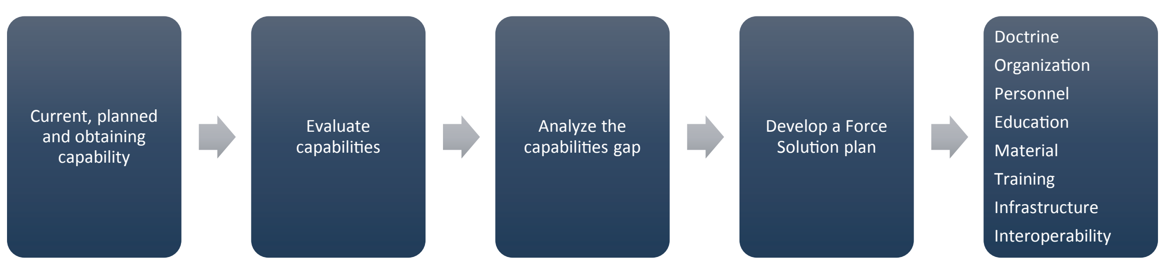
The capabilities diagnosis compares COMAER's current and planned situation against performance targets. Then, based on the gaps identified in the evaluation phase, that is, non-existent or deficient capabilities, Strength Solutions are prepared, which must follow the DOPEMAII analysis (COMAER, 2021a), as described in Figure 7.

Figure 6. Nature of Capability



Source: Taliaferro et al. (2019, with adaptations)

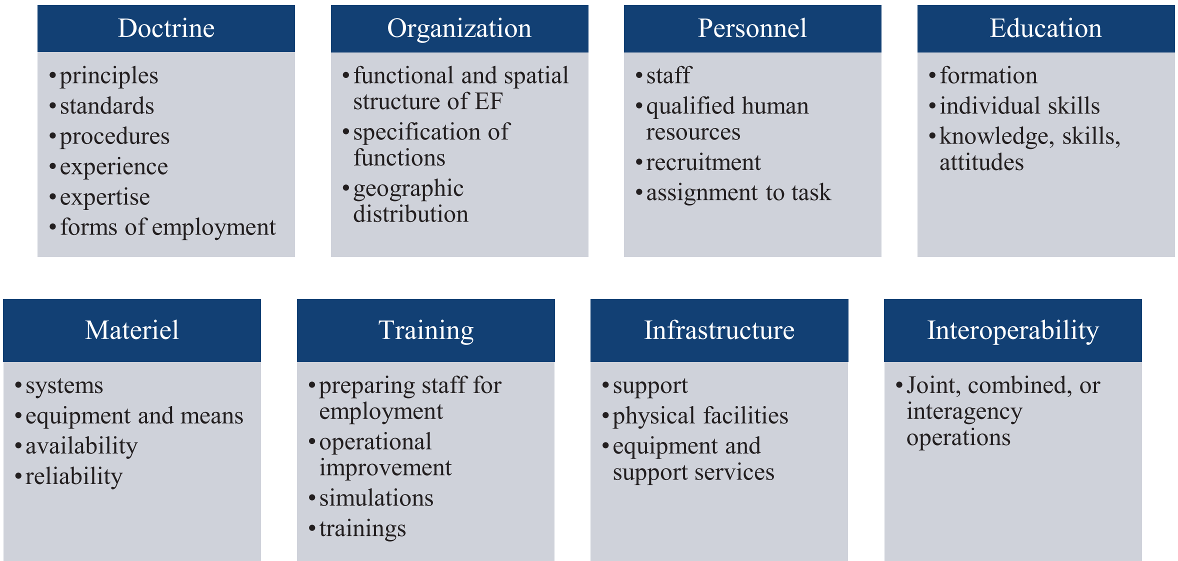
Figure 7. CBP processes at COMAER



Source: Own elaboration.

DOPEMAII consists of decomposing a given capability into each aspect of its acronym. In other words, the solution to obtaining the capability comes from acquiring or developing specific requirements (Figure 8) that meet the state's military defense needs over a defined time horizon, observing future scenarios and the budgetary and technological limits.

Figure 8. Capability components



Source: Own elaboration.

The capability is operationalized through the Element of Force[17] (EF), which can be an air, land, or sea platform, as well as a service provider or organization that performs tactical, operational, or strategic functions (Taliaferro et al., 2019).

Considering that the combined EF provides the capability, it is necessary to understand which capabilities each one can contribute (Taylor, 2013). Therefore, a questionnaire was applied to raise the perception of the SISCEAB EF on the C-UAS protection relative to each determining factor of DOPEMAII.

For this study, a literature review on UAS, C-UAS, and CBP was carried out using the main articles and books that deal with the subject. Furthermore, for data collection, a structured online questionnaire (survey) was applied, previously revised, regarding the integrity and accuracy of the questions by Brazilian Air Force personnel who implemented the CBP in the Ministry of Defense and Air Force Command. This questionnaire was intended to raise the opinion of SISCEAB specialists to verify, on a Likert scale of five degrees of perception, the perceived capability of protection against UAS in the Brazilian Air Navigation Management[18]. In addition, being guided by criteria established in government and academic documents on CBP, the questionnaire and its variables – which constitute the eight DOPEMAII factors – were sent to respondents via email[19].

17 EF is a doctrinally organized and distinct set of people, material and equipment, and facilities at a specific level of preparation necessary to carry out tasks and produce effects within a given period. (Taliaferro *et al.*, 2019).

18 Air Navigation Management is the action that consists of employing Air Force Means to, through the provision of air navigation services, manage the flow of air movements, as well as promote the safety of air navigation in Brazilian airspace (COMAER, 2020c).

19 Retrieved from https://forms.gle/g753Jj8E2YuE7HWDA. Accessed on: December 1, 2022.

To collect these representative perceptions of the Brazilian case, the sample consisted of 78 professionals from SISCEAB, from a population of 162 AVSEC[20] Managers – at local, regional, and national levels – and respective persons responsible for the integration of UAS in the Brazilian airspace of DECEA, precisely because AVSEC and UAS are part of these professionals' daily lives. The responses were analyzed using descriptive statistics, exploring each DOPEMAII factor to obtain an overview of the perceived protection capability of SISCEAB against UAS.

To understand PBC's connection with the protection of SISCEAB against UAS threats and its impact on aviation security, it is necessary to bring together prominent authors who explore Aerospace Power.

The Italian Giulio Douhet (2019) pioneered theorizing about airplane use and considered that the power necessary for command of air must pass through a well-developed civil aviation. This would represent a true reserve force for a war scenario where airports would serve as military bases and aircraft for transporting supplies, equipment, soldiers, surveillance, and search and rescue (Almeida, 2006).

This theoretical view about the dual use of civil aviation can be verified in practice, a century after the publication of his masterpiece – Il dominio dell' aria –, when more than 82,000 people were evacuated from Afghanistan in August 2021 in one of the largest airlifts in history (Fox & Stengle, 2021). In this episode, the US used the first stage of the Civil Reserve Air Fleet, requesting 18 commercial aircraft from different companies to assist in the evacuation efforts of Americans and allies (Kaufman et al., 2021), and demonstrated how the world's greatest Airpower uses civil aviation in complement to the military.

Alluding to the Clausewitzian concept of the enemy's center of gravity, John Warden, in an interview with Fadok (1995), defines it as the point where the enemy is most vulnerable and where an attack will have the best chance of being decisive. While prospecting the Brazilian reality, it is observed that:

Depending on the war scenario, the center of gravity may be inexorably anchored to its air defense and air traffic control system, so keeping them at their maximum employment capability and safeguarded from unlawful interference – even in times of peace – proves to be very relevant to the National Objectives and Aerospace Power. (Monreal, 2021, p. 33, our translation).

Carter (2020), in turn, highlights that the UAS can be used in all domains of war – air, land, sea, space, and cyberspace – in single or multiple scenarios, thus becoming the most potent weapon on a multidomain battlefield. Moreover, their potential for transporting explosive charges, identifying targets, bypassing the enemy defense system, and producing critical information about the target, combined with their characteristics of stealth, penetration, and low cost, make them ideal for asymmetric warfare.

As can be seen, the proliferation, accessibility, and technological advancement of these aircraft allow non-state actors a series of previously unattainable combat capabilities at a relatively low cost (Ball, 2017). So, how can we prevent this scenario from being envisaged for SISCEAB's airport infrastructures? It is believed that the answer to this question inevitably involves the assimilation and application of the CBP. As Lessa (2016) indicates, structuring the strategic potential of the Armed Forces around capabilities implies a change in posture. This transformation considers a future environment of high uncertainties, diffuse threats, and economic restrictions that impose the need for choices instead of traditional planning based on acquiring platforms or equipment, depending on opponents or defined scenarios.

20 The questionnaire was sent to the 154 AVSEC Local Managers – 75 Airspace Control Detachments (military) and 79 Telecommunications and Air Traffic Service Provider Stations (civilian) –, 5 AVSEC Regional Managers, 1 AVSEC National Manager and 2 responsible for the UAS area of DECEA.

Since data on DOPEMAII factors of National Defense Capabilities[21] are classified, because they are directly linked to national security, this research sought to base itself on the perceptions of AVSEC and UAS professionals at SISCEAB precisely because they are at the end of the line in regard to the conditions of protection of the organs of this system. Therefore, the questions in the applied questionnaire were designed to identify each factor that determines the capability to protect civil aviation against the new form of non-state threat, the UAS, as advocated by Ball (2017), Douhet (2019), and Carter (2020).

The responses to the questionnaire were organized through qualitative-quantitative correspondence to present a perspective of SISCEAB's C-UAS protection from the standpoint of CBP and DOPEMAII. The survey obtained a return rate of 48.1% of the total possible professionals, receiving 78 responses. According to Gil (2008), the formula for calculating samples for finite populations in social research, when the surveyed population does not exceed 100,000 elements, becomes the following:

$$n = \frac{\sigma^2 . p . q . N}{e^2(N-1) + \sigma^2 . p . q}$$

Where: n = Sample size

σ^2 = Chosen confidence level, expressed in the number of standard deviations

p = Percentage with which the phenomenon occurs

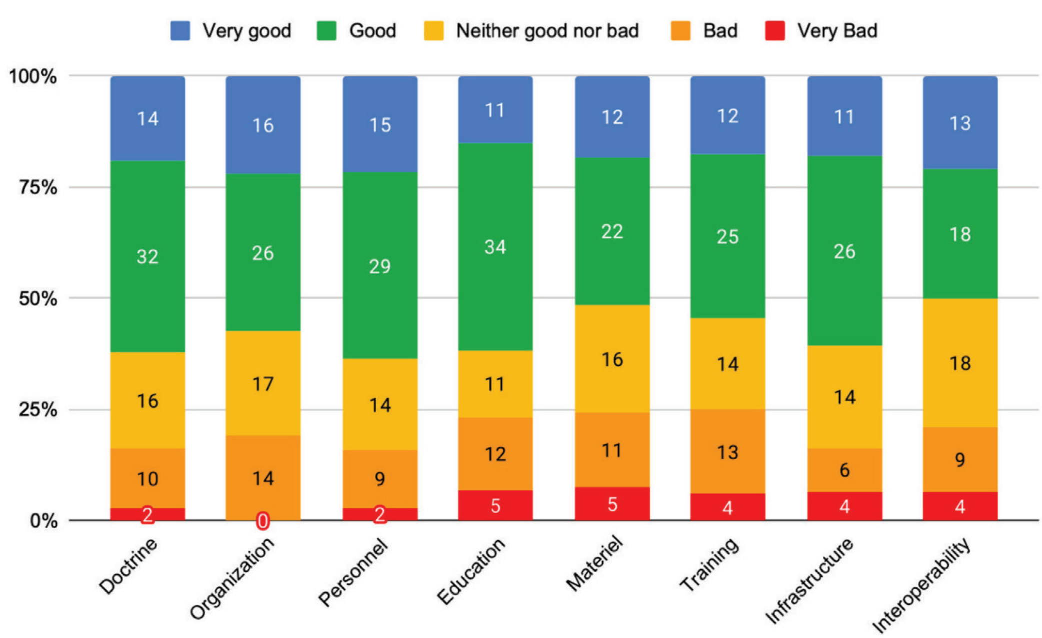
q = Complementary percentage

N = Population size

e^2 = Maximum allowed error

By adopting a sample size of 78, a confidence level of 95% (two standard deviations), and a population of 162, a maximum error of 3.6% was found. From the perspective of each determining factor, the picture of SISCEAB's current perceived capability to oppose the unlawful use of UAS, isolated or swarm, is presented in Graph 1.

Graph 1. Summary of responses



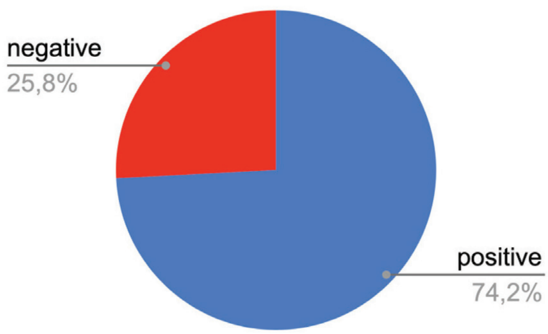
Source: Own elaboration.

21 National Defence Capabilities are those composed of different portions of expressions of National Power. They are implemented through the coordinated and synergistic participation of government agencies and, where appropriate, private entities oriented towards defense and security in its broadest sense (COMAER, 2018).

On the one hand, the perceived capability of SISCEAB to deal with the unlawful use of UAS stood out in the Doctrine, Personnel, Education, and Infrastructure factors. On the other hand, the numbers raised indicate that DECEA can further develop the Material and Interoperability factors to obtain C-UAS capability and, in this way, collaborate with protecting civil aviation against non-state threats.

From the numbers received, the values related to "Very bad" and "Bad" were added and classified as negative perceptions, as well as "Very good" and "Good" as positive perceptions, with the responses compiled and presented in Graph 2.

Graph 2. Perception of C-UAS protection in SISCEAB



Source: Own elaboration.

From the graphs above, it appears that the perceived capability of SISCEAB to protect against the unlawful use of UAS is 74.2% positive – ranging from 70.6% to 77.8% when using the found margin of error of 3.6% –, indicating that air navigation security operators, on average, consider the measures adopted by DECEA to be sufficient and proficient. This fact corroborates the importance of protecting civil aviation and aerospace infrastructure. Thus, ensuring the potential reserve of human and material resources needed for mobilization and support for aviation activities due to the continental dimension of the country as well as the economic importance of the nation (COMAER, 2020b), is safeguarded, as theorized by Douhet (2019).

In addition, the construction of new capabilities for the Brazilian Air Force over the coming decades is a challenge for "Força Aérea 100[22]" in its quest to understand, evaluate, adapt, and prepare for the future through a systematic process and continuous effort in building military capability to compose the main attempt of National Defense (COMAER, 2018).

The research had some limitations. Due to the nature of the subject, the classification of information related to accuracy, frequency, and range of radars did not allow the presentation of specific data on the performance of C-UAS systems tested by Brazilian government agencies. It is worth emphasizing that, although they could complement the research findings, the imposed limitations did not interfere with the result as they were not essential for achieving its general objective.

Conclusion

The present work sought to analyze the current perceived capability of SISCEAB to deal with the unlawful use of UAS. To this end, it contextualized the theme in the national and international scenarios and pointed out the importance of C-UAS for the safe and secure development of Brazilian aviation. The methodological dynamics, statistical analysis tools, and research limitations were presented, as were the principal authors who guided the studies, such as Douhet (2019), Carter (2020), and Lessa (2016).

The main threats related to UAS for civil aviation were discussed, correlating with the theories of Douhet and bringing current statistics of equipment numbers and requests for access to airspace. Furthermore, the hypotheses of use and the specifications of the UAS were described, referring to technical details such as the number of engines, level of autonomy, power supply, sizes and weights, sensors, and internal navigation systems, explaining the internal functioning of the systems of the UAS. Likewise, concepts of the illicit nature of

22 According to the Strategic Conception - Força Aérea 100, it refers to the planning of the transformation of the current COMAER, until the 100th anniversary of the creation of the Ministry of Aeronautics, which will take place in the year 2041 (COMAER, 2018).

these systems were exposed, possible advantages in using them by non-state threats were listed, and incidents and attacks on critical systems of the National Power were listed, thus demonstrating the potential of this threat.

Continuing, the leading civil and military C-UAS existing in the global market were detailed, and an extensive investigation was carried out on each technology and the respective methodologies of action to present options for countering the threats listed above.

Finally, an analysis of SISCEAB's perceived capability to oppose UAS was carried out from the perspective of DOPEMAII as part of a CBP survey for civil aviation. This was carried out using forms answered by those responsible for the security of civil aviation and UAS at DECEA. The responses indicated that the current perceived capability of SISCEAB to protect against the unlawful use of UAS is positive, thus demonstrating the importance of civil aviation for Brazilian Aerospace Power.

Considering the growth in the amount of equipment, the spectrum of employment, and the load potential, speed, autonomy, and range of the UAS, the threat intensifies in the same proportion, indicating to DECEA that investments in the area are crucial for maintaining the perception of protection at high levels of security.

It was observed that the number of incidents with isolated drones at airports has shown remarkable growth and is already causing minor impacts on the national air network, which could become a significant problem for civil aviation shortly. However, the answers to the questionnaires did not show any concern about the danger posed by swarms of drones, indicating that this threat is likely not credible for Brazilian air navigation.

Making an addendum and referring the problem to the national context, it is denoted that the authorities still have legal and regulatory gaps, mainly for interagency coordination for the activation of response instruments in the face of threats by drones registered in recent history. Furthermore, it was verified that the existing C-UAS systems in airports are private, lack specific regulation and inspection, and may become a risk to aircraft safety and air navigation by electronically interfering with the flight controls and CNS systems of modern aircraft, which is a latent imbroglio not only in Brazil but also in the global scenario.

The research found that SISCEAB acts in line with what Lessa (2016) recommends when working on each factor of the acronym DOPEMAII in C-UAS protection, thus confirming the change in the thinking of the Brazilian Air Force as a whole, specifically in the search to add human resources and materials to a new approach oriented to effects and no longer to specific threats in the complex identification of the limits of application of Aerospace Power. In this way, SISCEAB follows the rapid evolution of technologies, theaters of operation, and the multiplicity of dangers to international security, collaborating with the guarantee of national sovereignty.

References

Almeida, A. L. D. (2006). A evolução do poder aeroespacial brasileiro [Doctoral dissertation, Universidade de São Paulo]. https://doi.org/10.11606/D.8.2006.tde-19062007-153215

Air Force Research Laboratory (2021). Directed Energy Futures 2060: Visions for the next 40 years of U.S. Department of Defense Directed Energy Technologies. https://www.afrl.af.mil/Portals/90/Documents/RD/Directed_Energy_Futures_2060_Final29June21_with_clearance_number.pdf?ver=EZ4QY5MG5UK2LDdwiuPc6Q%3D%3D

Ball, R. J. (2017). The proliferation of unmanned aerial vehicles: Terrorist use, capability, and strategic implications (No. LLNL-TR-740336). Lawrence Livermore National Lab.(LLNL), Livermore, CA (United States). https://doi.org/10.2172/1410035

Ballard, T., Pate, J., Ackerman, G., McCauley, D., & Lawson, S. (2001). Chronology of Aum Shinrikyo's CBW activities. Monterey Institute of International Studies, Center for Nonproliferation Studies. https://nonproliferation.org/wp-content/uploads/2016/06/aum_chrn.pdf

Birch, G. C., Griffin, J. C., & Erdman, M. K. (2015). UAS detection classification and neutralization: Market survey 2015 (No. SAND2015-6365). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States). https://doi.org/10.2172/1222445

Brazilian Air Force Command (2018). Gabinete do Comandante. Concepção Estratégica - Força Aérea 100. https://www.fab.mil.br/Download/arquivos/DCA%2011-45_Concepcao_Estrategica_Forca_Aerea_100.pdf

Brazilian Air Force Command (2020a). Departamento de Controle do Espaço Aéreo. Instrução sobre Aeronaves não tripuladas e o Acesso ao Espaço Aéreo. https://www.gov.br/defesa/pt-br/arquivos/cartografia/divcar/2021/ica_100-40_trafegoaereo_22_05_2020.pdf

Brazilian Air Force Command (2020b). Estado-Maior da Aeronáutica. Doutrina Básica da Força Aérea Brasileira - Volume 1. https://www.sislaer.fab.mil.br/terminalcendoc/Busca/Download?codigoArquivo=6535

Brazilian Air Force Command (2020c). Estado-Maior da Aeronáutica. Doutrina Básica da Força Aérea Brasileira - Volume 2. https://www2.fab.mil.br/unifa/ppgca/images/conteudo/D-QBRN/DCA_1-1_DOUTRINA_BSICA_DA_FORA_AREA_BRASILEIRA_-VOLUME_2_2020.pdf

Brazilian Air Force Command (2020d). Estado-Maior da Aeronáutica. Diretriz que dispõe sobre a Sistemática de Planejamento e Gestão Institucional da Aeronáutica - Volume 1 - Planejamento. https://www.sislaer.fab.mil.br/terminalcendoc/Busca/Download?codigoArquivo=4737

Brazilian Air Force Command (2021a). Estado-Maior da Aeronáutica. Diretriz de Implantação do Planejamento Baseado em Capacidades no COMAER. https://www.sislaer.fab.mil.br/terminalcendoc/Busca/Download?codigoArquivo=12765

Brazilian Air Force Command (2021b). Departamento de Controle do Espaço Aéreo. Plano de Implementação ATM Nacional. https://publicacoes.decea.mil.br/publicacao/pca-351-3

Brazilian Institutional Security Office of the Presidency of the Republic (2019). Institui os Grupos Técnicos relacionados à área de Transportes, no âmbito da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo. https://www.in.gov.br/en/web/dou/-/resolucao-n-9-de-21-de-agosto-de-2019-212178923

Carter, C. (2020). Understanding C-UAS Purpose and Process. Counter Unmanned Aircraft Systems Technologies and Operations. https://newprairiepress.org/ebooks/31

Cieślak, E. (2021). Unmanned Aircraft Systems: Challenges to Air Defense. Safety & Defense, 1, pp. 72-83. https://doi.org/10.37105/sd.110

Cole, S. (2019, April 09). Counter-drone technologies are evolving to "counter" countermeasures. Military Embedded Systems. https://militaryembedded.com/unmanned/counter-uas/counter-drone-technologies-are-evolving-to-counter-countermeasures

Cook, K. L. B. (2007). The Silent Force Multiplier: The History and Role of UAVs in Warfare. IEEE Aerospace Conference, 1-7, http://doi.org/10.1109/AERO.2007.352737

Custers, B. (2016). Drones here, there and everywhere introduction and overview. In The future of drone use (pp. 3-20). TMC Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-132-6_1

Da Silva, C. D. (2020). O Planejamento Baseado em Capacidades e o advento do Exército do Futuro: convergências. Centro de Estudos Estratégicos do Exército: Análise Estratégica, 17(3), 35-44.

Department of Defense (2011, August 11). Joint Publication 3-0, Joint Operations. https://www.benning.army.mil/mssp/security%20topics/Potential%20Adversaries/content/pdf/JP%203-0.pdf

Douhet, G. (2019). The command of the air. University of Alabama Press.

Dudenhoeffer, D. D. (2020). Day of the Drone: Protecting Critical Infrastructure from Terrorist Use of Unmanned Aerial Systems. In Toward Effective Cyber Defense in Accordance with the Rules of Law (pp. 17-31). IOS Press. https://doi.org/10.3233/NHSDP20038

European Aviation Safety Agency (2016). Study and Recommendations regarding: Unmanned Aircraft System Geo-Limitations. https://www.easa.europa.eu/sites/default/files/dfu/GTF%20-%20Report_Issue2.pdf

Exec. Order No. 11237 (2022, October 18). Aprova as Estruturas Regimentais e os Quadros Demonstrativos dos Cargos em Comissão e das Funções de Confiança do Comando da Aeronáutica do Ministério da Defesa e da Caixa de Financiamento Imobiliário da Aeronáutica e remaneja e transforma cargos em comissão e funções de confiança. http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11237.htm#art9

Fadok, D. S. (1995). John Boyd and John Warden: Air Power's Quest for Strategic Paralysis. Air University. School of Advanced Airpower Studies. https://apps.dtic.mil/sti/pdfs/ADA291621.pdf

Fox, B., & Stengler, J. (2021, August 25). What's happening with Afghanistan evacuations? The Associated Press. https://apnews.com/article/middle-east-afghanistan-evacuations-d324fa6e55ec7050287395fafc3c2312

Gil, A. C. (2008). Métodos e técnicas de pesquisa social. 6ª ed. Editora Atlas SA.

Giri, D. V. (2004). High-power electromagnetic radiators: nonlethal weapons and other applications. Harvard University Press.

Gomes, R., Belderrain, M. C. N., & De Marchi, M. M. (2021). Proposta de Modelo para Avaliação de Capacidades no Contexto do PBC. https://www.sige.ita.br/edicoes-anteriores/2021/st/218627_1.pdf

Guvenc, I., Koohifar, F., Singh, S., Sichitiu, M. L., & Matolak, D. (2018). Detection, tracking, and interdiction for amateur drones. IEEE Communications Magazine, 56(4), 75-81. https://doi.org/10.1109/MCOM.2018.1700455

Haider, L. C. A. (2019). A Comprehensive Approach to Countering Unmanned Aircraft Systems. Joint Air Power Competence Centre (JAPCC). https://www.japcc.org/wp-content/uploads/A-Comprehensive-Approach-to-Countering-Unmanned-Aircraft-Systems.pdf

Hambling, D. (2018). Swarm Troopers: como os pequenos drones irão conquistar o mundo. Biblioteca do Exército.

Internacional Civil Aviation Organization (2019). Aviation Benefits Report. https://www.icao.int/sustainability/Documents/AVIATION-BENEFITS-2019-web.pdf

International Civil Aviation Organization (2020). Aviation Security. https://www.bazl.admin.ch/dam/bazl/de/dokumente/Fachleute/Regulationen_und_Grundlagen/icaonnex/icao_annex_17_security.pdf.download.pdf/icao_annex_17_security.pdf&usg=AOvVaw1jcNgh--hz5SY-Iqtg4MMG

International Civil Aviation Organization (2005). Rules of the Air. https://www.icao.int/Meetings/anconf12/Document%20Archive/an02_cons%5B1%5D.pdf

Jasper, F. N. H., & Nunes, A. F. (2022). Soberania e Controle do Espaço Aéreo: uma visão brasileira. Revista Tempo Do Mundo, (28), 345-366. https://doi.org/10.38116/rtm28art12

King, G., Keohane, R. O., & Verba, S. (2021). Designing social inquiry: Scientific inference in qualitative research. Princeton University Press.

Lessa, N. O. (2016). Avaliação de arquitetura de sistemas de defesa baseada no conceito de capacidade. [Doctoral dissertation, Instituto Tecnológico de Aeronáutica].

Lu, Y., Xue, Z., Xia, G. S., & Zhang, L. (2018). A survey on vision-based UAV navigation. Geo-spatial information science, 21(1), 21-32. https://doi.org/10.1080/10095020.2017.1420509

Lykou, G., Moustakas, D., & Gritzalis, D. (2020). Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies. Sensors, 20(12), 3537. https://doi.org/10.3390/s20123537

Lyu, C., & Zhan, R. (2022). Global Analysis of Active Defense Technologies for Unmanned Aerial Vehicle. IEEE Aerospace and Electronic Systems Magazine, 37(1), 6-31. https://doi.org/10.1109/MAES.2021.3115205

Mátyás, P., & Máté, N. (2019). Brief history of UAV development. Repüléstudományi Közlemények, 31(1), 155-166. https://doi.org/10.32560/rk.2019.1.13

Menezes, R. R. V. (2019). Análise do GNSS PPP multi-constelações com uso dos sistemas GPS, GLONASS e GALILEO. [Master dissertation, Universidade Federal de Viçosa]. http://www.locus.ufv.br/handle/123456789/24634

Monreal, E. A. (2021). Gerenciamento de riscos no controle do espaço aéreo brasileiro e a fase de identificação dos atos de interferência ilícita. [Master's dissertation, Universidade da Força Aérea]. https://redebia.direns.fab.mil.br/mobile/detalhe.asp?idioma=ptbr&acesso=web&codigo=78930&tipo=1&detalhe=0&busca=3

Monreal, E. A., & Vilar-Lopes, G. (2021). Cultura justa no incremento do Poder Aeroespacial brasileiro. In Anais do 11th Encontro Nacional ENABED, Rio de Janeiro, RJ. https://www.enabed2021.abedef.org/resources/anais/15/enabed2020/1635171773_ARQUIVO_d938598a9a91c47fe5bd0a6327b808fd.pdf

Miasnikov, E. (2005). Threat of terrorism using unmanned aerial vehicles: technical aspects. Moscow, Russia: Center for Arms Control, Energy, and Environmental Studies. https://www.armscontrol.ru/UAV/UAV-report.pdf

Miranda, E. A. (2021). Sistema de Contenção de Aeronave Não Tripulada (C-UAS - counter unmanned aircraft system) no SISCEAB. In II Simpósio de Defesa Anti SARP, Rio de Janeiro, RJ. http://www.esacosaae.eb.mil.br/images/phocagallery/2021/Simposio/00-palestras/006.pdf

National Museum of The United States Air Force. (2022). Kettering Aerial Torpedo "Bug". https://www.nationalmuseum.af.mil/Visit/Museum- Exhibits/Fact-Sheets/Display/Article/198095/kettering-aerial-torpedo-bug/.

Park, S., Kim, H. T., Lee, S., Joo, H., & Kim, H. (2021). Survey on anti-drone systems: Components, designs, and challenges. IEEE Access, vol. 9, pp. 42635-42659 https://doi.org/10.1109/ACCESS.2021.3065926

Patterson, D. R. (2017). Defeating the threat of small unmanned aerial systems. Air & Space Power Journal, 31(1), 15-26. https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-29_Issue-2/2017_2_03_patterson_s_eng.pdf

Radasky, W. A., Baum, C. E., & Wik, M. W. (2004). Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI). IEEE Transactions on electromagnetic compatibility, 46(3), 314-321. https://doi.org/10.1109/TEMC.2004.831899

Salameh, H. B., Otoum, S., Aloqaily, M., Derbas, R., Al Ridhawi, I., & Jararweh, Y. (2020). Intelligent jamming-aware routing in multi-hop IoT-based opportunistic cognitive radio networks. Ad Hoc Networks, 98, 102035. https://doi.org/10.1016/j.adhoc.2019.102035

Sanders, A. W. (2017). Drone swarms. [Master's Thesis, United States Army Command and General Staff College]. https://apps.dtic.mil/sti/pdfs/AD1039921.pdf

Sarma D; Quinn, P. (2018). Data protection, social, ethical and legal frameworks. http://aladdin2020.eu/wp-content/uploads/2018/04/ALADDIN_D3.1_DataProtectionSoEL_Framework_V1_0_PU.pdf

Schóber, T., Koblen, I., & Szabo, S. (2012). Present and potential security threats posed to civil aviation. Incas Bulletin, 4(2), 169. https://doi.org/10.13111/2066-8201.2012.4.2.17

Kaufman, E., Liebermann, O., Stracqualursi, V., & Benveniste, A. (2021, August 22). Pentagon activates US airlines to assist with evacuation efforts from Afghanistan. CNN. https://edition.cnn.com/2021/08/22/politics/pentagon-us-airlines-american-delta-united-afghanistan-evacuation/index.html/

Statista (2020). Consumer drone unit shipments worldwide from 2020 to 2030 (in millions). https://www.statista.com/statistics/1234658/worldwide-consumer-drone-unit-shipments/

Sun, R., Zhang, W., Zheng, J., & Ochieng, W. Y. (2020). GNSS/INS integration with integrity monitoring for UAV No-fly zone management. Remote Sensing, 12(3), 524. https://doi.org/10.3390/rs12030524

Taliaferro, A. C., Gonzalez, L. M., Tillman, M., Ghosh, P., Clarke, P., & Hinkle, W. (2019). Defense Governance and Management: Improving the Defense Management Capabilities of Foreign Defense Institutions - A Guide to Capability-Based Planning (CBP). https://apps.dtic.mil/sti/pdfs/AD1122378.pdf

Tamasi, G., & Demichela, M. (2011). Risk assessment techniques for civil aviation security. Reliability Engineering & System Safety, 96(8), 892-899. https://doi.org/10.1016/j.ress.2011.03.009

Taylor, B. (2013). Analysis support to strategic planning. https://cradpdf.drdc-rddc.gc.ca/PDFS/unc194/p801995_A1b.pdf

Taylor, B., & Wood, D. (2005, April). Guide to capability-based planning. In Meeting Proceedings of RTO-MP-SAS-055-Analytical Support to Defense Transformation: The RTO Studies, Analysis and Simulation Panel (SAS) Symposium (pp. 26-28). https://www.hsdl.org/?view&did=461818

Vergouw, B., Nagel, H., Bondt, G., & Custers, B. (2016). Drone technology: Types, payloads, applications, frequency spectrum issues and future developments. In The future of drone use (pp. 21-45). TMC Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-132-6_2

Wallace, R. J., & Loffi, J. M. (2015). Examining Unmanned Aerial System Threats & Defenses: A Conceptual Analysis. International Journal of Aviation, Aeronautics, and Aerospace, 2(4). https://doi.org/10.15394/ijaaa.2015.1084

Zohuri, B. (2016). Directed energy weapons. In Directed Energy Weapons (pp. 1-26). Springer, Cham. https://doi.org/10.1007/978-3-319-31289-7_1