ABIN

Intelligence Doctrine

BRASILIA
November 2023

PRESIDENCY OF THE REPUBLIC
OFFICE OF THE CHIEF OF STAFF
BRAZILIAN INTELLIGENCE AGENCY

Intelligence Doctrine

BRASILIA
November 2023

FEDERAL REPUBLIC OF BRAZIL
President Luiz Inacio Lula da Silva

OFFICE OF THE CHIEF OF STAFF
Minister Rui Costa

BRAZILIAN INTELLIGENCE AGENCY (ABIN)
Director-general Luiz Fernando Correa

PLANNING AND MANAGEMENT SECRETARIAT
Secretary Rodrigo de Aquino

SCHOOL OF INTELLIGENCE
Director Marco Cepik

COORDINATION
Coordination for Doctrine and Intelligence / School of Intelligence

INTERNATIONAL BIBLIOGRAPHIC CATALOGING AND STANDARDIZATION
Knowledge and Memory Division / School of Intelligence

GRAPHIC PUBLISHING
Coordination of Social Communications / ABIN

PRINTING
Division for Graphic Services / ABIN

COVER
Luciano Daniel da Silva / Coordination of Social Communications / ABIN

BRAZILIAN INTELLIGENCE AGENCY
SPO Área 5, quadra 1
CEP: 70610-905 – Brasília/DF

1a edition in english: January 2025

International Cataloging in Publication Data (CIP)

D726 Intelligence Doctrine. - Brasília: Abin, 2023.

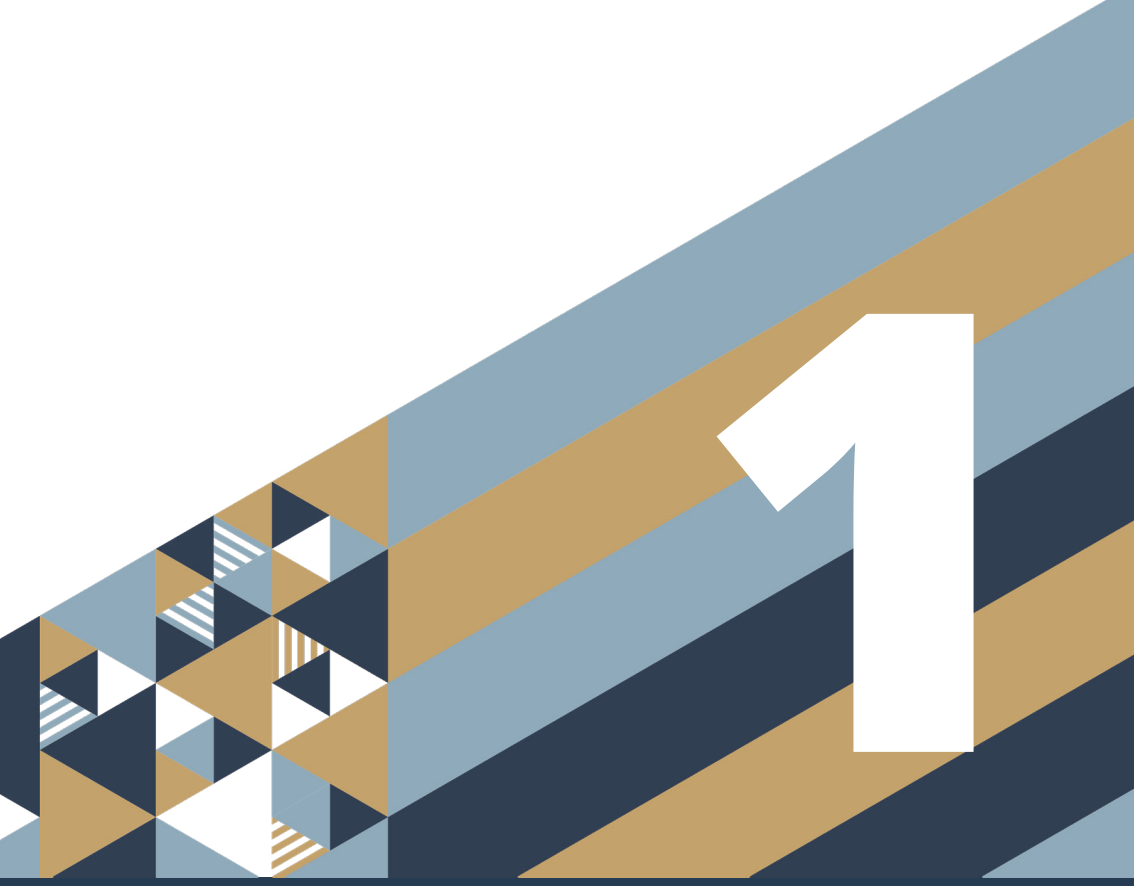
171 p.
Aprovada pela Portaria GAB/DG/ABIN/CC/PR nº 1.205, de 27 de novembro de 2023.
1. Atividade de Inteligência - doutrina – Brasil. 2. Atividade de Inteligência - ensino. I. Agência Brasileira de Inteligência. II. Título.

CDU 355.40(81)

ABIN

Intelligence Doctrine

Table of contents



1

Introduction

1. Introduction

This document is the current version of the Intelligence Doctrine adopted by the Brazilian Intelligence Agency (ABIN). It is important to clarify what is meant by doctrine and what the objectives of this publication are.

The term doctrine refers to a set of principles that serves as the basis for the functioning of any system of action and reflection. It is therefore declaratory, flexible, provisional knowledge, always subject to criticism. Such a set helps to educate and guide individual and collective practices of an organization. To properly serve this purpose, a doctrine needs to be clear, parsimonious, self-critical, and open to constant revision. This is the case here, as this version of the doctrine is expected to be revised and improved from time to time.

The prescriptive force of a doctrine is necessarily weaker than that of a law. Furthermore, doctrines are insufficient as a source of knowledge and a basis for action, since descriptive models, methods and explanatory theories are also necessary to resolve disagreements over questions of fact and value. Nor are doctrines capable of predicting the future, or even of guiding every single action in every imaginable context. However, doctrines are important precisely because they record conceptual understandings that provide a common prescriptive basis for acting in time and space. The aim of this document is to define and openly show the public ABIN's current understanding of intelligence activity and how it should be practiced by the Agency in Brazil, based on our Federal Constitution and legislation.

ABIN is an agency of the Presidency of the Republic dedicated to producing knowledge to support the decisions of the President of the Republic and his ministers. Its duties and activities are set out in Law 9,883/1999, which established ABIN and also created the Brazilian Intelligence System (Sisbin). Both Sisbin's structure and operation are regulated by Decree 11,693/2023. According to this decree and Ordinance GAB/DG/ABIN/CC/PR number 926, in November 2023, in addition to having ABIN as its coordinating body, Sisbin comprised eleven (11) permanent bodies, nine (09) dedicated intelligence bodies and fractions and twenty-seven (27) associate bodies. The new regu-

lations also provide for the possibility of integrating federal agencies into Sisbin, provided legal and procedural criteria are met.

Article 10, item XIV of the regulations also states that one of ABIN's duties is to encourage and support the development of doctrine for intelligence activity in the country. This document is not intended to replace or surpass other intelligence doctrines of Brazil's intelligence system, subsystems, and bodies. ABIN is obliged to have its own doctrine. The publication of its doctrine aims, under the terms of Decree 11,693/2023, to facilitate dialogue and synergy between the various components of Sisbin.

ABIN's understanding of intelligence activity is the result of its own experience since the agency was created in 1999. It also results from the incorporation of elements deemed relevant by other official Brazilian documents on various doctrines, by public debates held in the National Congress and within the civil society, by scientific and technical production on intelligence activity in Brazil and abroad, and even by the tacit knowledge available on the subject. As this is a guidance document aimed at facilitating communication between members of the agency and between the agency and society, including other bodies responsible for developing the country's intelligence activity, it was decided not to indicate the various sources examined on each page of the document. The interested reader will find, at the end of this publication, a preliminary list of texts and documents that inspired some of the understandings here adopted. These references also serve as further reading to foster the debate on intelligence doctrine in Brazil. Many other notions and concepts are the result of collective production by people working at ABIN. In this sense, the responsibility for the concepts, methods, processes, norms, principles and values systematized in this body of doctrine lies entirely with the Agency.

The adoption of this Doctrine also makes it possible to implement two additional principles: public control and impersonality in the conduct of the agency's employees. As it is an activity that involves secrecy (a form of public and legally delimited regulation of specific informational flows) as an instrument and, to a certain extent, as a condition for effectiveness, it must be overseen, both internally, by the

correct direction of its actions, and externally, by bodies established by law. This Doctrine expresses ABIN's commitment to strengthening such controls and impersonality in the application of procedures derived from common understandings about the meaning of actions within the scope of a Democratic State of Law, the very reason and purpose for the existence of ABIN itself and Sisbin.

The text is divided into eight parts, in addition to this Introduction. Section 2 presents the fundamentals of intelligence activity as we understand it at ABIN. This section explains the understanding that intelligence activity is divided into two branches (intelligence and counterintelligence) and two functions (analysis and operations). Each branch and function is discussed, respectively, in sections 3 to 6 of the text. A brief conclusion is offered in section 7. The text is completed by a glossary of terms used (section 8) and an incomplete list (section 9) of works considered relevant for the elaboration of this doctrine and for the debate on the topic.

Enjoy your reading.

2

Fundamentals of Intelligence Activity

2. Fundamentals of Intelligence Activity

Intelligence activity produces knowledge and carries out actions aimed at reducing vulnerabilities and neutralizing threats against the security of people and Brazilian institutions. It also aims to protect sensitive information, people, areas, facilities and means, by preventing, detecting, identifying, obstructing and neutralizing adverse intelligence actions. In accordance with the law, intelligence activity also identifies opportunities to achieve public policy objectives critical to the security and well-being of society.

In a world marked by rapid and radical global transformations in climate, demography, energy grid and Digital Age technologies, political coexistence between different societies is still largely defined by the existence of sovereign States, as recognized by the Montevideo Convention on the Rights and Duties of States (1933) and the Charter of the United Nations (1945). There are almost two hundred states in the world, which are very unequal to each other. There is also a dense network made up of thousands of international organizations, in addition to a huge diversity of companies, groups, networks and billions of individuals pursuing different goals in the world. When there are conflicts of interest and value, they are not always resolved by formal and informal international institutions. Therefore, the preservation of popular and national sovereignty, understood here as the collective capacity of Brazilians to make decisions and act in accordance with their Constitution, is an imperative that justifies and explains the need for intelligence services. It also explains why - just as is the case with armed forces and diplomacy - there are intelligence services in so many countries with very different constitutional orders in the contemporary world.

Under article 1 of the 1988 Constitution, the Federative Republic of Brazil is formed by the indissoluble union of states and municipalities and the Federal District. This union constitutes a Democratic State of Law and is based on sovereignty, citizenship, human dignity, the social values of work and free enterprise, as well as political pluralism. In article 3 of the Constitution, the fundamental objectives of this Republic are defined as the building of a free, fair and support-

ive society, the guarantee of national development, the eradication of poverty and marginalization, the reduction of social and regional inequalities, as well as the promotion of good for everyone, free of prejudice based on origin, race, sex, color, age and any other form of discrimination. In article 4, the principles that govern Brazil's international relations are defined and are, namely, national independence, the prevalence of Human Rights, the self-determination of peoples, non-intervention, equality between States, the defense of peace, the peaceful resolution of conflicts, the repudiation of terrorism and racism, the cooperation between peoples for the progress of humanity, the granting of political asylum and the integration of the peoples of Latin America.

Together with fundamental rights and guarantees (Title II of the Federal Constitution), constitutional norms and statutory laws define a set of objectives to be achieved, as well as the means to be employed, by all Brazilians in doing so, individually and collectively. Therefore, all intelligence activity conducted in Brazil must follow the same principles, which form the basic premises of ABIN's current Doctrine. Under the terms of Law No. 9,883/1999, the National Intelligence Policy, established by Decree 8,793/2016, and Decree No. 11,693/2023, complemented by other legitimately established legal and administrative provisions, intelligence activity in the Brazilian State is to be carried out by public organizations, permanently and methodically, by specialized professionals, assigned to their own continuous work structures, known as intelligence bodies.

2.1. Specialization

These bodies can be classified as intelligence services when their primary purpose is to carry out intelligence activities, or as intelligence units, when they are part of bodies that have other purposes. The intelligence centers of the armed forces, as well as the intelligence departments of police agencies and the intelligence coordination offices of other federal institutions, for example, belong to agencies that have their own purposes within the state. Sisbin is made up of various intelligence bodies that support the federal government's

decision-making process in areas of public policy relating to the provision of public security, foreign relations, national defense and other issues critical to national development and the common good.

To carry out the work defined by legislation and government priorities, ABIN's intelligence professionals monitor various issues defined by the agency's General Direction. Such issues are located in a national, international, transnational or even cyber environment. This informational dimension of intelligence work (production of knowledge to support decisions) is similar to what other research, statistical and advisory bodies carry out, but focuses specifically on security-related and conflict-related topics. In addition to its informational function, intelligence activity must also act in circumstances determined by law. Such circumstances include obtaining unavailable data, protecting knowledge, information and sensitive data and also people, areas, facilities and means that either store, have access to or disseminate such knowledge, information and data, as well as preventing, detecting, identifying, evaluating, obstructing and neutralizing actions by adverse intelligence.

To fulfill its dual mission, intelligence activity is organized into two branches: intelligence and counterintelligence. The branches are areas of expertise, indicating the application of specific knowledge to the practice of such activity. In this sense, they do not denote a specific organizational structure, which is contingent and defined by federal decree. What is relevant is to ensure that the professionals who will carry out each type of activity are trained to do so and operate according to a common legal, institutional and doctrinal basis.

Intelligence is the branch aimed at the production and dissemination of knowledge relating to facts, events, situations or phenomena that occur within and outside the national territory that may have immediate or potential influence on the decision-making process and government action and may present or indicate opportunities and threats to the fundamental objectives of the State.

Facts are verifiable objects, capable of description or prediction. Thus, a fact is a representation that is as objective as possible of a reality external to the observer trying to understand it, and can be

assessed by anyone using conceptual references and measurable and validated methods.

Events are occurrences located in time and space. An event is an occurrence that can be delimited geographically and chronologically by specific landmarks. Events are produced by mechanisms that link contexts, structures and actors.

Situations are occurrences contextualized from human experience. It is from experiences shared by a society that the conditions for interpreting these events are established and, thus, the situations in which they are inserted are determined. For intelligence, situations are a constituent part of the reality of events, designating the context in which one or more ongoing events must be evaluated.

Phenomena are processes made up by the unfolding of facts, events and situations, the dynamics between them and the effects they produce over time on human experience and the outside world.

For example, the high productivity of the Brazilian agro-industrial sector is a fact. Measures filed by countries with multilateral competitive regulatory bodies in order to block imports of Brazilian agricultural products are events. The situation of permanent international competition for markets for the export of agricultural products constitutes a situation. The dynamics of the formation of international trade blocs according to the development of global capitalism constitutes a phenomenon to be monitored and interpreted.

Another example: the existence of organized criminal groups is a fact. Serial riots, triggered in prison units with retaliations between antagonistic criminal groups, constitute events. A dynamic of conflict over money and territories of influence between criminal organizations, with an impact on society's security framework, is an example of a situation. In turn, the supply and request flows and the interactions of transnational organized crime, which give rise to this tense environment, constitute a phenomenon to be monitored and interpreted.

Opportunity is understood as a condition or factor favorable to the achievement of national interests established by the Constitution and legislation; a threat is understood as an antagonistic opposition to the pursuit of such interests and the safeguarding of sensitive

knowledge and data. Threats can be distinguished according to their degree of intentionality. An antagonism is a threat that intentionally opposes the achievement of national interests. An obstacle, in turn, interferes with national interests, but does not necessarily express the intentionality of an actor to cause harm, deprivation, violence and suffering to people and institutions.

Counterintelligence is the branch of intelligence that produces knowledge and develops specialized actions aimed at preventing, detecting, identifying, evaluating, obstructing and neutralizing adverse intelligence activities, including actions that are a threat to the interests of society and the State, the decision-making process, the safeguarding of knowledge, information and sensitive data, the safeguarding of those means where they are stored or through which they move, the safeguarding of their holders and the safeguarding of those areas and facilities where they are kept.

Adverse action is defined as intentional action by one or more actors, sponsored or not, that opposes the achievement of national interests through the illegitimate search for access to knowledge, information and sensitive data, threatening the security of people and institutions of the Federative Republic of Brazil. In the field of counterintelligence, adverse actions perpetrated by organizations and individuals that employ specialized techniques (adverse intelligence), such as recruitment, entry, deception, disinformation and propaganda, among others, are objects of monitoring and analysis. Other adverse actions, perpetrated by actors without the use of specialized intelligence techniques, are monitored and analyzed by the intelligence branch. Therefore, the threats dealt with by counterintelligence are always antagonisms and not mere obstacles.

Thus, the main function of counterintelligence is to face a threat posed by the existence of adverse intelligence actions, whether sponsored by a foreign national state or by some non-state entity. It is understood that the opposition to adverse intelligence activities, which use specialized techniques, is more effective if carried out by those who master such techniques, that is, by other intelligence professionals. That is why counterintelligence is a key function of intelligence bodies and fractions in almost every country.

In addition to the distinction between the branches of intelligence and counterintelligence, it is important to split intelligence activity into two functions: analysis and operations. In this case, intelligence professionals can be more or less specialized in each of the two functions, but the synergy between analysis and operations, with their own techniques and work methods, is a condition for the efficiency and effectiveness of intelligence fractions and bodies. These two fields are also critical for the legitimacy and efficiency in carrying out their functions. In different countries and organizations, analysis and operations functions may be assigned to specialized teams or even to different organizations. The important thing here is to recognize and highlight the requirements of each of these functions.

The analysis function is responsible for producing intelligence knowledge. Its main function is to inform. To this end, professionals linked to this function collect and gather inputs, process them, analyze them, produce knowledge in the form of reports and other products, which are disseminated to the competent authorities by the management of intelligence organizations. The inputs for analysis are made up of data, information and knowledge relevant to understanding the object being analyzed. Most of the inputs processed by intelligence activities are available and can be accessed without the use of confidential specialized techniques. However, it may be necessary to obtain an input that is not available, which will be done by the operations function, after a request sent in by the analysis function.

The operations function is responsible for carrying out confidential specialized actions to meet previously established objectives. Its main function is to execute. These actions are aimed at obtaining unavailable inputs, counteracting adverse actions and creating situations favorable to national interests. It is through operational actions that intelligence activity acts in the world. They are a way of getting around obstacles in order to achieve objectives determined by States in conflictive and adverse contexts.

It is important to reiterate that the characterization of intelligence activity as being made up by two branches (intelligence and counterintelligence) and two functions (analytical and operational) does not mean that all intelligence organizations in the world need

or can carry out such activity in their entirety. But, in fact, such characterization is a legitimate state function and, in the Brazilian case, legally ordered, which is part of the modern evolution of the international system and contemporary States.

Obtaining data and information to help a decision maker determine the best course of action is a very old activity. However, for a long time its use was sporadic, responding to situations of open conflict, that is, in which there was a clear relationship of adversity. Thus, military commanders sought to know the capabilities of their adversaries in advance to better prepare for battle. Likewise, heads of political units in economic competition sought to estimate the situation of their opponents to better position themselves in the dispute, acquiring competitive advantages over their competitors.

There were, however, no permanent structures and/or structures dedicated exclusively to obtaining data and information, specialized in providing information for government decisions. This situation first changed in the 19th century, when the development of intelligence activity became clearer in the armed forces, chancelleries and police and security bodies in different countries. From the mid-20th century onwards, the context of the Cold War and Afro-Asian decolonization increased the number of States in the international system and the technological, economic, political and cultural conditions in which such intelligence services developed. Since the 1990s, with the globalization of the international economic and legal system, driven by digital transformation, national intelligence systems have become more complex.

Countries today usually have an intelligence community, which may or may not be articulated, totally or partially, in a system. This community is made up of intelligence services, characteristic fractions of its three roots (military, diplomatic and police), but also of other units specialized in topics as diverse as environmental issues or finance, whose role in the activity was described later.

In Brazil, the National Information Service (SNI), established in 1964 in the context of the Military Dictatorship (1964-1985), was extinguished in 1990. In the early 1990s, intelligence activity in direct support of the Presidency of the Republic was carried out by intelli-

gence units of the Secretariat for Strategic Affairs (SAE). In 1994, an Intelligence Secretariat of the Presidency of the Republic was created, when the first public exam was held to provide civil servants for the body, as recommended by the 1988 Federal Constitution.

In December 1999, after deliberation by the National Congress, Law No. 9883/1999 was sanctioned by the President of the Republic, creating ABIN and Sisbin. The same law determined the creation of an Intelligence Activity Oversight Committee (IAOC) by the National Congress, which was to be permanent and formed by federal representatives and senators. Since then, Sisbin has been developing institutionally within a democratic and constitutional framework, although subject to crises and requiring permanent improvement.

2.2. Democracy

The state in Brazil is made up of three separate and mutually necessary power branches: the Executive, the Legislative and the Judiciary. Brazil's intelligence agencies are usually located in the Executive Branch, as is the case with ABIN, which is linked to the President's Office of the Chief of Staff, and the other bodies and units that make up Sisbin.

The post of Director General of ABIN is a special position, for which the person appointed by the President of the Republic must have his name approved by the IAOC of the National Congress and by the plenary of the Federal Senate.

The 1988 Federal Constitution defined Brazil as a democratic state governed by the legal rule, made up of three independent and harmonious powers. As such, the people have the power to define the direction of the country through voting and other forms of popular participation. The fundamental freedoms of citizens are guaranteed, as well as the impersonal nature of decisions and the exercise of public functions by elected public agents, civil servants and public employees, as well as the military. Everyone is equally obliged to follow the Constitution and laws. In 2021, Law No. 14,197/2021 added Title XII to the Brazilian Penal Code, repealing the National Security

Law (1983) and defining crimes against the Democratic Rule of Law. The preservation of democracy is a fundamental clause of the Federal Constitution.

In Brazil, the President of the Republic is both head of state and head of government. It is up to the intelligence activity to advise successive rulers, without being confused with them, always acting in accordance with legal designs and aiming to fulfill the objectives defined by the Constitution. In other words, it is up to intelligence to support the decision-making process within the Executive Branch in order to preserve national sovereignty, defend law and order and guarantee the dignity of the human person, as set out in Decree 11.693/2023.

Democratically elected governments exercise a power that emanates from the sovereign will of the population, through periodic, free, safe and secure elections. Intelligence, when advising successive governments, deals with issues related to national defense, foreign relations and public security, but always oriented towards promoting the development of the entire national population. This totality of people affected by the law in the national territory must be reached through the implementation of public policy obligations that reflect and preserve their dignity. Public policies are defined on the basis of stipulated goals for public action, selected by voters through the ballot, and translated into government priorities. One of the main expressions of this decision-making process is consolidated in the Multi-Year Plan (MYP), which, in line with the provisions of §1 of art. 165 of the Federal Constitution, must contain guidelines, objectives and targets defined with the aim of "enabling the implementation and management of public policies, guiding the definition of priorities and helping to promote sustainable development". Once drawn up, the Multi-Year Plan must be submitted to the National Congress for examination and approval.

Together, the objectives set out in the Constitution, the government guidelines and the MYP provide a solid basis for the periodic updating of the National Intelligence Policy (NIP), the National Intelligence Strategy (NIS) and the National Intelligence Plan (NIP), the main sectoral instruments for guiding the actions of ABIN and Sisbin.

In democratic regimes, however, oversight of public administration is fundamental for the realization of citizens' rights and for the proper functioning of the state machine. As a state function, intelligence activity needs to be controlled to ensure that it remains lawful, analytically sound and serves society and the legal norm. Due to its partially secretive nature, it is necessary to adopt specific oversight mechanisms, in addition to ordinary methods, both internal and external to the executive branch.

In the case of ABIN, there are internal controls for the executive branch of supervision, ombudsman, internal affairs and auditing. Ordinary internal control is carried out by the Comptroller General of the Union (CGU). In the specific case of ABIN, this control is also exercised by the Secretariat for Internal Control of the Presidency of the Republic (CISET/PR). The Public Integrity System of the Federal Executive Branch (SIPEF), including the Ethics Commission of the Presidency and Vice-Presidency of the Republic (CEPR), also makes up this branch of internal control of the Executive Branch. Specific laws, such as the General Data Protection Act (LGPD) and the Access to Information Act (LAI), reinforce the transparency and legitimacy mechanisms of intelligence activity.

External control is exercised by the Federal Court of Auditors (TCU), the Judiciary, especially the Federal Supreme Court (STF), and the National Congress IAOC. The IAOC has broad powers defined by Resolution No. 2 of 2013, which added the Committee's rules to the Common Rules of Procedure of the National Congress. According to the resolution, the IAOC is responsible for the external oversight and control of the intelligence and counterintelligence branches, as well as of the analysis and operations functions, developed in Brazil or abroad, by any bodies and entities of the Federal Public Administration, direct or indirect, especially by the components of Sisbin. This Committee may require each Sisbin body or entity to submit partial, general and extraordinary reports. In addition, the IAOC is empowered to carry out inspections in areas and facilities of the bodies that make up Sisbin, with the right to access documents and files.

Oversight of the National Intelligence Policy (NIP) and ABIN's actions is carried out by the President of the Republic, the Office of

the Chief of Staff and the Chamber of Foreign Affairs and National Defense (CREDEN) of the Government Council. Within the scope of Sisbin, ABIN is responsible for coordinating and facilitating the activities developed in accordance with NIP.

Oversight and control of ABIN's intelligence activity are facilitated by the existence of regulations such as a Code of Ethics, an Intelligence Doctrine, Procedural Manuals and Normative Instructions. On the one hand, these documents help to coordinate the actions of the fractions that produce intelligence knowledge and external communication, and, on the other hand, they guide the training of intelligence professionals working both in analysis and in operations.

Before stating the ethical and moral foundations of intelligence activity, it is important to introduce an additional distinction between the intelligence community and the intelligence system, so that the specific scope in which ABIN's activities are carried out is clear.

2.3. Organization

Intelligence activity, as understood in this doctrine, is carried out by intelligence bodies. It is worth reiterating that these organizations can be classified as intelligence services when their purpose is to carry out intelligence activities, or as intelligence fractions, when they are part of bodies that have other purposes.

The set of intelligence organizations in a country constitutes its intelligence community. The use of the term community here denotes the informal and factual nature of the interactions that may exist in such a community. When the intelligence community of a state, a functional subset or a country is subject, totally or partially, to formal and institutionalized regulations that govern their interaction, an intelligence system comes into being. It is worth noting that the community can be broader and more informal than a system. Several countries do not create an intelligence system, allowing coordination between members to take place in accordance with local customs.

In Brazil, federal intelligence agencies are organized in their own legally defined system, Sisbin. There are also sectoral subsystems, such as the Defense Intelligence System (SINDE), regulated by a Normative Ordinance of the Ministry of Defense, or the Public Security Intelligence Subsystem (SISP), regulated by a Federal Decree. The important thing is to note that the country's intelligence community is larger than Sisbin, also including state and municipal institutions, other powers of the Republic and private entities of interest to the activity. In this sense, Decree 11,693/2023, which regulates Sisbin, constituted a relevant change in that it established categories, criteria and collective goals for the institutionalization of the System.

Furthermore, ABIN and other Sisbin bodies are part of a factual reality, which can be called the international intelligence community. Levels of bilateral or multilateral cooperation reach different degrees of institutionalization, depending on bonds of trust and established international agreements. Such cooperation takes place on topics of mutual interest and involves the exchange of data, information and knowledge, meetings and the holding of training events for intelligence professionals. Brazil is part of this community through its intelligence attachés, established with the aim of supporting the work of Brazilian diplomacy and promoting exchanges with the countries in which they are accredited, and through their participation in various multilateral groups and forums.

In 2023, with the issuance of decree nº 11.693/2023, there was a structural reorganization at Sisbin. This reorganization had four pillars. Firstly, strengthening ABIN's role as facilitator and coordinator of Sisbin by appointing it as the central body of the system. Secondly, the repositioning of the Consultative Council, making it a high-level consultative structure formed by Ministers of State. Thirdly, the classification of bodies into categories (permanent, dedicated, associated and federated). Finally, the fourth pillar was the definition of criteria and procedures for the effective inclusion of Federation units into Sisbin. As of the decree, the creation of subsystems also becomes the responsibility of the central body, in order to organize sectoral intelligence integration initiatives, such as, for example, in fiscal, financial and tax cases.

ABIN's facilitating role as Sisbin's central body is expressed in the competencies set out in art. 10 of decree 11.693, such as "promoting cooperation between Sisbin member bodies and entities and integrating their intelligence activities", or "coordinating temporary or permanent integrated actions by Sisbin member bodies and entities", or, above all, "consolidating the specific knowledge needs informed by the bodies in their work plans".

The Advisory Council was reformulated by Decree 11.693 to clarify its role and the high level of its members and the issues it addresses. It will be up to the Advisory Council, for example, to propose updates to the NIP and analyze the management reports of the system's bodies. The Council is composed of the Chief of Staff of the Presidency of the Republic (who will preside over it), the Institutional Security Office of the Presidency of the Republic, the Ministry of Justice and Public Security (MJSP), the Ministry of Foreign Affairs (MRE) and the Ministry of Defense, in addition to the Director General of ABIN.

The classification of bodies into categories promotes greater organization to the System, adjusting expectations for member participation, according to the characteristics of their category. Decree 11.693, in its art. 7th, §1st, named the permanent bodies of Sisbin, representatives of the main expressions of the Brazilian State, namely: foreign relations, external defense and internal security. Such components were already provided for in art. 2 of Law No. 9,883/1999, but there was also the addition of the expression governability, represented by the Office of the Chief of Staff of the Presidency of the Republic and the Institutional Security Cabinet (GSI). Permanent bodies therefore express essential functions of State power (external defense, internal security and foreign relations), in addition to governability, treated from the perspective of reducing vulnerabilities and providing security for people and institutions.

The bodies deemed dedicated in Decree No. 11,693 are those that have units (fractions) dedicated to intelligence, that is, they are bodies with a consolidated intelligence culture and improved security standards. Furthermore, in their role, they need to work on strategic issues related to the National Intelligence Policy.

Bodies that do not have units dedicated to intelligence activities, but that work on topics related to the National Intelligence Policy (NIP), will be able to join Sisbin as members. Entry into the dedicated or associated categories depends on the entry procedure provided for in Ordinance No. 925, of September 6, 2023, of the General Director of ABIN.

This procedure involves evaluating applicants against the following criteria: function, data sensitivity, security standard, and available resources. The highest level of service will correspond to the dedicated category and the intermediate level will correspond to the associate category. This will promote professionalism and security at Sisbin. Decree No. 11.693 and Ordinance No. 925 allow the incorporation of state and municipal bodies as federated entities into Sisbin, generating greater legal security for the cooperation that ABIN and other Sisbin bodies may develop with such bodies and federated fractions.

In the new configuration established, ABIN now has greater capacity to collaborate with Intelligence work developed in common agreement with partners, for the purposes of superior advice and accountability to the IAOC. Consisbin also contributes as a body whose opinion is considered in the appraisal of Sisbin's management report. In turn, it becomes the obligation of the central body, as stated in art. 10, XI of Decree No. 11.693, "to provide tools for secure communication and digital platforms to support the sharing of Sisbin data, information and knowledge". This measure will provide greater security in document traffic, improving the traceability of what is produced and exchanged in the System. Ultimately, this obligation reinforces ABIN's commitment to improving management and control instruments.

Democratic institutions, sovereignty and national interests need an agile, coordinated, competent and legitimized intelligence system, capable of neutralizing threats and identifying opportunities. In this sense, Sisbin's new operating model reinforces the need for ethical principles and common guiding values for all intelligence professionals both at ABIN and within Sisbin.

2.4. Ethics

Ethical behavior is an essential work component in intelligence activities. It is through ethical behavior that specific internal social control is carried out, that is, that which is exercised by intelligence professionals themselves, for reasons of conscience, over their action. Intelligence professionals are, first and foremost, people, Brazilian citizens and members of the people they serve. Their ethics are professional, as part of public administration, but they are also personal.

The distinction between right and wrong lies at the heart of the definition of ethical behavior. In their personal life, each citizen is able to attribute relative value to both concepts, depending on their family and cultural background. In their professional life, public servants already find these values defined in a more constant way, within the legal framework that defines their activities. Right refers to respect for current norms and wrong refers to their violation. Thus, in the professional sphere, the ethical procedure is a way of respecting the legal, constitutional and infra-constitutional order and jurisprudence; of avoiding personal costs, for oneself, for others and for the people; and of preventing political losses for the government and the State.

Furthermore, public servants have a responsibility for the well-being of society. This orientation serves to qualify even more acutely the concern not only with respect for standards, but also for their scope and their possible impact on the proper functioning of the current social organization. It is in the ethical instance that the people cease to be a piece of rhetoric, an icon to invoke legitimacy, and become the reference that ensures the constitutionality of a decision. Thus, government action is legitimized by the ethical sustainability of its purpose. Constant care for the public good adds, to the server's work, an additional layer of attention to ethical issues that are not necessarily present in the daily lives of ordinary citizens.

Even more strikingly, an intelligence professional is involved in a third layer of ethical concern. Due to their specialized work, the need for secrecy that involves the production of knowledge and the permanent possibility of access to sensitive data, professionals must

be able to make ethical choices that go beyond the simple distinction between right and wrong and that go beyond concern for the public good and the well-being of society.

An ethical conduct also represents the defense of an intelligence professional's own dignity, with a view to promoting the correct performance of this activity. The discretion and restraint that favor the activity are traits of conduct that must be considered in order to achieve the confidentiality that characterizes it. Given that work in intelligence activities constitutes a profession, it must be considered that professionalism in this category implies a sense of collective responsibility associated with high standards of technical competence and a commitment to meeting social interests. Therefore, it must be of great interest to the activity not to be an object or means of political and economic exploitation.

Responsible treatment of ethical issues in intelligence activity implies recognizing that its product is directed to the State and only for democratically legitimized purposes. These purposes aim to support state institutions in the formulation and exercise of policies, programs and operations aimed at achieving national objectives, taking into account the benefits generated for the people. In this way, intelligence activity is committed to providing satisfaction for its actions to itself and others and to acting in the most competent way possible. As it involves moral choices and deliberations, its exercise is necessarily susceptible to ethical examination.

In order to deal with the ethics of intelligence activity, three sources capable of guiding intelligence employees as members of a specific professional category are highlighted, namely: the code of professional ethics, the principles of intelligence activity contained in this Doctrine and the academic literature on the topic.

Specifically regarding the analysis function, the main aspect of ethics to observe is the duty to represent the truth, even when this representation is inconvenient for the user of the intelligence product. To achieve veracity, this professional must also respect the methodology of producing intelligence knowledge, striving to prevent precipitation and assumptions that would lead to the distortion of reality. An intelligence analyst is also expected to be professional and to adopt

appropriate security measures when dealing with inputs and knowledge produced, respecting the secrecy and discretion inherent to their work. Although intelligence activity uses secrecy, under the terms of the law, to guarantee the preservation of the security of society and the State, its performance and that of its professionals is subject to the scrutiny of external and internal oversight bodies.

Regarding the performance of the intelligence operations function, confidential actions are carried out in the search for unavailable data, information or knowledge, or in countering threats from adverse intelligence. These characteristics give operational actions a potential that requires the public servants involved to take greater care to act ethically and legally. Every servant is responsible for their actions, which must be in accordance with current legislation and its limits: any manifestly illegal order must be rejected, not serving as a justification for inappropriate conduct.

Brazilian legislation provides for the use of intelligence operations to obtain data and detect, identify, obstruct and neutralize adverse actions. This provision, however, does not allow for indiscriminate action. In addition to the ethical principles set out in the Code of Professional Ethics for Public Servants, established by Decree 1171/1994, there are the following principles: impersonality in dealing with targets; respect for the democratic rule of law; promotion of the interests of society and the State.

Although confidential, intelligence activity must be subject to internal and external control, being as transparent as possible. Ethical conduct protects the operations function, promoting correct and dignified performance from its professionals. In this sense, operational planning and execution must observe three rules:

- Suitability: the means and techniques chosen will lead to the achievement of the objective of the confidential action.
- Indispensability: the operational means and techniques chosen are necessary alternatives to achieve the objective of the confidential action.

- Proportionality: the means and techniques chosen will be carried out to the extent strictly necessary to achieve the objective of the confidential action.

Furthermore, ethical conduct in intelligence operations must take into account some rules for the work of professionals in the field. The first rule concerns the tools and systems available to the operations function that cannot, under any circumstances or justification, be accessed for personal use or to meet requests external to the institutional missions of the intelligence organization. The second deals with data and information of a personal nature, obtained within the scope of operational work, that is not relevant to the objective of the confidential action, will not be recorded or stored by the operations function, and must be disposed of in a secure manner with respect for the privacy of their holders. Finally, all operational work must adopt checking and accountability instruments in its various stages, for better management and control of the development of its actions.

In summary, the ethical duties of an intelligence professional are: representing the truth; applying methods in the elaboration of knowledge, rejecting conclusions and any non-republican interference in the knowledge production process; promoting the country through its activities; treating business matters with discretion; consider individual dignity and collective interest as a reference for the acquisition and production of knowledge; considering, when dealing with foreigners, the principle of reciprocity and human rights; and critically reflecting on the need for and moral implications of their actions and decisions.

These ethical duties prevent an intelligence professional from transforming knowledge into power, which is the user's prerogative and his alone. From an ethical perspective, intelligence activity does not act in consideration of society and the State – two relatively abstract and impersonal entities –, but in consideration of the people, the population, the people, as recipients of constitutional and democratic obligations. This attention is the main decision-making and technical resource for intelligence activities to avoid political bias and participate in the building of a better country.

2.5. Principles

Intelligence activity is governed by basic rules of conduct, compliance with which is essential so that it can be carried out appropriately and effectively. Such standards are divided into general principles, which cover the activity as a whole, and sectoral principles, which especially affect one of its constituent elements.

The general principles of intelligence activity are: Control, Cooperation, Objectivity, Opportunity, Traceability, Security, Simplicity and Usefulness.

The principle of control determines that all intelligence activity actions must be subject to oversight, which must guarantee the conformity of its means and the correct purpose of its application. When applied to the analysis function, the principle of control ensures the quality standard of intelligence knowledge, by establishing instances of validation between peers and by management of both the results of the methodology steps and the product. When applied to the operations function, the principle of control determines that the outlined actions are coordinated to avoid compromise and dispersion of efforts. Parallel and uncoordinated actions can cause work to be redone or hinder the achievement of its objectives. In this sense, there is a need for a body to control the actions undertaken, a body that is capable of centralizing efforts and results, thus guaranteeing the effectiveness of actions carried out by the operations function.

The principle of cooperation prescribes that intelligence activities be carried out collaboratively. When applied to the analysis function, the principle of cooperation encourages analysis to be done in teams and the optimization of efforts, in a collaborative manner, sharing inputs whenever necessary, with a view to production objectives and mitigation of biases. When applied to the operations function, the principle of cooperation establishes and enhances exchanges that make it possible to optimize efforts to achieve the objectives outlined for each action to be carried out.

The principle of objectivity prescribes that intelligence professionals act towards clear and delimited objectives, avoiding unneces-

sary efforts and waste of resources. When applied to an analysis function, the principle of objectivity requires that the objects of analytical monitoring be previously defined and outlined. When applied to the operations function, the principle of objectivity indicates that the objective of operational actions is clear and well defined, in order to facilitate planning, and the correct application of available resources, thus reducing costs and efforts.

The principle of opportunity determines that the work carried out by intelligence professionals present results within an appropriate period of time, so that it can be used effectively. When applied to an analysis function, the principle of opportunity indicates that analysis and production efforts are adequate for the necessary time, so that they can be useful to the user of intelligence knowledge. When applied to the operations function, it requires that the results of operational actions be disseminated in a timely manner for use.

The principle of traceability stipulates that the actions carried out in intelligence activities be recorded, to ensure that they can be audited in accordance with previously and formally defined mechanisms and instruments. When applied to the analysis function, the principle of traceability determines that control be maintained over production procedures and inputs, from the step of obtaining data, information or knowledge, to the product, in order to ensure that the process of preparing intelligence knowledge is verifiable, validatable and auditable. When applied to the operations function, the traceability principle requires that the planning and execution of operational actions be duly recorded and controlled, to ensure that the process carried out can be verified.

The principle of security imposes the adoption of safeguard measures appropriate to each situation, aiming to ensure that the knowledge produced and actions carried out are duly protected. When applied to the analysis function, the security principle recommends that such measures be implemented in order to guarantee the correct classification of data, information, knowledge and intelligence obtained, processed and disseminated by the intelligence activity, in addition to protecting them from harmful exposure to society and the State. When applied to the operations function, the principle of

security determines that the planning and execution of confidential actions ensure the security of the intelligence agency, the team involved in carrying them out and the action itself.

The principle of simplicity establishes that the actions carried out by the intelligence activity be planned and executed in order to avoid unnecessary complexity, costs and risks. When applied to the analysis function, the principle of simplicity indicates that the process of producing knowledge should focus on simple gathering, processing and dissemination measures, resulting in clear and accessible intelligence. When applied to the operations function, the principle of simplicity presupposes optimization of resources and reduction of operational efforts that do not add value to the desired result, reducing time, costs and risks. This implies that efforts should be directed in a combined way, from the simplest to the most complex, from the most economical to the most expensive and from the safest to the riskiest, taking into account the complexity of the operational environment and the importance attached to the expected results.

The principle of usefulness stipulates that the actions of the intelligence activity should be based on the needs of those who will use it, thus providing a potentially useful product. When applied to the analysis function, the principle of usefulness indicates that the themes, sections and approaches made during the knowledge production process consider the intended use of intelligence knowledge. When applied to the operations function, the outlined action, its objective and its execution consider the usefulness that the result will have for those who will receive it, process it and act based on it.

In addition to these general principles, each constituent function of intelligence activity has principles that guide their practices.

The analysis function must develop its actions guided by the general principles of intelligence activity, as well as by the group of principles typical of the analytical profession: scope, impartiality and critical thinking.

The principle of scope establishes that the objects of the analysis should be approached with the necessary scope to elucidate the proposed subject as fully as possible. The aim should be to exhaust

the possibilities of gathering information on the objects and their possible repercussions for the country's conduct, in order to guarantee a consistent basis for decision-making.

The principle of impartiality determines that the objects of analysis should be approached impartially, in order to prevent value judgments which may arise from interests, personal convictions or preconceived ideas from distorting the results of production.

The principle of critical thinking requires an analyst to maintain high criticality regarding their own understanding of reality. In order to mitigate the incidence of biases and heuristics in the process of generating intelligence knowledge, organizations must invest in initiatives to understand these phenomena and tools to control their effects.

The operations function must carry out its actions guided by the general principles of intelligence activity, as well as by the group of principles specific to the operational role: adaptability, availability, purpose, integration and resilience.

The principle of adaptability stipulates that the planning and execution of operational actions should allow for the rapid and efficient implementation of necessary adjustments and redirections. Intelligence operations are developed in potentially unstable, complex and hostile environments, whose characteristics can surprise teams in the field. Furthermore, the context in which the operation takes place may undergo unpredictable changes. The operations function must be flexible and capable of adapting its action, absorbing surprises and possible changes and adapting to new contexts.

The principle of availability determines that the operations function should be structured in such a way as to enable its immediate activation whenever necessary, with the maximum scope possible, considering the threats listed in the intelligence activity directive instruments.

The principle of purpose states that confidential actions should be carried out in support of the realization of the interests of society and the State, with the common good as its motto. These actions must serve a collective purpose, with respect to what is established in the

general legal system, the National Intelligence Policy and other regulations specific to intelligence activity.

The principle of integration recommends that the actions of the operations function be integrated, in an orderly, systematic and continuous manner. The hybrid and complex nature of threats and opportunities, points of interest in intelligence activity, requires professionals to act with total methodological synergy and joint effort. For actions to progress properly, it is necessary that they work in a collaborative, complementary, integrated and harmonious way. Furthermore, intelligence operations generally involve varied resources and the use of different techniques, at different times. Therefore, it is common for operational actions to rely on the support of teams made up of individuals with multiple capabilities and varied technical resources. The integration of resources and the multidisciplinary nature of the operational team presuppose that all the resources necessary for the fluidity of the operation have been assimilated and available to the field team.

In turn, the principle of resilience establishes that operatives – those working in the operations function – should be resistant to difficulties and frustrations, in order to be able to notice, evaluate and react quickly to adverse situations and control their performance so as not to compromise the operational actions being developed. Intelligence professionals usually deal with complex and changing contexts. In the field, this situation requests balanced responses and control actions.

2.6. Values

The actions developed by the intelligence activity are conducted based on a set of characteristics, the promotion of which is considered essential for safe, permanent and effective action. They are:

Continuous training of intelligence professionals

The nature of intelligence activity requires that the professionals who carry it out be properly prepared through continuous learning, research and extension processes. The use of specialized techniques, whether analytical or operational, requires the continued training of professionals who work at ABIN. Therefore, it is important that these professionals periodically attend training events to remain prepared to carry out the activity. Furthermore, it is desirable that, whenever possible, experiences, good practices, possible errors and learning be continually shared among them.

Professionals in analysis need to be up to date with the topics they monitor and the tools used in this monitoring. The need to mitigate biases also requires investment in the study of diverse disciplines in the field of Cognitive Psychology – such as perception, emotion, thought and consciousness – and Linguistics – such as language, discourse analysis and semantics. Furthermore, it is essential that these professionals be continually encouraged to develop creativity, reflective criticality and the ability to keep an open mind when faced with new perspectives on old subjects.

Operatives need to be prepared to apply specialized techniques in a hostile environment, a situation that poses risks to the intelligence agency and the people responsible for executing its actions. Therefore, technical qualification for agents in the operations function is essential for their good performance. Therefore, the operations function must encourage a systematic development of professionals and an exchange of experiences between teams.

Reliability When It Comes to Security

The safety management system adopted by an institution must be effective and reliable. Reliability when it comes to security is an essential factor in building an institution's reputation, favoring interaction with other intelligence bodies and deterring possible adverse actions.

Deterrence is an institution's ability to deter its opponent from attempting to take an adverse action. It is important that the institution be able to persuade its opponent that the risks or costs arising from implementing such an action would be greater than the benefits arising from it. It is important that the institution's opponents realize that security levels have been increased and that actions taken may pose risks to its agents, as well as to the image of their sponsor.

In addition to being a deterrent to the adversary, having highly reliable security measures favors cooperation and interaction between intelligence agencies, which, in turn, increases the data available for monitoring their objects, generating more effective countermeasures and opportunity assessment.

Critical thinking

An intelligence professional is interested in becoming aware of the mental model that compromises his impartial judgement. Critical thinking is a way of thinking in which the thinking subject constantly questions the act of thinking itself while thinking. With this, he improves his mental pattern and deepens his reflective ability, which allows him to increase the quality of the response resulting from rational effort. Therefore, thinking critically corresponds to the cognitive process of thinking driven by the conscious work of thinking about thinking.

Critical thinking can be learned and reinforced through repetition. In addition to becoming aware of one's own presumptions and motivations, another resource for strengthening criticality is training in intellectual accuracy techniques. After each judgment made, an intelligence professional must ask himself about its clarity and precision. He must also take into account whether the scope in which it was considered and the depth with which it was treated make this judgment relevant. The result of mental work must also be logical for the interlocutor, meaningful for the activity and useful for the user. This evaluation circuit is not followed in isolation, but submitted to other professionals trained to detect flaws in reasoning and logical inconsistencies.

Alongside institutional measures, an intelligence professional dedicated to analysis must also strive for constant improvement that favors the mitigation of the effects of biases on the results of their work. This includes the development of continuous actions of self-knowledge and the adoption of an unpretentious, collaborative, curious attitude focused on constant learning. Therefore, an analyst should understand their own thinking model and question their own degree of impartiality. This entails becoming aware of how one's work is influenced by one's personal history, one's peculiarities and political and ideological tendencies; and how one's social condition, educational background and professional development impact the construction of their worldview and perception of reality.

Results Orientation

The actions carried out by intelligence activity are directed towards clear objectives and pre-determined by a competent authority. In its two functions, informing and executing, its professionals act to advise the national decision-making process and assist the country in achieving national interests. Therefore, this activity is carried out with a view to achieving results.

The execution of analytical actions must always be guided by the State's objectives, seeking to adapt the monitored object, its scope and its approach to national interests. What guides an analytical action is its potential usefulness in achieving the State's objectives. Analytical efforts must consider the relevance of a topic and the opportunity to disseminate knowledge, in order to guarantee the usefulness of its product.

The execution of operational actions must be guided by the adequacy between the requests received, objectives, available resources, risks involved, characteristics of the target, operational environment and ethical and legal considerations. What guides an operational action are the principles of efficacy, effectiveness, efficiency and legitimacy of public administration acts.

Active Transparency

Brazil is a Democratic State based on the rule of law, and as such is governed by respect for laws, individual freedoms and rights and the popular will. One of the rights to be observed is the right to access information, from which derives the Access to Information Law, Law 12527, dated November 18, 2011, and which constitutes a fundamental element for government transparency. Transparency in public management is a relevant factor in the conduct of the State, as it allows society to know what is being done, facilitates the evaluation of the administration by the population, and ensures the oversight of its activities by the competent bodies. There are, however, exceptions to the right to access information. Personal data held by the State, for example, cannot be accessed by third parties. Certain legal proceedings, due to the nature of their object, are carried out in secret, etc.

Intelligence activity deals with issues related to defense and security. It operates in competitive environments, open or covert, between Brazil and other actors in the international arena. For this reason, it is important that the planning and execution of your actions be covered in secrecy. Its use occurs precisely on occasions when it is necessary to seek difficult-to-access information that guarantees the State and the society competitive advantages in achieving their interests. If these actions are previously disclosed, or if they are open to consultation by anyone, including opponents, the competitive advantage ceases to exist.

The confidential nature of intelligence activity, however, does not exempt it from establishing frank, open and constant dialogue with the society it serves. Whenever possible, it must inform society about its actions in a safe way. In this sense, it is essential that its bodies proactively make information of public interest available, the disclosing of which should pose little harm to the conducting of their activities.

Having defined the foundations of intelligence activity as it should be practiced by ABIN, it is important to specify the doctrinal understandings about the branches of intelligence and counterintelligence, as well as the analysis and operations functions.

3

The Intelligence Branch

3. The Intelligence Branch

Intelligence is the branch of intelligence activity that focuses on its informational function. Its professionals are responsible for obtaining, processing and disseminating data, information and knowledge relating to facts, events, situations or phenomena that constitute or indicate opportunities and threats to the fundamental objectives of the State. Its scope of production encompasses events that occur inside and outside the national territory, with immediate or potential influence on the decision-making process and government action. The main purpose of this branch is to advise the State in achieving and protecting national objectives and providing elements that offer decision-making advantages to the ruler, observing the principles that govern the Democratic Rule of Law and Brazil's international relations.

3.1. Classification

The production of knowledge in the intelligence branch can be grouped by purpose, time frame or nature of the data gathered. These classifications serve to better understand the nature of the work to be carried out and, thus, optimize the performance of intelligence, helping to generate niches of specialization among its professionals.

Classification by purpose

Classification by purpose differentiates intelligence products according to their scope and intended use. In this sense, knowledge can support decision-making in the design of a public policy (Strategic Intelligence), in the actions proposed for its achievement (Tactical Intelligence), in the operationalization of these actions (Operational Intelligence). It can even form the basis for understanding the framework that gives rise to the adoption of such a policy (Basic Intelligence). Each of these instances requires its own approach to assist in the production of useful knowledge for the user, providing assistance to the decision-making process.

Basic Intelligence aims to build a set of foundations and references for understanding and contextualizing the topics it covers, serving as a subsidy for other analyses with a sharper focus. It results from the ordinary thematic monitoring carried out by intelligence professionals. The user of this product is generally internal to the intelligence activity and will use it to produce subsequent knowledge.

The knowledge produced in Basic Intelligence aims to understand facts, events, situations, actors, relationships and statistical data that characterize the object of study. To develop basic knowledge, a professional considers the historical development of the topic analyzed and the actors related to it, and raises data and information relevant to understanding the topic and the basis for inferences and subsequent analyses.

The product resulting from Basic Intelligence is narrative-descriptive or interpretative knowledge, in which events and situations of interest to the user are reported, allowing them to understand the context of a given topic. Occasionally, this product may be disseminated to users outside the organization to give them some context on the topic or object.

Examples of Basic Intelligence include explanations about the domestic politics of countries and their institutions, economic statistics and studies on the historical development of actors of interest to society and the State.

Strategic Intelligence analyzes and interprets phenomena that may impact the State's fundamental objectives and interests. This intelligence seeks to highlight trends and scenarios that may indicate threats and opportunities for the Brazilian society and the State, advising decision-making on public policies in the topics covered.

Strategic Intelligence monitors the dynamics and variables related to the phenomena of interest, carrying out research aimed at understanding them. Its professionals must have a consolidated understanding of the topics being monitored and be able to analyze data, information and knowledge, to validate, interpret and contextualize them.

The product resulting from Strategic Intelligence is interpretative or prospective knowledge about a phenomenon of interest to society and the State. Examples of Strategic Intelligence are short-term projections about the political and economic situation of other countries and their impact on Brazil; monitoring transnational phenomena, such as the actions of criminal organizations, extremist groups and cyber actors in the form of Advanced Persistent Threats (APTs); and the analyses of recurring social demands.

Tactical Intelligence gathers data, information and knowledge in support of the development of previously defined government policies. The knowledge resulting from this intelligence is used to advise on decisions relating to the implementation of public policies, seeking to assist State intervention. It is the result obtained from monitoring specific situations and actors.

Through Tactical Intelligence, the actors and variables related to the situation of the object of study are observed by carrying out research aimed at understanding them. Just like in Strategic Intelligence, its professionals must have a consolidated understanding of the topic being monitored, be able to integrate and interpret recent significant information and contextualize it in order to understand and explain the situation studied.

The product resulting from Tactical Intelligence is narrative-descriptive, interpretative or prospective knowledge about a situation of interest to society and the State. This product should be useful in advising decision-making on a specific case or within the scope of a previously determined policy.

Examples of Tactical Intelligence are analyses of the feasibility of executing a given public policy and its likely challenges; survey of the position of specific countries on the adoption or support of a specific international policy of interest to Brazil; identification of groups responsible for cyberattacks; and analysis of actions that can promote national development in Brazil and abroad.

Operational Intelligence offers contextualization for a specific State action, in support of the execution of actions already defined within the scope of a given public policy. In this sense, it advises the

operationalization of this action. It results from monitoring ongoing facts and events, with an emphasis on obtaining data to support previously established State actions. To this end, Operational Intelligence needs to know the action plans to be supported and understand the context in which the State will act.

The product resulting from Operational Intelligence is narrative-descriptive or interpretative in nature, seeking to facilitate decisions involving the use of human and logistical resources in a given action. This product is not developed for senior government management, but for those responsible for carrying out outlined actions.

Examples of Operational Intelligence include preliminary trips to deal with the security of the head of state and other authorities on official visits; actions to support the clearing of indigenous lands and intelligence-led policing; and technical indicators of ongoing cyberattacks.

Classification by time frame

Classification by time frame differentiates intelligence products according to the chronological distance that the product has in relation to its object. It concerns the timeliness of the knowledge to be developed, with attention to the appropriate deadline for its use, and the degree of anticipation expected of it. In this sense, knowledge can aim to develop scenarios in the distant future, helping to determine long-term policies; it can relate to short-term developments in current situations; it can involve monitoring ongoing events and anticipating situations that will require state intervention. Each of these categories requires its own approach, to assist in the production of useful knowledge for the user, assisting in the decision-making process.

Alert Intelligence aims to anticipate events that may impact the achievement of constitutional objectives, national order or the security of society and the State. It is based on diagnosis and prediction and results obtained from the monitoring of threats, adversaries, hostile actors, antagonisms or obstacles that oppose the fundamental objectives of the State, in order to inform state action. The purpose

of this intelligence is to give decision makers time to avoid threats or mitigate their effects. To this end, antagonistic actors, their histories, intentions, motivations and means are considered, which must be mapped out and permanently monitored.

The product resulting from Alert Intelligence is the issuance of a warning which contains the evidence - followed by appropriate representations - that led to the alert, as well as the description of the anticipated threat and the likelihood of it taking place.

Examples of Alert Intelligence include alarms about health, economic or political situations, and about imminent conflicts that could have an impact on society and the State, both in Brazil and abroad. Alert Intelligence can also be used to anticipate adverse situations in the context of the deployment of Brazilian forces in peacekeeping operations.

Current Intelligence aims to keep decision-making authorities continuously updated on events and situations in progress and their development. It is objective in nature, with a descriptive and interpretative focus, and focuses on relevant facts and actors involved in the process being monitored and how it unfolds. To this end, Current Intelligence considers all previous production on the situation being monitored, seeking to understand the actors and variables involved, and how the interaction between them takes place.

The product of this intelligence is short, direct and periodic descriptive knowledge, in which the evolution of a situation or event is reported and, if possible, interpretative knowledge, showing how the situation is likely to unfold in the short term. Examples of Current Intelligence are the monitoring of demonstrations and strikes with disruptive potential to the national order; information about illegal access to strategic infrastructure computing networks; monitoring emergencies and monitoring economic and environmental crises, whether they occur in Brazil or abroad.

Explanatory Intelligence aims to continuously advise the national decision-making process on facts, events, situations and phenomena that may represent threats or opportunities to the achievement of the State's fundamental objectives. It results from

constant monitoring of themes and objects of interest to society and the State. To this end, Explanatory Intelligence brings together data, information and knowledge about such topics and objects, contrasts them with other knowledge and makes brief projections about their developments.

The product resulting from this intelligence is concise descriptive or interpretative knowledge, in which its object is explained and keys are offered to predict its evolution. Examples of Explanatory Intelligence are explanations about phenomena of interest to society and the State, such as social dynamics, the actions of extremist groups, cyberattacks against critical infrastructure, interaction of actors in the international arena and prognoses for the near future.

Prospective Intelligence aims to offer scenarios about the future to advise on the direction of state action. To this end, it has a diagnostic and prognostic nature and must highlight the variables and actors that influence the phenomenon under analysis and infer its progress over a stipulated period, as well as the mode of interaction between these variables and actors. Ideally, it will indicate the most likely developments of the phenomenon in question.

The product resulting from Prospective Intelligence is interpretative-prospective knowledge, used to advise the decision-making process on future events, resulting from the systematized study of the elements affecting the trajectory of the object, with its peculiarities and values, aiming to reduce uncertainties and guide towards a better decision about the future. Examples of Prospective Intelligence are studies that anticipate the development of transnational situations, possible profit or loss on investments in foreign countries, the relevance of signing international agreements and actions of national groups in the long term.

Classification by data origin

Classification by data origin differentiates the production of knowledge on the basis of the characteristics of the sources from which the data comes. There are three categories in this classification: Intelligence from Human Sources, Intelligence from Technical

Sources and Intelligence from Open Sources. These categories and their subcategories are designated by acronyms derived from their English names. Ideally, these different types complement and validate each other.

The main characteristic of each category below is related to the nature or way of generating or obtaining the data itself, which imposes different measures, needs and skills for its treatment and processing. This has implications for the planning, use, analysis and scope of the results presented, requiring specialization in the training of employees. Furthermore, it enables the establishment of specific units within the intelligence agency, with different structures for collection and analysis in each category.

Human Intelligence (Humint) is intelligence based on data obtained from people. It brings together data, information, knowledge and perceptions originating from reports made by individuals outside the intelligence agency or brought in by them. Its challenges are to deal with perception flaws and natural heuristic simplifications resulting from observations, interpretations, generalizations and interests present in people's reports.

When analyzing the inputs received, a distinction must be made between the origin of the data (source) and the sender through which the data reaches the intelligence body (channel). The further away the source is, the greater the possibility of data distortion along the way. Its correct interpretation requires the application of discourse analysis techniques and the perception of the place where the discourse is being delivered, as well as the filters through which it passes until it reaches a recipient.

Intelligence from Technical Sources (Technical Intelligence – Techint) is intelligence based on data obtained through technical means. It gathers information and data originating in the use of equipment, which requires expertise in handling. It is based on specific techniques for analyzing each type of input obtained.

This category of intelligence has the general limitations of requiring specific operating capacity of the equipment and requiring additional information related to obtaining data for contextualiza-

tion. It is made up of several types, each with its own methodologies and techniques for collecting and processing data. In a non-exhaustive type list, we have: Sigint (Signals Intelligence): Imint (Imagery Intelligence); Geoint (Geospatial Intelligence; and Masint (Measurement and Signature Intelligence).

Sigint (Signals Intelligence) is originally based on data obtained by interpreting and decoding communications and electromagnetic signals. Signals Intelligence was the name traditionally used for all collection that does not come from the use of human sources but from equipment, and is therefore not subject to human fallibilities when describing or reporting data, but rather it is subject to the technical restrictions of a device. It includes, for example, audio, video and photo recordings, made with any equipment. With the evolution of electronic equipment, it has gained relevant subdivisions. In recent decades, the term Sigint has also come to encompass intelligence produced based on data obtained in cyberspace, which is understood as the set of interconnected computing and telematics infrastructures that comprise hardware and software, data and users, and any logical relationships between them.

Imint (Imagery Intelligence), Image Intelligence, is based on data obtained through the production of photographic and multispectral images. It can range from specialization in geospatial images obtained by satellites to the evaluation of digital or analogue photos. Geoint (Geospatial Intelligence) is based on images and geolocation data obtained to describe, evaluate and visually represent physical characteristics or geographically referenced activities.

Masint, Measurement and Signature Intelligence, is based on data obtained by measuring certain types of emanations, such as seismic and thermal, generally resulting from signatures of events, such as atomic explosions. It focuses on elements, traces and patterns or signatures of measurements, such as, patterns observed on radar, sonar or measurements of radiological, biological or chemical elements. Their data are generally descriptive and do not, by themselves, allow prescription or diagnosis.

Among the subtypes of Masint is Acint, Acoustic Intelligence, which is the intelligence carried out by collecting data resulting from

acoustic signatures obtained by ships, submarines and, occasionally, aircraft flying close to the surface, such as helicopters.

Open Source Intelligence (Open Source Intelligence – Osint) is intelligence based on available data, that is, freely accessible. The term Osint acquired relevance with the advent of the Internet, but it also includes other public ways of obtaining data.

Osint is carried out by using specialized techniques for the methodical collection of available data and is supported by specific means for analyzing each type of input obtained. It uses data, information and knowledge present in inputs available to anyone, even if such access has to be paid for. It allows for the collection of a large volume of data, enabling the identification of behavior patterns. This type of intelligence has the limitations of requiring a lot of research time, as well as constant updating and mastery of collection tools.

A subcategory of Osint is Socmint (Social Media Intelligence), focused on information and data published on social media and metadata associated with them. This subtype allows for, say, the collection of a large volume of information intended for sentiment analysis, publication patterns and mass assessment of how relevant topics are.

Interaction between categories

The different types of classification presented are not exclusive. There are several possible combinations. Thus, some knowledge can be tactical, prospective and made from data and information gathered by technical means. Other knowledge can be strategic, alert and coming from human sources and images and so on.

In general, knowledge will have only one purpose and one timeframe (which can be combined in different ways), but it can contain data from different sources. Once obtained and processed, these data will be compared, analyzed and interpreted together, following the process referenced to in the part dedicated to the analysis function.

The type of document to be produced depends on the use it will serve. Sometimes, the applicant requests a document from a certain category, for a specific use at their discretion. At other times,

the intelligence professional responsible for producing a document chooses its category based on the projection of the use to be made of it, considering the role of advising the national decision-making process.

3.2. Areas of Operation

The intelligence branch follows various topics and produces knowledge about them. Some themes are limited to the domestic environment, in which knowledge users can exercise a greater degree of intervention by defining government policies and actions. Others deal with phenomena and situations that occur in the international sphere, where the State's actions depend on its interaction with other actors. Some themes have domestic and foreign implications, requesting an approach that understands these two aspects of the phenomenon. Finally, other themes are related to cyberspace, requiring action from the State in the face of threats in this environment.

Each of these types of production involves its own framing and approach, which takes into account the environment in which a decision will be made, the limits of the user's power in relation to the subject and alternatives for achieving national objectives. The intelligence knowledge developed in the different areas of operation must be capable of contextualizing and informing the user about facts, events, situations or phenomena analyzed, actors and variables related to them, as well as about the consequences of their occurrence for society and the State.

Foreign intelligence deals with topics on which the State has little or no decision-making power or unilateral intervention, and which requires international positioning strategies for negotiation and achievement of national interests. The focus of this intelligence is to gather data, information and knowledge to understand and contextualize facts, events, situations and phenomena that occur in the global context, as well as their impact on Brazil's performance in the international arena.

The knowledge produced by foreign intelligence allows Brazil to seize opportunities, counter threats and define strategies to achieve the interests of the society and the State abroad, in compliance with the principles that govern the country's international relations. Examples of foreign intelligence include political and economic monitoring of other countries, multilateral forums for interaction between countries, the arms issue, the global economic situation, and advice on cultural policies with the aim of promoting Brazil's international image.

Domestic intelligence, in turn, deals with topics that are entirely within the State's intervention competence, adhering to the country's political and legal situation. Its focus is to gather data, information and knowledge in support of the State's actions in the national territory, advising on the design of long, medium and short-term public policies.

The knowledge produced by domestic intelligence allows Brazil to define strategies for achieving the interests of the society and the State internally, in compliance with the objectives and restrictions expressed in the Federal Constitution and other regulations. Examples of domestic intelligence include observing persistent social demands, monitoring the implementation of public policies and monitoring the environmental situation in the country.

Transnational intelligence deals with cross-border issues, partially under the State's capacity for intervention, but which require international negotiations and partnerships to adopt effective policies to achieve the State's objectives. Its focus is to gather data, information and knowledge to support Brazil's actions on topics that transcend the national environment to the international arena and vice versa, helping the country to position itself in a well-informed manner.

The knowledge produced by transnational intelligence allows Brazil to counter threats and define strategies for achieving the interests of the society and the State on topics that require both compliance with the objectives and restrictions expressed in the Federal Constitution and other national regulations, as well as the application of the country's foreign policy. Examples of Transnational Intelligence are

the monitoring of international extremism that has ties to Brazil or cells in in this country; migratory phenomena and the monitoring of Brazilian criminal organizations that operate in other countries.

Cyberintelligence deals with topics related to cyberspace, whose ubiquitous, distributed and decentralized nature implies limited capacity for State intervention. Its focus is to gather data, information and knowledge in support of Brazil's actions in the face of cyber vulnerabilities and threats, informing public policies and state plans in this domain, as well as monitoring and evaluating capabilities, intentions and activities of external actors in cyberspace.

The knowledge produced by cyberintelligence allows Brazil to identify, characterize and confront threats from State and non-State origin in cyberspace, in compliance with the objectives and limits expressed in the Federal Constitution. Examples of Cyber Intelligence are the analysis of cyber incidents against critical infrastructures, the technical attribution of cyberattacks and advice on national strategies in cybersecurity and defense.

3.3. Threats and Opportunities

The intelligence branch focuses on recognizing threats and opportunities to achieve the fundamental objectives and interests of the Brazilian society and the State. These objectives and interests are materialized in the various public policies and in the planning and execution of actions that enable Brazil to obtain competitive advantages. In short, we seek to understand reality to facilitate political action capable of generating common good. Thus, we work with a double perspective: perceiving and exploring opportunities to achieve these objectives and interests, and identifying and countering threats to their achievement.

Opportunities are favorable circumstances, events of which one can take advantage to boost such interests and guarantee competitive advantages for the country. The search for opportunities includes highlighting and interpreting facts, events or situations capable of

helping the country achieve a better state, based on the achievement of its fundamental objectives.

Threats are circumstances that make it difficult to achieve these same interests, events that postpone or prevent their being achieved. In the context of intelligence activity, there are threats arising from adverse intelligence actions, which, as they result from the use of specialized techniques, are subject to monitoring by the counterintelligence branch. All other threats, however, belong to the intelligence branch and must be monitored by it.

In this sense, extremist acts can be monitored by intelligence, which will contextualize their occurrences, identify and understand their actors, analyze and interpret the phenomenon of which they are a part. However, when the use of a specialized technique is noticed in its execution, it will be necessary to use counterintelligence measures to counter this threat. What determines whether or not a threat belongs to the intelligence branch is not the subject or theme to which it is linked, but the probability that the agents responsible for its execution will or will not use specialized intelligence actions.

In the intelligence branch, threats can be intentional (antagonisms), that is, purposefully aimed at preventing or hindering the achievement of national interests. But they can also be fortuitous (obstacles), that is, without the intention of causing harm, therefore not resulting from actions specifically directed against the realization of such interests. The differentiation between antagonisms and obstacles is necessary to estimate the probability of these threats persisting and to outline the best way to counter them.

Thus, the facts, events, situations and phenomena described, interpreted and explained by the intelligence branch are defined in terms of achieving the fundamental objectives and national interests of the Brazilian society and the State. The development of intelligence knowledge is driven by these objectives and interests and seeks to inform users of favorable and unfavorable factors for them.

3.4. Intelligence Cycle

The functioning of the intelligence branch can be illustrated by a cycle composed of five phases, characterized by actions: setting an objective, monitoring, informing, deciding and acting. The first three phases are carried out by intelligence agencies, but the final two phases usually take place in other spheres. Decisions are always up to the user, and actions are up to the instances determined by them.

Although the phases are arranged in an orderly manner for didactic purposes, it is worth noting that the actions of one phase may overlap or merge with those of the next phase, depending on the dynamics of the topic addressed.

The cycle begins with the phase that is conventionally called setting an objective, in which the themes, sections and approaches to the areas that will be worked on by the intelligence branch are determined. During this phase, objects of continuous monitoring of intelligence professionals are defined. It is here that the intelligence body will evaluate the interests and objectives, either expressed or implicit, of the Brazilian society and the State.

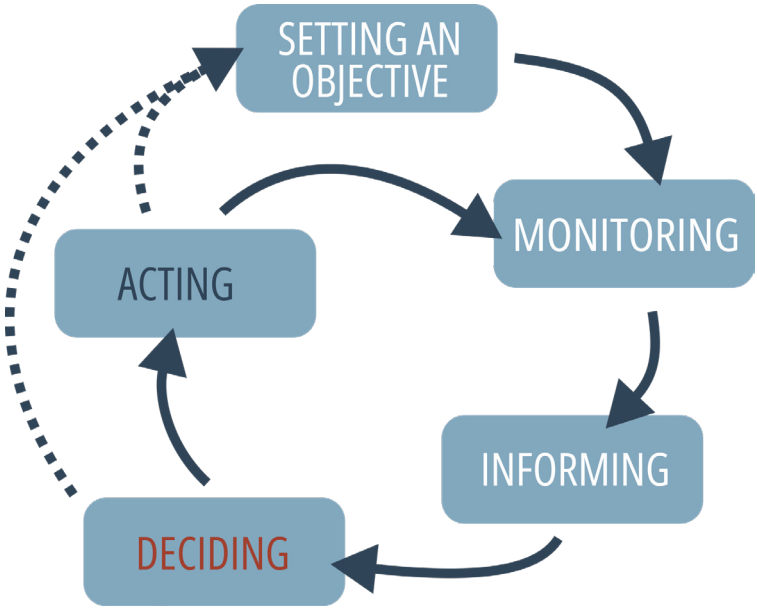


Figure 1: Intelligence cycle

The purpose of this phase is to turn requests arising from public policies, guidelines and diagnoses drawn up by government authorities into monitoring objects. By specifying the key themes for processing, the aim is to make the intelligence agency's actions more focused and effective.

The setting-an-objective phase is generally carried out by the top management of intelligence organizations, based on the stimuli received in their interaction with users. What interests them? What are their priorities? What goals do they intend to make possible in the search for achieving the fundamental objectives of the State? These are definitions of scope and purpose that are constantly reviewed in light of the policies adopted by the Brazilian State.

Just as it is important to understand national interests, it is essential that the intelligence agency understand the contexts in which such interests will be pursued or contradicted. What interests could conflict with those of Brazil? What are the obstacles and threats to their implementation? On the other hand, what opportunities can be envisioned for its achievement? In what way or under what aspects could these contexts be explored to benefit the fundamental objectives of the Brazilian State? These inputs assist the intelligence body in its role of advising decision makers. Defining the areas to be covered by the Intelligence branch, its focus, the resources to be allocated and the organization of work is part of the setting-an-objective phase.

At the end of the setting-an-objective phase, it is expected that the body will have a defined agenda, for action aimed at achieving the interests of the Brazilian society and the State. Traditionally, this agenda is formalized in the Intelligence Plan document, which contains the guidelines for carrying out the activity, the intelligence objectives and the knowledge necessary for the monitoring of areas of interest to be effective.

The second phase, monitoring, usually occurs continuously throughout the cycle. It concerns the constant process of planning, gathering and processing data, information and knowledge relating to the areas monitored. This is the phase in which the intelligence professional examines the topic under his responsibility, defined in the previous phase, seeking to determine the scope, function and pur-

pose of production. To do this, it is necessary for the professional to understand the national interests and the fundamental objectives of the State related to their subject.

The purpose of the monitoring action, therefore, is to allow intelligence production units to perceive threats and opportunities to obtain the aforementioned interests and objectives, as well as to remain updated on phenomena that require decision-making by the federal Executive Branch. This monitoring is a vital part of the basis for the advice to be provided to the national decision-making process.

In the monitoring phase, studies are conducted to understand the contexts into which national interests and the State's fundamental objectives relating to each area are inserted. What variables impact their achievement? What aspects are favorable and what aspects are unfavorable to their achievement? Are there conflicting interests? Which actors oppose them? What is the acting capacity of these actors? How do they usually act? This is continuous monitoring that aims to allow an intelligence professional to interpret and contextualize facts, events and situations that occur in these areas and are of interest to the Brazilian society and the State.

At the end of the monitoring phase, it is expected that the intelligence organization will have been updated on the stage of achievement of the State's fundamental objectives and the contexts into which they are inserted. This phase is formalized through Basic Intelligence construction mechanisms and tools. It is desirable that the resulting knowledge be accessible to intelligence professionals who have adequate security clearance and a need to know about it.

When the processing indicates that relevant knowledge needs to be produced for decision-making, we move on to the informing phase. In this phase, the knowledge produced to advise the various government bodies is formatted and disseminated. This is the phase in which intelligence describes, narrates, contextualizes and explains to the competent authorities the facts, events, situations or phenomena that may indicate the need for decision-making on one or more areas of intelligence interest. It comprises the stages of formalization and dissemination of knowledge and is the result of the monitoring carried out in the previous phase.

The informing phase occurs whenever the team responsible for monitoring a given area notices the occurrence of a fact, event or situation that must be reported to the competent authorities, either to assist in the situational diagnosis or to require a position from the State. It can also result from an explicit request from a user, who requests the production of knowledge about a certain phenomenon and its repercussions.

The means of formalizing and disseminating the knowledge produced must take into account the timeliness of its transmission, that is, the knowledge must be made available in a timely manner for its use. The relevant security requirements for its processing must also be considered. Therefore, speed in providing access to knowledge must be prioritized, but without neglecting the layers of protection necessary to guarantee effectiveness in the processes of elaboration and use of knowledge. The dissemination of knowledge can be done through textual documents, audio, image or video files, graphics with consolidated data or through face-to-face or synchronous remote meetings, among other available means.

At the end of the informing phase, it is expected that intelligence knowledge will have been produced and disseminated that is able to situate the decision-maker in the issue being monitored, in terms of its context, nature, stage of development, impact on the achievement of the state's interests and potential consequences. With this knowledge, the competent body will, in the next two phases, decide how to act, taking into account the resources available to the state. The acting stage will be carried out by other government bodies responsible for implementing public policies concerning the intelligence in question.

Deciding is the phase in which the decision maker, at the appropriate level, defines how to proceed in the search for achieving a national interest. This decision must have as one of its basic elements knowledge provided by intelligence that considers the interest and its context and results in the definition of an action to be implemented by the State. The complexity of such an action, the circumstances of its implementation and its implications for the country will determine which officials will decide on this action.

Thus, at this stage there is deliberation, by those entitled to do so, on the measures to be implemented to achieve an objective, as well as the order derived from such deliberation. Not acting and not deciding are also possibilities for the decision maker. The role to be played by the intelligence professional in this phase is to provide assistance to the decision-making process, taking as a starting point the intelligence knowledge disseminated in the previous phase. In the end, it is expected that intelligence will have assisted the decision-making process on the topic being monitored, facilitating decision-making.

Acting is the phase in which the State adopts measures and procedures to implement what was decided in the previous phase. When acting, depending on the context, more than one course of action may be adopted simultaneously. These are State actions that usually involve actions of other public bodies or higher level officials. The completeness of the acting phase is not the responsibility of the intelligence agency. On the contrary, the implementation of the action defined in the decision phase is the responsibility of other bodies, directly involved in the execution of the country's foreign policy and public policies. These bodies may eventually request intelligence assistance, in accordance with the law, generating new knowledge. At the end of the acting phase, it is expected that intelligence will have helped to build favorable conditions for achieving national objectives.

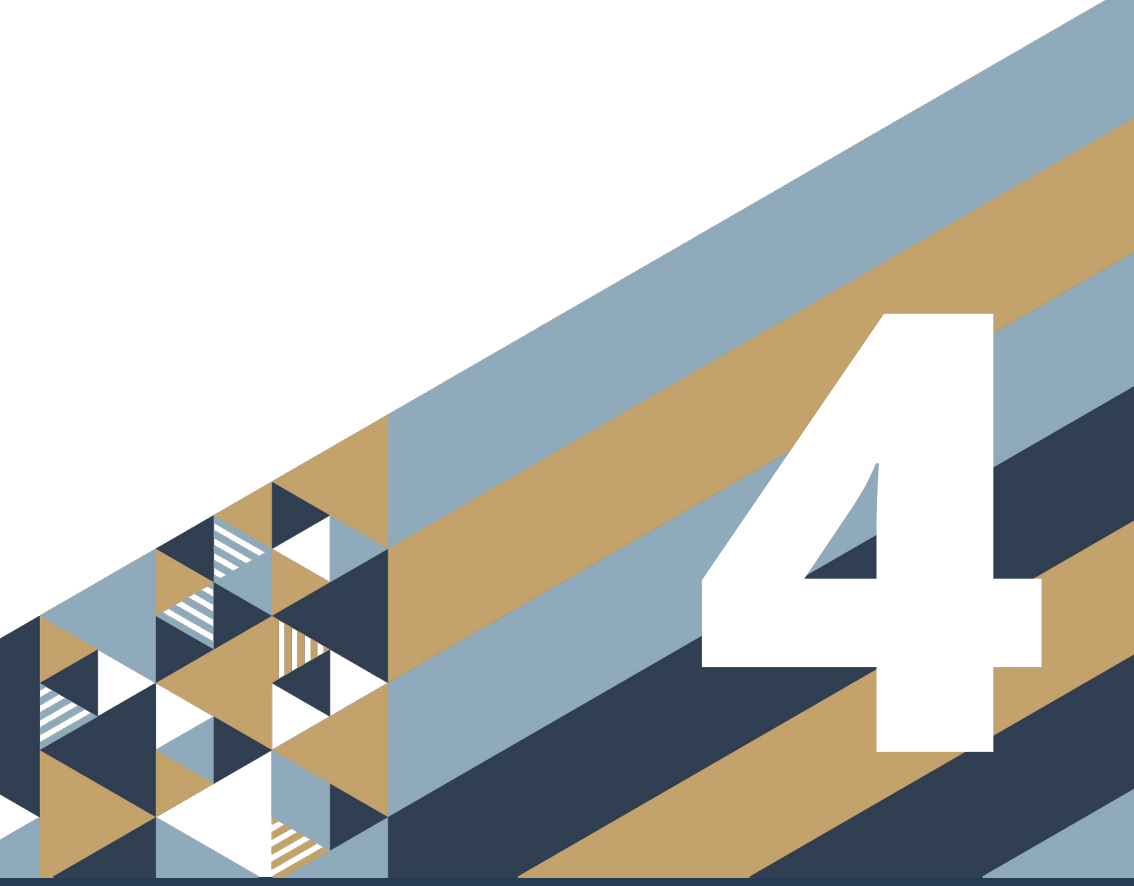
Once the fifth phase of the intelligence cycle, (acting), is complete, a self-assessment of the advisory process is conducted, in which best practices and observed failures are listed, with a view to improving the performance of the intelligence branch. Sometimes the issue being monitored itself will need to be redefined after the decision has been executed. The actions taken by the public authorities may result in modifications that, in turn, give rise to changes in the scope and approach of such issue, add new monitoring topics or, conversely, indicate that the scope of this area may be reduced. In this case, we return to the setting-an-objective phase. However, if none of this is necessary, the issue continues to be monitored according to the same premises and guidelines previously outlined.

The purpose of the intelligence branch is, mainly, to provide knowledgeable assistance to the national decision-making process in

achieving the State's objectives and, occasionally, to act as a facilitating instrument for this achievement. It is necessary, therefore, that its professionals seek to understand national interests and how intelligence can act to achieve them. Therefore, in addition to knowing these objectives, one of the fundamental aspects of this branch is understanding the nature, dynamics and role of intelligence and how it can be used by the State.

In summary, the intelligence cycle offers a useful methodological framework for the work of professionals in the field, systematizing procedures into phases that feedback on each other. The actions in the monitoring phase are permanently carried out, based on the definition of the branch's areas of activity, consolidated in the phase of setting an objective. The third phase, (informing), is ideally carried out whenever a fact, event or situation occurs that impacts the conduct of domestic public policy or the country's external positioning, and must be reported to the competent authority. The decision-making phase necessarily takes place outside the intelligence agency, by those who have the mandate or prerogative to implement the country's government policy. Similarly, the acting phase will usually be led by the bodies responsible for this implementation. The monitoring phase continues after the execution of the action decided on, and includes monitoring of its effects and results. Occasionally, after self-assessment of the process by the professionals involved, a new approach may be adopted or a new monitoring topic may be included after the deciding and acting phases. At these moments, the cycle returns to its first phase, setting an objective.

After the Intelligence branch has been thoroughly discussed, it is worth approaching its counterpart, the Counterintelligence branch, highlighting the characteristics that differentiate them.



4

The Counterintelligence Branch

4. The Counterintelligence Branch

Counterintelligence is the branch of intelligence activity that develops specialized actions aimed at preventing, detecting, identifying, evaluating, obstructing and neutralizing adverse intelligence actions that pose a threat to: the interests of the State and society; the decision-making process; and the safeguarding of knowledge, information and sensitive data, the means where they are stored or through which they pass, their holders, their areas and facilities. In this sense, counterintelligence is focused on protecting the interests of the State, seeking to make it difficult for adversaries to obtain advantages, and to neutralize any advantages acquired through adverse intelligence actions.

The measures recommended by the CI are grouped into two segments: preventive counterintelligence, relating to anticipating and protecting threats; and active counterintelligence, relating to countering threats.

This division helps to operationalize counterintelligence, generating sub-specialization in the work of its professionals. It does not imply, however, that the two areas are dissociated. On the contrary, they are interdependent. Actions carried out by preventive counterintelligence serve as the basis for active counterintelligence. At the same time, countermeasures carried out by active counterintelligence increase the perception of security and act as a deterrent to other attempts from adverse action, reflected in the practice of preventive counterintelligence.

4.1. Preventive Counterintelligence

Preventive counterintelligence is the segment of counterintelligence that advocates the adoption of preventive measures and procedures aimed at safeguarding knowledge, information and sensitive data and their holders, as well as materials, areas, facilities, means of production and storage and communication channels that are of interest to society and for the State to protect. It is also the segment

that seeks to prevent the implementation of adverse intelligence actions designed to influence the national decision-making process, such as actions of foreign interference, terrorism and sabotage.

Therefore, preventive counterintelligence must act in partnership with objects of interest for adversaries, that is, potential targets for adverse intelligence, which may include people, institutions, facilities or information. To this end, professionals working in this field must evaluate intelligence interests of competitors in the country, and identify possible targets for adverse action.

Likewise, it is important that these professionals know how to determine and prioritize objects that are in the interest of society and the State to protect. This segment is based on the assessment of the risks perceived by objects of interest for adversaries, and the prevention and security measures adopted by them, which must be appropriate to their profile and context of operation.

Preventive counterintelligence is subdivided into the following areas: protection of sensitive knowledge, protection of physical infrastructure, and prevention of actions that interfere with decisions.

Knowledge Protection

It is the segment of preventive counterintelligence that advocates the adoption of measures and procedures designed to prevent, detect and obstruct antagonisms directed at holders of sensitive, confidential or classified knowledge and data, the physical structures that contain them, the means that conveys them and the locations where their holders are located, be they people, documents, materials, means of information technology, and areas and facilities. Antagonisms, within the scope of counterintelligence, are actions planned with the aim of accessing, stealing, disclosing or damaging information, thus hindering its use. The work can be carried out at the request of interested institutions or upon the suggestion of counterintelligence, after an object of interest for adversaries has been identified.

Sensitive knowledge and data are understood to be those that, due to their importance for the development and security of the State

and society, require special protection measures. Confidential knowledge and data are understood to be those who, due to their indispensability to the personal security of citizens, society or the State, have their dissemination controlled and their access restricted to accredited people. Classified knowledge and data are understood as those who, due to their importance for the security of the State or society, have their access restricted and are assigned a degree of secrecy. This knowledge and data will be declassified after a period determined by current legislation, and will then be able to be accessed and published.

Preventive actions to protect knowledge include raising awareness of, guiding and training national strategic institutions to safeguard assets of interest to the State and society, promoting the adoption of security behavior and measures. Furthermore, counterintelligence can also act to identify and assess vulnerabilities in an institution's protection systems and present recommendations for incident risk reduction.

Knowledge protection work is carried out by a team, and includes promoting a culture of knowledge protection in partner institutions; identifying threats; identifying vulnerabilities in the protection systems of these institutions; assessing risk; and monitoring the implementation of actions to protect their sensitive knowledge. The protection of knowledge is the result of the combination of understanding the way in which actors operate and the techniques that actors use, to gain undue access to restricted data and the best internationally recognized security and information management practices. Protection work is carried out in layers, considering five didactically distinct areas: governance; people; documents and materials; information and communications technology; and physical areas and facilities. In practice, these areas blend.

The protection of knowledge aims to enable and ensure that any knowledge, information and sensitive data have the following characteristics:

- Availability: state of being available and usable at the request of a specific person, organization, system or entity.

- Integrity: state of not having been altered or destroyed in an unauthorized manner.
- Secrecy: state of being revealed only to the person, organization, system or entity authorized and accredited for that disclosure.
- Authenticity: state of identifying who produced, sent, modified or destroyed it.

Critical Infrastructure Protection

Critical infrastructure protection is the aspect of preventive counterintelligence that advocates the adoption of measures and procedures designed to prevent, detect and obstruct threats of any nature directed at national critical infrastructures. They are considered critical infrastructures (CI), in accordance with art. 1, paragraph one of one, of Decree 9573/2018 (National Critical Infrastructure Security Policy), "facilities, services, goods and systems whose interruption or destruction, in whole or in part, will have serious social, environmental, economic, political, international or security impact on the State and society".

Critical infrastructure security, on the other hand, aims to coordinate the development of preventive security procedures for human resources, equipment, facilities, services, systems, information and other resources that ensure the maintenance and operation of services and activities that are essential to the State and society in various spheres of the public and private sectors.

Each State uses its own criteria to define which are its critical infrastructures. Thus, what is considered critical infrastructure for one state may not be so for another. In any case, what must be protected are infrastructure operations that are considered vital for the management of the State and the development of society. There is, therefore, an emphasis on ensuring its continued full operation. In addition, we seek to understand the functioning of critical infrastructures and their importance in different sectors, in order to map chain effects which any interruption or destruction of infrastructure may cause.

The critical infrastructures of Information and Communication Technology (ICT) have the peculiar characteristic of being able to be part of, with horizontal interdependencies, several critical infrastructures, that is, the information generated by a certain priority area of a critical ICT infrastructure can be input for other critical infrastructure, thus emphasizing its high degree of coupling and interdependence. This fact increases the need to identify essential information assets, as well as the addressing of the risks to which they are exposed, as the impact caused by the loss or unavailability of those assets could compromise the entire chain of existing critical infrastructures.

When a comprehensive list of critical infrastructures is not present in the legal system, the criticality of the infrastructure is assessed based on indicators related to the impact of the interruption or destruction of said infrastructure. To this end, criteria such as the dependence between them can be adopted; intra-sectoral, economic and population impacts; reconstruction time in case of destruction; and damage caused to the image of the State. The variables to be considered are:

- Interdependence, defined as the relationship of dependence between critical infrastructures or interference of one critical infrastructure into another, or of a priority area of critical infrastructures into another area. It evaluates the impacts of interruption of infrastructure functioning (caused by operational changes or shutdown) on other strategic sectors for the Brazilian State. Examples: a thermoelectric plant that supplies energy to airports (relationship with the transport sector); a roadblock that prevents the flow of grains, impacting the agricultural sector.
- The immediate impact on the population that will be directly affected by the interruption to the provision of services, resulting from the inactivation of an infrastructure. Examples: number of people using a blocked highway; people directly affected by a port shutdown. People affected by the cascade effect are not taken into account in this assessment.

- The economic impact of rebuilding critical infrastructure, which refers to the cost of rebuilding the infrastructure in the event of its destruction.
- The intra-sectoral impact, defined as the impact of infrastructure disruption within its own sector. For example, a refinery at a standstill affects fuel distribution; the shutdown of Brasilia airport impacts Goiania airport. A contingency analysis makes it possible to evaluate options within the sector that can make up for the absence of the infrastructure evaluated.
- The time required to rebuild the infrastructure. In the case of highways, the reconstruction time for critical points for their operation must be considered.
- Damage to the State's image, resulting from the repercussions of the shutdown or destruction of an infrastructure, generating a loss of the population's confidence in the government's ability to guarantee their well-being and solve the problem. This criterion concerns exclusively the impact on the State's image, and does not consider other repercussions of the action, for example, environmental impacts of a disaster.

Preventing interference in the decision-making process

It is the segment of preventive counterintelligence that advocates the adoption of measures and procedures to prevent adverse intelligence actions that aim to interfere in the national decision-making process, in the conduct of public policies or in the achievement of the State's fundamental objectives.

Actions of interference in decisions are considered to be those intended to intervene illegitimately, including in a veiled manner or with the use of violence, in the national decision-making process, in the conduct of public policies or in the achievement of the fundamental objectives of the State. Such actions can be direct, when they seek to directly persuade the decision-maker, such as through direct influence in a certain area or through the recruitment of people with decision-making capacity within the State. But they can also be indi-

rect, when they use different means, such as campaigns that aim to manipulate public opinion. Indirect actions also include the use of violence to create popular commotion or manipulate community perception of a certain event or situation, leading to social pressure that interferes in the national decision-making process.

Actions of interference in the decision differ from actions of influence, which are legitimate and overt ways of persuading the decision-making process to maintain or modify its behavior. Legitimate influence has as its constituent elements the fact that the sponsor of the action is obvious and known; the sponsor's objective is to be transparent; and the tactics used in the action are considered legitimate by the State.

Each country has its own understanding of what type of foreign influence is acceptable or unacceptable, be it legally determined or politically implied. This definition considers the real risks or threats that foreign influence poses to national interests, social values and State sovereignty. The way in which States position themselves varies over history and in different political and legal contexts. In other words, what may be considered an action of unacceptable influence at one time and before a certain actor, at another time may be treated as legitimate influence.

Prevention of interference actions results from the identification and analysis of the actors who carry out these actions, their objectives and capacity to act; and understanding the way they operate and the operational techniques they use to carry them out. It is most effective if carried out in collaboration with potential targets for adverse intelligence. Therefore, it is also necessary to map and guide them so that they themselves can establish measures that seek to prevent or hinder the implementation of adverse actions.

In the case of violent interference actions, such as terrorist or extremist attacks, intelligence also seeks to advise possible targets of these actions, so that they can adapt their security levels to the perceived threat. Furthermore, individuals and groups identified as potential adverse agents are monitored to promote disengagement and de-radicalization policies.

When evaluating potential adverse actions, the following criteria should be considered:

- Scope: this factor is defined by the area to which this action is directed, that is, whether it seeks to influence decisions or behaviors of the Brazilian State domestically, externally or transnationally.
- Degree of influence: a factor measured by the impact that the completion of this action would have on the decision-making process and the behavior of the Brazilian State and the society, in relation to a given topic.
- Degree of violence: a factor determined by its estimated level of potential to cause harm.
- Potential for coercion: a factor established by the probability that the completion of this action would have to pressure for or induce a change in decision or behavior by the Brazilian State and its society, in relation to a given topic.

4.2. Active Counterintelligence

It is the segment of counterintelligence that advocates the adoption of measures and procedures designed to detect adverse action and identify its agent, in addition to evaluating, obstructing and neutralizing the action of adverse intelligence. Active counterintelligence comprises actions carried out by counterintelligence, counterinterference, counterinsurgency and counterterroris.

Counterespionage

It is the segment of active counterintelligence that advocates the adoption of measures and procedures designed to detect, identify, evaluate, obstruct and neutralize espionage actions carried out by adverse agents.

Espionage is understood to be any activity aimed at the unauthorized obtention of sensitive, confidential or classified data, infor-

mation or knowledge to benefit States, groups of countries, organizations, factions, interest groups, companies or individuals. Thus, espionage is characterized by the access to and acquisition of data, information or knowledge that would not be accessible to the adverse agent without the use of specialized techniques.

Counterespionage (CE) is a continuous effort to counter search actions carried out by adverse agents. To do so, counterintelligence professionals need to understand the objectives, interests and ability of adversaries to employ specialized techniques. When reporting a concrete action of espionage by adverse intelligence, its stage of development must be assessed and its real or potential effects must be determined. The action and the likely interests behind it will be assessed and strategies for obstruction or neutralization will be developed.

Counterinterference

It is the segment of active counterintelligence that advocates the adoption of measures and procedures designed to detect, identify, evaluate, obstruct and neutralize interference actions perpetrated by adverse agents that threaten national interests and the security of the State and society.

Foreign interference is a covert way of projecting power, being an instrument to influence others to alter their behavior according to the interests of the sponsor of the action. Its veiled nature serves to shape events in favor of such sponsor, who needs to remain hidden as a prerequisite to achieve their desired results.

Foreign interference actions have defined strategic objectives, which generally focus on the political-social or economic field. In the political-social field, among the various possible objectives, the action can seek to directly influence the decision-making process; seek to distract or manipulate a specific audience; undermine an opponent's political and social capital; support internal groups for public policy changes; or ultimately change the political regime of another State. In the economic field, some of the frequent objectives are to harm

competitors; restrict technological, economic or commercial development; encourage boycotts; and destabilize markets.

To achieve their objectives, actors generally coordinate multiple operational actions and various tools that may not be exclusive to foreign interference, combining overt and covert elements. The more complex a foreign interference operation is, the more it will be able to coordinate tactics and instruments to deceive and trick those for whom it is intended.

Foreign interference actions can be categorized according to their objective, means used and level of offensiveness. Below are some examples of foreign interference actions.

Adverse propaganda is the set of actions carried out using social communication techniques and methods to, in some way, persuade target audiences and influence their attitude, opinion, emotion and behavior. These actions are carried out with the dissemination of edited, manipulated or contextually distorted information, through direct and media channels, to promote the sponsor's ideological, political or economic interests.

Disinformation is the set of actions that deliberately disseminates false information, to deceive or confuse a specific target audience to cause harm, mislead or manipulate a situation or event in favor of the sponsor's interests. On social media, dissemination of misinformation is generally carried out in an inauthentic and coordinated manner. To be most effective, disinformation must contain elements of veracity or plausibility in its content.

The recruitment of agents of influence is the action aimed at the recruitment and control, by foreign entities, of people, used as instruments to issue messages and interfere in politics, the market and society in order to favor the interests of their sponsor. Government officials, politicians, academics and influencers, among others, may be the subject of such recruitment.

Covert promotion of groups and entities is a type of action that aims, in a covert way, to create, structure, finance, co-opt or maintain groups or entities that promote the interests of their sponsor. This can be done by stimulating a pre-existing group that has already been

selected or by articulating a group that originated in the context of political dissent that already exists, albeit in a latent form, in the target society.

Support for legal manipulation (lawfare) is the use of legal maneuvers to seek to prevent or hinder the achievement of the adversary's interests that conflict with those of the sponsor. To support and facilitate this manipulative practice, typical resources of external interference are commonly used, such as disinformation, recruitment, adverse propaganda and promotion of groups and entities that may act as parties in legal processes.

Sabotage is a type of action that aims to destroy, damage, compromise or render useless, in whole or in part, knowledge, data, materials, equipment, facilities, logistical systems, production chains and critical infrastructures of a country, and thus affect the ability to meet the essential needs of its population and the interests of the State. Sabotage actions can be of a material nature, when carried out on machines, equipment or installations; chemical and biological, through the manipulation of explosives, viruses or bacteria; nuclear, with the use of radioactive sources and elements; and cyber, through invasions and damage to computer systems and networks.

Counterinsurgency

Counterinsurgency is the segment of active counterintelligence that advocates the adoption of measures and procedures designed to detect, identify, evaluate, obstruct and neutralize adverse actions by insurgent people and groups. An insurgency is an armed rebellion against an established power carried out or planned by a group formed or supported by a portion of the population. Insurgencies vary according to the context in which they occur, and may have different social, cultural and economic aspects. They can be carried out through paramilitary movements, attempted coups d'état, revolutions, guerrillas, civil wars or wars of liberation.

Counterterrorism

Counterterrorism is the segment of active counterintelligence that advocates the adoption of measures and procedures designed to detect, identify, evaluate, obstruct and neutralize adverse actions by violent extremist people and groups. Violent extremism refers to the planning, preparation, promotion, financing and execution of violent acts motivated by extremist ideologies that violate fundamental constitutional precepts. According to extremist ideologies, collective violence against people, groups and institutions that represent existential enemies, or at least that is how they are perceived, is an essential condition to guarantee their survival or implement their worldview.

Violent extremism is a broad concept. It allows us to include, for example, people and groups who advocate the use of violence against society or part of it, but who have not yet committed actions that could be classified as terrorist acts. The term violent extremism is an alternative to describe certain violent conduct in contexts in which the term terrorism lacks a uniform and unambiguous meaning, such as when there is no consensus among States on the official designation of terrorist groups or when there is a lack of legislation classifying terrorism or a terrorist act.

Although there is no consensus on the definition of terrorism, the following characteristics are usually associated with the phenomenon: use of violence and the threat of violence as a tactic or strategy of coercion and propaganda; use of terror as a tool of psychological warfare, generating widespread fear, anxiety and a feeling of insecurity among the population; attack on indiscriminate victims, in which the main victims tend to be civilians, non-combatants, defenseless or innocent people, without direct responsibility for the conflict that gave rise to the acts of terrorism; illegal nature of the acts; the predominantly political nature of terrorist violence, observable in its motivation and its repercussions on society.

In Brazil, Law 13260/2016 defines terrorism as consisting of the practice, by one or more individuals, of the acts provided for in §1 of Article 2, for reasons of xenophobia, discrimination or prejudice based on race, color, ethnicity and religion, when committed with the

purpose of provoking social or generalized terror, exposing people, property, public peace or public safety to danger, to bring about terror.

4.3. Counterintelligence and Security

Security and counterintelligence are related concepts, but they are not to be confused. Security concerns the maintenance of a state of balance that guarantees stability for carrying out everyday or extraordinary actions. Counterintelligence refers to the prevention and counteraction of adverse intelligence actions, which are carried out by using specialized techniques.

Security is a multidisciplinary area. It is not restricted to the role of an intelligence professional. In fact, it must incorporate all types of knowledge that can raise protection levels and increase the perception of security and trust of the parties involved. This includes assessments relating to civil defense, analyses by technicians specialized in areas relating to perceived risks, threat assessments by other types of professionals, such as social scientists, anthropologists, psychologists, etc.

Security is an essential part of all intelligence activities, which includes the branch of counterintelligence, but is not limited to it. Security deals with protection against all types of threats, which, doctrinally, includes antagonisms and obstacles, that is, intentional and unintentional actions. Security concerns the prevention and management of perceived risks.

Every intelligence organization must pay attention to security aspects of its areas and facilities, and its personnel – which includes social investigation routines and monitoring of staff. Intelligence organizations must also take care of the security of their practices. It is these practices that will define the organization's safety culture. The stronger this culture, the less permeable the body will become.

The desirable security culture in an intelligence organization includes observing the principle of compartmentalization and not discussing work-related matters or getting involved in compromising

situations, that could give rise to pressure or blackmail. Security must be observed by all employees, both in-house and outsourced.

Counterintelligence is aimed at opposing adverse intelligence, which includes active countermeasures. All of its work is aimed at frustrating the adversaries' efforts to gain competitive advantages through the use of specialized techniques.

In-house security is an internal activity within organizations, responsible for implementing security measures, prevention measures and, whenever relevant, countermeasures. In this sense, it can be said that it combines security and counterintelligence actions.

This activity adopts measures and procedures aimed at safeguarding people, materials, areas, facilities and means of production, storage and communication of knowledge and data, within the scope of the body or institution itself. In-house security is also responsible for promoting and strengthening institutional security culture. Corporate social communication resources can be used to carry out awareness and guidance campaigns to encourage compliance with safety standards and procedures.

In-house security is responsible for internal application of the two aspects of counterintelligence - preventive counterintelligence and active counterintelligence. As such, it comprises all segments of counterintelligence, and may use any of its measures, as long as they are appropriate to the context of use.

In an institution, it is up to the fraction responsible for in-house security to design, or at least coordinate, its security management system. It is also responsible for developing actions to counter the action of adverse intelligence that targets the body, its personnel, its knowledge, areas, facilities, or information and communications technology.

In the case of an intelligence body, these responsibilities are the responsibility of more than a fraction. Thus, in order to detect and identify adverse actions and counteract them, coordination between the In-house security fraction and other units responsible for counterintelligence monitoring actions is necessary, generating data that continually supports the study of threats and adverse actors.

4.4. Counterintelligence Cycle

The functioning of counterintelligence can be illustrated by a cycle composed of six phases, characterized by actions: monitoring, guiding, detecting, evaluating, deciding and acting. In principle, this cycle has the same action in its starting and ending point: monitoring. It is possible, however, that it will begin at other stages, depending on the stimuli received by the agency or intelligence professional.

The actions in each phase do not end when the next phase begins. On the contrary, the first two phases, monitoring and guiding, tend to occur permanently and in parallel throughout the entire cycle. These are actions that are maintained even if no adverse action is perceived. The other four phases, represented in the center of the diagram, occur whenever an adverse action is perceived.

Monitoring is the phase in which counterintelligence examines adversaries, sponsored by a state or otherwise, that are in open or covert competition with the State or national private institutions. The objectives of the monitoring action are to understand the interests, capabilities and ways in which these adversaries act, and to identify institutions, groups or people that could be of interest to them. By carrying out this monitoring, the intelligence organization seeks to anticipate potential adverse actions carried out by adversaries on national targets.

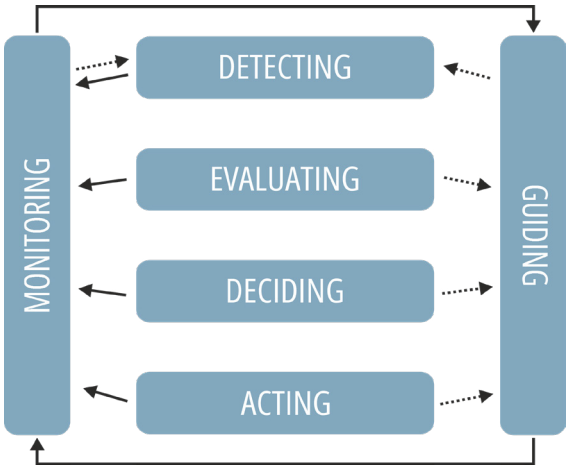


Figure 2: Counterintelligence cycle

In the monitoring phase, studies are conducted to understand the context in which the adverse intelligence activity operates. Who are their actors? What are the objectives of such actors? Who sponsors them? What are the techniques and resources used to achieve these objectives? And how are they being employed? This is continuous monitoring, that aims to allow a counterintelligence professional to develop analyses on the identity, capacity and mode of action of adverse intelligence.

Just as it is important to understand our adversaries, it is essential that the counterintelligence professional seek to understand the Brazilian position. To what extent do our interests conflict with those of other countries? What are our vulnerabilities and how can they be exploited? What are we developing, that could become a target of interest for adverse intelligence? In what way or under what aspects? This knowledge enables a counterintelligence professional to perceive more effective ways of preventing threats.

Those routine practices of counterintelligence fractions are included in this phase, such as monitoring foreign intelligence organizations and insurgent, terrorist and extremist groups, identifying possible targets of adverse actors and evaluating the development of adverse actions over time. At the end of the monitoring phase, it is expected that counterintelligence will know which actors are most likely to pose a threat to the interests of the Brazilian State and society, as well as their modes of operation and likely targets.

Guiding is the phase in which counterintelligence offers instructions to those responsible for potential targets of adverse interest, seeking to make them aware of the need for protection, in order to avoid or minimize harm to the State and society. This guidance establishes a communication channel between an intelligence organization and institutions perceived as likely targets, with the purpose of advising them on the implementation of the necessary security measures.

Once potential objects of interest of adverse actors have been identified, the aim is to increase the level of protection of knowledge and data relating to such targets, seeking to prevent or minimize losses to the State and society. Likewise, if these objects are consid-

ered national critical infrastructures, CI is also responsible for guiding the responsible bodies on measures to increase the level of physical protection of these installations. A CI professional is responsible for advising national bodies and entities on the implementation of the necessary security measures. This advice includes risk assessment regarding the potential target, suggestions for improvement, awareness events for the adoption of security measures and explanation of such measures and their effects.

The guiding phase also serves to sensibilize potential targets to the threats they may face, to help them obstruct such threats, and to create a communication channel between the targets and the intelligence organization. Therefore, this phase includes contacts that the CI fractions make with potential targets, elaborate risk assessments and guidelines for implementing measures to prevent and obstruct adverse actions. At the end of the guiding phase, it is expected that the potential target will have improved its level of security and established sensors capable of detecting possible adverse action, as well as channels for activating CI in the event of adverse action or signs of potential occurrence.

Detecting is the phase in which counterintelligence detects possible adverse action that has either been completed or is ongoing. Such action may involve improper access, subtraction or damage to knowledge, data, materials, equipment, areas, facilities, systems or processes produced, used or held by potential targets, or may consist of an attempt to interfere in the national decision-making process.

Detection can result from monitoring, when the priority interests of a given adversary are estimated. After understanding possible adverse interests and the capacity for action of certain actors, an intelligence organization or professional would look for signs of adverse intelligence acting in achieving the presumed interests.

Another form of detection is mediated by the perception of the occurrence of an adverse action on the part of those who suffer it. To this end, it is important that, in the guiding phase, communication channels have been established between counterintelligence and the possible object of adverse action, so that suspicious situations are reported by the latter to counterintelligence. The same can hap-

pen internally to the agency, due to the counterintelligence link with the fraction responsible for In-house Security. Counterintelligence is activated through sensors established for this purpose and the suspicious action is preliminarily analyzed.

Adverse actions can also be envisioned when they are still being planned, if counterintelligence has managed to carry out an intrusion. This occurs when an agent is positioned within the adverse intelligence body. Depending on the position of this agent, he or she may have prior knowledge of the organization's plans, enabling detection even before the adverse action is initiated. Sometimes, detection occurs based on information voluntarily provided by third parties, including those linked to adverse intelligence itself, who seek counterintelligence for various reasons, such as finance, ideology and politics.

It is possible that the identification of an adverse agent precede the detection of its action. This occurs when the presence of people whose connection with adverse intelligence has been raised in the monitoring stage is noticed. When this happens, it is up to the counterintelligence professional to monitor the activities of these individuals to try to discover their objectives and potential targets in the country. Included in this phase are contacts made with potential targets of adverse intelligence, to estimate the occurrence of hostile actions, and monitoring of people linked, or supposedly linked, to adverse intelligence organizations. At the end of the detecting phase, if there is sufficient evidence of an adverse action taking place, it is expected that counterintelligence will have a concrete case to evaluate.

The detecting phase is followed by the evaluating phase. To do so, it is necessary to consider the objective of the adverse action, how it is conducted, its likely sponsors and the consequences of its possible implementation for the target country. Not all of these elements are always available or can be estimated. The only essential elements for the evaluation are the raising of hypotheses about the objective of the adverse action and its stage of development.

Thus, after detection, a counterintelligence professional will seek to determine the likely intention of the adverse intelligence and will attempt to identify the authorship, sponsorship and stage

of development of the action (whether it was completed or not). The authorship of the action is attributed to the adverse agent, that is, the person in charge of carrying out the adverse intelligence action. Sponsorship of the action is attributed to the State, organization, institution, group or person who conceived, requested, promoted, financed the adverse action or who will make use of its results or gains.

The investigation of the circumstances of the adverse action must occur through the analysis of the inputs gathered and the intelligence knowledge produced in the monitoring phase, as well as the inputs provided by people linked to the potential targets of the adverse intelligence. The counterintelligence professional will seek to gather more data, information and knowledge about the threat, seeking to estimate the objective of the action, at what stage it was carried out and what the damage would be if it were completed. In the case of an action already completed, an attempt is made to estimate the advantages obtained by its sponsor.

After gathering and analyzing this data, knowledge is produced and disseminated to the decision-making body, which will define the course of action to be taken. This instance may be internal or external to the body, depending on the nature of the threat and where and when the intervention will take place. It is at this stage that counterintelligence produces a document informing the decision-making body about the risk represented by the adverse action. This document must contain the necessary elements so that the decision maker can evaluate existing courses of action and deliberate on what to do or not do in the face of the threat. Not acting can also be a line of conduct to be adopted by the decision-maker.

Lines of action must be outlined to counter the threat, which can be requested for advice from the decision-maker. At the end of the evaluating phase, it is expected that counterintelligence will have knowledge capable of informing the decision-maker about the context of the adverse intelligence threat, its nature, stage of development and potential harm caused.

Based on the evaluation, the competent body will decide how to act, according to the best viable course. This action will be carried out by using existing tools, after careful planning. Deciding is the

phase in which the decision-maker, at the appropriate level, defines how to proceed to prevent, obstruct or neutralize the adverse action, be it completed or ongoing. This decision is based on knowledge that considers the nature, authorship, circumstances and potential damages of the adverse action. The complexity of the case, the stage of development of the adverse action and its implications for the country will determine who should decide on counteractions.

Thus, at this stage there is deliberation, by those entitled, on the measures to be implemented in the face of the adverse action, completed or in progress, as well as the order derived from such deliberation. Not acting and not deciding are also possibilities for the decision-maker.

The role to be played by an intelligence professional at this stage is to provide assistance to the decision-making process. The starting point is the assessment made in the previous phase, consolidated in the knowledge produced. Based on this knowledge, it is necessary to decide whether to, on the one hand, interrupt the adverse action or, on the other, not to interfere directly in its development, seeking to observe and misinform the adverse agent. If one chooses to interrupt the action, it will also be necessary to decide whether to expose such action, embarrassing its agents or sponsors; or whether to counter it discreetly.

Important factors to be estimated are the degree of sensitivity and scope of the detected adverse intelligence action. Sensitivity is understood as the property of a certain subject or action to generate tension or harm, if it is unduly revealed and explored. In this sense, the losses arising from the completeness of the action and its disclosure must be carefully evaluated.

The decision is an action of the State, and it is not limited to the intelligence organization. This decision defines whether or not the role of carrying out the intelligence activity will be used, that is, whether the intelligence organization will act to actively counter a threat. The exercise of this function may have an impact on the country's external relations or national interests of various types. Therefore, the decision rests with whoever has the ability to better assess the broader context.

In some cases, the decision may be internal to the intelligence organization. In others, it will necessarily be taken by a different, generally higher, body. Depending on the situation, one of the courses of action to be considered may be not to act, that is, to bear possible losses, if it is understood that they would amount to less than the damages resulting from any action to counteract the adverse action.

When the decision-maker chooses to act and decides that the intelligence agency should take action, there is a second decision-making moment within the agency. The analysis function will be able to trigger the operations function and, based on the agency's capabilities, choose the best course of action to carry out the countermeasure. At the end of the decision-making phase, counterintelligence is expected to have clear and unambiguous guidance on the course of action to be taken to confront the adverse action detected and the threat it represents.

Acting is the phase in which the State adopts measures and procedures to implement what was decided in the previous phase. In the acting phase, depending on the context, more than one course of action can be taken. As in the previous phase, this is a State action that may or may not be limited to the activities of the intelligence professional. Included in this phase are actions to obstruct and neutralize the actions of adverse intelligence; guidance to other bodies to implement actions of this nature; actions aimed at disinformation and deradicalization of potential adverse agents; and monitoring these activities.

Counterintelligence will obstruct an ongoing adverse action when it seeks to prevent its development. To do this, it can act in partnership with the target object of the adverse action, increasing its level of security. Intervention may also be carried out on the adverse agent, seeking to dissuade them from proceeding with the action or making it difficult for them to access the object of interest.

Actions that have already been completed will need to be neutralized. This aims at reducing the advantages obtained by opponents. The nature of neutralization procedures depends on the type of action and the context in which the adverse intelligence is operating.

In some cases, it will be necessary to obstruct the adverse action and neutralize advantages already obtained. An adverse intelligence action can be simple and specific, but it can also be complex and prolonged, consisting of several steps. Therefore, the strategy to counter this action will be equally complex, and will probably consist of more than one stage.

It is also necessary to take into account the capacity of counterintelligence, its resources, abilities and limits. It is possible that obstruction or neutralization actions require the support of other public administration bodies, if one chooses to declare an agent persona non grata, expel them from the country or open an investigation of a crime, for example. Thus, the completeness of the acting phase is not necessarily under the governance of the intelligence agency. The implementation of the action may even be the sole responsibility of other bodies. It is up to counterintelligence, however, to monitor the implementation of the action, to observe its effects and reevaluate it, with the aim of guaranteeing the completeness of the counterposition.

The acting phase is the moment in which the analysis and operations areas work more closely, both to evaluate the best courses of action for counteraction, and to define the control steps to evaluate the course of the action and its effectiveness. Throughout the active counteraction stage, effectiveness measures are evaluated for further development or for the adoption of corrective measures. At the end of the acting phase, it is expected that counterintelligence will have carried out the relevant actions, based on one or more plans to counteract the actions of adverse intelligence.

Once the sixth phase of the Counterintelligence Cycle is completed, a debriefing of the situation is carried out, in which the best practices and flaws observed in the process are listed, with a view to supporting the study on Adverse Intelligence in the monitoring phase, and improving the practice of counterintelligence.

Application of the Counterintelligence Cycle

The objective of counterintelligence is to prevent the success of adverse intelligence actions. It is therefore necessary that profes-

sionals seek to understand these actions, their objectives and purposes and their configurations. The objective of the action is understood to be what the actors intend to achieve upon its completion. Its purpose is the goal that the action serves, i.e. what the sponsor's intended advantage is, that led them to plan the action. Therefore, understanding the nature, dynamics and repercussions of the threat posed by adverse intelligence constitutes one of the fundamental aspects of counterintelligence.

The Counterintelligence Cycle offers a useful methodological framework for the work of professionals in the field, systematizing procedures into phases that interchange and feed back into each other. The monitoring and guiding actions are permanent, independently of the perception of the occurrence of adverse action. The other four phases (detecting, evaluating, deciding and acting) are ideally triggered whenever an adverse action is perceived. The detection of this action establishes a concrete case to be worked on.

The detecting phase is the point of intersection between preventive counterintelligence and active counterintelligence. In the monitoring and guiding phases, the aim is to spot adverse action that has either been planned or implemented. Therefore, concern about detection is present from the beginning of the cycle and must be considered in guidelines and prevention measures. The occurrence of detection is the starting point for the evaluating, deciding and acting phases. Countermeasures are taken in the event of a specific case of adverse action, and begin with such detection.

Once an adverse action is detected, counterintelligence must seek to understand its objective, and the best way to counter it and then act. Once this stage is complete, we return to the monitoring phase to evaluate the effectiveness of the measure taken. At any time in the cycle, the guiding phase can be resumed, as necessary. All phases of the cycle result in new components for the action to follow.

The adoption of obstruction measures can occur at two moments in the cycle. In preventive counterintelligence, these measures are taken to prevent the achievement of an adverse threat in the abstract. In active counterintelligence, they are carried out when the

adverse action is still ongoing. Such measures are tailored to stop the development of this adverse action.

Working in counterintelligence requires integration between the areas of analysis and operations, whose actions complement each other. The development of work throughout the counterintelligence cycle implies a continuous exchange of informational subsidies between the two areas. At the end of each phase, it is desirable to examine the context of the adverse action, and the relevance and effectiveness of the countermeasures taken up to that point. These instances of examination must involve both analytical and operative professionals who are working on the case.

Thus, the counteraction is made through the interaction between analysis and operations in the deciding phase and, subsequently, in the actions carried out in the acting phase. During this phase, in order to assess the effectiveness of the measures, it is necessary for information on both the execution of the action itself and the perceived effects to be discussed between the operations function and the analysis function. At the end of this discussion, new courses of action can be considered.

The application of the Counterintelligence Cycle is the starting point for the formulation of both policies to prevent adverse threats and policies to safeguard knowledge, information, data and the means that store or transmit them; their holders; the areas and facilities of interest to the State and society. The development of such policies must be carried out with the aim of guiding possible targets of adverse intelligence, to prevent and obstruct threats, as well as to open communication channels that enable these targets to activate counterintelligence, in the event of suspected adverse intelligence action.

Having presented the intelligence and counterintelligence branches, we must move on to analysis and operations, which constitute the practical exercise of intelligence activity.

5

The Analysis Function

5. The Analysis Function

Intelligence activity is characterized by the permanent exercise of specialized actions to fulfill two functions: inform and execute. The analysis function is, *par excellence*, the main responsible for fulfilling the informing function.

Analysis transforms inputs, data, information and knowledge into potentially useful products for the national decision-making process. During analytical production, intelligence professionals process these inputs, with the aim of making them suitable for consumption by a decision-maker, through procedures that will generate intelligence knowledge. Therefore, analysis is the essence of the intelligence activity content generation process.

Analysis procedures include identifying, obtaining and selecting inputs of interest, which will be broken down for evaluation and subsequently regrouped into a coherent and useful whole. The externalization of the results of the processing and the resulting interpretation is also part of this process. To generate the final product, intelligence professionals make use of a wide range of procedures, which will be selected and combined according to the available inputs, the nature of the issue to be resolved and the specificities of the production conditions. The analytical effort undertaken to generate the intelligence product will be expressed in the Activity's own format, the language of intelligence.

Such an effort is carried out based on rational or logical principles, supported by evidence and aims to search for truth. This last aspect is a necessary condition for the production of intelligence activity, which aims to assist decision-making in contexts of insecurity and uncertainty. It can only be achieved by overcoming assumptions and pre-notions, on the one hand, and corroborating demonstrable statements, on the other. Therefore, it is important to understand, basically, the process of knowledge construction, in order to favor the conscious production of intelligence knowledge, according to criteria of rationality, truth and demonstrability.

5.1. Theoretical Aspects

Knowledge derives from the combination of three elements: reality, the object of knowledge itself; the perspective of the subject, who builds knowledge by observing and thinking; and inter-subjectivity, originating in the exchange of statements or impressions between the subject and their peers. This third element constitutes the test of knowledge. An analyst may be convinced that his conclusion about a certain problem or subject is true, according to evidence and logic. But only the validation of his conclusions by his peers offers a kind of guarantee, albeit precarious, about the representation of reality as true. This guarantee is very common in everyday life and in the methodical production of knowledge.

It is assumed that there is a reality outside of consciousness, but it can only be perceived in part, according to the subject's perspective. The perspective is a cut-out of the object imposed by the human limits of apprehension of reality. In other words, we are unable to grasp all the infinite dimensions of reality as they are. We have limits of understanding that necessarily lead us to perceive it in a fragmented and incomplete way. In this sense, our understanding of any object is the result of the aspects we perceive. It is important to be aware that there will always be aspects that are not perceived.

Any object (concrete, social, psychological, conceptual) can be approached in different ways. The position from which this object is accessed will modify the way it is captured. In contact with external reality, only part of its composition can be obtained, and this is imposed by the perspective, expressed by the "point of view" or "way of seeing". Consequently, secure knowledge does not only refer to evidence, but also to the exchange of manifest perspectives. This exchange is a kind of test, to find out if what an observer sees corresponds to what others see, that is, if there is consensus. Otherwise, the observer would be trapped in his own perspective and would never be able to be sure about the relevance of his representation of the object.

Perspective depends on three groups of factors: environmental (distance, angle, time, duration, visibility, acoustics, scale, physiological needs such as hunger, sleep, temperature and excretion), psy-

chological (acuity of the sense organs and functioning of the nervous system, which includes here the peculiar ways in which the brain processes stimuli, leading to inevitable cognitive biases, and idiosyncratic conditions such as aptitude and age, among others) and sociological (informal and formal education, culture, class, interpersonal or social relationships, ideals, profession). It is important to move away from any notion that "perspective" is "one's own truth." Perspective is just a point of view, that is, the point from which something is observed and which conditions the representation of the object. Whether something is true or not will depend on tests based on certain criteria such as evidence, logic and debate. Perspective does not make anything the truth; it only limits one's intellectual or cognitive contact with something.

When developing intelligence knowledge, it is important to consider the professional aspect of the perspective. Objects interest (or not) people in different ways, or are interesting to certain groups of people (observers, specialists, dilettantes, curious people) for different reasons. An intelligence professional must approach reality according to a specific socially oriented perspective. Ideally, this perspective factor is expected to compete with – and in some cases, outweigh – other factors. The intelligence perspective is composed of two elements: cognitive field and search for the truth. The cognitive field is the imagined set of objects that intelligence activity is interested in knowing. These are the themes, areas and subjects that should be the subject of the production of intelligence knowledge. The search for truth is the idea of value that guides the approach to these objects, that is, the purpose to know what they are from a dispassionate, impartial and detached approach.

The building of intelligence knowledge privileges the abstract apprehension of the analyzed objects. An intelligence professional approaches the objects, rationally represented, based on a previously formulated question, seeking to establish methodically constructed hypotheses for their interpretation. These hypotheses must be validated by their peers. In this sense, it can be stated that knowledge of intelligence necessarily derives from a rational way of knowing.

Rational ways of knowing

The rational forms that act at the level of knowledge and intelligence include idea, judgment and reasoning. These forms stand out for being decisive for the production of intelligence knowledge, as they make up the content that deals with reality and can then be articulated through language.

The idea is the generalization of a given object, reflecting only its essential aspects (e.g. chair, earthquake, person). It is conceived as a conceptual representation, reflecting essential aspects of the object as a form of generalization. When constructing this type of representation, the intelligible, common and universal characteristics of a class of objects are abstracted, which makes the concept, therefore, valid for all of them. Ideas are the raw material for formulating judgments and reasoning.

Judgment is a relationship between ideas, composing a proposition or assertion about an object (e.g.: wooden chair, 4.5-degree earthquake on the Richter scale, tall person). It is formulated as a relationship between ideas, composing a statement about some real or ideal object, dealing with their relationships or actions. A judgment associates two ideas using verbs. Thus, a judgment is, necessarily, a way of expressing a thought, attributing universal ideas to particular objects, in order to describe them. Logically, the object is the subject of the sentence, and the idea linked to it is its attribute or predicate.

Reasoning is the mental elaboration from which previous judgments allow a new judgment to be logically generated. It usually involves a conclusion (e.g. the chair is made of very dense wood, so it must be fire-resistant). Reasoning is a sophisticated thought process that reveals properties or facts about the object that are not available to immediate apprehension. Judgments from which reasoning starts form the basis of the conclusion, in other words, they are the reasons on which it is based.

Truth

Knowledge is an individual representation that can be justified as true. To do this, it is necessary to determine whether this quality of truth can be attributed to its content. There are three conceptions of truth that make this evaluation possible: correspondence, coherence and consensus.

The first conception considers truth to be a quality of reality external to the mind. It is up to the mind to achieve it. What is true is what exists as such, and truth depends on reality manifesting itself. This conception assumes that there is, in fact, a reality outside the mind, apprehensible through observation and reasoning. True knowledge is constituted by a rational intellectual perception of the truth of the object. The criterion of truth is the adequacy of the intellect to this object. This is the conception of truth by correspondence. The temporal reference of this conception, given that it demands evidence of the object, is the present.

The second conception sees truth as a quality of language developed by the human mind. For this conception, true knowledge is the rigorous and precise composition of discourse which, in its enunciations and argumentation, is capable of generating the impression of fidelity to the facts. The criterion of truth is internal and external coherence, which depends on the rules of correct statements. This is the concept of truth by coherence. It is important to note that the will, in this way of conceiving truth, is a constitutive element of knowledge, since the statement is a human artifact, elaborated by decision and action. It interferes in the relationship between the representation and the object. The subject needs to want to produce a coherent statement. Truth depends on the ability to observe and remember, on the one hand, and, on the other, the ability to formulate statements that seem to correspond to the facts that happened. That's why the temporal reference in this case is the past.

The third conception sees truth as a quality of the similarity of perceptions between interpreters of the object. This conception is based on trust in the sincerity of the people interested in true knowledge, according to agreements and pacts. Its hallmark is respect for

the universal conventions that derive from the fact that we are beings endowed with language, reason and morality. All these elements play an effective role in a community of people who are able to discuss and evaluate representations about the objects they want to know. The value of truth will be attributed, or not, by the members of the community. This is the concept of truth by consensus. The consensus paradigm indicates what should happen with the plurality of perspectives: debate, comparison, criticism, argumentation and, finally, a decision on the truth. The temporal reference of this conception is the future, which is the moment when the truth will be declared.

Truth cannot be achieved in just one of the conceived ways. The search for truth needs to make use of evidence, coherence and consensus, even though these elements have different weights depending on the situation. Depending on the dynamics of conceptions of truth, the representation of an object can be taken as more or less consistent, generating different states of mind, when faced with such a representation of truth: certainty, probability, possibility and ignorance.

States of the mind before the representation of truth

The analysis function aims to search for truth and its representation through the elaboration of intelligence knowledge. Here, truth is understood as the agreement between a fact, event, situation or phenomenon with its respective mental elaboration. However, reality is more complex than human beings have the capacity to grasp. The world perceived by the mind is a simplification, resulting from its sensory limits and its capacity for interpretation. Likewise, material circumstances of perception and understanding of the truth, such as scarcity of resources, sources and deadlines, also contribute to the reduction of the quality of certainty.

In addition to the uncertainties arising from cognitive limits, the way reality presents itself can be obscured by misinformation or dissimulation. The harmful potential of misleading news (fake news) accompanies the exponential growth of mass information through social networks and the technological sophistication of digital resources, which are increasingly cheaper and more accessible. There-

fore, the understanding of the truth does not usually occur fully or sufficiently for full conviction.

There are occasions when the mind completely agrees that the image formed by it corresponds to the object. In others, this agreement is only partial. There are also occasions in which the mind is unable to choose a particular image, when faced with alternative options. Finally, the mind can find itself in a null state in relation to the object, that is, without the ability to create a mental image.

The states or gradations in which the mind can find itself in relation to what it perceives as truth are certainty; probability or opinion; possibility or doubt; and ignorance.

Figure 3: States of the mind in the face of the truth

The gradation of states of the mind in the face of the truth expresses the limits between certainty and uncertainty, with implications for the production of knowledge, which aims to result in true knowledge. In response to the challenge of providing credibility to the advice they offer, intelligence organizations adopt methodological analysis models that seek to reduce errors, mitigate biases and remove ideological influences. Although this procedure is not capable of fully eliminating imprecision, it allows the analysis function to produce knowledge within a regular, uniform and controllable pattern.

One of the solutions provided by analysis methods is the attribution of varying degrees of certainty to the result of the process. Thus, when addressing problems of interest to the State, the analysis function can offer answers with probabilistic assessments in relation to the truth. To be useful, this judgment must be close to a usable degree of certainty, which allows the user a sufficient understanding of reality to make decisions.

Certainty is the state of the mind in which the individual considers that their mental interpretation of reality fully corresponds

to the real object under consideration, that is, the individual understands that they have fully achieved the truth. This agreement is complete due to sufficient evidence to reach the conviction of full compliance. The mind, in this state, believes that there are no significant gaps between the mental image and reality.

If knowledge of the object is based on evidence, linguistic coherence and consensus, the mind tends to accept this representation as true. This position allows the subject to assume knowledge as certain, reaching a state of certainty. As a subjective state, certainty is not guaranteed to have reached the definitive truth about the object. New data and knowledge may show that it is no longer possible to sustain this state of the mind.

Occasionally, even in the absence of some criterion of truth, a state of certainty regarding the veracity of a representation can be assumed. Depending on the case, this is due to the conviction of the subject who knows the object. For example, when there seems to be no probability that those criteria will be refuted by another, this may lead the subject to fully accept their representation of the object as true.

The state of certainty may demonstrate overconfidence on the part of the intelligence professional, as certainty may be illusory. The danger of certainty is that it tends to be absolute. When there is certainty, but the evidence of the reality does not support the mental image achieved, and denotes an inadequate, incompatible or insufficient relationship, there is an error, that is, the illusion of truth.

Probability is the state of the mind in which the individual believes that their interpretation of reality corresponds to the real object, but recognizes that there is some chance of deception. In this state, the elements of conviction – immediate evidence; coherence of statements; or consensus between two or more subjects, who evaluate the representation and assume it as true – are limited and insufficient to reach a full state of certainty. The correspondence is then only partial. It is therefore said that the correspondence is likely to be true.

The state of probability, therefore, is expressed through terms that indicate probability or level of confidence. An example of a tex-

tual description in a state of probability would be: "it is likely that new fires will emerge, due to the high level of illegal disposal of combustible material in conditions of high temperature and low humidity".

Possibility, or doubt, is the state of mind in which there is not enough evidence to support a definitive mental image. The criteria of truth are contradictory in themselves and among themselves. The evidence may not be completely unambiguous, the language that portrays or reports the object may not be coherent internally and externally, debate among peers establishes controversy rather than consensus. It may be that one criterion leads to the refutation of another, without the condition of pointing out which one is correct.

The mind, therefore, is unable to affirm or deny the truth of the representation created by it. One of the objectives of the Knowledge Production Methodology (KPM) is the search for evidence, to increase the degree of credibility of intelligence content, leaving the state of possibility, to reach the state of certainty or probability.

In this state, the truth appears only as possible. Intelligence activity does not use this state in intelligence knowledge. Even though the state of possibility does not constitute intelligence knowledge, in production situations it is normal for this state to be recorded with the purpose of generating indications of hypotheses for future exploration, both by the analysis and the operations functions.

Ignorance is the state of the mind characterized by the complete lack of any image of reality. In this situation, the intelligence professional is unaware of any characteristic or does not have evidence about the object. In the mental state of ignorance, the subject is either unable to form any representation about the object, which is inaccessible to their understanding, or what they have are only data that do not allow them to generate a usable meaning.

Even though an intelligence professional's main objective is to obtain the truth, a wide range of obstacles stand between reality and the best possible representation. Therefore, the production of intelligence knowledge entirely in a state of certainty is the exception, not the rule, because, in the effort to reduce uncertainty through intelligence advice, the most common thing is for solutions to be offered

within a spectrum of probability. As a consequence, in each product delivered to the user, the institutional mission is satisfied by expressing a sufficiently reliable and useful degree of credibility.

5.2. Inputs for Analysis

The preparation of intelligence knowledge consists of the gathering, evaluation, integration, interpretation, formalization, validation and dissemination of different production inputs. These inputs are of four types: data, information, knowledge and intelligence knowledge. There is a relationship of progression and regression between them, the latter being a particular categorization of intelligence activity, which, in addition to being an input, is also the product of analytical work itself.

These inputs must be managed to ensure that they are traceable and auditable, a function for which the processing of metadata is essential. Through them, it is possible to store and retrieve inputs in databases for use in production, as well as to comply with legal requirements and accountability. Metadata are contextualization elements linked to some input, important for the judgment of those who have not yet been evaluated by an intelligence professional. Examples of metadata for knowledge production purposes are: author, origin, equipment used to obtain such metadata, creation date, location, description, modification history, sensor type and accuracy, and format.

Datum

Data are registered or unregistered representations of an aspect of reality with decontextualized meaning. Datum is considered here in its most atomized expression, as the smallest unit of qualitative or quantitative representation of an aspect of reality, without attribution of meaning that goes beyond the direct process of registration. The data can be generated by a person or technical means. Data is normally classified into structured data (such as that organized in spreadsheets and databases) and unstructured data (not organized in

a predefined way, such as that contained in texts, images, videos and audios).

The data are decontextualized because they do not present a broad structure of description – definition, appearance, composition, function or performance –, nor a structure of narration – what, who, when, where, why, how. Their analysis requires, first of all, the effort to identify elements that can be attributed to the composition of description and narration, as appropriate. Here, it is not possible to evaluate it immediately.

In computer science and data science, it is common to refer to data in the sense of a record, a term understood as any unitary record made in a computational system. Thus, data, information, knowledge or intelligence knowledge, when simply stored in a database, is called data for management purposes. A name, the identification code on a vehicle's license plate, the value of a purchase or a rainfall index, considered in isolation, are examples of data.

Information

Information is a registered or unregistered representation of an aspect of reality with a contextualized meaning according to a methodical, rational and objective processing.

Information is the first step towards understanding a fact, event, situation or phenomenon. It results from the processing work (cleaning, correction, selection, crossing, organization, translation, formatting, summarization and ordering) and interpretation of data, ideally with the help of metadata. Information is a record identified by the context of a descriptive or narrative structure, but which does not contain corroboration or demonstration that justifies its capacity to be true. Its analysis requires examining statements and other sources, seeking internal and external coherence. Here, it is possible to evaluate it immediately.

As a result of data processing and interpretation, information has understandable content and meaning. It helps answer questions

such as "what", "who", "when" and "where", and can be generated both by people and by computational means, without human intervention.

A graph that represents links between a person (identified by their name), an address and a specific vehicle (identified by its license plate), produced with the help of software, is an example of information. Likewise, the annual report on deforested area in a given region of Brazil, with records of its monthly evolution, as well as a table made from a sequence of rainfall indices for a given location over a specific period, are also examples of information.

Knowledge

Knowledge consists of a registered or unregistered representation of an aspect of reality with a contextualized meaning assumed to be true and validated.

Knowledge contains the meaning of the observed object, and its decisive property is the belief that this representation is justifiably plausible, that is, credible according to criteria that allow demonstration, verification and replication. Typically, knowledge is a production of specialists (scholars, experts, scientists, analysts, intelligence officers, certain bureaucrats), dedicated to the methodical and systematic study of objects in a certain significant field, being proven by experience, experimentation or application of processes analysis and validation, such as the scientific process. It promotes the understanding or extrapolation of facts, events, situations or phenomena, using reasoning and verification of results.

Knowledge justifies its capacity to be true through diverse, rational and methodological means. Its analysis requires understanding this justification or being based on other resources such as reliability, history, reputation and other people's evaluations. Here, it is possible to evaluate it immediately.

As an expression of the truth, that is, sufficiently coherent with reality, knowledge can be used to make decisions, and that brings it closer to the concept of intelligence knowledge. The proximity comes from the fact that both are the result of a mental process of analysis

and synthesis, involving the identification of cause and consequence relationships, through processes of personal conviction and peer convincing, replicable through the logical relationship of evidence.

Knowledge helps in understanding questions such as "why" and "how", being, until now, the exclusive domain of human cognitive processes. Technical and scientific documents, such as a study that demonstrates changes in the rainfall regime in a given region over the last 15 years, are examples of knowledge.

Intelligence knowledge consists of a registered or unregistered representation of an aspect of reality contextualized and assumed to be true according to methodical procedures of intelligence activity, useful for the decision-making process. Intelligence knowledge is characterized, in comparison to the concept of knowledge, by its purpose, which is to serve the Brazilian State, and by its production, which uses its own procedures. The production of intelligence knowledge occurs through the application of the Knowledge Production Methodology (KPM), although it may involve other complementary techniques and methodologies.

5.3. Intelligence Knowledge

The informational function of intelligence activity is materialized in the production of intelligence knowledge, a type of representation characterized by addressing objects for advising the national decision-making process, considering the reasons for the Democratic Rule of Law, with a focus on the interests of the people. This knowledge results from the application of methodical procedures typical of intelligence activity which, in turn, enable its content to be assumed as true.

As a product, intelligence knowledge must be true, timely and useful, that is, a real or probable representation of reality, delivered in a timely and useful manner to a user with decision-making power. It can be narrative-descriptive, interpretative and interpretative-prospective, according to the following attributes: rational way of knowing, through the presence of judgments or judgments and reasoning;

and temporality, by considering past, present, immediate future and distant future.

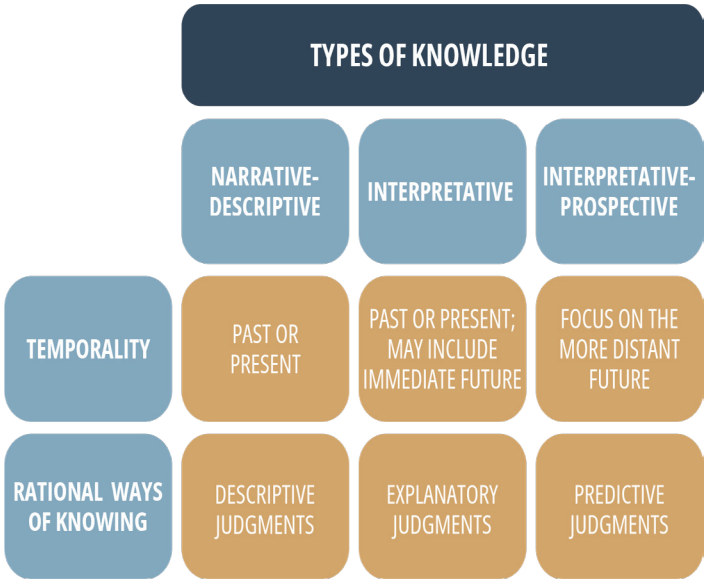


Figure 4: Type of Knowledge, Temporality and Way of Knowing

Narrative-descriptive intelligence knowledge, traditionally called a report, is the result of judgments about past or present facts, events, situations or phenomena. It is restricted to narrating or describing objects of analysis, either because the request received so guides production, or because the evidence gathered did not allow for the elaboration of reasoning. A report on a terrorist attack about which there are still no elements for interpretation in a state of probability or certainty is an example of narrative-descriptive knowledge. Similarly, a report produced by the operations function, which merely describes the dynamics of a past or ongoing demonstration, in response to a request from the analysis function, is also an example of narrative-descriptive knowledge.

Interpretive intelligence knowledge, traditionally called an appreciation, is the result of judgments and reasoning about past or present facts, events, situations or phenomena. This type of knowledge allows the projection of objects of analysis into the immediate future, expressing trends or developments. However, this projection is

not prospective in nature. An intelligence report on the political-electoral framework of a South American country, which projects probable immediate impacts for Brazil, resulting from the upcoming results of a presidential election, is an example of interpretative knowledge. Likewise, a report that narrates and describes an act of sabotage and, through the evaluation and interpretation of evidence, indicates a degree of probability regarding its authorship or sponsorship, is also an example of interpretive knowledge.

Interpretive-prospective intelligence knowledge, traditionally called an estimation, is the result of judgments and reasoning about the future unfolding of facts, events, situations or phenomena, with a focus on the distant future. Due to its nature, it requires the use of additional techniques to the KPM (see item 7.2). An intelligence report that presents different scenarios about the impacts of the climate crisis on the Brazilian agro-industrial sector over the next 15 years is an example of interpretive-prospective knowledge. Likewise, a report that demonstrates which – and how – factors influence the future achievement of a desired scenario in the context of combating organized crime in Brazil, within a five-year horizon, is also an example of interpretive-prospective knowledge.

Intelligence activity works with four temporal situations: past, present, immediate future and distant future. The present considers an object in its current temporal state, in a probable process of evolution. In intelligence knowledge, the immediate past is considered as present time, that is, the immediate moment before its dissemination. The past considers an object whose evolution is thought to be complete.

The future tense, in turn, considers an object whose emergence or evolution is likely to occur at a later time, which may be in the immediate future or the distant future. The immediate future deals with the emergence or evolution of this object in a close range of time. Typically, short time periods are considered. The distant future considers an object whose emergence or evolution is likely to occur in even more distant projected time frames or wide ranges of time in the future. Due to the complexity of constructing future scenarios, the

further they are projected in time, the more complex the estimation techniques for treating the future are.

5.4. The Analysis Cycle

The production of intelligence knowledge is a cyclical process, composed of a sequence of interrelated procedural steps. This process, the analysis cycle, generates products that respond to a formulation of interest to the State or society, through the transformation of data, information and knowledge into intelligence knowledge. The varied techniques used to enforce the process have, in common, tasks that consist of identifying and gathering inputs, examining and interpreting them, to compose the product to be delivered to a specific user, meeting parameters previously established in planning.

The analysis cycle describes the logical development of intelligence knowledge, which begins in a specific production situation and ends with the user's evaluation of the product. Questions of national interest are transformed, via a logical-argumentative process, into aspects to be answered. The answers are subjected to veracity confirmation procedures, and finally integrated into a set that aims to meet a specific gap in the decision maker's knowledge.

Although guided and executed by analysts, the analytical cycle integrates the efforts of intelligence professionals from different areas in addition to those specialized in analysis, such as operational search, human sources management, administration and information technology and support units such as logistical, financial and administrative units.

The production situation that initiates the knowledge production process can be an external trigger (by an authority or similar body), or a scheduled assignment in an intelligence plan or an initiative by the unit itself. Different production situations impose different production needs, which are broken down in the planning.

The analysis cycle is fed back by the historical generation of content. Each request that is answered tends to generate new production situations, whether due to an external request, the need to

change work plans or an increase in the analyst's need to follow up. Regardless of the level of completeness of the previous response, new plans are created, activated sources continue to produce content and open processing fronts continue to operate. Likewise, receiving the user's evaluation tends to trigger new analysis cycles.

This cycle is carried out by the Intelligence Knowledge Production Methodology (KPM), used by different Brazilian intelligence agencies. This methodology allows the use of additional techniques and resources in a complementary way, according to the premises and needs of each production situation.

Every process of producing intelligence knowledge begins with the identification of a request for advice, which can come from three sources: external requests, which are those triggered by a user, authority or institution seeking to elucidate an issue; internal requests, which are those triggered by a request from a hierarchical superior, an authority within the institution or an internal production plan; and the agency's own initiative, when the request comes from an intelligence professional themself, when they identify a threat or opportunity for national interests.

After identifying the production opportunity, the professional proceeds to apply the KPM, starting with the planning phase. At this stage, the production proposal must be approved by their immediate superior. Approved planning formalizes production and guides the mobilization of resources and the control of processes and results.

Then, the intelligence professional proceeds to execute what was planned, starting with gathering inputs. During production, the main procedures of each phase, as well as their results, are recorded for future retrieval.

In the end, once the intelligence knowledge has been obtained and disseminated, good practices, mistakes and lessons learned are recorded to be incorporated into the next production cycles, and the production team is demobilized.

Intelligence Knowledge Production Methodology (KPM)

KPM is made up of six phases: planning; meeting; evaluation; integration and interpretation; formalization and validation; dissemination and results.

Although the KPM phases are presented in chronological sequence, in practice they do not imply strictly ordered procedures, nor do they have precise limits. These are phases that interpenetrate, interrelate and are interdependent. Still, all of them must be complied with, for the full realization of intelligence knowledge, and most of their procedures are necessary.

These procedures can take place in sequence, in parallel or they can overlap, depending on factors such as the composition and organization of the team, deadlines and production circumstances. Despite acknowledging the existence of specific realities, it is important to characterize each phase of the KPM.

Figure 5: Intelligence Knowledge Production Methodology (KPM)

Planning phase

It is the phase in which the planning of the work to be developed is prepared, based on a request for knowledge production. This is a fundamental phase for the entire process, as it is here that the intelligence professional defines the scope of their work, production conditions, activities to be carried out and team needs.

The planning phase comprises the proposition and approval of the following definitions: Subject; User; Goal; Study time limits; Deadline; Essential aspects; Preliminary indication of secrecy; Dissemination formats; Expectation of actions to be carried out; and Team Proposal.

When a request comes from an external, hierarchically superior user, or is scheduled in the institution's strategic plans, several of these definitions may be partially determined, as in the case of subject, user, purpose and delivery time, and the intelligence professional is the one responsible for evaluating the adequacy of these conditions and for making any necessary adjustments.

When a request is the result of an intelligence professional's own initiative, it is up to them to propose all the aforementioned definitions, always keeping in mind aspects such as relevance, opportunity and usefulness for the user.

Among the steps necessary for planning, are: defining the subject and the essential aspects. Defining the subject implies formulating a question, in a thematic area, that needs to be answered. This initial subject is usually a provisional determination, since its perception by the intelligence professional may change during the production process.

Defining the essential aspects consists of determining subsidiary questions to elucidate the issue formulated from the subject. The essential aspects are questions about elements that make up the object of knowledge, the answers to which clarify the defined subject. They are divided into two types:

- Known essential aspects: questions about the subject whose answers are already in the possession of the intelligence professional, as a result of the evidence he already has on the object; and
- Essential aspects to know: questions about the subject to which no answers have yet been obtained or which still require further investigation. The essential aspects to know are the main motivators for collecting and searching for evidence in the gathering phase (see item 5.1.2).

Even after approval by higher authorities, planning can and should be revised throughout the entire production process, both due to changes in conditions and circumstances, and due to the emergence of evidence that changes the initial perception of the subject matter.

Gathering phase

It is the phase in which actions are undertaken to obtain and prepare inputs with the purpose of responding to the essential aspects to be known, that is, the questions listed in the planning phase, that aim to elucidate the problem formulated on the basis of the subject matter.

These inputs can be data, information, knowledge or even other intelligence knowledge, gathered according to a gathering plan. The gathering phase is divided into two stages: formulation of the gathering plan; and execution of the gathering plan, taking measures to obtain and process inputs for the evaluation phase.

The gathering plan aims to guide efforts to collect and search for inputs, without being restrictive or imposing, serving as a guide for collectors' activities.

Gathering actions are procedures carried out by intelligence professionals to obtain the necessary inputs to produce intelligence knowledge. They are divided into collection and search actions. Collection consists of specialized actions to obtain inputs, carried out or activated by the intelligence professional allocated as collector. Examples of collection actions are: consultation of databases, national and

foreign counterparts, individuals, units of the agency; research etc. Search consists of specialized actions, carried out by the intelligence operations function, using operational techniques, to obtain unavailable data, information and knowledge, after all other means of collection have been exhausted. Search actions normally involve situations of high sensitivity, risk and complexity.

All inputs gathered in the gathering phase, based on the meeting plan, must go through two verification steps, carried out by the collector themself. The relevance check is confirmation that at least a fraction of the input gathered is relevant to resolving the issue. In turn, the significance check consists of confirming that at least a fraction of the input responds to at least one essential aspect.

If a fraction of the input responds to both the subject and an essential aspect, that fraction is considered a significant fraction and should be separated for evaluation at a later stage. Both the original input and its extracted or delineated fractions and their metadata must be recorded as input for the evaluation phase, ideally in a database.

Evaluation phase

This is the phase in which the inputs gathered in the gathering phase are evaluated, resulting in a credibility rating for each input evaluated. It is undertaken by an intelligence professional in the role of evaluator.

The evaluation phase comprises four steps:

a. Validation of relevance and significance: the evaluator will check whether the fractions are relevant to the subject and significant for one or more essential aspects, that is, whether the fractions outlined in the inputs are significant fractions.

b. Verification of existing credibility: the evaluator will check, if the input being processed is intelligence knowledge (or a fraction of this knowledge) which was previously produced, what level of credibility they assigned to it. If the previous assessment remains valid,

there is no need to re-apply the Data, Information and Knowledge Assessment Technique (DIKAT) to these fractions. Occasionally, however, the evaluator may identify the need to reevaluate fractions of intelligence knowledge in light of new facts or evidence that was not then known, for example. In these cases, the evaluator must carry out a new evaluation, once again applying the DIKAT to the knowledge inputs in question for a new credibility determination.

c. Validation of metadata: the evaluator will check and validate the metadata concerning to the inputs.

d. Application of the Data, Information and Knowledge Assessment Technique (DIKAT): the evaluator will apply the DIKAT to the selected inputs, in order to establish a degree of credibility to significant fractions.

The aim of DIKAT is to assign a degree of credibility to the inputs of intelligence knowledge production by means of an intelligence professional's evaluation of all types of inputs, be they data, information or other knowledge.

There are two assessment steps to complete the DIKAT:

a. Source evaluation: verification of aspects related to the source of the input, with the purpose of establishing a suitability classification, which is valid only in relation to the specific input obtained. This assessment is revised for each new input authored by the source. The aspects here considered are: authenticity, trust and competence.

b. Content evaluation: verification of aspects of the input content, with the purpose of establishing a veracity classification for this content. The aspects considered here are: internal coherence, compatibility and external similarity.

After evaluating both source and content, through the application of DIKAT, the evaluator is able to determine the credibility of the significant fractions and establish whether they are in a state of possibility, probability or certainty. In cases where the degree of probability

or certainty is reached, these significant fractions become considered fractions of intelligence knowledge, capable of being integrated into new intelligence knowledge.

Integration and interpretation phase

It is the phase in which the subject matter is clarified, that is, the provision of answers to the question defined in the planning. To this end, fractions in a state of certainty or probability are analyzed, integrated and interpreted, generating coherent textual elaboration that allows the subject matter to be clarified. In this sense, this phase is characterized by analysis and synthesis efforts.

Analysis is the mental operation that involves the breaking down of a whole into its constituent elements, with the purpose of understanding the function of each element in the set. Synthesis is the mental operation in which the composition or recomposition of a whole is conceived from already analyzed constituent elements, providing a coherent and understandable set.

Clarifying the subject matter in the integration and interpretation phase can occur in two ways. By simple integration, which occurs when the integration of significant fractions in a narrative-descriptive text is sufficient to elucidate the problem or issue. And by interpretation, when, in addition to the integration of significant fractions, it is necessary to respond to formulated hypotheses, which implies the construction of arguments and conclusions, based on the evidence presented.

Simple integration occurs when the question defined in the subject matter requires a merely descriptive-narrative answer, without the construction of arguments and conclusions. In this case, the product is restricted to the use of judgments, without explicit reasoning.

Interpretation occurs when, in addition to the process of integrating significant fractions that describe the object, the evidence found is used to construct arguments that support (or argue against) hypotheses, resulting in conclusions. In this sense, interpretation goes beyond the limits of the object under analysis, going beyond

mere description or narration, and offers interpretive content (appreciation) or interpretive-prospective (estimation) as a product. In this process, based on the judgments that highlight aspects of the object, an intelligence professional infers derivative judgments (reasoning). This extrapolation of the object allows the intelligence professional to infer identities, causes, responsibilities, consequences and future developments of facts, events, situations or phenomena.

The conclusion offers a full or partial solution to the problem expressed in the subject matter. Its construction involves the development of reasoning by inference (deduction or induction), necessarily linked to evidence present in the text.

Formalization and validation phase

This is the phase in which, considering the dissemination formats proposed in the planning, the proofreading and final formatting of intelligence knowledge, and its analytical and technical validation, are carried out. The formalization and validation phase comprises three stages: proofreading, formalization and validation.

Proofreading is the checking of the textual composition as a whole - grammatical correctness, internal logic, suitability for intelligence language, presence of biases, suitability for the user, etc. This is a less formal process and is usually carried out by the analyst in charge, as well as by other available intelligence professionals. It takes place before the formalization and validation phases.

Formalization is the final formatting of the document, with the insertion of formal elements of identification, control and security. It consists of a technical process that involves applying specific formatting to intelligence knowledge. It is the stage in which intelligence knowledge is consolidated into an official document, in accordance with internal regulations and relevant legislation, including an indication of secrecy.

Validation is the rigorous verification of the final product, regarding analytical and technical aspects, in order to ensure that the intelligence knowledge has been produced with methodological rigor,

and meets the quality standards required for dissemination to the user. This is a formal process, necessarily carried out by an intelligence professional from outside the production team, with sufficient competence to understand the topic and to judge the methodology and procedures used in its preparation. The role of the validator implies a portion of responsibility for the product, which is why validation must be formally registered before subsequent bureaucratic processes.

Dissemination and results phase

It is the phase in which procedures are carried out for the dissemination of intelligence knowledge, as well as the evaluation of results to improve subsequent production cycles.

The dissemination and results phase is divided into two stages: Dissemination, when intelligence knowledge is made available to the user and to internal units of the agency, and Results Evaluation, which includes evaluation of production processes and product evaluation.

The dissemination process occurs after registration of validation, by the validator, and approvals for dissemination, by the production manager and their hierarchical superiors. Dissemination to the user is done through secure means, physical or digital, observing the principles of opportunity and security. Dissemination can be done through textual documents, audio, image or video files, graphics with consolidated data or via synchronous face-to-face or remote meetings, among other available means. When on digital platforms, dissemination to external users occurs in parallel with the availability to potentially interested production units, internal to the body, and with the provision of knowledge for research and archiving in internal systems.

In the results evaluation stage, a general assessment of the production carried out is made, with the aim of promoting continuous improvement in future production cycles, and providing metrics for improving management processes. There are three processes to be carried out, in sequence:

a. Process evaluation: carried out with the assistance of the entire production team and by considering comments provided by the validator. Process evaluation provides for personal feedback from each team member (production manager, responsible analyst, collectors, data preparers, evaluators, support analysts, reviewers) on their impressions, regarding the production process, to identify problems faced and opportunities for improvement.

b. Product evaluation: carried out based on an assessment of intelligence knowledge carried out by the user. It is based on the interpretation, by the analyst in charge, of the results of the evaluation carried out by the user on aspects of quality and opportunity and on the practical results of intelligence knowledge, after its consumption.

c. Final evaluation report: carried out by the analyst in charge, based on process and product evaluations. The KPM cycle ends only after the final assessment report has been completed. This report contains the interpretation of the results of process and product evaluations, in addition to recording metrics and impressions for institutional use. Once completed, the report is made available to the unit responsible for production and other team members, so that lessons learned, problems detected and best practices can be used in future production cycles.

5.5. Analysis Support Techniques

KPM can be used together with accessory techniques and other additional resources, whenever the production team deems it necessary. These techniques must be used in a complementary manner, respecting the procedures recommended by the KPM. Examples of analysis support techniques include structured analytical techniques, expert consultation methods, visual analysis resources and collection techniques.

Structured Analytical Techniques (SAT)

Structured Analytical Techniques are additional tools to traditional intelligence production methods, which have historically developed through intuitive analyses, based on logical thinking and available evidence. These techniques do not seek to replace knowledge production methodologies, such as KPM, but are used in harmony and in addition to them. Thus, the results of its application are submitted to the KPM itself before being integrated as intelligence knowledge into final products.

The use of SAT provides systematic means to externalize individual mental processes, which allows analytical work to be subject to the control and scrutiny of peers, reviewers, superiors and validators, making the process more transparent and less exposed to cognitive biases and other deficiencies in intuitive thinking.

There are several SATs listed in specific manuals, available to the general public, useful for intelligence analysis work. The choice of a certain structured technique, by an analyst or production team, must take into account, among other issues, the type of problem that the professional or group intends to face, or the type of cognitive bias that they want to mitigate. To this end, there are techniques aimed at generating ideas, breaking down and visualizing elements, challenging hegemonic analytical lines, creating scenarios and indicators, generating and testing hypotheses, among other examples. Some examples of SAT are:

Brainstorming

Brainstorming is a technique designed for use in groups, to generate new ideas and stimulate creative thinking, according to specific rules and steps that guide the process. It is recommended for identifying multiple variables, factors, actors, hypotheses, possible solutions to problems, creating scenarios, etc. The presence of people relatively unrelated to the topic is useful, to avoid the predominance of the "groupthink" bias. The results of brainstorming still need to

be subjected to other methods and specific evaluations, they are not immediate solutions for analysts.

Cross impact matrix

It is an idea generation technique, recommended for the initial phases of an analysis project, when the analyst or analysis team is still seeking to understand a complex situation. It consists of listing in a simple matrix several variables identified in relation to the problem under analysis, in order to discuss how each variable interacts with the others. The impact of this interaction can be positive, neutral or negative and with greater or lesser intensity. Recording the group discussion around the matrix in text makes it easier for everyone on the team to understand how premises, arguments and conclusions were constructed throughout the process.

Chronology and timeline

These are decomposition and visualization techniques, indicated above all for analyzing subject matters that are systematically monitored over time. It consists of placing facts and events in chronological order, in order to identify possible patterns or correlations, the existence or not of causes and effects, trends, anomalies, key events and knowledge gaps.

Network analysis

It is a visualization technique used mainly to monitor the activities of individuals, mapping networks, interactions and connections between people, groups and other entities of interest. The large volume of data and information in certain contexts usually requires the support of specific computer programs, as well as staff training, to interpret the links, as it is up to the analyst to attribute meaning to the graphs and diagrams generated by the application of this technique. It comprises at least two specific techniques: creating network graphs and social network analysis (in English, Social Network Analy-

sis – SNA). SNA involves the mathematical measurement of variables and mapping of relationships between people, groups, organizations, computers, URLs, IPs, and other connected information entities. In this context, entities are generally called nodes and the relationship between them is called a link.

Indicators

It is a technique designed to provide warnings about future events, to identify emerging trends or unwanted changes in scenarios under monitoring. Its use is recommended for monitoring situations or phenomena of interest, whenever it is necessary to evaluate or anticipate changes in the situation over time, in order to foresee unwanted scenarios, for example. It consists of drawing up a list of indicators, that is, observable or potentially observable factors whose simultaneous occurrence indicates the probability of a certain fact, event, situation or phenomenon materializing. This list of indicators serves as a guide for gathering actions and its constant monitoring contributes to the generation of alerts at a strategic, tactical or operational level.

Devil's Advocate

It is a technique designed to challenge established lines of analysis, mental models or analytical consensus. It consists in designating a person or team to develop consistent arguments contrary to a certain proposition or conclusion. Its objectives are to encourage the consideration of other possible explanations for facts or events, verify the plausibility of arguments and evaluate opposing hypotheses and evidence.

Red Hat

Red Hat is a technique designed to help understand how other actors or adverse agents tend to act or behave in certain situations. It is useful in monitoring extremist groups, criminals or foreign leaders.

Its use is recommended when you want to avoid cultural mirroring, that is, the natural tendency of human beings to imagine that others share their own or their group's view and experience of the world. It consists of simulating a context in which the opponent or competitor is inserted, in a given situation, by putting yourself in the other person's shoes. This technique requires in-depth knowledge of the target's language, culture and personal history.

Competing hypothesis analysis (CHA)

It is one of the best-known techniques for developing and challenging hypotheses. It is recommended for analyzing complex situations, in which there are multiple factors and evidence that can support different arguments, alternative explanations and contradictory conclusions. It consists in relating evidence to propositions in a matrix, in order to compare them to verify consistency relationships. The aim is to refute – and not ratify – each hypothesis listed, which helps to avoid confirmation biases. The process of developing different plausible hypotheses for the same situation under analysis also helps to explain the uncertainty present in most of the issues addressed by the intelligence activity. The application of CHA seeks to make the analyst aware of this, also contributing to the reduction of these uncertainties in analytical work.

In addition to the structured analysis techniques mentioned above, it is also relevant to highlight different ways of incorporating expert consultation and the use of analytical techniques.

Consultation with experts

There are specific questions that, due to their complexity or particularity, go beyond the knowledge or capacity of a given intelligence professional or production team to provide adequate answers. There are also cases in which the agency's analysts do not have the empirical data necessary to analyze a problem, but other entities, researchers or professionals can collaborate in generating these

inputs or filling these gaps. In these cases, the intelligence body may resort to the assistance of experts outside its own staff.

This resource generally takes place through questionnaires sent to different experts, in which the expert is asked to evaluate variables or key topics, assigning, depending on the case, subjective judgments about the probability of occurrence of certain events, for example. Specific procedures are adopted both for formulating the questionnaires and for processing the responses obtained. Different methods can be used in these situations, including some used in academic and scientific circles.

The inputs generated from a consultation with experts will still have to be evaluated, according to the KPM, through the TAD, before being integrated into intelligence knowledge in production. Some examples of techniques or methods for consulting experts are the Delphi Method and Bayesian Inference.

The Delphi method allows for collective communication and, occasionally, the gradual building of consensus between geographically separated experts. It consists in drawing up a set of questionnaires which are answered in sequence and individually by the participants. With each new round of consultations, the respondents have access to a summary of the group's responses to the previous questionnaires, thus creating the possibility of an indirect dialog between the experts, and the formulation of a collective response to a given problem, as each participant has the opportunity to refine, change or defend their own ideas to the researchers. It can be used to gather opinions on trends or anticipations of future events, in the production of interpretative-prospective knowledge, for example.

Bayesian Inference is used in the field of statistics to support data-based decision-making in the face of uncertainty. The objective is to estimate the probability of an event happening, based on an initial event. This technique allows an expert's subjective responses to be processed and updated after that person is exposed to new evidence, contributing to obtaining more accurate results. It requires analysts to have in-depth knowledge of mathematics and statistics, and to be familiar with the method. Depending on the complexity of the problem, it requires the assistance of specific computational resources.

Visual analysis

The increasingly common use of visual and computational resources for processing data, information and knowledge opens a new field for analytical activity, and offers new ways of presenting and disseminating the intelligence knowledge produced. Thus, it is possible to interpret large volumes of collected and structured data, with the aim of enhancing predictive analysis. The use of some of these resources requires specific training from analysts and, sometimes, also some prior knowledge on the part of users. The assistance of tools that help the analyst to organize inputs and generate succinct and attractive visual presentations of intelligence knowledge for users is recommended in certain situations, such as in the current monitoring of dynamic events, in which new inputs obtained or generated feed a database of data, and change the situation at every moment.

Collection Techniques

As a specialized action, collection must be methodical and carried out using different techniques that aim to obtain the inputs that will be analyzed. Open source intelligence, for example, uses techniques that seek to discover new inputs relevant to a research question, based on keywords and operators, and may depend on Application Programming Interfaces (API). Among these techniques is Data Scraping, which involves systematic extraction to gather specific patterns or data, usually focusing on web pages. To this end, tools are used that access the coding of these pages, identify the desired data, such as texts, images and links, and organize the collection in a structured format.

5.6. The Language Used in Intelligence

Knowledge of intelligence is expressed through oral or written language, which gives discursive form to thought. Despite being dependent on the specific context in which the product is generated, the language used in intelligence has characteristics of its own, such

as simplicity, objectivity, conciseness and neutrality. These peculiarities make it possible to distinguish an intelligence report from other types of written production, such as academic, journalistic, rhetorical, legal or literary texts.

This means that the success of an analyst's work, when turning knowledge as a process into knowledge as a product, depends on their ability to mobilize linguistic resources for the benefit of the logical and objective representation of reality. The intention is for the text to convey a message in as few words as possible and to be clear enough to allow the user to grasp its object in a single reading. To achieve this objective, an intelligence professional must be proficient in the language in which he or she expresses themselves. Semantic inaccuracies, syntactic inaccuracies and stylistic inadequacies compromise the credibility of the product and the image of the organization.

However, it is not enough for the text to be grammatically correct. Methodological aspects, such as evidence built on facts and conclusions based on logical processes, provide precision, coherence, objectivity and impartiality to the process and its result. This contributes to ensuring the characteristics of impersonality and neutrality that characterize intelligence content. An analyst's ability to choose the best analytical technique and apply it appropriately in the production of knowledge is, therefore, at the origin of the quality that characterizes the language used in intelligence.

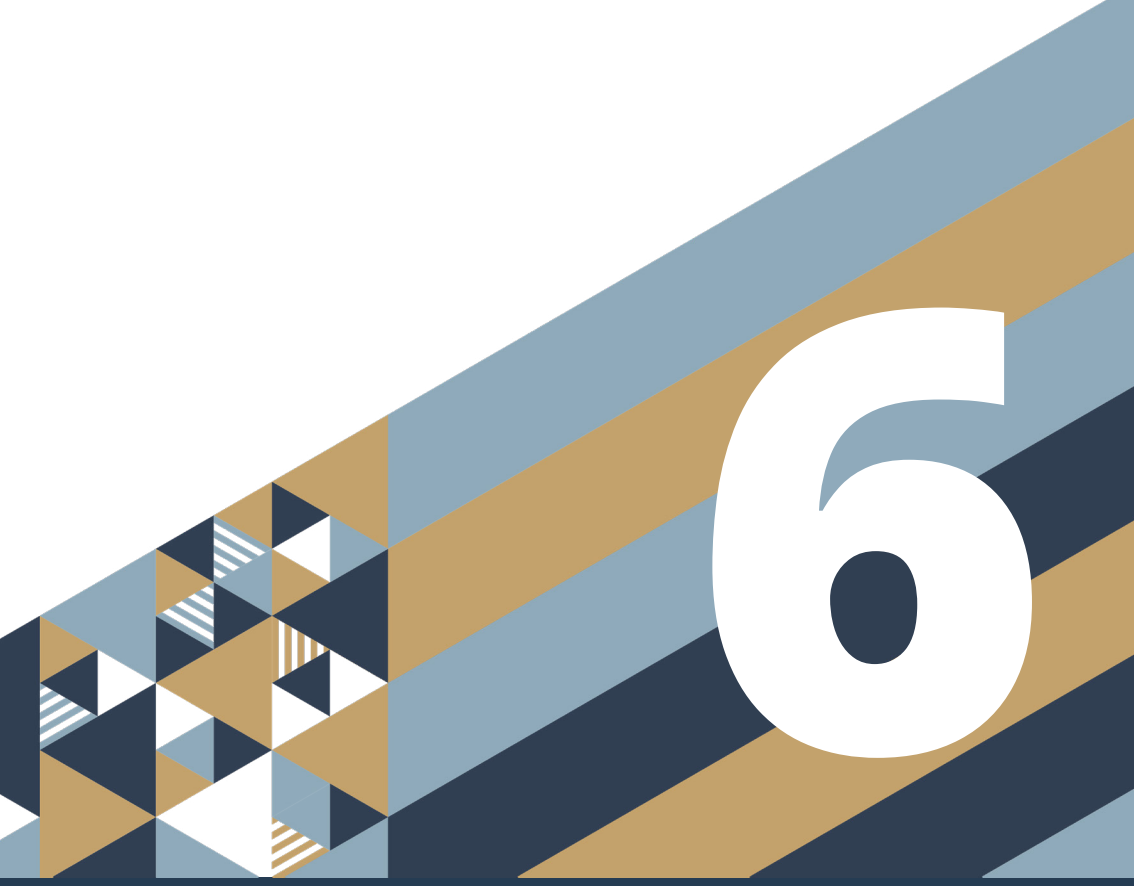
In processing the inputs gathered, the language used in intelligence is the resource that expresses the degree of credibility attributed to the evidence integrated into the knowledge. The cross-referencing of this evidence gives rise to conclusions, also expressed linguistically in degrees of certainty or probability, according to the analyst's conviction. Thus, in order to convey to the user the answers to the problem formulated in the subject, the intelligence professional makes use of the verb tenses corresponding to the results found throughout the process. The faithful and reliable representation of reality therefore depends on the quality of the language used.

The use of language resources to express the degree of credibility of a given representation should derive naturally from the rigorous application of KPM. Expressions such as "it is probable that", as well

as verbs in the future tense, serve to attest to probability in relation to the evidence and conclusions to which they apply, integrating them into the content of intelligence. On the other hand, judgments and reasoning that do not go beyond the qualitative degree of possibility are not considered satisfactory to make up the product to be disseminated and are sent back to the beginning of the processing phase to improve their level of confirmation. This set of methodological procedures provides the precision and objectivity that characterize the language used in intelligence.

Thus, the study of phenomena related to the language use in intelligence aims not only to make knowledge clearer and more useful, but above all to avoid manipulation that alters the representation of reality in favor of personal, organizational or ideological interests. Disciplines from different areas contribute to the development of the analyst's skills in the field of language, such as Portuguese (grammar and writing, and proofreading), linguistics (discourse analysis, content analysis and textual linguistics), communication (written expression and storytelling), psychology (perception, cognition, mental models, heuristics and cognitive biases), statistics and data analysis. This knowledge gives intelligence professionals more confidence, when dealing with language, and ensures that the knowledge produced is more reliable.

After describing how analysis is organized and how it works, it is time to specify the other way in which intelligence activity is carried out, operations.



6

The Operations Function

6. The Operations Function

Intelligence activity is characterized by the permanent exercise of specialized actions to fulfill two functions: inform and execute. The operational function is, *par excellence*, the main responsible for fulfilling these functions.

Intelligence operations are the unique way in which intelligence activity acts in the world. This action is mainly focused on obtaining inputs for the production of intelligence knowledge and the production of events. Freely accessible data, information and knowledge can be collected using prospecting techniques in open sources, without the need for operational action on the part of intelligence professionals. There are, however, unavailable inputs, that is, they are difficult to obtain, either because they are located in environments with restricted access, or because they are protected by whoever owns them. Obtaining these types of input requires the use of specialized operational actions, which are confidential, due to their nature.

Intelligence operations can also be used in the production of events, aimed at implementing measures to counter adverse actions, carried out within the scope of the counterintelligence branch. This condition is imposed by the fact that adverse intelligence, whenever it operates, uses specialized actions that cannot be avoided by an individual who is not trained in them.

In both the informational and executing functions, the use of intelligence operations is a way of circumventing obstacles, in order to achieve certain objectives in an adverse context.

The use of secret actions by the Brazilian State is provided for in articles 3 and 4 of Law 9883/1999 and in the National Intelligence Policy, established by Decree 8763/2016. Its main purpose is to gather and then disseminate data, information and knowledge in a timely manner in order to support the production of intelligence analysis and the decision-making process, helping to achieve the interests of the Brazilian society and the State. Intelligence operations are carried out after the operational planning has been expressly approved by the agency's highest authority, or by the authority to which the

prerogative has been delegated. This approval requires the exercise of judgments on the legitimacy of intelligence operations. To this end, criteria must be considered to ensure compliance with the law, thematic relevance of the objects being monitored and the reasonableness and appropriateness of the resources to be used. Operations, like all of ABIN's intelligence activities, are subject to the same procedures established by law for internal and external control of compliance, quality and impact.

6.1. Theoretical Aspects

The use of the operations function is characterized by action in the field, with the secret use of human and technological resources, in physical or virtual environments, in a planned and coordinated manner. Therefore, the work of intelligence professionals in this field is always potentially risky. For this reason, their actions require trained personnel, detailed planning and careful execution, as well as strict compliance with the legal precepts governing the Brazilian State, its sponsor.

Components

An operative is the person who takes action to achieve the objectives of an operation. They may belong to the intelligence agency, an in-house agent, or a person employed to execute or facilitate the execution of a certain action, without formal links with the agency. In this case, they will be classified as an external agent.

In-house agents are duly qualified in the use of specialized operational techniques, and are tasked with obtaining unavailable data, information and knowledge or carrying out actions to detect, identify, obstruct and neutralize adverse actions. External agents are identified, approached and trained to carry out their actions. They are permanently subjected to specific control measures, designed to reduce the safety risks to which they are subjected, and evaluate the quality of their work.

An operational action is the application of these specialized techniques. In this sense, the technique is the procedure and method to be used and the action, the act of using it.

A target is the object on which the covert action acts to fulfill its objective. Based on the target, its characteristics and the context in which it is inserted, the necessary actions are established to obtain the expected result of the operation. The target is usually the person who holds the desired data, information or knowledge. In the case of counter-actions, the target will be the person carrying out the adverse action or the means used to achieve that action. They can be located in physical or virtual environments, at home or abroad. Targets can be characterized as simple objects, when they are easily delimited and qualified, or as complex objects, when they are diffuse and difficult to determine. Operational action on complex objects requires a systemic and multifaceted approach and usually requires the execution of multiple covert actions.

An intelligence operation, being made up of more than one action, may have more than one operational environment. Furthermore, depending on the dynamics of the operation, it is possible that new environments will need to be incorporated into the initial planning. Therefore, it is important that room be made for adjustments and adaptations that may be necessary when an action is being carried out.

Operational techniques are specialized procedures and methods for employing personnel and material in covert actions. Intelligence professionals working in operations must be continuously trained in the use of these specialized techniques.

Action, Operation and Operational Cases

Operational actions are the covert use of specialized operational techniques to achieve a previously determined objective based on a request received from the client. Intelligence operations are the planned and coordinated use of operational actions, each with an objective. Ideally, the achievement of the objectives of the actions

employed leads to the accomplishment of the operation's mission, i.e. a satisfactory answer to the request that generated it.

There are situations in which the operational fraction works on requests that require the use of more than one intelligence operation, either due to the complexity of the issue being addressed, the diffuse condition of its targets, or the multiplicity of factors that influence the context of the operation and the operational environment. This situation leads to the establishment of operational cases.

Operational cases are the planned and coordinated use of intelligence operations around a specific theme with multiple missions and targets. In other words, an operational case is worked in a defined, usually complex context, with multiple, and sometimes also diffuse targets, which require the use of different operational efforts.

Functions

A search is the combined application of operational techniques to obtain unavailable data, information and knowledge. It is required in the gathering phase of the Analysis cycle, and differs from the collecting phase, which implies the collection of data, information and knowledge, without the application of operational techniques.

A search is generally used when the desired data, information or knowledge cannot be obtained by overt means. This may be because it is necessary to conceal the intelligence agency's interest in obtaining this data, information or knowledge; or because it is not located in publicly accessible places; or because it is under the protection measures of its holders, in which case it is referred to as denied data.

An event production is the set of actions carried out in a secretive manner, aimed at producing events to meet the objectives of intelligence activity. The main use of this type of action is aimed at detecting, identifying, obstructing and neutralizing the work of adverse intelligence, which occurs in the context of the counterintelligence branch.

Finally, operational action can also be used for protection. Occasionally, in case the planning or even the changing reality of the

operational environment needs to be altered, it will also be necessary for the operations function to carry out the Protection function. This involves using complementary measures to protect the integrity and identity of the agents employed, the secrecy and objectives of the operational action and the intelligence agency itself.

Client and User

A client is whoever activates the operations function, bringing in the request that will define the objective of the operational actions to be used. A client can be the organization's analysis function or the manager of the operations function itself, according to clearly established and administratively justified working relationships and procedures.

A request received from a client usually needs clarifying or resizing, during the planning of an operational action. Similarly, the needs of the intelligence activity are dynamic and it may be necessary to change the initial objectives, during the course of operational actions. Therefore, the dialogue between the operations function and the client must be systematic throughout the operation, so that the relevant adjustments can be made in order to achieve the best results. Any adjustments to the operations plan must be duly recorded and justified administratively, and are subject to the same internal and external controls as intelligence activities as a whole.

A user is the final consumer of the result of the operational action, in accordance with a hierarchical chain, and well-established and auditable administrative procedures. It is the person for whom the knowledge that will be produced from the data, information or knowledge obtained by the search is intended. The users of Brazilian national intelligence are the government authorities, at their respective levels, and in their legally defined areas of responsibility.

6.2. Types of Actions

Intelligence actions are classified according to their purpose, nature and scope. Purpose indicates the goal of the operation. Nature refers to the resources and operational methods primarily applied. Scope expresses the extent and duration of the operation.

Purpose

In relation to their purpose, intelligence actions are classified as search actions, which include the execution of operational actions aimed at obtaining unavailable data, information or knowledge; event production actions, which include the execution of operational actions aimed at creating events, mainly in the context of the counterintelligence branch; and protection actions, which include the execution of operational actions aimed at protecting the agent and the operation.

Nature

In terms of nature, actions can be of the following types: human resources-based action, when they prioritize the specialized use of human resources; technical resources-based action, when they prioritize the specialized use of technical resources, and cyber action, when they take place in cyberspace, and can combine the use of human and specialized technical resources in the same action.

Range

In terms of scope, the actions are classified as exploratory, which consists of carrying out specific actions, providing specific results at a given time, with a pre-established start and end, or systematic, which consists in carrying out continuous actions, resulting in a constant flow of data, with a pre-established start and an undetermined end.

The type of action to be carried out depends on the adequacy between the requirements of the objective to be achieved, the characteristics of the target, the safety of the agents involved and the available resources. Regardless of the type of action to be employed, it should be noted that its planning must seek integration in the application of human and technological resources available to the operations function, aiming to comply with the principle of opportunity as much as possible, with minimal risks and careful evaluation of costs.

6.3. Operations Cycle

Intelligence operations begin with a request from a client, justified on the basis of the need to produce timely and relevant knowledge for users. Once the request has been received, an intelligence professional is assigned responsibility for planning the operation and maintaining communication with the client. This professional usually carries out a situation study to support their planning of actions. They also manage other professionals in their sector who are involved in the operation. This professional will be the operations function's main interlocutor with the client, with whom they must maintain constant communication, in order to evaluate results, understand and reassess requests. This is the professional in the operations function who works closest to the analysis function.

The results obtained from operational actions must be disseminated in a timely manner. This allows the analysis function to contextualize and interpret the data, information and knowledge obtained

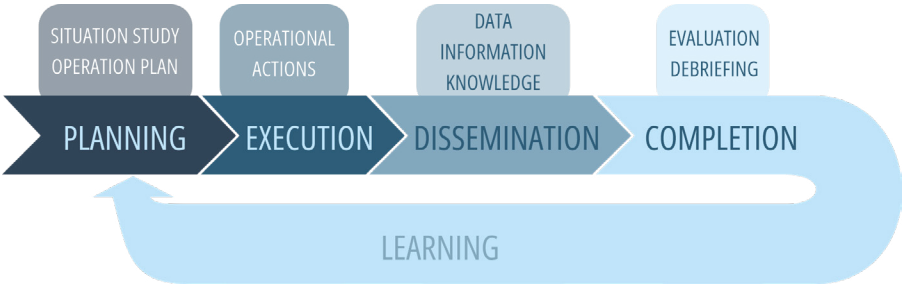


Figure 6: Operational cycle

more quickly, facilitating timely advice for the decision-making process. It also makes it possible to broaden the understanding of reality, which can result in new requests on the part of the client or even the user.

Each intelligence operation follows a cycle composed of four phases: planning, execution, dissemination and completion. These phases have flexible limits, allowing, whenever necessary, changes resulting from the development of confidential actions.

Planning

This is the phase of the operational cycle in which the professional in charge assesses the request received and systematizes the work to be carried out, establishing the composition of the necessary resources and the way to conduct operational actions to achieve their objectives with minimum expenses and risk.

Operational planning should be carried out in stages with as much detail as possible, seeking to establish realistic and appropriate actions to achieve the desired result. In this sense, each time a request is made, it must be carefully analyzed, and if possible always consulting the client. Actions must then be meticulously planned, according to the operational reality, assessing the feasibility of executing each one and prioritizing them according to the logic that makes it possible to optimize and speed up deliveries. Finally, the defined operational resources must be prepared for the deployment that will take place in the next phase.

At the end of the planning phase, the operations function is expected to have understood the objectives and missions that are to be achieved, have an approved preliminary plan of how to carry them out, and be ready to start executing them.

Execution

This is the phase in which the actions established in operational planning are carried out, with the aim of fulfilling the mission.

The professional in charge of the operation coordinates the covert actions, verifying their development, assessing the results obtained and evaluating the need to alter the previously planned actions.

The management of operational activity must guarantee the correct allocation and management of available resources, with a view to maximum safety and excellence in operational performance. To this end, it is essential that tasks be correctly distributed among the agents involved.

The use of the operations function in highly complex contexts, which include actions related to complex adaptive systems, requires the agents involved to act with resilience and the ability to adapt quickly to changing behavioral patterns. In other words, the team in the field must also be able to act as a complex adaptive system. This requires high sensitivity to changes in their targets and operational environments, and constant reprogramming of planning, as well as good internal dialogue within the operations function. Therefore, among the main characteristics of an intelligence operation in complex contexts are flexibility, adaptability, the possibility of customization and the incremental improvement of its actions.

After the action has been carried out, an evaluation meeting is planned, in which the procedures carried out, the results obtained and the difficulties encountered are presented and examined, as well as the level of exposure of agents, equipment and support facilities. At the end of this phase, it is expected that the actions outlined will have been carried out, and the professional responsible for the action will be able to present the results obtained from the operational action.

Dissemination of the results obtained

This is the phase in which the results of the operation are disseminated to clients, generally by the professional responsible for the action.

During the course of the mission, the operational action team processes the results obtained and disseminates the data, information or knowledge found or intelligence produced to the client, using ana-

lytical techniques. Depending on the complexity of the operation, the data, information or knowledge obtained or produced can be broken down into gradual deliveries, according to the periodicity established in the initial planning and the prioritization of the action's objectives and mission requirements.

The evaluation of clients and users after each delivery, as well as constant interaction between the professional responsible for the operation and the customer, are essential for re-planning subsequent operational actions. The results obtained can be communicated to the client via formal text documents, secure messaging channels, oral reports and other means that might be necessary and appropriate. At the end of this phase, the client is expected to have received the results of the operational actions, and assessed their relevance, completeness and usefulness.

Completion

This is the phase in which the end of the case or operation is determined. It can be terminated for the following reasons: fulfillment of the mission; expiry of the stipulated time limit; a decision from a higher level official; or a reduction in acceptable safety levels.

Closing an operation or operational case requires carrying out a general assessment of the actions taken, their consequences, successes and failures, called final debriefing. When necessary, procedures must be defined to mitigate, with maximum discretion, any negative impacts on the user, the agency or agents involved.

The operations function must pay special attention to knowledge management, when conducting specialized actions, which includes: the sharing of information about the development of actions with the team; the correct treatment of data, information and knowledge obtained; quality control levels; and the preservation of institutional memory. Periodic meetings, held throughout operational efforts, are important tools for the operations function to learn, in the search for continuous improvement and adaptability, which should guide the work of its professionals.

Whenever relevant, collaborative management or project management tools must be used by in-house agents in these segments to assist in planning, conducting and controlling operational actions. Furthermore, the systematic use of this type of tools facilitates the construction of institutional memory and experience base for the operations function. In this sense, the documents used in operational activity must be objective, complete, clear and simple, both when describing the results of the actions and when expressing the plans carried out and the management and control mechanisms used.

At the end of this phase, it is expected that the operational actions will have been completed, and that the professional responsible for these actions will have conducted a consistent assessment of the overall results obtained, listing the technical, human and managerial difficulties faced, the engagement and relationship between the various actors and fractions involved, and any other aspects they deem relevant. The evaluation of the execution of the operation, in which any opportunities for learning and successes are highlighted, should be taken into account in subsequent planning of operational actions, with a view to a process of constant learning and refinement of the intelligence professionals at work.

6.4. Operational Techniques

Operational techniques are specialized methods and procedures, used in the execution of covert actions, which are typical of intelligence activities. Each technique has a specific purpose, for which it employs the available operational resources in a characteristic way.

Their use is a necessary instrument for overcoming obstacles to obtaining unavailable data or counteracting adverse actions. Due to their peculiarities and objectives, their exercise requires detailed planning and careful execution.

Operational techniques are rarely used in isolation. On the contrary, they are usually applied simultaneously or consecutively. Their employment must be carried out in strict compliance with con-

stitutional guarantees and prerogatives and current legislation, and they are subject to internal and external control.

7

Final Considerations

7. Final Considerations

Intelligence activity has become an essential State institution for States to operate in the international environment, since the second half of the 20th century. The emergence of non-state actors, such as criminal organizations and extremist and terrorist groups, has broadened the traditional scope of intelligence agencies, adding themes to their internal work that go beyond protection against the actions of adverse intelligence.

Today, intelligence agencies work on a wide range of topics, such as technological changes, environmental issues, large flows of people and economic markets. The purpose of analyzing such diverse topics is the same: to deliver reliable and timely knowledge to government authorities. Based on this knowledge, these authorities will be able to make more informed decisions about public policies, taking advantage of opportunities, and mitigating threats to the achievement of national interests.

No country that wants to be relevant in the international arena can do without strong and active intelligence agencies, aimed at promoting the fundamental objectives of the State. The strength of any institution is anchored in its legitimacy of action, which, in democratic States governed by the rule of law, is conferred by respect for the legal order in force in the country, and the mechanisms of political, administrative and social control to which all institutions must be subject.

The Brazilian intelligence service is governed by ethical precepts, and by the impersonality of its actions. Its professionals are continuously trained to carry out their work, analysis and operations, always seeking the common good as their ultimate goal.

The intelligence activity of a democratic country serves its people. This activity operates based on the requests presented by elected rulers, instructed by what they believe to be the interests of the State, and acting under the control of its parliamentary representatives. Thus, it is a reflection of the society in which it operates, of

the ways in which power is exercised in this society, and of the priorities of its leaders.

8

Glossary

8. Glossary

This glossary defines ABIN's understanding of key intelligence terms. It therefore aims to facilitate consultations and promote the consolidation of a common vocabulary and shared understandings among intelligence professionals, without prejudice towards other definitions and concepts existing in related areas and different social and institutional contexts.

A

Access: possibility or opportunity to obtain classified data, information or knowledge, resulting from official authorization, issued by a competent authority or from overcoming safeguard measures.

Accessory techniques: techniques used to support, in a complementary way, the production of intelligence knowledge, respecting the procedures recommended by the KPM.

Accreditation: official authorization, granted by a competent authority, which entitles a certain person to have access to data, information or knowledge at different levels of secrecy.

Acting: phase of the intelligence and counterintelligence cycles in which the State implements the decision taken in the deciding phase.

Adaptability: principle of the operations function, which states that the planning and execution of operational actions must allow for the rapid and efficient implementation of adjustments and redirections that may be necessary.

Adverse action: intentional action, whether sponsored or not, that opposes the achievement of national interests, seeks access to knowledge, information and sensitive data or threatens the security of the Brazilian society and the State.

Adverse actors: States, organizations, groups or people who have an interest and capacity to act in the context of each of the counterintelligence aspects.

Adverse intelligence: activity carried out by a State or non-State agent, using specialized actions, to promote the interests of its sponsor, through undue or unauthorized access to data, knowledge, people, areas or facilities, or using techniques designed to change perceptions and behaviors of the State and society, to the detriment of national interests.

Adverse propaganda: set of actions carried out using social communication techniques and methods to, in some way, persuade target audiences and influence their attitude, opinion, emotion and behavior.

Agent: person in charge of acting to achieve the objectives of the operational action, who may belong to the intelligence agency (in-house agent) or may be a person employed to execute or facilitate the execution of a certain action, without formal links with the agency (external agent).

Alert intelligence: classification by time frame of intelligence production, aimed at anticipating events that could impact the achievement of constitutional objectives, national order or the security of society and the State.

Alert: warning issued by intelligence activity that aims to anticipate events that may impact the achievement of constitutional objectives, national order or the security of society and the State, which contains the evidence that led to the issuance of the alert, as well as a description of the anticipated threat and its likelihood of occurrence. (See also: alert intelligence).

Analysis Cycle: cyclical process composed of a sequence of interrelated procedural steps, aimed at generating products that respond to a formulation of interest to the State or society, through the transformation of data, information and knowledge into intelligence knowledge. (See also: Intelligence Knowledge Production Methodology)

Analysis Function: a constituent sector of intelligence activity responsible for the production of intelligence knowledge, whose professional work involves the collection and gathering of inputs, analysis, processing and dissemination of the result to the competent authorities.

Analysis of competing hypotheses (ACH): technique for developing and challenging hypotheses, suitable for analyzing complex situations, in which there are multiple factors and evidence that can support different arguments, alternative explanations and contradictory conclusions.

Analysis: mental operation that involves breaking down a whole into its constituent elements, in order to understand the function of each element in the whole.

Analyst in charge: role performed by an intelligence professional in charge of production management, and primarily responsible for the final product.

Analyst: role performed by an intelligence professional who carries out production activities, under the supervision of a production manager.

Antagonisms: threats that intentionally oppose the achievement of national interests.

Authenticity: condition of identifying who produced, sent, modified or destroyed a given piece of knowledge, information or sensitive data.

Availability: 1) condition attributed to data, information or knowledge, that it is available and usable upon request by a specific person, organization, system or entity. 2) principle of the operations function which recommends that this sector should be structured in such a way as to enable its immediate activation whenever necessary, with the maximum scope possible, considering the threats listed in the directive instruments of intelligence activity.

B

Basic intelligence: classification of intelligence production by purpose, aimed at building a set of foundations and references, to understand and contextualize the issues being monitored, as a subsidy for other analyses with a more defined focus.

Bayesian inference: a method based on Bayes' formula, used in the field of statistics, to support decision-making based on data in the face of uncertainty, the aim of which is to estimate the probability of an event happening, based on an initial event.

Brainstorming: technique designed, for use in groups, to generate new ideas and stimulate creative thinking, according to specific rules and steps that guide the process.

Brazilian Intelligence System (Sisbin): system established by Law 9883/1999, made up of bodies and entities under the terms of Decree No 11693/2023, which can directly or indirectly produce knowledge of interest to intelligence activities. (See also: Intelligence Community and Intelligence System)

C

Channel: sender through which data, information and knowledge reaches the intelligence organization.

Chronologies and timelines: decomposition and visualization techniques, particularly suitable for analyzing subjects that are systematically followed over time.

Collection: specialized action aimed at obtaining freely accessible data and information.

Collector: role performed by an intelligence professional responsible for collecting and recording inputs and their metadata.

Compartmentalization: restriction of access based on need to know.

Compromise: loss of security resulting from unauthorized access.

Consultation with experts: resource used by intelligence professionals to address specific issues that, due to their complexity or particularity, go beyond their knowledge or professional capacity.

Control: general principle of intelligence activity that determines supervision over all intelligence activity actions, in order to guarantee the conformity of its means and sound purpose of its application.

Cooperation: general principle of intelligence activity that prescribes the collaborative conduct of all intelligence activity work.

Counterinsurgency: branch of active counterintelligence that advocates the adoption of measures and procedures aimed at detecting, identifying, evaluating, obstructing and neutralizing adverse actions by insurgent individuals and groups.

Counterintelligence (CI): branch of intelligence activity that aims to prevent, detect, identify, obstruct and neutralize adverse intelligence and actions that constitute a threat to the safeguarding of data, knowledge, people, areas and facilities of interest to the security of society and the State.

Counterintelligence branch: a branch of intelligence activity that carries out specialized actions aimed at preventing, detecting, identifying, evaluating, obstructing and neutralizing adverse intelligence activities, including actions that constitute a threat to the interests of society and the State, to the decision-making process, to the safeguarding of sensitive knowledge, information and data, the means that hold them or in which they transit, their holders and their areas and facilities.

Counterintelligence cycle: cycle composed of six phases, characterized by actions: monitoring, guiding, detecting, evaluating, deciding and acting.

Counterterrorism: branch of active counterintelligence that advocates the adoption of measures and procedures aimed at detecting, identifying, evaluating, obstructing and neutralizing adverse actions by violent extremist individuals and groups.

Covert promotion of groups and entities: action that aims, in a veiled manner, to create, structure, finance, co-opt or maintain groups or entities that promote the interests of the sponsor.

Critical infrastructures: facilities, services, goods and systems whose total or partial interruption or destruction would have a serious social, environmental, economic, political, international or security impact on the State and society.

Critical thinking (I): ability to analyze an object with clarity and rationality, using grounded approaches to interpret it in an impartial, reflective and ethical way, based on the construction of arguments based on reliable data, information and knowledge, and factual evidence.

Critical thinking (II): principle of the analysis function that recommends that the analyst must maintain high criticality regarding their own understanding of reality.

Cross-impact matrix: idea generation technique, recommended for the initial phases of an analysis project, when an analyst or an analysis team is still seeking to understand a complex situation.

Current intelligence: classification by time frame of intelligence production, aimed at keeping decision-making authorities, continuously updated on events and situations in progress and their evolution.

Cyber intelligence: area of intelligence focused on issues related to cyberspace, the production of which seeks to support Brazil's actions in the face of cyber vulnerabilities and threats, the informing of public policies and State plans in this area, as well as the monitoring and the evaluating of the capabilities, intentions and activities of external actors in cyberspace.

Cyber operational action: operational action that takes place in cyber space and can combine the use of specialized human and technical resources in the same action.

D

Data, Information and Knowledge Assessment Technique (DIKAT): technique aimed at assigning a degree of credibility to the inputs of intelligence knowledge production through the evaluation of all types of inputs by an intelligence professional, be they data, information or other type of knowledge.

Data: registered or unregistered representation of an aspect of reality whose meaning is decontextualized.

Debriefing: evaluation meeting on intelligence activity actions, held after its completion, in which best practices and observed failures are discussed, from which the professionals involved are supposed to learn and the institution is supposed to improve.

Deception: intentional manipulation of the characteristics of a given object or data, information, knowledge, either real or not, to disguise the capacity or intention of the action or mislead an adversary.

Decision-making: phase of the cycles of the intelligence and counterintelligence branches in which the user will define the course of action to be taken, in light of the knowledge disseminated to them.

Declassification: cancellation, by the competent authority or due to the expiration of a period, of a classification, which will make data, information or knowledge ostensible.

Degree of secrecy: gradation attributed to data, information, knowledge, materials, systems, areas and facilities considered to be confidential, due to their nature or content.

Delphi method: method that allows collective communication and, occasionally, a gradual building of consensus between geographically separated experts, consisting in drawing up of a set of questionnaires that are answered in sequence and individually by participants.

Denied data: informational element that is under the protection of its holder, whose access by the intelligence agency requires the use of operational techniques.

Deradicalization: reversal of the radicalization process of extremist or insurgent groups or people.

Detecting: 1) discovering an adverse action which has either been planned or carried out, which has been completed or is ongoing, and understanding its characteristics. 2) phase of the counterintelligence cycle in which possible adverse activities are detected, be they completed or ongoing.

Devil's advocate: technique designed to challenge established lines of analysis, mental models or analytical consensus, consisting of designating a person or team to develop consistent arguments contrary to a given proposition or conclusion.

Diplomatic Intelligence: intelligence activity aimed at anticipating positions to be taken by other countries, that may impact the achievement of national interests.

Disinformation: set of actions that deliberately disseminate false information, with the aim of deceiving or confusing a specific target audience to cause harm, mislead or manipulate a situation or event in favor of the sponsor's interests.

Dissemination and results: KPM phase in which procedures are carried out for the dissemination of intelligence knowledge, as well as the evaluation of results, to improve subsequent production cycles.

Doctrine: a set of concepts, methods, processes, norms, principles and values that guide and discipline the exercise of intelligence activity, standardizing and regulating procedures.

Document: unit of recording data, information and knowledge, whatever the support or format.

Domestic intelligence: area of intelligence activity focused on topics that are entirely within the State's intervention competence, respecting the country's political and legal situation.

E

Espionage: any activity aimed at the unauthorized acquisition of sensitive, confidential or classified data, information or knowledge to benefit States, groups of countries, organizations, factions, interest groups, companies or individuals.

Evaluating: 1) action that consists of analyzing, integrating and contextualizing a threat and its actual and potential damage to Brazil. 2) phase of the counterintelligence cycle in which the objective of the adverse action is considered, its modus operandi, its probable sponsors and the consequences of its possible implementation for the target country are considered.

Evaluation: phase of the KPM in which the inputs gathered in the gathering phase are evaluated, resulting in a credibility rating for each input assessed.

Evaluator: role performed by an intelligence professional responsible for applying the evaluation phase procedures to inputs that have not yet been evaluated by an intelligence professional, as well as recording the results of the evaluations.

Event production operational action: comprises the execution of operational actions aimed at creating events.

Event production: actions carried out in a confidential manner that aim to produce events to meet the objectives of intelligence activity.

Events: occurrences which can be geographically and chronologically delimited by specific landmarks. (CDI)

Execution function of intelligence activity: that which will execute previous decisions within the scope of the State's foreign policy. In the context of counterintelligence, it seeks to obstruct and neutralize actions carried out by adverse intelligence.

Explanatory intelligence: classification of intelligence production by time frame, aimed at continuously advising the national decision-making process on facts, events, situations and

phenomena that may represent threats or opportunities to the achievement of the State's fundamental objectives.

Exploratory operational action: consists of carrying out specific operational actions, providing specific results, with a pre-established beginning and end.

F

Facts: verifiable occurrences that can be described or predicted and measured by anyone, using appropriate references or methodologies.

Financial resources: capital available to carry out a secret action.

Foreign intelligence: area of intelligence focused on topics over which the State has little or no decision-making power or unilateral intervention, and which requires international positioning strategies for negotiation and achievement of national interests.

Foreign interference: deliberate action by governments, interest groups, individuals or legal entities that can influence the political course of the country, with the aim of favoring foreign interests to the detriment of national ones.

Formalization and validation: KPM phase in which, considering the dissemination formats proposed in the planning, the proofreading and final formatting of Intelligence knowledge, and its analytical and technical validation are carried out.

Freely accessible data, information and knowledge: unprotected information elements, freely accessible to anyone who wishes to obtain them.

G

Gathering: phase of the KPM, in which actions are undertaken to obtain and prepare inputs, with the purpose of responding to the essential aspects to be known, that is, the questions listed in the

planning phase, that aim to elucidate the problem formulated about the subject matter.

Geoint: acronym in English for Geospatial Intelligence. See: geospatial intelligence.

Geospatial intelligence: classification of intelligence data by origin, based on images and geolocation data obtained to describe, evaluate and visually represent physical characteristics or geographically referenced activities. (See also: Geoint)

Guiding: phase of the counterintelligence cycle, in which instructions are offered to those responsible for potential targets of adverse interest, seeking to make them aware of their need for protection, in order to avoid or minimize losses to the State and society.

H

Human intelligence: classification of intelligence data by origin, based on data, information and perceptions originating from reports made by individuals or brought by them. (See also: Humint)

Human source: person who is a source of data, information or knowledge. (See also: Channel; Source; and human intelligence)

Humint: acronym in English for Human Intelligence. See: Human intelligence.

I

Idea: generalization of a given object, reflecting only its essential aspects.

Identifying: attributing the authorship or co-authorship of an adverse action to an agent (person or entity), including as an intellectual mentor or sponsor.

Image intelligence: classification by the origin of the Intelligence data, based on data and information obtained through the

production of photographic and multispectral images. (See also: Imint)

Imint: acronym in English for Image Intelligence. See: Image intelligence.

Impartiality: principle of the analysis function, that determines the impartial approach to the objects of analysis, in order to prevent value judgments, arising from interests, personal convictions or preconceived ideas, from distorting the results of production.

Indicators: a technique designed to provide warnings about future events, to identify emerging trends or unwanted changes in scenarios under monitoring, among others.

Indispensability: rule that operational planning and execution must observe, regarding the operational means and techniques, chosen as necessary alternatives to fulfill the objective of the confidential action.

Information: recorded or unrecorded representation of an aspect of reality, with contextualized meaning according to methodical, rational and objective processing.

Informational function of intelligence activity: that which is responsible for informing the State about matters of interest to it.

Informing: phase of the intelligence branch cycle, that takes place whenever the team responsible for monitoring a given area notices the occurrence of a fact, event or situation that should be reported to the competent authorities, either because it helps with the situational diagnosis, or because it requires the State to take action.

In-house security: activity responsible for implementing security measures, prevention measures and, whenever relevant, countermeasures.

Input preparer: a role performed by an intelligence professional, who is responsible for the initial processing of collected inputs, if necessary, as well as cleaning, correcting, checking for gaps and

inaccuracies, summarizing, correcting formats, translating and organizing, to facilitate evaluation and analysis.

Insurgency: rebellion against an established power carried out or planned by a group formed or supported by a portion of the population.

Integration and interpretation: KPM phase, in which the subject is clarified, i.e. answers are provided to the question defined in the planning. To this end, fractions in a state of certainty or probability are analyzed, integrated and interpreted, generating coherent textual elaboration, which allows the subject to be clarified.

Integration: 1) in counterintelligence, it includes measures that take into account the context of the object of adverse interest, seeking to encompass not only the institution, group or person that may be subject to the adverse action, but also those who facilitate access to the object and may favor the agent. 2) the principle of the operations function, which advocates that its action must be integrated, in an orderly, systematic and continuous manner.

Integrity: condition attributed to data, information or knowledge attesting that it has not been altered or destroyed in an unauthorized manner.

Intelligence activity: permanent State activity, exercised through the use of specialized techniques and actions aimed at producing knowledge, which constitutes an instrument for advising successive governments, with a view to state security and the well-being of society.

Intelligence analysis: set of actions developed by the analysis function of an intelligence organization, whose responsibility is to produce and disseminate knowledge, to assist the decision-making process and government action. (See also: analysis functionand knowledge production)

Intelligence body: nonstop structure responsible for the professional exercise of intelligence activity. (See also: Intelligence service and Intelligence fraction)

Intelligence branch cycle: cycle made up of five phases, characterized by actions: setting an objective, monitoring, informing, deciding and acting.

Intelligence branch: branch of intelligence activity, that aims to produce and disseminate to the competent authorities knowledge: concerning facts, events, situations or phenomena, taking place inside or outside national territory, of immediate or potential influence on the decision-making process and government action, which constitute or indicate opportunities or threats to the fundamental objectives of the State.

Intelligence community: group formed by intelligence organizations that establish cooperative relationships. (See also: International Intelligence Community, Intelligence System and Brazilian Intelligence System)

Intelligence fraction: section in charge of carrying out intelligence activity, in bodies that have other purposes. (See also: Intelligence body/organization and Intelligence service)

Intelligence knowledge: recorded or unrecorded representation of an aspect of reality that is contextualized and assumed to be true, according to the methodical procedures of intelligence activity, that is useful to the national decision-making process.

Intelligence Knowledge Production Methodology (KPM): methodology that covers the entire analysis cycle, consisting of six phases: planning; gathering; evaluation; integration and interpretation; formalization and validation; dissemination and results. (See also: Analysis Cycle)

Intelligence operations: set of operational actions aimed at obtaining unavailable data, information and knowledge, in addition to implementing measures to counter adverse actions, as a way of circumventing obstacles and achieving objectives, within a context of adversity.

Intelligence plan: document that guides actions aimed at complying with the National Intelligence Policy, and serves as a parameter

for organizations that carry out intelligence activities to prepare their specific plans.

Intelligence services: bodies whose sole purpose is to carry out intelligence activities. (See also: Intelligence body and Intelligence fraction)

Intelligence system: set of intelligence bodies of a State, subject, in whole or in part, to regulations that govern their interaction. (See also: Intelligence community and Brazilian Intelligence System)

International intelligence community: group formed by all intelligence services active in the world. It is divided into sub-communities. (See also: Intelligence Community)

Interpretative intelligence knowledge: knowledge resulting from judgments and reasoning about past or present facts, events, situations or phenomena, allowing the projection of objects of analysis into the immediate future, expressing trends or developments, but not prospective in nature.

Intrusion: introduction of agents into an adverse environment, in a physical or digital environment, to detect actions, identify adverse agents and influence their behavior.

J

Judgment: Relationship between ideas, composing a proposition or assertion about an object.

K

Knowledge: recorded or unrecorded representation of an aspect of reality with a contextualized meaning, that is assumed to be true and validated.

Knowledge production: an intellectual process, in which human capacity, aided by its own methodology, makes it possible to produce specialized and structured knowledge based on

data, duly evaluated and analyzed, to meet the requests of the decision-making process, at any of its levels.

L

Leak: unauthorized disclosure of confidential data, information and knowledge.

M

Masint: acronym in English for Measurement and Signature Intelligence. See: Measurement intelligence.

Material: substance, model, prototype, mold, machine, equipment or the like, that represents data, information and knowledge.

Measurement intelligence: classification by the origin of intelligence data, based on data and information obtained by measuring certain types of emanations, such as seismic and thermal, generally resulting from event signatures, such as atomic explosions. (See also: Masint)

Metadata: contextualization element linked to a record, be it data, information, knowledge or intelligence knowledge.

Military Intelligence: intelligence activity aimed at assessing adversaries with whom the country it serves may engage in a warlike conflict, seeking to obtain data, information and knowledge about their enemy's disposition, movements, the morale of their troops, and about the terrain and climatic conditions, in which the confrontations will take place.

Monitoring: phase of the intelligence and counterintelligence cycles, which involves the constant process of planning, gathering and processing data, information, and knowledge on the subjects in question.

N

Narrative-descriptive intelligence: knowledge resulting from judgments about past or present facts, events, situations or phenomena, restricted to narrating or describing objects of analysis, either because the request received so guides production, or because the evidence gathered did not allow for the elaboration of reasoning.

National decision-making process: set of actions, carried out within the scope of the Executive Branch, that culminate in the choice of government objectives, the formulation of policies and the definition of strategies to achieve or maintain them.

National Intelligence Policy (PNI): the highest level document guiding the country's intelligence activity, conceived in the light of the fundamental values and principles enshrined in the Federal Constitution, the obligations arising from treaties, agreements and other international instruments to which Brazil is a party, the conditions of the country's international insertion and its social, political and economic organization.

National interests: the society's desires and aspirations that contribute to Brazil's progress, and the achievement of well-being, security and defense for all citizens, preserving them for the enjoyment of future generations.

National objectives: identification of needs, interests and aspirations, that our nation seeks to satisfy.

Need to know: 1) availability of significant fractions extracted from data, information and knowledge, to the extent necessary, so that the intelligence professional can carry out his activities with due accuracy and comprehensiveness. 2) condition inherent to the effective exercise of a position, function, employment or activity, essential for the holder of a security clearance to have access to confidential data, information or knowledge.

Network analysis: visualization technique, used mainly to monitor activities of individuals, to map networks, interactions and

connections between people, groups and other entities of interest.

Neutralization: reduction of the impact caused by an adverse action, seeking to reverse or mitigate its results, which can be carried out by using specialized actions, such as counter-propaganda, disinformation, compromise of the adverse agent and controlled leakage of information to the media.

Neutralize: nullify or mitigate the effects of a completed or ongoing adverse action.

O

Objectivity: general principle of intelligence activity that prescribes orientation towards clear and delimited objectives, on the part of intelligence professionals, avoiding unnecessary efforts and waste of resources.

Objects of adverse interest: people, data, information, knowledge, areas, facilities, goods, services, materials or equipment, information and communications systems, targeted by adverse agents.

Obstacles: threats that stand in the way of national interests, but are not intended to cause harm.

Obstruct: prevent the initiation of an adverse action, whose planning has been detected, or interrupt its development once it has begun.

Obstruction: impediment to the achievement of adverse action, initiated in the orientation phase, when preventive counterintelligence protection measures are implemented, in addition to others, necessary for the situation under monitoring.

Open source intelligence: classification of the intelligence data by origin, based on available, i.e. freely accessible data, information and knowledge. (See also: Osint).

Open Sources: See open source intelligence.

Operation: basic structure of the operations function, responsible for managing and executing specialized actions.

Operational action: confidential use of specialized operational techniques to achieve a determined objective, based on a request received from the client.

Operational action based on human resources: operational action that prioritizes the specialized use of human resources.

Operational action based on technical resources: operational action that prioritizes the specialized use of technical resources.

Operational cases: planned and coordinated use of intelligence operations around a specific theme, with multiple missions and targets.

Operational client: the one responsible for activating the operations function, presenting the request that will define the objective of the operational actions to be used.

Operational environment: physical or virtual space, where operational actions take place.

Operational intelligence: classification of intelligence production by purpose, aimed at offering contextualization of a specific State action, in support of the execution of actions already defined within the scope of a given public policy.

Operational protection action: comprises the execution of operational actions aimed at protecting the agent and the operation.

Operational resources: combined application of human, technical, financial and logistical capabilities available to the operations function.

Operational search action: comprises the execution of operational actions that aim to obtain unavailable data, information or knowledge.

Operational techniques: specialized procedures and methods for using personnel and materials in covert actions.

Operations Cycle: cycle made up of the planning, execution, dissemination and completion phases, with flexible limits between them.

Operations Function: constituent sector of intelligence activity, responsible for carrying out confidential specialized actions, aimed at obtaining unavailable inputs, to counter adverse actions and to create situations favorable to national interests, in order to meet previously established objectives.

Opportunity: favorable condition or factor for achieving national interests.

Ordinary external control: control and oversight of the intelligence agencies, to which all public bodies are subject, exercised by the National Congress, with the help of the Federal Court of Auditors (TCU). It consists of accounting, financial, budgetary, operational and asset control, and requires permanent accountability.

Ordinary internal control: control and oversight of intelligence agencies, to which all public agencies are subject, carried out by the Office of the Comptroller General (CGU). In the specific case of ABIN, this oversight is also exercised by the Secretariat for Internal Control of the Presidency of the Republic (Ciset/PR), which carries out internal control over the application of the Agency's budget funds. The Public Integrity System of the Federal Executive Branch (Sipef) and the Ethics Commission of the Presidency and Vice-Presidency of the Republic (CEPR) also make up this area of control and oversight.

Osint: English acronym for Open Source Intelligence. See: Open Source Intelligence.

P

Phenomena: processes that modify situations. A phenomenon is made up of the evolution of facts, events and situations, the dynamics between them, and the way in which these dynamics are reflected in human experience.

Planning: KPM phase in which the plan for the work to be developed is prepared, based on a request for knowledge production.

Prevent: anticipate threats in the abstract, with a view to preventing their materialization or mitigating their effects.

Production manager: role performed by an intelligence professional, responsible for supervising the team, providing support, approving actions, and controlling deadlines and deliveries.

Proofreader: role performed by an intelligence professional, responsible for ensuring that simpler and more superficial problems can be detected, before sending the product to the validator, including issues such as suitability for the user, grammatical correction, suitability for intelligence language principles, and argumentation problems and logic.

Proportionality: rule of the operations function, that determines that the means and techniques chosen will be carried out to the extent strictly necessary to achieve the objective of the covert action.

Prospective intelligence knowledge: knowledge resulting from judgments and reasoning about the future evolution of facts, events, situations or phenomena, with a focus on the distant future, requiring the use of techniques ancillary to the Knowledge Production Methodology (KPM), due to its nature.

Prospective intelligence: classification of intelligence production by time frame, aimed at providing scenarios about the future, to help direct government action.

Protection: use of complementary measures to protect the integrity and identity of the agents employed, the secrecy and objectives of the operational action, and the intelligence agency itself.

Purpose: principle of the operations function, stating that covert actions must be conducted in support of the interests of society and the State, having their common good as its motto.

R

Reasoning: mental elaboration, from which previous judgments allow a new judgment to be logically generated.

Reclassification: change in the degree of secrecy assigned.

Recruitment: action that aims to convince a person to work, consciously or unconsciously, for the benefit of an intelligence agency.

Recruitment of influence agents: action aimed at the recruitment and control, by foreign entities, of people, used as instruments to issue messages and interfere in politics, the market and society, in order to favor the interests of their sponsor. Government officials, politicians, academics and influencers, among others, may be the subject of this recruitment.

Red hat: technique designed to help understand how other actors or adverse agents tend to act or behave in certain situations.

Resilience: principle of the operations function that recommends that this sector must prove resilient, when faced with difficulties and frustrations, in order to be able to perceive, evaluate and react quickly to adverse situations, and control its performance, so as not to compromise the operational actions that are being developed.

S

Sabotage: action aimed at destroying, damaging, compromising or rendering useless, in whole or in part, data, information, knowledge, materials, equipment, installations, logistics systems, production chains and critical infrastructures of the country, thus affecting its ability to meet the essential needs of the population and the interests of the state.

Scenarios: set of events that shape a future picture, along with its evolution.

Scope: principle of the analysis function that determines the necessary extent of the objects of analysis, for the fullest possible elucidation of the proposed subject.

Search: combined application of operational techniques to obtain unavailable data, information and knowledge.

Secrecy of sources: guarantee of protection of the confidentiality of data sources, information and knowledge, used in the preparation of the intelligence product.

Secrecy: condition attributed to data, information or knowledge that it is revealed only to the person, organization, system or entity authorized and accredited to do so.

Security Credential: a certificate that grants official authorization, by a competent authority, for a certain person to have access to data, information and knowledge, of varying degrees of secrecy.

Security culture: a process of education which seeks to create, develop and maintain an effective security mindset, in procedures involving sensitive data, information or knowledge.

Security Intelligence: intelligence activity aimed at detecting and evaluating actors, within the State, that could jeopardize the achievement of its objectives, and threaten the well-being of society.

Security: general principle of intelligence activity, that imposes the adoption of safeguard measures appropriate to each situation, aiming to ensure that the knowledge produced and actions carried out are duly protected.

Sensitive data, information and knowledge: informational elements that, due to their indispensability to the personal security of citizens, society or the State, have controlled dissemination, and whose access is restricted to accredited people.

Setting an Objective: phase of the intelligence branch cycle, in which the themes, sections and approaches to the areas that will be worked on are determined.

Sigint: acronym in English for Signals Intelligence. See: Signals intelligence.

Signals intelligence: classification by origin of intelligence data, based on data and information obtained by interpreting and decoding communications and electromagnetic signals. (See also: Sigint)

Simplicity: general principle of intelligence activity, that establishes actions planned and executed by the intelligence activity, in order to avoid unnecessary complexity, costs and risks.

Situations: occurrences contextualized from human experience, being a constituent part of the reality of events, designating the context in which one or more ongoing events must be evaluated.

Social investigation: a process of researching the background of each candidate, designed from the point of view of counterintelligence, to hinder infiltration and prevent the hiring of personnel with potential to compromise confidential knowledge and data.

Social media intelligence: classification by origin of intelligence data, based on data and information obtained from social media and metadata associated with them, allowing for sentiment analysis, publication patterns and relevance assessment of mass topics. (See also: Socmint)

Socmint: acronym in English for Social Media Intelligence. See: Social media intelligence.

Source: origin of data, information or knowledge.

Specialized actions: all actions that employ techniques typical of intelligence activities, such as: structured collection of freely accessible data; application of protective measures; confidential use of operational techniques; processing of data, information and knowledge based on the Intelligence Knowledge Production Methodology.

Specific external control: control and oversight of intelligence activity, carried out by the Legislative Branch, through the Joint

Committee for the Oversight of Intelligence Activities (CCAI) of the National Congress, according to its own regulations.

Specific internal control: control and supervision of intelligence activities by the Foreign Relations and National Defense Chamber (Creden), of the Government Council, which is responsible for overseeing the implementation of the National Intelligence Policy (NIP).

State Intelligence: activity carried out by Intelligence organizations, that are part of the structure of the Brazilian State.

State of certainty: a state of the mind in which the individual considers that their mental interpretation of reality fully corresponds to the real object under consideration, i.e. the individual believes that he or she has fully attained the truth.

State of ignorance: a state of the mind characterized by a complete lack of any image of reality.

State of possibility: a state of the mind in which there is insufficient evidence to support any mental image, with reasons both to accept and deny the different possibilities for representing reality.

State of probability: a state of the mind in which the individual considers that their interpretation of reality corresponds to the real object, but with some chance of being mistaken.

Strategic intelligence: classification of intelligence production by purpose, aimed at analyzing and interpreting phenomena with potential to impact fundamental objectives and interests of the State.

Structured analytical techniques (SAT): additional techniques to traditional intelligence production methods, which provide systematic means to externalize individual mental processes.

Suitability: rule of the operations function, that determines which means and techniques chosen will lead to the fulfillment of the objective of the covert action.

Support analyst: role performed by an intelligence professional, responsible for supporting the analysis efforts of the lead analyst, collaborating on tasks and receiving delegated analysis actions.

Support for legal manipulation: legal manipulation (Lawfare) is the use of legal maneuvers to seek to prevent or hinder the achievement of an adversary's interests, that conflict with those of their sponsor's.

Synthesis: mental operation in which the composition or recomposition of a whole is conceived, based on analyzed constituent elements, thus providing a coherent and understandable set.

Systematic operational action: consists of the development of continuous actions, resulting in a constant flow of data, information and knowledge, with a pre-established beginning and an indefinite end.

T

Tactical intelligence: classification of intelligence production by purpose, aimed at gathering data, information and knowledge in support of the development of defined government policies.

Target: object on which covert action acts to fulfill its objective. It holds data, information and knowledge essential to intelligence activity, or is used to carry out adverse actions.

Techint: English acronym for Technical Intelligence. See: Technical intelligence.

Technical intelligence: classification by origin of the intelligence data carried out on the basis of data and information obtained by technical means. (See also: Techint)

Technical means: material and technological resources used in an intelligence operation, within the limits of the body's legal possibilities of action.

Terrorism: practice, by one or more individuals, of the acts provided for in §2 of Article 2 of Law No 13260/2016, for reasons of xenophobia, discrimination or prejudice, based on race, color, ethnicity and religion, when committed with the purpose of provoking social or generalized terror, exposing people, property, public peace, or public safety to danger.

Threat: condition or factor, unfavorable to the achievement of national interests, and to the safeguarding of sensitive knowledge and data.

Timeliness: general principle of intelligence activity, that determines the presentation of results, within an appropriate period of work, carried out by intelligence professionals, so that it can be used effectively.

Traceability: general principle of intelligence activity, that stipulates the recording of actions carried out in intelligence activity, to ensure that they can be audited.

Transnational intelligence: area of intelligence focused on cross-border issues, partially under the State's capacity for intervention, but which require international negotiations and partnerships, to adopt effective policies to achieve the State's objectives.

U

Unavailable data: information element not freely accessible to the intelligence agency.

Usefulness: general principle of intelligence activity, that provides for the orientation of the results of intelligence actions, based on the needs of those who will use it, thus providing a potentially useful product.

User: government authority or entity, recipient of knowledge produced.

V

Validator: role performed by an intelligence professional, responsible for the assessment and technical validation of the analytical quality of intelligence knowledge.

Violent extremism: refers to the planning, preparation, promotion, financing and execution of violent acts motivated by extremist ideologies that disrespect fundamental constitutional precepts.

Visual analysis: tool used by intelligence professionals to organize inputs and generate succinct and attractive visual presentations of intelligence knowledge for users, in certain situations, such as the ongoing monitoring of dynamic events, in which new inputs, obtained or generated, feed a database; and the constant update of a situation.

9

Additional Sources and Reading

9. Additional Sources and Reading

Books and articles

AGRELL, Wilhelm; TREVERTON, Gregory F. **National Intelligence and Science: Beyond the Great Divide in Analysis and Policy**. New York: Oxford University Press, 2015.

AGRELL, Wilhelm; TREVERTON, Gregory. **National Intelligence Systems: current research and future prospects**. Cambridge University Press, 2009.

ANDREW, Christopher; ALDRICH, Richard J.; WARK, Wesley K. (eds) **Secret intelligence: a reader**. Routledge, 2019.

CEPIK, Marco (org.). **Inteligência Governamental (Government Intelligence): contextos nacionais e desafios contemporâneos (national contexts and contemporary challenges)**. Impetus, 2011.

CEPIK, Marco. **Espionagem e democracia (Espionage and democracy): agilidade e transparência como dilemas na institucionalização dos serviços de inteligência (agility and transparency as dilemmas in the institutionalization of intelligence services)**. Parabellum, 2023.

COULTHART, Stephen. *An Evidence-Based Evaluation of 12 Core Structured Analytic Techniques*. In: **International Journal of Intelligence and CounterIntelligence**, v.30, n.2, 2017, pp. 368-391.

GEORGE, Roger Z.; BRUCE, James B. (ed.) **Analyzing Intelligence: Origins, Obstacles, and Innovations**. Georgetown University Press, 2008.

GILL, Peter; MARRIN, Stephen; PHYTHIAN, Mark (eds.). **Intelligence Theory: key questions and debates**. Routledge, 2008.

GONÇALVES, Joanisval. **Políticos e espiões (Politicians and spies)**. Impetus, 2018.

HERMAN, Michael. **Intelligence power in peace and war**. Royal Institute of International Affairs/Cambridge University Press, 1996.

JOHNSON, Loch (ed.). **Strategic Intelligence (5 volumes)**. Praeger, 2007.

LANDON-MURRAY, Michael. *Putting a Little More "Time" into Strategic Intelligence Analysis*. In: **International Journal of Intelligence and CounterIntelligence**, v. 30, n. 4, 2017, pp. 785-809.

MCDOWELL, Don. **Strategic Intelligence: a handbook for practitioners, managers, and users**. Scarecrow Press, 2009.

MCGLYNN, Patrick; GARNER, Godfrey. **Intelligence Analysis Fundamentals**. Boca Raton: CRC Press, 2019. 334 p.

PHERSON, Randolph; HEUER Jr., Richards. **Structured Analytic Techniques for Intelligence Analysis**. CQ Press, 2021.

PHYTHIAN, Mark. *Intelligence analysis and social science methods: exploring the potential for and possible limits of mutual learning*. In: **Intelligence and National Security**, v. 32, n. 5, 2017, pp 600-612.

REVISTA BRASILEIRA DE INTELIGÊNCIA (Brazilian Intelligence Review). nº 17 (dez. 2022). Brasília, DF: Agência Brasileira de Inteligência (Brazilian Intelligence Agency). 162p.

SHULSKY, Abram e SCHMITT, Gary. **Silent warfare: understanding the world of Intelligence**. Potomac books, 2002.

SIMS, Jennifer E. **Decision Advantage: intelligence in international politics from the Spanish armada to cyberwar**. Oxford University Press, 2022.

Legislation

BRASIL. Decreto de 15 de dezembro de 2017. Aprova a Estratégia Nacional de Inteligência (Decree of December 15, 2017. Approves the National Intelligence Strategy). **Diário Oficial da União**

(Official Journal of the Union), n. 241, Brasília, DF: 18 dez. 2017. Seção 1, pp. 36-40.

BRASIL. Decreto nº 10.777, de 24 de agosto de 2021. Institui a Política Nacional de Inteligência de Segurança Pública (Decree n. 10777, of August 24, 2021. Establishes the National Intelligence Policy for Public Security). **Diário Oficial da União (Official Journal of the Union)**, n. 161, Brasília, DF: 25 ago. 2021. Seção 1, p.2.

BRASIL. Decreto nº 10.778, de 24 de agosto de 2021 Aprova a Estratégia Nacional de Inteligência de Segurança Pública (Decree n. 10778, of August 24, 2021. Approves the National Intelligence Strategy for Public Security). Disponível em: **http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/d**. Access on Apr. 20, 2022

BRASIL. Decreto nº 11.693, de 6 de setembro de 2023. Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência (Decree n. 11693, of Sep. 6, 2023. Regulates on the organization and functioning of the Brazilian Intelligence System). **Diário Oficial da União (Official Journal of the Union)**, n. 171-A, Brasília, DF: 25 ago. 2021. Seção 1 – Extra A, p.1.

BRASIL. Decreto nº 8.793, de 29 de junho de 2016. Fixa a Política Nacional de Inteligência (Decree n. 8793, of June, 29, 2016. Sets the National Intelligence Policy). **Diário Oficial da União (Official Journal of the Union)**, n. 124, Brasília, DF: 30 jun. 2016. Seção 1, p.5.

BRASIL. Lei nº 9.883, de 7 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN, e dá outras providências (Law n. 9883, of December 7, 1999. Introduces the Brazilian Intelligence System, creates the Brazilian Intelligence Agency – ABIN, and lays down other provisions). Disponível em: **http://www.planalto.gov.br/ccivil_03/leis/l9883.htm**. Accessed on: Nov. 16, 2023.

BRASIL. Portaria GAB/DG/ABIN/CC/PR Nº 925, de 6 de setembro de 2023. Fixa os critérios e procedimentos de ingresso de órgãos e entidades no Sistema Brasileiro de Inteligência como órgãos dedicados, associados e federados, e dá outras providências

(Ordinance GAB/DG/ABIN/CC/PR Nº 925, of September 6, 2023. Sets the criteria and procedures for the entrance of other bodies and agencies into the Brazilian Intelligence System, as dedicated, associate and federated bodies, and lays down other provisions). **Diário Oficial da União (Official Journal of the Union)**, n. 175, Brasília, DF: 13 set. 2023. Seção 1, p.4.

BRASIL. Portaria GAB/DG/ABIN/CC/PR Nº 926, de 6 de setembro de 2023. Estabelece o rol de órgãos e de entidades que integram o Sistema Brasileiro de Inteligência - Sisbin como órgãos dedicados e associados, e dá outras providências (Ordinance GAB/DG/ABIN/CC/PR n. 926, of September 6, 2023. Establishes the roll of bodies and agencies that integrate the Brazilian Intelligence System – Sisbin, as dedicated and associate bodies, and lays down other provisions). **Diário Oficial da União (Official Journal of the Union)**, n. 175, Brasília, DF: 13 set. 2023. Seção 1, p.5.

Doctrines and Manuals

BRASIL. Presidência da República. Ministério da Justiça. Secretaria Nacional de Segurança Pública (Presidency of the Republic. Ministery of Justice. National Secretariat of Public Security). **Doutrina Nacional de Inteligência de Segurança Pública – DNISP. – 4. ed. rev. e atual. (National Intelligence Doctrine of Public Security)** – Brasília: Secretaria Nacional de Segurança Pública, 2014.

BRASIL. Exército. Comando de Operações Terrestres (Brazilian Army. Land Forces Command). **Manual de Campanha – Contrainteligência (Campaign Planning Handbook – Counterintelligence)** EB70-MC-10.220. Brasília, DF: Estado Maior do Exército, 2019.

BRASIL. Exército. Comando de Operações Terrestres (Brazilian Army. Land Forces Command). **Manual Técnico – Produção do Conhecimento de Inteligência (Technical Handbook – Intelligence Knowledge Production)** EB70-MT-10.401. Brasília, DF: Centro de Doutrina do Exército, 2019.

CASA CIVIL

BRAZILIAN GOVERNMENT

UNITING AND REBUILDING

CASA CIVIL