Journal of Business and Economics, ISSN 2155-7950, USA
January 2024, Volume 15, No. 1, pp. 54-60
DOI: 10.15341/jbe(2155-7950)/01.15.2024/006
© Academic Star Publishing Company, 2024
http://www.academicstar.us

The Intelligence Cycle Applied in Compliance and "ESG"

André Ronaldo Teófilo, Débora Reinert Raspantini, Francisco de Assis Claveria Gallucci de Carvalho
(Brazilian Institute of Tax Studies, Brazil)

Abstract: Intelligence can be defined as a systematic process of collecting, analyzing and disseminating information to help in making strategic decisions. In other words, the Intelligence activity seeks to obtain relevant, reliable and up-to-date information on a given subject or environment to support informed decision-making. Thus, as a whole, we have something that can be called the "Intelligence Cycle", which can be defined as a broad science that has at its core the management of fundamental processes with a strategic scope in obtaining information that is also used for the Compliance/Compliance of companies, whose doctrines are used, e.g., for (i) Combating Frauds, (ii) Strategic Planning and Value Generation, (iii) Internal Controls, (iv) Management and Audit Processes; (v) Identification of Risks and Formulation of Guidelines, (vi) Information Security, (vii) Sustainability and all other items included in the "ESG" concept. The methodology used was bibliographical research. In conclusion, it was found that the use of knowledge from the Armed Forces Intelligence Cycle can be used in the corporate environment for application in Compliance and "ESG".

Key words: intelligence, compliance, ESG, military doctrine

JEL codes: K1, K2, O33

1. Introduction

This article uses some of the military knowledge and doctrines from the War College of the Federative Republic of Brazil, whose teachings are also passed on to the civilian sector through "ADESG — the Association of Graduates of the War College", whose association offers specific courses through its branches, such as "CEPE — Course of Studies in Politics and Strategy" and "CEIAMC — Special Course in Intelligence Applied to the Corporate Environment". We are also supported by extensive teaching material made available by the institutions, as well as bibliographical research.

There are immense advantages in using such knowledge for application in Compliance and "ESG", since both the armed forces and private organizations have similar organizational structures, such as:

1) Hierarchy and Organizational Structure

Both the armed forces and private organizations generally have a well-defined hierarchical structure, and both levels of leadership, from the highest echelons to the lowest levels of execution. In addition, both depend on an efficient chain of command to make decisions and execute tasks effectively.

2) Objectives and Missions

André Ronaldo Teófilo, Post-graduate, Lawyer, Brazilian Institute of Tax Studies. E-mail: andre@teofiloadvogados.com.br.
Débora Reinert Raspantini, Post-graduate, Lawyer, Brazilian Institute of Tax Studies. E-mail: debora@teofiloadvogados.com.br.
Francisco de Assis Claveria Gallucci de Carvalho, Post-graduate, Lawyer, Brazilian Institute of Tax Studies. E-mail: galluccidecarvalho@gmail.com.

A country’s armed forces have the primary mission of defending and protecting the nation against external threats. Their objectives are related to national security, territorial sovereignty and the defense of the country’s interests. On the other hand, private organizations have as their main objective the pursuit of profit and economic protection. Their objectives are related to the provision of goods and services, customer satisfaction and maximizing the value for shareholders.

3) Strategy and Planning

Both the armed forces and private organizations depend on well-developed strategies to achieve their goals. The armed forces develop military strategies to respond to threats, protect territory and project power. As private organizations develop business strategies to compete in markets, they achieve competitive advantages and long-term success.

4) Human Resources and Training

Both the armed forces and private organizations value and invest in their human resources. Both institutions need to recruit and train qualified personnel to perform their duties. The armed forces train soldiers to operate weapons, military operations and maintain discipline. Private organizations train their employees in the skills needed to carry out their tasks and achieve the organization’s objectives of the organization.

5) Resource and Logistics Management

Both the armed forces and private organizations need to efficiently manage their resources and logistics. The armed forces manage resources such as weapons, equipment, supplies and personnel strategically to support their military operations. Similarly, private organizations manage financial, material and human resources to ensure the efficient production and delivery of goods and services to customers.

6) Decision-making and Agility

Both the armed forces and private organizations need to make quick and effective decisions in order to adapt to constantly changing situations. The ability to respond quickly to threats or opportunities is crucial for both institutions. Agility, flexibility and the ability to adjust to unforeseen circumstances are key factors for the success of both armed forces and private organizations.

The fact is that military knowledge and doctrines have already been consolidated, and several organizations, especially large corporations, have been hiring high-ranking military personnel as advisors. After all, in addition to a hostile corporate world, the knowledge of procedures involving Compliance and “ESG” is perfectly applied to the systematization of military work.

In the case in point, we have this knowledge in the “Intelligence” sector, which is an activity that dates back to the dawn of humanity. Since ancient times, human beings have been looking for ways to collect information and use it to make better decisions. However, modern intelligence activity has evolved significantly in recent centuries, especially after the First World War, with special development in the Cold War era. Cold War, and today we can use it in the corporate environment as a tool for Compliance and even to help with environmental, social and governance sustainability. (Environmental, Social and Governance) of private organizations.

In the United States, corporate intelligence activity has grown significantly in recent decades, not least because of issues related to corruption and the sustainability of corporate ventures. North American private organizations are pioneers not only in the Compliance system and the set of standards and good practices practices included in the “ESG” concept, but also in the use of military intelligence tools to make strategic intelligence tools for strategic decision-making.

Intelligence can be defined as a systematic process of collecting, analyzing and dissemination of information to help make strategic decisions. In other words, intelligence seeks to obtain relevant, reliable and up-to-date information on a given subject or environment to support informed decision-making.

Within this scenario, we also have Counterintelligence, which can be defined as a set of measures and activities aimed at protecting an organization's information and sensitive systems of an organization against internal and external threats; it is the activity of detect, prevent and neutralize hostile intelligence activities that seek to obtain critical and sensitive information from an organization.

While Intelligence focuses on gathering relevant and reliable information to ultimately aid decision-making, Counterintelligence seeks to protect the organization's critical and sensitive information from hostile intelligence activities. In other words, Counterintelligence is the "defensive intelligence" of the organization, while Intelligence is the "offensive intelligence".

In general, the Intelligence Activity is an important tool for governments, private organizations and non-governmental organizations, which need to be informed about the environment in which they operate in order to make strategic and well-founded decisions.

Thus, as a whole, we have something that can be called the "Intelligence Cycle", which can be defined as a broad science that has at its core the management of fundamental processes with a strategic scope to obtain information that is also used for obtaining information that is also used for Compliance in private organizations, whose doctrines are used, e.g., for (i) Combating Fraud, (ii) Strategic Planning and Value Generation, (iii) Internal Controls, (iv) Management and Audit Processes; (v) Risk Identification and Formulation of Guidelines, (vi) Information Security, (vii) Sustainability and all the other items included in the "ESG" concept.

2. Concepts and Terms

The Intelligence Cycle involves a series of concepts and terms that are essential for its understanding and application. its understanding and application, and among these concepts we can highlight:

a) Information gathering: this is the process of obtaining relevant information for decision-making, and can be carried out in various ways, depending on the purpose, it should be noted that this collection must be legal;

b) Information Analysis: is the process of evaluating and interpreting the information collected. and involves the identification of patterns, trends and insights that may be useful for decision-making;

c) Dissemination of Information: this is the process of sharing the information with the relevant people or areas within the organization; it can be done through reports, presentations or meetings;

d) Strategic Intelligence: this is a type of Intelligence that aims to identify internal and external risks, provide Corporate Governance with strategic information, assess opportunities and threats and plan future actions;

e) Competitive Intelligence: is a type of Intelligence that focuses on collecting and analyzing information about competitors and aims to understand the strategies, strengths and weaknesses of competitors in order to better position themselves in the market;

f) Market Intelligence: is a type of Intelligence that focuses on collecting and analyzing information about the market in which the organization operates and aims to understand the behaviour behavior of customers, suppliers, competitors and market trends;

g) Security Intelligence: this is a type of intelligence that focuses on preventing or neutralizing internal or external threats to the organization, and involves identifying and monitoring of potential threats, such as industrial espionage or terrorism, within the legal national and international legal precepts;

h) Operational Intelligence: is a type of intelligence that focuses on collecting and analyzing information to support an organization's daily operations of an organization, and aims to identify opportunities for improvement and minimizing the risks inherent in an organization's area of activity;

i) Tactical Intelligence: this is a type of Intelligence that focuses on information that can be can be used by Corporate Governance to drive immediate actions and operational decisions and aims to gain competitive advantage in specific situations;

j) Economic intelligence: a specific area of intelligence that focuses on information related to the economy, such as market trends, prices, demand, legislation and regulation;

k) Technological Intelligence: this is a type of Intelligence that focuses on information on emerging technologies, patents, intellectual property and technological competitors, as well as the use of such tools for Intelligence and Counterintelligence purposes;

l) Environmental intelligence: this is a specific area of intelligence that focuses on information related to the environment, such as environmental regulations, sustainable practices, climate change and renewable energy sources;

m) Political Intelligence: this is a specific area of Intelligence that focuses on political information, such as governments, political parties, elections, political conflicts and intergovernmental relations;

n) Legal Intelligence: this is a specific area of Intelligence which, on the one hand, uses national regulations and international treaties for compliance and, on the other hand, monitors social political trends that may change the understanding of certain norms of a nation or community in which it is inserted.

3. Basic Fundamentals

The Intelligence Cycle applied to Compliance is based on basic fundamentals that are essential for its effective practice, and among these fundamentals we can highlight:

a) **Objectivity:** Intelligence must be impartial, based on facts and within the law. Personal bias or the influence of personal or political interests must be avoided;

b) **Timeliness:** the knowledge produced by the Intelligence Cycle must be presented to the decision-maker within a timeframe that allows it to be put to best use;

c) **Confidentiality:** the Intelligence Cycle involves the collection and analysis of sensitive and confidential information, and it is of the utmost importance to maintain the security of this information in order to avoid the exposing sources or jeopardizing corporate security, where data leaks can have serious financial and reputational implications;

d) **Legality:** Intelligence Cycle must be carried out within the laws and regulations and international treaties, always respecting collective and individual rights. individual rights;

e) **Multidisciplinarity:** the Intelligence Cyvle involves various areas of knowledge, such as information technology, law, economics, political science, sociology, ecology and environmentalism. It is important to have knowledge in different areas for a complete and accurate analysis of the information;

f) **Proactivity:** the Intelligence Cycle must be proactive, i.e. it must anticipate possible risks and threats before they occur, allowing preventive or corrective measures to be taken. corrective measures;

g) **Partnerships:** Intelligence Cycle may involve partnerships with other organizations, governments or institutions for the collection and analysis of information, where such partnerships can be valuable for increasing the effectiveness of the Intelligence Cyle;

h) **Flexibility:** the Intelligence Cycle must be flexible and adaptable to changes in the environment and threats. environment and threats, and must be able to adjust strategies and approaches according to new information and situations;

i) **Integration:** the Intelligence Cycle must be integrated into the activities of the organization or government, and should be used to support decision-making and action, rather than being a separate or isolated process. At this point, the organization must be integrated with the Local government to combat corruption and support social and environmental projects;

j) **Communication:** the Intelligence Cycle involves the clear and accurate communication of relevant information, where those involved must have effective communication skills to convey information clearly, concisely, accurately and correctly;

k) **Updating:** the Intelligence Cycle must be constantly updated and revised, in order to ensure that the information is accurate and relevant to current and future decisions, keeping up to date with trends and changes in the environment and threats.

4. Disciplines

The Intelligence Cycle involves various disciplines that contribute to collecting and analyzing relevant information for decision-making. Among the main disciplines, we can highlight:

a) **Open Source Intelligence Cycle (OSINT):** is the collection and analysis of publicly available information,, such as news, reports, government data, among others. It is a discipline in intelligence activity, as often the most valuable information is publicly available;

b) **Human Source Intelligence Cycle (HUMINT):** is the collection of information through human sources, and this discipline involves skills such as persuasion, negotiation and interviewing;

c) **Signals Intelligence Cycle (SIGINT):** is the collection and analysis of information through electromagnetic signals, such as radio, telephone and internet communications. This discipline requires advanced knowledge of information technology and cryptography and must operate within the law;

d) **Image Intelligence Cycle (IMINT**): this is the collection and analysis of information through images, such as satellite photos or drone videos, and requires skills in visual analysis and georeferencing;

e) **Financial Intelligence Cycle (FININT):** is the collection and analysis of information related to finance, such as banking transactions, money laundering and suspicious financial movements. and requires knowledge of finance, accounting and law;

f) **Cyber Intelligence Cycle (CYBINT):** is the collection and analysis of information related to cybersecurity, such as hacker attacks, system vulnerabilities and cybercrime, and requires advanced knowledge of information technology and information security;

g) **Intelligence analysis**: this is the discipline responsible for analyzing and interpreting the information collected by the different intelligence disciplines, and involves skills such as statistical analysis, data modeling and interpretation of complex information;

h) **Counterintelligence:** is the discipline responsible for identifying and neutralizing threats to the security of organizations or governments, such as espionage and sabotage, and involves the collection and gathering and analyzing information to identify possible threats and develop strategies to neutralize them;

i) **Intelligence management**: is the discipline responsible for managing and coordinating the different intelligence disciplines involves strategic planning, the allocation of resources and the and coordination of information collection and analysis activities.

The disciplines listed above are interdependent and complementary, and together they provide a broad and detailed view of the organization's environment. The choice of intelligence disciplines to be used depends on the objectives of the intelligence activity and the context in which it will be applied within the concept of Compliance and “ESG”.

5. Report

As far as the Intelligence Cycle Report is concerned, this is a document that presents information collected, analyzed and interpreted by intelligence professionals, with the aim of inform and guide decision-making. The intelligence report can contain various elements, such as data analysis, information from human sources, analysis of threats, risks and opportunities, among others.

Reports can be produced in different formats, from formal written reports to presentations. The important thing is that the report is clear, objective and presents accurate and relevant information

We can briefly give three examples of reports:

a) Intelligence Cycle Report that analyzes and highlights whether the organization’s actions are in compliance with certain laws, norms and rules, as well as whether the work is being carried out in accordance with corporate policies. The report should contain all legal and accounting analysis, demonstrating whether or not the organization is in compliance with the regulations, guidelines and laws that govern its operations, as well as, if this is the case, guiding the solution for the organization to correct what is detected as “non-conformity”;

b) Intelligence Cycle Report that presents an analysis of cybersecurity risks for a company that must protect its information, e.g., as a result of Brazil's General Personal Data Protection Law (Law No. 13709/2014). In this report, intelligence professionals collected information on possible cyber threats, such as hacker attacks, phishing and malware, and analyzed the risks of these threats to the company’s security, as well as the legal risks arising from information leaks. The report can include recommendations for mitigating the risks identified;

c) Intelligence Cycle Report on Corporate Governance and Best Practices, which presents an analysis of the state of Corporate Governance and the Principles that the purpose of preserving and optimizing the long-term economic value of the organization, and may include recommendations for the company to adjust its operating strategy.

In summary, the Intelligence Cycle report is an important document for decision making based on accurate and relevant information; it can be drawn up in different formats and in different formats and contain various analyses, depending on the needs of the organization or government.

6. Conclusion

The science involved in the Intelligence Cycle contains extensive knowledge. article aims to demonstrate how military indoctrination can be applied in Compliance and “ESG”.

Private organizations are constantly looking for ways to optimize their operations and improve their performance in the competitive global market. In this sense, and parallel, military doctrines have been developed throughout history to enable the armed history to enable armed forces to achieve specific objectives and gain an advantage over their opponents. These doctrines are based on fundamental principles such as strategic planning, leadership, discipline, teamwork and resource management, and understanding and adapting these principles provides private organizations with a solid foundation for success and growth to achieve success and growth.

Thus, it is advantageous to explore and adopt the doctrines and their fundamental military principles of the Intelligence Cycle in the business context, especially in the creation of corporate strategies and corporate management practices in Compliance and “ESG”, since this is solid knowledge, systematized and tested over decades.

References

Brazil Ministry of Defense (MDD) (2016). *National Defense Policy*, Brasília, DF: MD.

War College (2021). *Strategic Planning Methodology*, Rio de Janeiro: ESG.

Gonçalves Jonisvaldo Brito (2018). *Intelligence Activity and Related Legislation*, Rio de Janeiro. Publisher Impetus.

Gonçalves Jonisvaldo Brito (2018). *Politicians and Spies — The Control of Intelligence Activity*, Rio de Janeiro. Publisher Impetus.

PLATT, Washington (1974). *Production of Strategic Information*, Translated by Major Álvaro GaIvão Pereira and Captain Heitor Aquino Ferreira. Rio de Janeiro, Army Library. Livraria Agir Publisher.

Ribeiro Brasiliano and Antonio Celso (2003). *Risk Analysis Manual*, São Paulo. Publisher Sicurezza.