INTELLIGENCE ȘI CULTURA DE SECURITATE

CONFERINȚA STIINȚIFICĂ STUDENȚEASCĂ
CONFERENCE PROCEEDINGS

VOLUMUL 4
2025

Editura Academiei Naționale de Informații
„Mihai Viteazul”

INTELLIGENCE
ȘI CULTURA DE SECURITATE

nr. 4 – 2025

– Conferința Științifică Studențească –

Editura Academiei Naţionale de Informaţii „Mihai Viteazul”

Bucureşti, 2025

Editura Academiei Naţionale de Informaţii „Mihai Viteazul”
© ANIMV
Bucureşti, 2025
Telefon: 0377720.000/1216
Fax: 0377721.134; 0377721.125
ISSN 2972 – 1350 ISSN-L 2971 – 8139

CUPRINS

CRIMINALITATEA DE MEDIU
ŞI SECURITATEA GLOBALĂ 5
Livia MANDU, Cornel RACOVEANU

CÂND ATACATORII DEVIN VICTIME:
VULNERABILITĂŢILE GRUPĂRILOR DE CRIMINALITATE
CIBERNETICĂ 25
Claudia – Alecsandra GABRIAN

NOUA ORDINE MONDIALĂ ÎN CONTEXTUL DIFUZIEI PUTERII –
ÎNTRE IERARHIE ŞI DEZORDINE 41
Octavian-Alexandru-Ştefan BROŞTEANU

ASTROTURFING ŞI RĂZBOIUL PSIHOLOGIC PE FACEBOOK:
GRILE DE VERIFICARE A CONTURILOR FALSE 59
Cristian HAIDĂU

FRANCE AND EUROPEAN STRATEGIC AUTONOMY:
BETWEEN REGIONAL LEADERSHIP AND NATO COMMITMENTS 91
Daniel-Aurel BUCUR

MUTAREA CENTRULUI DE GREUTATE AMERICAN ÎN ASIA-PACIFIC:
COMPETIŢIA SINO-AMERICANĂ ÎNTRE REALISM
ŞI BLUF STRATEGIC 119
Paul-Alexandru SITEA

AUTONOMIA STRATEGICĂ – ELEMENT DISCURSIV
ŞI REALITATE EUROPEANĂ 135
Mălina-Maria RÎNDAŞU

THE GRAY ZONE PROBLEM, SECURITY ISSUES ARISING FROM THE
INTERSECTION OF MILITARY AND CIVILIAN AFFAIRS 159
George-Mihai NICULA

TRACE: A STRUCTURED AI-SUPPORTED MODEL FOR CULTIC RISK
AND NATIONAL SECURITY THREAT ASSESSMENT 177
Iancu-Marius BUFNEA

DRAGNETING THE DRAGON: THE PEOPLE'S REPUBLIC OF CHINA, EUROPEAN UNION AND FIVE EYES, CAUGHT IN THE WEB OF MUTUAL ESPIONAGE 211
Alida Monica Doriana BARBU

ADVANCING A C2I FRAMEWORK FOR ENHANCED INTELLIGENCE SECURITY IN THE SHIPPING INDUSTRY 227
Anastasios-Nikolaos KANELLOPOULOS

BUNE PRACTICI ÎN PREVENIREA RADICALIZĂRII ȘI A EXTREMISMULUI VIOLENT LA NIVEL EUROPEAN: REVIZUIREA SISTEMATICĂ A LITERATURII DE SPECIALITATE 245
Ioana CHIȚĂ

ADVANCING A C2I FRAMEWORK FOR ENHANCED INTELLIGENCE SECURITY IN THE SHIPPING INDUSTRY

Anastasios-Nikolaos KANELLOPOULOS*

Abstract:

The Shipping industry, known for its strong revenues and political weight, functions within a complex and evolving global landscape. To navigate this complex landscape, companies must adopt competitive operational and tactical processes that encompass both offensive and defensive capabilities. Offensive capabilities, such as Competitive Intelligence, are essential for gathering information on competitors and gaining a strategic advantage. Defensive capabilities, including Counterintelligence, are equally important for protecting businesses from malicious actions by competitors.

This paper explores the potential coexistence of Competitive Intelligence and Counterintelligence within a unified operational framework within the Shipping industry, highlighting their complementary roles in addressing the challenges of the internationalized business world. The study follows a qualitative conceptual approach based on a review and synthesis of academic and professional literature on Competitive Intelligence, Counterintelligence, and the Shipping business environment, in order to develop an integrated operational framework. Subsequently, it proposes a unified C2I Business Framework for shipping companies, supporting the establishment of a centralized C2I Office that combines intelligence collection, analysis, and protective countermeasures to improve decision-making, reduce operational vulnerabilities, and strengthen strategic resilience.

Keywords: Competitive Intelligence, Counterintelligence, Shipping Industry, C2I Business Framework.

Introduction

The global shipping industry has evolved into a highly competitive and influential sector, playing a pivotal role in the world economy. As global trade agreements proliferate and supply chain systems become increasingly dynamic, shipping companies are compelled to navigate complex challenges to maintain competitiveness.

* PhD Candidate in Intelligence, Department of Business Administration, Athens University of Economics and Business, Greece. Email: ankanell@aueb.gr

Despite operating theoretically under perfect competition, the reality of the shipping sector presents unique barriers to entry, distinct regional dynamics, and a continuous flux of social and geopolitical influences that shape market opportunities.

The objective of this paper is to examine how Competitive Intelligence (CI) and Counterintelligence can coexist within a unified operational framework in the Shipping industry, and to propose an integrated corporate model that strengthens both competitive positioning and organizational protection. In this volatile environment, the importance of Competitive Intelligence and Counterintelligence has grown significantly. CI involves systematically gathering and analyzing data about competitors, customers, and the broader market to inform strategic decision-making. Meanwhile, Counterintelligence focuses on protecting sensitive business information from external threats, including espionage and cybersecurity risks. Both intelligence frameworks are crucial for shipping companies striving to secure their assets, anticipate market shifts, and enhance operational efficiency.

Methodologically, this paper follows a qualitative conceptual approach based on a structured review and synthesis of academic and professional literature on CI, counterintelligence, and maritime business dynamics. Through comparative analysis of the two intelligence functions, it develops a unified C2I framework adapted to the operational realities and threat environment of the Shipping industry. A comprehensive C2I framework addresses not only competitive dynamics but also internal vulnerabilities, integrating proactive intelligence gathering with protective measures. The establishment of a C2I Office within a shipping organization serves as a strategic hub for intelligence activities, bridging the gap between data collection and actionable insights. Led by a Chief Intelligence Officer (CINO), this office fosters a unified intelligence culture, leveraging human intelligence networks, open-source data, and technological tools to detect emerging threats and capitalize on new opportunities.

By institutionalizing intelligence practices, shipping companies can enhance their strategic foresight and adaptability, positioning themselves advantageously in a highly unpredictable business landscape. The adoption of a C2I framework is not just an operational necessity but a strategic imperative, helping organizations navigate the complexities of globalization, technological advancements, and evolving competitive forces.

Theoretical Background: Intelligence in the Shipping Business Environment

Shipping Environment and Intelligence

The Shipping Industry has become globalized and highly influential in the world economy due to the increasing use of ships, the dynamic development of global supply chain systems, and the emergence of international trade agreements between states and corporations. To illustrate the sector's economic significance, maritime transport remains the dominant mode for global trade: over 80 % of the volume of international trade in goods is carried by sea, according to the United Nations Conference on Trade and Development, and in many contexts this figure is reported at around 90 % of world merchandise trade by volume. Ships serve as the backbone of global supply chains, linking producers, markets, and consumers across continents and sustaining economic growth and development worldwide (UN Trade & Development, 2025). Adam Smith highlighted Shipping as a fundamental cornerstone of global economic development in his book "The Wealth of Nations." Shipping contributed to the international trade system, fostering competition, specialization, and efficiency in the global economy. Stopford (2008) further explores the impact of globalization on the Shipping sector in his book "Maritime Economics," emphasizing how technological advancements and changing economic and business environments affect companies' competitiveness.

Shipping is a unique sector with characteristics that distinguish it from other industries. Theoretically, it operates under conditions of perfect competition and exhibits a highly globalized nature. Numerous shipping businesses compete with each other in an elastic and globally regulated market, striving to gain a competitive advantage (D'agostini et al., 2019). No shipowner has ever acquired a double-digit market share (Emmanuelides and Tsavliris, 2019). Lorange (2009) argues that shipping is a perfectly competitive part of the world economy, and even innovative segments of the sector gradually become perfectly competitive due to the potential for imitation by new entrants. While perfect competition implies no entry or exit barriers and equal access to information for all shipping corporations, in reality, this is rarely the case, as different parts of the Shipping market have distinct barriers to entry and exit (e.g., capital requirements for vessel acquisition, access to finance, regulatory and compliance costs, port access and slot

availability, long-term charter contracts, shipyard capacity and delivery times, and technological/cybersecurity requirements), and companies' information is not always identical.

Furthermore, few industries worldwide are subject to as many social and geopolitical influences as Shipping due to its operational nature and direct correlation with overall world trade. Local changes and trade discontinuities constantly reshape the global trade map, altering the supply-demand balance at local and regional levels and creating a continuous stream of shipping opportunities (Emmanuelides and Tsavliris, 2019). Therefore, the dynamics of the Shipping business environment are unique for each company, often influenced by internal corporate intelligence culture (David, 2013; Chen et al., 2015).

CI The frequent changes in the macro business environment pose limitations and concerns for business decision-making (Miller, 2001). Effective decision-making requires obtaining a comprehensive understanding of qualitative data in a business sector and its competitive landscape (Bose, 2008; Nasri and Zarai, 2013; Kula and Naktiyok, 2021). Companies form their perception of competition through a systematic scanning process that leads to competitive advantages (Nasri, 2012). CI is the process used to gather, process, and analyze data and information related to competitors, customers, and products, thereby supporting business decision-making (Franco et al., 2011; Dabrowski, 2018). It involves the transfer of knowledge from the business environment to corporations, following established analytical rules (Phathutshedzo and Tiko, 2011; Tahmasebifard, 2018), which enhances the understanding of the competitive landscape (Ferrier, 2001; Nasri, 2011; Carvalho, 2021).

In addition, CI differs from Business Intelligence in terms of its information sources. Business Intelligence primarily relies on companies' internal systems, while CI incorporates both internal and extensive external data sources (Gieskes, 2000; Bose, 2008; Saxena and Lamest, 2018; Barnea, 2021). CI traces its roots back to the middle of the 20th century when it was primarily used for military intelligence gathering (Greene, 1966). It is worth noting that there is no universally established international definition for CI (Global Intelligence Alliance, 2005; Franco et al., 2011). An intriguing definition proposed by Tena and Comai (2004) describes CI as a systematic process recognized and embraced throughout an organization for searching, selecting, analyzing, and distributing information about the business environment to gain a

significant competitive advantage. This definition portrays CI as a holistic process that involves the entire company, rather than limiting its capacity and capabilities to specific individuals, groups, or departments.

Moreover, CI combines defensive and offensive intelligence to inform about competitors' plans, strategies, weaknesses, and opportunities. It is not merely a framework for scanning and collecting data, information, and intelligence from the corporate environment; it also entails adding value to companies through intelligence processes and analysis that empower managers to be proactive and make informed decisions (Auster and Choo, 1994; Prescott, 2001; Johns and Van Doren, 2010; David, 2013). CI operates within a completely legal framework for collecting, managing, analyzing, and disseminating information and intelligence, facilitating decision-making processes and the formulation of business strategies (Hedin, 2004; Amiri et al., 2017).Eventually, CI procedures yield two main results: an alert intelligence product that highlights immediate and significant changes in the macro and micro business environment, and an operational or strategic intelligence product that aids in formulating business strategies and making future decisions (Porter, 1991; García-Madurga and Esteban-Navarro, 2020).

Competitive Intelligence Business Framework

The CI framework consists of the development of intelligence analysis products within a specific time period, following existing procedures and based on an intelligence cycle (Prescott, 1999; Bartes, 2013; Kula and Naktiyok, 2021). The Intelligence Cycle, as described by the American Productivity and Quality Center (1996), is a dynamic and interactive process that allows organizations to gather data and information from various sources, analyze it, and take action based on the insights gained. It is an ongoing process that serves as a daily framework for keeping businesses informed about the competitive landscape and supporting informed decision-making.

According to Dishman and Calof's research (2008), the Intelligence Cycle framework is built upon CI awareness and structure. "Competitive Intelligence awareness" refers to the need for an appropriate analytical and operational culture that supports the effective management of information within the company (Miller, 2005; Gaspareniene et al., 2013; Chen et al., 2015). Through the establishment of a CI business culture, company executives play a crucial role in

collecting, managing, and analyzing information, effectively acting as the recipients of necessary information and data. This enables the company to have the required resources to conduct proper analyses and support decision-making processes by managers (Auster and Choo, 1994; David, 2013). Global Intelligence Alliance (2004) suggests the application of a CI cycle consisting of eight steps, drawing on approaches by Bernhardt (1994), Hussey (1995), and Kahaner (1996). This cycle incorporates the fundamental steps of the Intelligence Cycle while addressing the intelligence needs of modern business environments.

Furthermore, Cloutier et al. (2013) proposed a six-step CI Cycle that includes planning and direction, collection, analysis, communication, decision, and evaluation. This model acknowledges the contextual influences that impact an organization, taking into account various internal and external factors. These influences highlight the necessity of establishing appropriate information systems, intelligence frameworks, and a culture that supports informed decision-making. Fostering a CI culture involves upskilling employees, shaping their mentality, incorporating essential environmental knowledge, and promoting operational stability within the business.

Counterintelligence and its Business Framework

Counterintelligence in business refers to the use of tactics and strategies to protect an organization's sensitive information, human resources, and decision-making processes from malicious competitors. It incorporates operational procedures based on frameworks used in the intelligence sector, such as the Intelligence Cycle, which includes functions like collection, analysis, and dissemination of information. While traditionally employed by state intelligence services, counterintelligence is now being adapted for the private sector due to the rapidly changing business environment.

Counterintelligence in the business context is a topic of interest for both executives and academic researchers in fields like International Relations and Business Studies. The literature on counterintelligence is divided between former national intelligence officials and reputable academics and research authors. It is described as the process of safeguarding internal information systems from CI collection efforts by other corporations (Strauss, 1999). Counterintelligence also plays a role in neutralizing operational threats in the business environment (Bernhardt, 2003). The protection of national security is another aspect emphasized in counterintelligence, as highlighted in works such as

"Counterintelligence and National Strategy" by Michelle K. Van Cleave (2007) and "VAULTS MIRRORS AND MASKS Rediscovering U.S.A. Counterintelligence" by Jennifer E. Sims and Burton Gerber (2009), which delve into counterintelligence within the U.S.A. intelligence services, specifically addressing economic and industrial espionage.

In the current business landscape, safeguarding sensitive data, information, and intelligence is crucial for ensuring continuous and uninterrupted operation. Counterintelligence executives are responsible for creating and enforcing comprehensive data security policies and procedures. They also train corporate staff on handling sensitive information properly. Innovative technological means such as data masking, data loss prevention, and encryption applications and hardware are utilized to protect business data systems from unauthorized access. Counterintelligence frameworks are also employed to protect corporate human resources from profiling targeting and espionage activities, as well as to prevent external interference in business decision-making processes (Smith and Brooks, 2013).

Counterintelligence frameworks draw on various sources to operate effectively in a business environment. These include corporate Human Intelligence (HUMINT) based on insider intelligence networks, Open-Source Intelligence (OSINT), and competitor intelligence. Internal counterintelligence networks function as information collection systems to monitor activities that may indicate insider threats (Cho and Lee, 2016). These networks gather and deliver relevant information to the appropriate executives. OSINT collection is important in two directions: detecting threats from internal and external business executives by utilizing publicly available sources such as social media, search engines, and news outlets through advanced analytics and machine learning software (Smith and Brooks, 2013; Elmellas, 2016).

Considering the significance of counterintelligence, its implementation requires an overall counterintelligence culture among the human resources of a business (Chen et al., 2015; Kanellopoulos, 2022). In practice, this means that employees at all levels understand basic information-protection principles, recognize indicators of social engineering and insider-risk behavior, and follow standardized procedures for handling, sharing, and storing sensitive operational and commercial data. Such a culture reduces information leakage and strengthens organizational resilience by ensuring that counterintelligence is embedded in daily routines rather than treated as a purely technical or isolated security function.

Counterintelligence and Competitive Intelligence position in an organization

Counterintelligence and CI hold distinct positions within an organization. The configuration of CI teams can vary depending on the business environment, with some companies having dedicated departments or outsourcing the process to external partners. Internal CI teams collect, process, and analyze data to provide relevant insights to high-level decision-makers (Barnea, 2019). These teams employ CI specialists with different backgrounds, levels of experience, and knowledge of analysis methodologies. They often establish shared access special applications for executives across various departments to facilitate the flow of necessary information and intelligence (Gibbons and Prescott, 1996; Prescott, 2001; Marin and Poulter, 2004; David, 2013; Gaspareniene et al., 2013).

Executives are responsible for organizing the CI framework to ensure the delivery of the best information to decision-makers. Traditional intelligence collection and analysis methods may need to be updated to account for external micro and macro-economic and political influences (Ghoshal and Westney, 1991; Babbar and Rai, 1993; Salles, 2006; Zheng et al., 2011; Abraham, 2012; Gaidelys and Meidute, 2012). The analysis methodologies should not solely rely on individual executives' knowledge and experience or be overly influenced by tactical level changes in the business environment (Levitas et al., 1997; Sliton, 1998; Gaidelys, 2010; Solberg Søilen, 2016).

Furthermore, counterintelligence, as part of the intelligence sector, needs to focus on the business environment. Although it primarily focuses on protecting internal operations and addressing insider threats, it also relies on information and intelligence collected from the external business environment, with a particular emphasis on competitors and CI frameworks (Smith and Brooks, 2013). The counterintelligence team should consist of highly skilled and trusted executives who operate independently and have a deep understanding of the company's plans, objectives, and strategies. Their background should include prior experience in information protection and security positions in both the public and private sectors. Their training should encompass a combination of knowledge from the intelligence and business sectors. Eventually, the counterintelligence team should report directly to the company's CEO.

Competitive Intelligence and Counterintelligence Framework in Shipping

The Shipping industry, with its international nature and reliance on information and intelligence, faces vulnerabilities in terms of cybersecurity and espionage threats. To navigate these challenges and stay competitive, shipping companies can benefit from implementing frameworks such as CI and Counterintelligence.

CI in the shipping industry involves acquiring and utilizing information and intelligence from other companies to gain insights into technological innovation, business environment developments, and shipping cycles. This knowledge enables companies to enter new sub-sectors, apply competitive strategies at the right time, and make informed decisions.

Counterintelligence is crucial in protecting a shipping company's internal resources and information from threats. It involves safeguarding against cybersecurity risks, detecting insider threats, and implementing appropriate protection measures. Counterintelligence in shipping can also focus on preventing intellectual property theft and industrial espionage.

To effectively implement CI and Counterintelligence in the shipping industry, a common Shipping Intelligence framework can be adopted. This framework integrates both functions and utilizes methodologies and processes from the intelligence sector, such as the Intelligence Cycle (Kanellopoulos and Ioannidis, 2024).

Developing an C2I Framework for Shipping industry

To properly execute a Competitive Intelligence and Counterintelligence (C2I) framework in the shipping industry, we propose the establishment of a dedicated corporate-level C2I Office. This office serves as the central hub for strategic intelligence activities, integrating both external competitive insight and internal protective mechanisms. It is designed not only to gather critical information but also to ensure that intelligence is translated into meaningful action, protecting the organization from emerging threats while enabling strategic foresight and agile decision-making.

The C2I Office is structured around two executive groups with distinct but interdependent roles. The first group is tasked with the

collection and management of information. This involves identifying and acquiring relevant data from a wide range of internal and external sources, including open-source maritime intelligence, competitor monitoring, trade networks, and geopolitical analysis. Beyond passive collection, this group actively develops and maintains intelligence networks – both internal, through human intelligence contributions from trained employees, and external, through strategic partnerships with entities such as port authorities, regulatory bodies, and supply chain collaborators. The team also oversees the classification, secure storage, and accessibility of collected information to support operational and analytical readiness across the organization.

The second group within the office focuses on analysis, protective measures, and organizational training. Their primary function is to interpret the data collected by the first group using structured intelligence analysis methodologies. From this analysis, they produce actionable insights that directly inform corporate strategy, operational decisions, and risk mitigation. This group also has a critical role in deploying protective counterintelligence measures. These include cybersecurity protocols, insider threat detection systems, and crisis management procedures, all designed to safeguard the organization's sensitive information and operational integrity. Additionally, the group is responsible for embedding an intelligence-aware mindset across the company. They design and deliver training programs that build awareness among employees about intelligence procedures, threat indicators, and secure communication practices. These efforts are essential to cultivating a workforce that is both alert and actively engaged in the company's broader intelligence mission.

Oversight of the C2I Office is assigned to a senior executive with specialized expertise in intelligence operations. This Chief Intelligence Officer (CINO) must possess comprehensive knowledge in areas such as information collection, competitive analysis, and corporate security. Serving as the strategic bridge between intelligence operations and executive leadership, the CINO reports directly to the CEO and the Board of Directors. This reporting structure ensures that intelligence findings are aligned with top-level decision-making and that intelligence capabilities are positioned as a strategic asset rather than a support function. The CINO plays a critical role in maintaining the cohesion of the office's two groups, balancing proactive intelligence efforts with reactive

protection, and ensuring that outputs are relevant, timely, and actionable at the highest levels of the organization.

A key component of the proposed framework is the development of a shared intelligence culture within the company. This culture represents a significant departure from traditional siloed approaches to information security and market analysis. It encourages active participation from all levels of staff in identifying relevant information, recognizing unusual activity, and contributing local or operational insights to the broader intelligence function. This cultural shift not only increases the flow of intelligence from within the organization but also strengthens its ability to anticipate and respond to changes in the external environment. The emphasis on culture is further supported by the cultivation of human intelligence networks that span both internal departments and external relationships. These networks serve as early warning systems, allowing the organization to detect weak signals and emerging trends that may otherwise go unnoticed.

Operationally, the C2I framework is built around a six-stage cycle that mirrors and enhances traditional intelligence methodologies. The first three stages – Collection, Management, and Networking – are led by the information gathering group and are focused on acquiring and organizing data while building reliable sources of intelligence. The second three stages – Analysis, Measures, and Training – are managed by the analytical group and revolve around processing information into actionable insights, implementing protective strategies, and strengthening organizational resilience through employee education. These stages are iterative and interconnected, forming a dynamic cycle that allows the office to adapt continuously to new challenges and refine its activities based on evolving needs.

Crucially, the success of this model depends on the efficient communication of intelligence products and risk assessments to senior leadership. Intelligence must be presented in a manner that is clear, concise, and relevant to decision-making, enabling executives to understand not only what is happening, but why it matters and how the company should respond. The outputs of the C2I Office should inform both immediate operational choices and long-term strategic planning, serving as a reliable compass in a complex and often volatile global shipping environment.

By establishing a formal, well-resourced C2I Office, shipping companies can institutionalize intelligence as a foundational pillar of

their business model. This approach offers substantial strategic benefits: earlier identification of competitive opportunities, improved detection and mitigation of threats, and enhanced decision-making agility. The model supports resilience and adaptability in a landscape marked by geopolitical uncertainty, technological disruption, and increasing information asymmetries. It transforms intelligence from a reactive support function into a proactive force multiplier that secures assets, enables innovation, and supports sustained competitive advantage.

Conclusion

The global shipping industry's inherent complexities, driven by globalization, technological advancements, and geopolitical shifts, require companies to develop robust frameworks for maintaining competitiveness and protecting vital information. As shipping companies operate within a volatile environment marked by rapid changes and diverse threats, adopting a structured Competitive Intelligence and Counterintelligence framework becomes essential. Integrating these intelligence practices not only strengthens a company's strategic position but also ensures resilience against internal and external challenges.

A well-organized C2I Office, led by a CINO, plays a critical role in navigating this dynamic landscape. By centralizing intelligence functions, the C2I Office fosters an organizational culture where data-driven decision-making and proactive threat management become the norm. The dual focus on gathering competitive insights and implementing counterintelligence measures enables shipping companies to identify emerging opportunities while simultaneously mitigating risks such as industrial espionage and cybersecurity breaches.

Moreover, embedding intelligence awareness at every organizational level encourages collaboration and responsiveness, transforming intelligence from a reactive function into a proactive strategic asset. This holistic approach not only informs long-term strategic planning but also empowers daily operational decisions, thereby enhancing the company's capacity to adapt to market disruptions and geopolitical uncertainties.

Eventually, in an industry where information asymmetry and evolving global trends can significantly impact profitability, the ability to

anticipate changes and safeguard corporate intelligence becomes a competitive differentiator. Shipping companies that embrace the C2I model can better position themselves to thrive, leveraging intelligence to secure assets, drive innovation, and make informed strategic choices. As the shipping environment continues to evolve, maintaining an agile and intelligence-oriented approach will be key to sustaining competitive advantage and ensuring long-term success.

Bibliography

1. Abraham, S. C. 2012. *Strategic planning: A practical guide for competitive success*. Emerald.

2. American Productivity and Quality Center 1996. *Leveraging Information for Action*. Houston, TX.

3. Amiri, N., Shirkavand, S., Chalak, M., and Rezaeei, N. 2017. "Competitive Intelligence and developing sustainable competitive advantage". *AD-Minister*: 173–194. https://doi.org/10.17230/ad-minister.30.9.

4. Auster, E., and Choo, C. W. 1994. "How senior managers acquire and use information in environmental scanning". *Information Processing & Management*, 30(5): 607–618. https://doi.org/10.1016/0306-4573(94)90073-6.

5. Babbar, S., and Rai, A. 1993. "Competitive Intelligence for International Business". *Long Range Planning*, 26(3): 103–113. https://doi.org/10.1016/0024-6301(93)90012-5.

6. Barnea, A. 2019. "Big Data and Counterintelligence in Western Countries." *International Journal of Intelligence and CounterIntelligence* 32 (3): 433–47. https://doi.org/10.1080/08850607.2019.1605804.

7. Barnea, A. 2021. "Big Data Can Boost the Value of Competitive Intelligence". *Competitive Intelligence Magazine*, 26(1).

8. Barnea, A., and Meshulach, A. 2020. "Forecasting for Intelligence Analysis: Scenarios to abort strategic surprise". *International Journal of Intelligence and CounterIntelligence*, 34(1): 106–133. https://doi.org/10.1080/08850607.2020.1793600.

9. Bartes, F. 2013. "Five-phase model of the intelligence cycle of competitive intelligence". *Acta Universitatis Agriculturae Et Silviculturae Mendelianae Brunensis*, 61(2): 283–288. https://doi.org/10.11118/actaun201361020283.

10. Bernhardt, D. C. 1994. "'I want it fast, factual, actionable'—tailoring competitive intelligence to executives' needs". *Long Range Planning*, 27(1): 12–24. https://doi.org/10.1016/0024-6301(94)90003-5.

11. Bose, R. 2008. "Competitive intelligence process and tools for intelligence analysis". *Industrial Management & Data Systems*, 108(4): 510–528. https://doi.org/10.1108/02635570810868362.

12. Bouthillier, F., and Jin, T. 2005. "Competitive intelligence professionals and their interactions with CI technology: Areseach agenda". *Journal of Competitive Intelligence and Management*, 3(1).

13. Carvalho, P. S. de. 2021. Fundamentals of Competitive Intelligence (CI). IF Insight & Foresight.

14. Chen, Y., Ramamurthy, K. and Wen, K.-W. 2015. "Impacts of comprehensive information security programs on information security culture". *Journal of Computer Information Systems*, 55(3): 11–19. https://doi.org/10.1080/08874417.2015.11645767.

15. Cho, I., and Lee, K. 2016. "Advanced risk measurement approach to insider threats in Cyberspace". *Intelligent Automation and Soft Computing*, 22(3): 405–413. https://doi.org/10.1080/10798587.2015.1121617.

16. Cloutier, A. 2013. "Competitive Intelligence Process Integrative Model based on a scoping review of the literature". *International Journal of Strategic Management*, 13(1): 57–72. https://doi.org/10.18374/ijsm-13-1.7.

17. D'agostini, E., Nam, H.-S., and Kang, S.-H. 2019. "Gaining competitive advantage at sea: An overview of shipping lines' strategic decisions". *International Journal of Transportation Engineering and Technology*, 5(4): 74. https://doi.org/10.11648/j.ijtet.20190504.12.

18. Dabrowski, D. 2018. "Sources of market information, its quality and new product financial performance". *Engineering Economics*, 29(1). https://doi.org/10.5755/j01.ee.29.1.13405.

19. David, F. R. 2013. *Strategic Management Concepts and cases: A competitive advantage approach*. Pearson.

20. Dishman, P. and J. Calof 2008. "Competitive intelligence: a multiphasic precedent to marketing strategy," *European Journal of Marketing*. 42(7/8): 766-785.

21. Du Plessis, T., and Gulwa, M. 2016. "Developing a competitive intelligence strategy framework supporting the competitive intelligence needs of a financial institution's decision makers". *SA Journal of Information Management*, 18(2). https://doi:10.4102/sajim.v18i2.726.

22. Elmellas, J. 2016. "Knowledge is power: The evolution of threat intelligence". *Computer Fraud and Security*, 2016(7): 5–9. https://doi.org/10.1016/s1361-3723(16)30051-3.

23. Emmanuelides, G., and Tsavliris, P. 2019. *Winning shipping strategies. theory and evidence from leading shipowners*. Economia Publishing.

24. Ettorre, B. 1995. "Managing competitive intelligence". *Management Review*, 84(10).

25. Ferrier, W. J. 2001. "Navigating the competitive landscape: The drivers and consequences of competitive aggressiveness". *Academy of Management Journal*, *44*(4): 858–877. https://doi.org/10.5465/3069419.

26. Franco, M., Magrinho, A., and Ramos Silva, J. 2011. "Competitive intelligence: A research model tested on Portuguese firms". *Business Process Management Journal*, 17(2): 332–356. https://doi.org/10.1108/14637151111122374.

27. Gaidelys, V. 2010. "The role of competitive intelligence in the course of business process". *Economics and Management*, 15.

28. Gaidelys, V., and Meidute, I. 2012. "Instruments and methods of competitive intelligence". *Economics and Management*, 17(3). https://doi:10.5755/j01.em.17.3.2122.

29. García-Madurga, M., and Esteban-Navarro, M. 2020. "A project management approach to competitive intelligence". *Journal of Intelligence Studies in Business*, 10(3). https://doi.org/10.37380/jisib. v10i3.636.

30. Gaspareniene, L., Remeikiene, R., and Gaidelys, V. 2013. "The Opportunities of the Use of Competitive Intelligence in Business: Literature Review". *Journal of Small Business and Entrepreneurship Development*, 1(2): 9–16.

31. Gelb, B., and Zinkhan, G. 1985. "Competitive Intelligence Practices of Industrial Marketers". *Industrial Marketing Management*, (14): 269-275.

32. Ghoshal, S., and Westney, D. E. 1991. "Organizing competitor analysis systems". *Strategic Management Journal*, 12(1): 17–31. https://doi.org/10.1002/smj.4250120103.

33. Gibbons, P., and Prescott, J. 1996. "Parallel competitive intelligence processes in organisations". *International Journal of Technology Management*, 11(1). https://doi.org/10.1504/IJTM.1996.025425.

34. Gieskes, H. 2000. "Competitive intelligence at lexis-nexis". *Competitive Intelligence Review*, 11(2): 4-11. https://doi.org/10.1002/(sici)1520-6386(200032)11:23.0.co;2-e.

35. Global Intelligence Alliance. 2004. Introduction to Competitive Intelligence. *GIA White Paper*, 1.

36. Greene, R. 1966. *Business Intelligence and Espionage*. Homewood: Dow Jones- Irwin.

37. Harber, J. R. 2009. "Unconventional spies: The counterintelligence threat from non-state actors". *International Journal of Intelligence and CounterIntelligence*, 22(2): 221–236.
https://doi.org/10.1080/08850600802698200.

38. Hedin, H. 2004. Introduction to Competitive Intelligence (1/2004). GIA White Paper.

39. Hussey, D. E. 1995. *Rethinking strategic management: Ways to improve competitive performance*. Wiley.

40. Johns, P., and Van Doren, D. C. 2010. "Competitive intelligence in service marketing". *Marketing Intelligence & Planning*, 28(5): 551–570. https://doi.org/10.1108/02634501011066492.

41. Kahaner, L. 1996. *Competitive Intelligence*. New York: Kane Associates.

42. Kanellopoulos, A.-N. 2022. "The Importance of Counterintelligence Culture in State Security". *Global Security and Intelligence Note*, 5.

43. Kanellopoulos, A-N and Ioannidis, A. 2024. "*Enhancing Maritime Security: Adopting an integrated Intelligence Strategy in the Shipping Sector". NATO* Maritime Interdiction Operations Journal, 26.

44. Kula, M. E., and Naktiyok, A. 2021. "Strategic thinking and competitive intelligence: Comparative research in the automotive and communication industries". *Journal of Intelligence Studies in Business*, 11(2).

45. Levitas, E., Hitt, M. A., and Dacin, M. T. 1997. "Competitive intelligence and tacit knowledge development in strategic alliances". *Competitive Intelligence Review*, 8(2): 20–27. https://doi.org/10.1002/cir.3880080206.

46. Lorange, P. 2009. *Shipping strategy: Innovating for success*. Cambridge University Press.

47. Magee, A. C. 2010. "Countering Nontraditional Humint Collection Threats". *International Journal of Intelligence and CounterIntelligence*, 23(3): 509–520. https://doi.org/10.1080/08850601003798807.

48. Marin, J., and Poulter, A. 2004. "Dissemination of competitive intelligence". *Journal of Information Science*, 30(2): 165-180. https://doi.org/ 10.1177/0165551504042806.

49. Miller, J. P. 2005. "Information science and competitive intelligence: Possible collaborators?". *Bulletin of the American Society for Information Science and Technology*, 23(1): 11-13. https://doi.org/10.1002/bult.33.

50. Miller, S. 2001. "Competitive intelligence - An overview". *Society of Competitive Intelligence Professionals*.

51. Nasri, W. 2011. "Competitive intelligence in Tunisian companies". *Journal of Enterprise Information Management*, 24(1): 53–67. https://doi.org/ 10.1108/17410391111097429.

52. Nasri, W. 2012. "Conceptual Model of Strategic Benefits of Competitive Intelligence Process". *International Journal of Business and Commerce*, 1(6).

53. Nasri, W., and Zarai, M. 2013. "Key success factors for developing competitive intelligence in organization". *American Journal of Business and Management*, 2(3). https://doi.org/10.11634/216796061302397.

54. Phathutshedzo, N., and Tiko, I. 2011. "A Framework for Enhancing the Information Systems Innovation: Using Competitive Intelligence". *The Electronic Journal of Information Systems Evaluation*, 14(2).

55. Porter, M. 1991. "Towards a dynamic theory of strategy". *Strategic Management Journal*, 12(2): 95–117. https://doi.org/10.1002/smj.4250121008.

56. Prescott, J. 1999. "The Evolution of Competitive Intelligence - Designing a process for action". *Association of Proposal Management Professionals*.

57. Prescott, J. E. 2001. "Competitive intelligence: Lessons from the Trenches". *Competitive Intelligence Review*, 12(2): 5-19. https://doi.org/10.1002/cir.1013.

58. Saayman, A., Pienaar, J., De Pelsmacker, P., Viviers, W., Cuyvers, L., Muller, M., and Jegers, M. 2008. "Competitive intelligence: Construct exploration, validation and equivalence". *Aslib Proceedings*, 60(4): 383-411. https://doi.org/10.1108/00012530810888006.

59. Salles, M. 2006. "Decision making in SMEs and information requirements for competitive intelligence". *Production Planning & Control*, 17(3): 229–237. https://doi.org/10.1080/09537280500285367.

60. Sapkauskiene, A., and Leitoniene, S. 2010. "The Concept of Time-Based Competition in the Context of Management Theory". *Inzinerine Ekonomika-Engineering Economics*, 21(2).

61. Saxena, D., and Lamest, M. 2018. "Information overload and coping strategies in the Big Data Context: Evidence from the hospitality sector". *Journal of Information Science*, 44(3): 287–297. https://doi.org/10.1177/0165551517693712.

62. Sims, J. E., and Gerber, B. L. 2009. *Vaults, mirrors, and masks: Rediscovering U.S. counterintelligence*. Georgetown University Press.

63. Sliton, P. 1998. "Society of Competitive Intelligence Professionals, various proceedings and publications". *Competitive Review*, 9(2).

64. Smith, C. L., and Brooks, D. J. 2013. *Security science: The theory and practice of security*. Butterworth-Heinemann.

65. Solberg Søilen, K. 2016. "A research agenda for Intelligence Studies in business". *Journal of Intelligence Studies in Business*, 6(1). https://doi.org/10.37380/jisib.v6i1.151.

66. Stopford, M. 2008. *Maritime economics: Martin Stopford*. Routledge.

67. Strauss, K. G. 1999. *Marketing Telecommunication Services*. Artech House Telecom Company.

68. Tahmasebifard, H. 2018. "The role of competitive intelligence and its sub-types on achieving market performance". *Cogent Business & Management*, 5(1): 1540073. https://doi.org/10.1080/23311975.2018.1540073.

69. Tena, J. and Comai, A. 2004. *La Inteligencia Competitiva en las Multinacionales Catalanas*. Barcelona: Emecom.

70. UN Trade and Development (UNCTAD) 2025. *Review of Maritime Transport 2025: Staying the course in turbulent waters. Available at:* https://unctad.org/publication/review-maritime-transport-2025 (Accessed in 26/01/2026).

71. Van Cleave, M. 2007. Counterintelligence and national strategy. https://doi.org/10.21236/ada471485.

72. Weiss, A., and Wright, S. 2006. "Dealing with the Unknown - A Holistic Approach to Marketing and Competitive Intelligence". *Competitive Intelligence*. 9(5).

73. Zheng, E., Fader, P., and Padmanabhan, B. 2011. "From business intelligence to competitive intelligence: Inferring competitive measures using augmented site-centric data". *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1323587

Aceasta este al patrulea volum de proceedings al Conferinței Științifice Intelligence și Cultura de Securitate (ICS), care cuprinde lucrările prezentate în cadrul ediției din 2025 - ICS 2025, publicat de Academia Națională de Informații „Mihai Viteazul" (ANIMV). ICS continuă să ofere studenților o platformă pentru dialog academic și pentru a împărtăși realizările lor științifice.

Ediția actuală își extinde participarea la un spectru mai larg de contributori, incluzând atât doctoranzi, cât și studenți din programele de master, cu un interes crescut pentru domenii precum intelligence, securitate națională, istorie și relații internaționale.

Organizarea conferinței a fost posibilă datorită eforturilor continue ale doctoranzilor și ale conducătorilor de doctorat din cadrul Școlii Doctorale Intelligence și Securitate a ANIMV.

Anticipăm cu entuziasm noi discuții și schimburi de idei în viitoarea ediție a conferinței.

EDITURA ANIMV

ISSN 2972-1350
ISSN-L 2971-8139