

HAPSc Policy Briefs Series

Vol 4, No 2 (2023)

HAPSc Policy Briefs Series



Security Risk Analysis as a Strategic Counterterrorism Tool for National Security: The Case of Frontex Common Integrated Risk Analysis Model (CIRAM)

Anastasios Nikolaos Kanellopoulos

doi: [10.12681/hapscpbs.36659](https://doi.org/10.12681/hapscpbs.36659)

Copyright © 2023, Anastasios Nikolaos Kanellopoulos



This work is licensed under a [Creative Commons Attribution 4.0](https://creativecommons.org/licenses/by/4.0/).

To cite this article:

Kanellopoulos, A. N. (2023). Security Risk Analysis as a Strategic Counterterrorism Tool for National Security: The Case of Frontex Common Integrated Risk Analysis Model (CIRAM). *HAPSc Policy Briefs Series*, 4(2), 35–44. <https://doi.org/10.12681/hapscpbs.36659>

Security Risk Analysis as a Strategic Counterterrorism Tool for National Security: The Case of Frontex Common Integrated Risk Analysis Model (CIRAM)¹

Anastasios-Nikolaos Kanellopoulos²

Abstract

Security Risk Analysis consists an important tool that can be leveraged to properly process information related to National Security and draw useful conclusions through appropriate analytical products. The European Union formulated the appropriate legislation and established new organizations to ensure its external and internal security such as Frontex, designed and developed, in collaboration with the member states, a new security risk analysis tool, the Common Integrated Risk Analysis Model (CIRAM). This paper seeks to approach and examine descriptively, both the elements of this model and its appropriateness to carry out Counterterrorism Risk Analysis.

Keywords: National Security, Security Risk Analysis, Strategy, Counterterrorism, Frontex, CIRAM.

Introduction

Security Risk Analysis is a process that assists in identifying, assessing, and managing potential risks and vulnerabilities. It is an essential component of risk management and plays a crucial role in ensuring the protection of sensitive information and state infrastructure. Also, it is closely related to the study of National Security threats and vulnerabilities.

Moreover, European Union (EU) has established various initiatives and agencies to enhance border security and manage migration flows, such as the European Border and Coast Guard Agency (Frontex). This agency is responsible for coordinating and supporting the management of the EU's external borders, in accordance to collecting, managing, analyzing and disseminating analytical products, that lead to specific operations on the field (Fernández-Rojo, 2021). In this context, the agency generated a new Common Integrated Risk Analysis Model (CIRAM), in order to perform its new analytical duties and lead the intelligence sharing and collaboration between the EU member states (Liashuk and Tsaruk, 2021).

The term Counterterrorism Risk Management refers to the strategies and measures set in place to identify, assess, and mitigate the risks associated with terrorist activities. It involves analyzing potential threats, vulnerabilities, and consequences to develop effective countermeasures and

¹ To cite this paper in APA Style: Kanellopoulos, A. N. (2023). Security Risk Analysis as a Strategic Counterterrorism Tool for National Security: The Case of Frontex Common Integrated Risk Analysis Model (CIRAM). *HAPSc Policy Brief Series*, 4(2), 35-44. <https://doi.org/10.12681/hapscpbs.36659>

² Athens University of Economics and Business, Greece.

response plans (Hughes, 1982). The goal is to prevent or minimize the impact of terrorist attacks and protect individuals, infrastructure, and National Security.

The present paper examines the aspects and components of CIRAM, as a new analytical approach in the sector of Security Risk Analysis and aims to evaluate its importance as a strategic Counterterrorism analytical tool.

National Security Strategy and Security Risk Analysis

National Security consists an inclusive term, encompassing all the aspects of a state's security. The term tends to vary between different states, due to the diversified national priorities and interests. Charles S. Maier refers to National security as the “capacity to control those domestic and foreign conditions, that the public opinion of a given community believes necessary to enjoy its own self-determination or autonomy, prosperity, and wellbeing” (Maier, 1993, p. 5). Moreover, Ann Fitz-Gerald mention that “National Security differs from country to country, and indeed from institution to institution” (Fitz-Gerald, 2008, pp.5-6).

Furthermore, the nature of National Security and the wide range of its components, mandates the collection of information and intelligence from a vast network of open and closed (maybe classified) sources. This information is collected, managed and analyzed through the utilization of specific analytical tools, concluding to the formation of a National Security Strategy (Lowe, 2014).

Additionally, Security Risk Analysis models are analytical tools utilized to allocate data, information and intelligence sources, aiming to maintain an up-to-date strategic and operational picture, regarding security threats such as serious organized crime or terrorism. The frameworks that generate the formation and application of these models, arise from ISO publications like the ISO 31000 and 31100, that are generally offer a “regulation path” for the development of specialized Risk Analysis Models. Hence, Risk Analysis methodology provides the capability of information analysis based on the final intended results, attempting to predict the likelihood future events' occurring (Bonta, Law, & Hanson, 1998). Moreover, the methodology offers facile adaptation to the nature of the information, as it supports the information management from multiple databases and information inputs.

Frontex Common Integrated Risk Analysis Model (CIRAM)

In accordance to Schengen Catalogue (2002), the activities of border checks, controls and management should be based on risk analysis. Subsequently in 2004, the European Parliament created Frontex, including to its tasks, the conducting of a security risk analysis and in 2006 established a plan of Integrated Border Management (IBM) procedures (Léonard, 2010). The development of an IBM system continued until 2013, leading to EUROSUR regulation establishment. EUROSUR is the

first intelligence sharing system for the European border protection and law enforcement agencies, offering the capability of information and analysis sharing, in both operational and strategic level (Jeandesboz, 2020).

As the legislative and institutional developments of the European family promoted the formation of special channels for the exchange of classified information at the analytical level, the need for a “common analytical language” appeared. The central role that Risk Analysis had to play in conformity with European Council of Seville in 2002 and Helsinki in 2003, led to the formation of a specialized Risk Analysis Model that encompassed the intelligence needs of both border security and law enforcement agencies (Hansen, and Pettersson, 2021). The Regulation establishing the Schengen Borders Code in 2006, places common rules for crossing the EU external borders and sets risk analysis as the main tool of data and information analysis. Following that, the Frontex regulation of 2011, reinforces the role of Frontex in EU external border management and positions the border risk analysis procedures in its functions (Fernández-Rojo, 2021).

Frontex in collaboration with EU member states, created the first version of a European Common Integrated Risk Analysis Model (CIRAM) in 2012, (Frontex, 2012). CIRAM is the conceptual framework developed by the European Border and Coast Guard Agency, to assist in the preparation of risk analyses within the Schengen Zone. It aims to promote a common understanding of risk analysis and contribute to greater coherence in the management of the external borders (Léonard, 2010; Liashuk and Tsaruk, 2021).

In particular, CIRAM adapts a management approach to risk analysis, defining risk as a function of threat, vulnerability, and impact. This approach aligns with the spirit of the Schengen Borders Code, which determines risk analysis as the key tool for ensuring the optimal allocation of resources within constraints of budget, staff, and equipment efficiency. The model provides the framework for conducting risk analyses, which helps Frontex and Member States in making informed decisions regarding border management and resource allocation. By analyzing various factors such as threats, vulnerabilities, and potential impacts, CIRAM enables the identification and assessment of risks associated with cross-border activities (Hansen, and Pettersson, 2021). This information allows the implementation of the appropriate measures to address or mitigate the identified risks (Jeandesboz, 2020).

In addition, the Schengen Zone consists of the EU Member States and Schengen-associated countries that share common external borders. For maintaining the integrity of the Schengen area it is crucial to ensure the security and effectiveness of the borders (Manjarrez, 2015; Oliveira Martins et al., 2022).

CIRAM plays a significant role in supporting Member States and Schengen-associated countries by providing analysis and insights into cross-border crime and risks (Liashuk and Tsaruk, 2021). This information allows them to take appropriate measures to address the identified risks and maintain border security (Fernández-Rojo, 2021).

CIRAM Intelligence Cycle

Intelligence is placed in the heart of CIRAM leading to the utilization of Intelligence Cycle procedures, so as to receive, handle, manage, analysis and disseminate analysis (Frontex, 2012). Specifically, the cycle contains the steps:

Tasking: This step involves identifying the specific intelligence requirements and objectives, as well as establishing the overall management and guidance for the intelligence effort.

Collection: In this step, relevant information is collected from various sources, such as human intelligence (HUMINT), open-source intelligence (OSINT), and more. The collection process aims to gather data and insights that can contribute to the analysis and understanding of potential threats.

Evaluation: This step serves several purposes such as assessment of information quality, validation of intelligence by comparing it with other sources, cross-referencing information, and verifying its accuracy, analysis of information relevance and identification of intelligence gaps.

Collation: This step includes consolidation of information and data and identification of patterns and connections, by ensuring the completeness through avoiding oversight or missing critical details that could impact the accuracy and reliability of the intelligence.

Analysis & Interpretation: The purpose of this steps is to identify intelligence patterns and trends based on the collated data, information and intelligence. Plus, it is important to derive useful insights and conclusions.

Reporting: Reporting is an essential step in the CIRAM intelligence cycle. It involves the production and dissemination of intelligence reports based on the analysis and interpretation of collected information. The reporting step serves also, the purpose of communicating the findings and insights derived from the intelligence analysis to relevant stakeholders, decision-makers, and consumers of the intelligence.

Dissemination: It is a crucial step involving the distribution of finished intelligence reports and findings to the intended consumers, such as policymakers, security agencies, or risk management teams. The goal of dissemination is to ensure that the relevant stakeholders receive the information, effectively and timely, so as to utilize it effectively for decision-making and risk management.

Review: This step occurs at the end of the intelligence cycle and involves assessing the effectiveness and accuracy of the intelligence analysis. Its key points include the evaluation of analysis, its accuracy and completeness, the verification of the findings, the feedback incorporation for the future analytical procedures and the continues improvement of the analysis methodologies.



Figure 1: CIRAM 2.0 Intelligence Cycle

CIRAM Threat, Vulnerability and Impact components

As it was mentioned above, the model application relays as a function on threat, vulnerability, and impact. The final risk is considered as an assessment of these three components, following the application and establishment of ISO 31000 and 31100 basic principles, in its function. In the components assessment, the analyst should take into consideration both qualitative and quantitative data and cover a specific time period and geographical area.

$$\mathbf{R = f (TVI)}$$

Moreover, the threat is defined as a force or pressure acting upon the external borders that is characterized by both its magnitude and likelihood (Frontex, 2012). The analysis should identify, describe and measure the factors both inside and outside the EU that affect the threat volume. The threat assessment includes the sections of:

Modus Operandi: It refers to methods or patterns of operation, particularly in the commission of a crime, terrorism or generally illegal activity.

Who, where, when: The basic analytical questions to establish the main need of threat assessment.

Trends and predictions: Referring to quantitative indicators that arise from past statistical reports and lead to future occurrence predictions.

Push factors: Indicators and factors that “push” people to leave areas and travel toward other places.

Routes and access to facilitation: Factors that indicate travel routes and the existence of facilitation in specific areas.

Additionally, vulnerability assessment provides an overall evaluation of the vulnerabilities present in the border management systems and processes (Frontex, 2012). It takes into account upcoming challenges, monitoring of the situation along the external borders, and the assessment of Member States' contributions to the rapid reaction pool. It includes the sections of:

Border permeability: It refers to ease or difficulty with which individuals, goods, or illicit activities can cross a border, encompassing various aspects such as terrain, infrastructure, capabilities, and flows that can affect the ability to control and secure the border.

Operational activities: Various actions and tasks carried out as part of border management and security operations. These activities can include border surveillance, patrolling, intelligence gathering, risk assessment, and response planning.

Effectiveness of countermeasures: Specific descriptive comparison of measures taken in the external and internal EU area in accordance to EU border protection and the level of their success.

Pull factors: Factors associated with migration or mobility patterns, attracting or pulling individuals or communities towards specific locations or countries. These factors may include economic opportunities, employment prospects, social benefits, or other favorable conditions that make a particular destination attractive for migration.

Ultimately, impact assessment appears to be related to the evaluation or analysis of potential impacts associated with threats, taking into consideration the vulnerabilities that are related also to the threat (Frontex, 2012). Impact encompasses the sections of:

Border and Internal security: It contains all the possible impacts in the border and internal security, connected to law enforcement and border security personnel, infrastructures, as well as the states and governments' physical and economical assets and nationals.

Ability to manage legitimate passenger flow at border: The EU member states ability to manage properly without any problem the passenger passing flow in every border crossing point.

Humanitarian impact: It includes every impact on human lives.

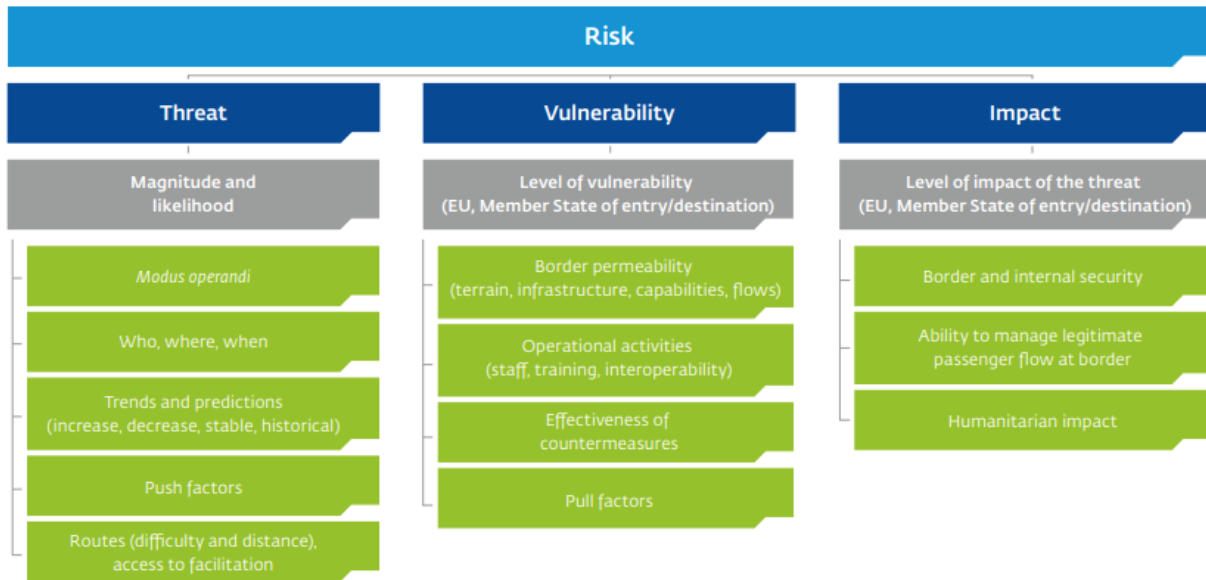


Figure 2: CIRAM 2.0 Risk Assessment parts

Counterterrorism and Security Risk Analysis

Counterterrorism generally refers to strategies and efforts, in the tactical, operational and strategic level, aiming to prevent, respond to, and mitigate acts of terrorism (Richards, 2018). It involves various measures that aim on detecting, deterring, and disrupting terrorist activities, as well as protecting individuals, infrastructure, and societies from terrorist threats (Hughes, 1982). The main methodologies of countering terrorism acts, incorporate law enforcement intelligence collection and analysis that lead to decision making in regard of the countermeasures and operations need to be settled (Bures, 2010). Also, because of the internationalized nature of the threat, it is crucial important for the states to promote international agencies' cooperation and information sharing, as expertise helps in identifying and tracking these transnational networks (Lowe, 2014).

In the Border Security level, counterterrorism efforts often include strengthening border security and management to prevent the movement of terrorists, weapons, and illicit goods across borders. This may also involve implementing advanced technologies, intelligence sharing, and coordinated border control operations. In this regard, Risk Analysis model, eventually containing information and intelligence of terrorism threat, a specific area's vulnerabilities and the impact the terrorism, could be applied (Rios, and Insua, 2011).

Eventually, in Europe the threat of terrorism primarily arises from jihadist terrorism, but there has also been a rise in right- and left-wing extremism (Zmire, and Kim, 2017; Marrero Rocha, 2018). The evolution towards the radicalization of the persons involved is a complex process differs, depending on the social and physical environment (Webb, and Sutton, 2016). The environment may determine in a high volume the appearance of behavioral tendencies to support specific terrorist organizations (Kumar and Mandal, 2012; Nesser et al, 2016). In regard of the well-known case of Abdelhamid Abaaoud, specific factors such as the feeling of belonging to an ethnic population and religious group, the involvement from an early age in organized crime and connections with persons in foreign countries, can lead to the inclusion of persons in the cycle of terrorist activity (Van Vlierden, 2015; Teich, 2016; Marrero Rocha, 2018).

In due course, the set of quantitative data and information on the occurrence of terrorist attacks and actions, as well as its qualitative characteristics, can be an information source, which under an appropriate methodology of intelligence cycle and in accordance to risk analyses processes, can yield synergistic analytical products, in the direction of dealing with the terrorism phenomenon (Rios, and Insua, 2011; Richards, 2018).

CIRAM application on Counterterrorism

Since at European level the protection of external borders tends to be based on CIRAM, it is decisive to examine the appropriateness of the model, both in terms of data and information collection and management procedures, as well its capabilities the analysis of all available information and intelligence (Liashuk and Tsaruk, 2021).

Beginning with the threat components, it is obvious that is a platform for combining information that is essential for mapping terrorism. It is widely known that terrorist organizations often present concrete structure based on qualitative data of ethnic or religious origin. For example, terrorist organizations such as al-Qaeda and the Islamic State present different qualitative characteristics with organizations such as Hezbollah, both in terms of the geographical origin of their members and in terms of their religious beliefs. However, this operational approach is not fixed and can vary on a case-by-case basis, such as the occasions of joint operational activity by members of Shia and Sunni Salafist organizations in the Middle East and the Balkans (Đorđević, 2018; Marrero Rocha, 2018). In these instances, the processing of information such as the modus operandi the illegal transit routes utilized by the terrorists, can clarify the organization of their origin. Besides, social and religion push factors can determine the focus of terrorist activity of specific population groups (Đorđević, 2018).

Furthermore, the CIRAM vulnerability function, embrace all the possible aspects that could be threatened by terrorism. Specifically, terrorism often aiming to strike vital border protection and internal security infrastructure of a state, so as to cause chaos and security uncertainty for citizens. Damage invitations often target border infrastructure, causing problems in their perpetual operation (such as airports). At this level, getting aware of the effectiveness of measures to protect infrastructure, borders and the internal state security is decisive for defining future needs and reducing possible exposure to risks. Plus, it is important to identify and monitor specific pull factors that drive terrorists to travel to regions and countries, such as the maintenance of terrorist networks and terrorist financial infrastructure, such as the hawala system (Hancock, 2008).

Moreover, the impact of terrorism can be far-reaching and significant. The loss of life, the property, infrastructure and property damage, the possible suspension of economic activity, the reduction of citizens' trust in the internal security of the state and other factors, can lead to macro-environmental problems. The components of CIRAM impact assessment, includes the whole possible aspects, determining significantly the total Risk assessment of a threat.

Conclusions

Consequently, the legislative and institutional evolution of the European Union led to the formation of institutions, services, and analysis methodologies with aim to protect the external borders of the Union and the internal and national security of the Member States.

In this direction, the creation of CIRAM is a serious evolution of the formation of the appropriate procedures for the proper collection, processing, management, analysis and exchange of information and intelligence. The elements of CIRAM seem to correspond to the intelligence processes for dealing with terrorist threats and appear to be ideal for studying and promoting Counterterrorism measures. Finally, a future study of the model can be done regarding its applicability in the field of Counterintelligence.

References

- Bonta, J., Law, M., & Hanson, K. (1998). The prediction of criminal and violent recidivism among mentally disordered offenders: A meta-analysis. *Psychological Bulletin*, 123(2), 123-142.
- Bures, O. (2010). Eurojust's fledgling counterterrorism role. *Journal of Contemporary European Research*, 6(2), 236-256.
- Đorđević, V., Klemenc, J. and Kolářová, I. (2018). Regional security cooperation reinvented: Western Balkans counterterrorism initiative. *European Security*, 27(4), 415-433.
- Fernández-Rojo, D. (2021). *EU migration agencies: The operation and cooperation of Frontex, EASO and Europol*. Edward Elgar Publishing.

- Fitz-Gerald, A. (2008). A UK National Security Strategy: Institutional and Cultural Challenges. *Defence Studies*, 8 (1), 4-25.
- Frontex, Common Integrated Risk Analysis Model a comprehensive update (2012). Warsaw.
- Frontex, Common Integrated Risk Analysis Model Summary booklet (2013). Warsaw.
- Frontex, Guidelines for risk analysis units: Structure and tools for the application of CIRAM version 2.0 (2012). Warsaw.
- Hancock, D. A. (2008). *The olive branch and the hammer: A strategic analysis of hawala in the financial war on terrorism*. Monterey. CA; Naval Postgraduate School.
- Hansen, F. and Pettersson, J. (2021). Contradictory migration management? Differentiated security approaches to visa overstay and irregular border crossings in the European Union. *European Security*, 31(1), 117–134.
- Hughes, M. (1982). Terrorism and National Security. *Philosophy*, 57(219), 5–25.
- Jeandesboz, J. (2020). European border policing: Eurosur, knowledge, calculation. *The Policing of Flows*, 92–121.
- Léonard, S. (2010). EU border security and migration into the European Union: FRONTEX and securitisation through practices. *European Security*, 19(2), 231–254.
- Liashuk, R. and Tsaruk, A. (2021). Experience of information and analytical activities in the field of Border Protection of the European Union. Proceedings of the International Conference on Economics, Law and Education Research (ELER 2021).
- Lowe, D. (2014). Surveillance and International Terrorism Intelligence Exchange: Balancing the Interests of National Security and Individual Liberty. *Terrorism and Political Violence*, 28(4), 653–673.
- Maier, C. (1993). Peace and security for the 1990s, Social Science Research Council.
- Manjarrez, V. M. (2015). Border Security: Defining it is the Real Challenge. *Journal of Homeland Security and Emergency Management*, 12(4), 793–800.
- Marrero Rocha, I. (2018). The European Union’s Foreign ‘terrorist’ fighters. *Jihadism, Foreign Fighters and Radicalization in the EU*, 44–63.
- Nesser, P., Stenersen, A. and Oftedal, E. (2016). Jihadi Terrorism in Europe: The IS-Effect. *Perspectives on Terrorism*, 10(6), 3-24.
- Oliveira Martins, B., Lidén, K. and Jumbert, M. G. (2022). Border security and the digitalisation of sovereignty: insights from EU borderwork. *European Security*, 31(3), 475–494.
- Regulation (EC) 2007/2004, OJ L 349/1.
- Regulation (EC) 562/2006, OJ L 105/1.
- Richards, J. (2018). Intelligence and counterterrorism. *Routledge Handbook Of Terrorism And Counterterrorism*, 395–405.
- Rios, J. and Insua, D. R. (2011). Adversarial Risk Analysis for Counterterrorism Modeling. *Risk Analysis*, 32(5), 894–915.
- Teich, S. (2016). Islamic Radicalization in Belgium. International Institute for Counter-Terrorism.
- Updesh Kumar and Manas K. Mandal (2012). *Countering Terrorism: Psychosocial Strategies*. New Delhi: Sage Publications Pvt. Ltd.
- Van Vlierden, G. (2015). Profile: Paris Attack Ringleader Abdelhamid Abaaoud. *CTSENTINEL*, 8(11), 30-35.
- Webb, E. and Sutton, R. (2016). An Enduring Threat: Europe’s Islamist Terror Networks Then and Now. [online] The Henry Jackson Society - Centre for the Response to Radicalisation and Terrorism. Available at: <<https://henryjacksonsociety.org/centre-on-radicalisation-and-terrorism/>> (Accessed: 18/09/2023).
- Zmire, Z. and Kim, Y. (2017). *Causes of Rising Homegrown Terrorism in Europe: A Case Study of 2015 Paris Attacks*. Master. Hanyang University.