Dr Marián Kolenčík, President of the Management Board of the International Security and Emergency Management Institute on detection of CBRN and explosive terrorist act risk indicators

Watching the indicators

Introduction

Terrorist attacks involving explosives and CBRN materials are a persistent global threat, shaped by advances in technology and changing geopolitical landscapes.[1,8] Historical data shows that while explosive attacks are prevalent, CBRN use remains limited, with for instance western Europe experiencing only 47 such incidents between 1970 and 2019 compared to thousands of explosive and firearms attacks.[12] Countries like the UK, France, and Spain have faced the highest number of terrorist incidents in general, underscoring the need for vigilant security strategies. That said, CBRN threats remain a significant challenge in the global security landscape, and early detection is crucial task for law enforcement and intelligence agencies.

In response to such threats, predictive profiling and behavioural analysis have emerged as key counterterrorism measures. These techniques use behavioural patterns and manipulation with various objects or physical appearances to identify potential threats. Though effective when combined with technologies like screening machines, detectors or bomb sniffer dogs,[2,5] these approaches raise ethical and privacy concerns, as critics question their reliability and potential for bias.[14,6] Nonetheless, they have shown promise in preventing high-risk situations, particularly in settings like airports and transportation hubs[4].

Governments worldwide have developed robust measures to combat CBRN terrorism, particularly in high-risk areas like public transport.

Predictive profiling and behavioural analysis have emerged as key counterterrorism measures ©M. Kolencik

Watching the indicators

Countries such as the US, UK, and France have implemented specialised training programmes and surveillance measures following incidents like the 9/11 attacks.[7,11] In another example, Georgia's response to the Tbilisi airport Yperite attack highlights the importance of CBRN-specific preparedness, including training security forces.[9,10] International cooperation remains critical, as such attacks can cause mass casualties, psychological trauma, and widespread societal disruption.[3,13]

Research approach

We therefore decided to investigate the importance of identifying early warning signs of CBRN or explosive terrorism, including unusual behaviour, use of certain tools, digital footprints, symptoms of contamination, infection or intoxication and other alarms. Case studies and archival analyses, including CCTV footage and police reports, reveal patterns that can aid predictive profiling. While our research focussed on Europe, these findings have global implications, offering strategies to enhance law enforcement capabilities and improve early detection. Alongside countermeasures, policymakers and security agencies must balance the need for effective counterterrorism with respect for civil liberties, integrating advanced technology and public transparency into their approaches, to safeguard against evolving threats.

The research combined quantitative and qualitative methodologies, prioritising the latter as they are able to explore complex topics in depth, where standardised methods might fail. The methodology involved three key steps; a systematic literature review, case studies utilising the ISEM Institute's internal resources (including prosecution files, court decisions, and CCTV footage), and an online survey targeting law enforcement and intelligence agency officers from 12 countries and two EU agencies.

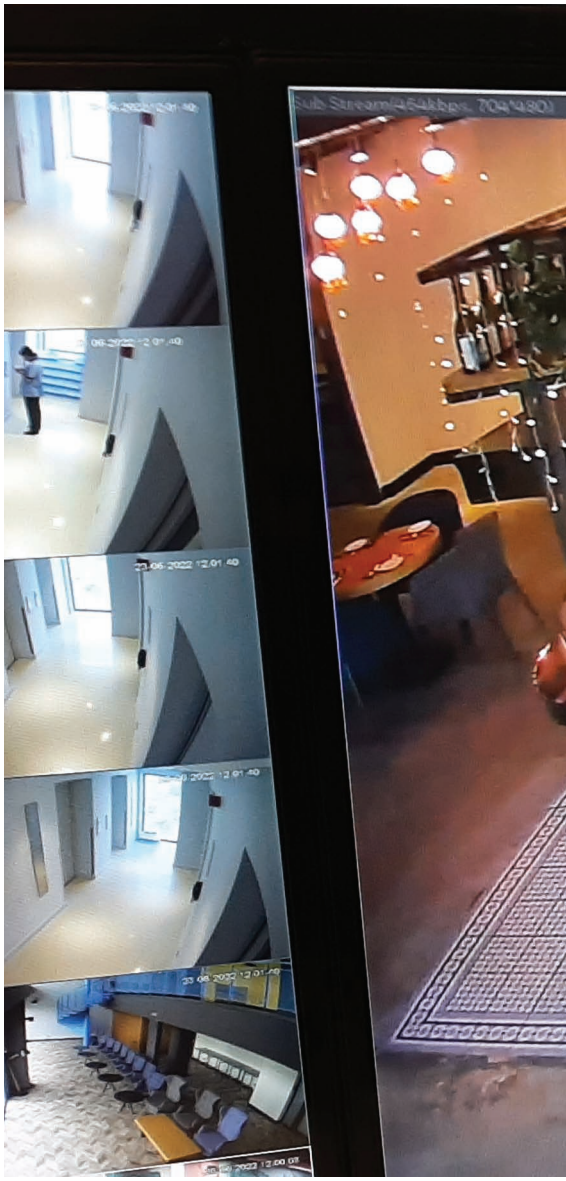
A comprehensive search strategy was used for the literature review, encompassing academic articles from leading journals in security, criminology, psychology and counterterrorism, as well as credible legal documents and guidelines like those from the European Border and Coast Guard Agency, Frontex. Sources were carefully evaluated for quality and relevance, leading to the selection of 103 articles out of 126 initially identified. Keywords, inclusion and exclusion criteria, and specific parameters like language and publication dates guided the process to ensure rigorous analysis of CBRN and explosive terrorism risk indicators.

This approach allowed us to develop a robust framework for identifying potential risk indicators associated with CBRN and explosive crimes, considering case studies, observed behaviours, and technological markers.

Created categories and their indicators were included in the survey. This most important part of the research, served to assess the importance and priority of CBRN and explosive related risk indicators among law enforcement and intelligence agencies from 12 European countries, along with Frontex and the EU Agency for Law Enforcement Training, Cepol. Facilitated by the ISEMI Institute, the study took a comprehensive approach to gathering expert input while ensuring ethical standards, anonymity and confidentiality.

Participants were selected by various national authorities based on their expertise in dealing with real cases of counterterrorism and CBRN/explosive ordnance disposal, and evaluated the reliability and relevance of identified indicators. The questionnaire, developed from systematic reviews and case studies, included informed consent protocols and complied with ethical standards. It aimed to validate risk detection strategies while ensuring practical and secure data collection. Statistical analysis, such as chi-square tests, explored correlations between respondent demographics, like age and experience, and their evaluations of risk indicators. This helped refine operational and investigative tactics in detecting imminent threats.

Using ISEMI's secure platform, SIENA X IT, the survey collected feedback from police and intelligence officers identified as the target population, accounting for their professional duties and participation in ISEMI's established network. The study emphasised collaborative, non-discriminatory analysis, ensuring that indicators were assessed holistically to avoid bias or inefficiency. A total of 50 participants from Belgium, Bosnia and Herzegovina, the Czech Republic, Estonia, Finland, France, Georgia, Germany, Luxembourg, Portugal, Slovakia, the UK, and Frontex and Cepol participated in the survey. Although the targeted participant number was not

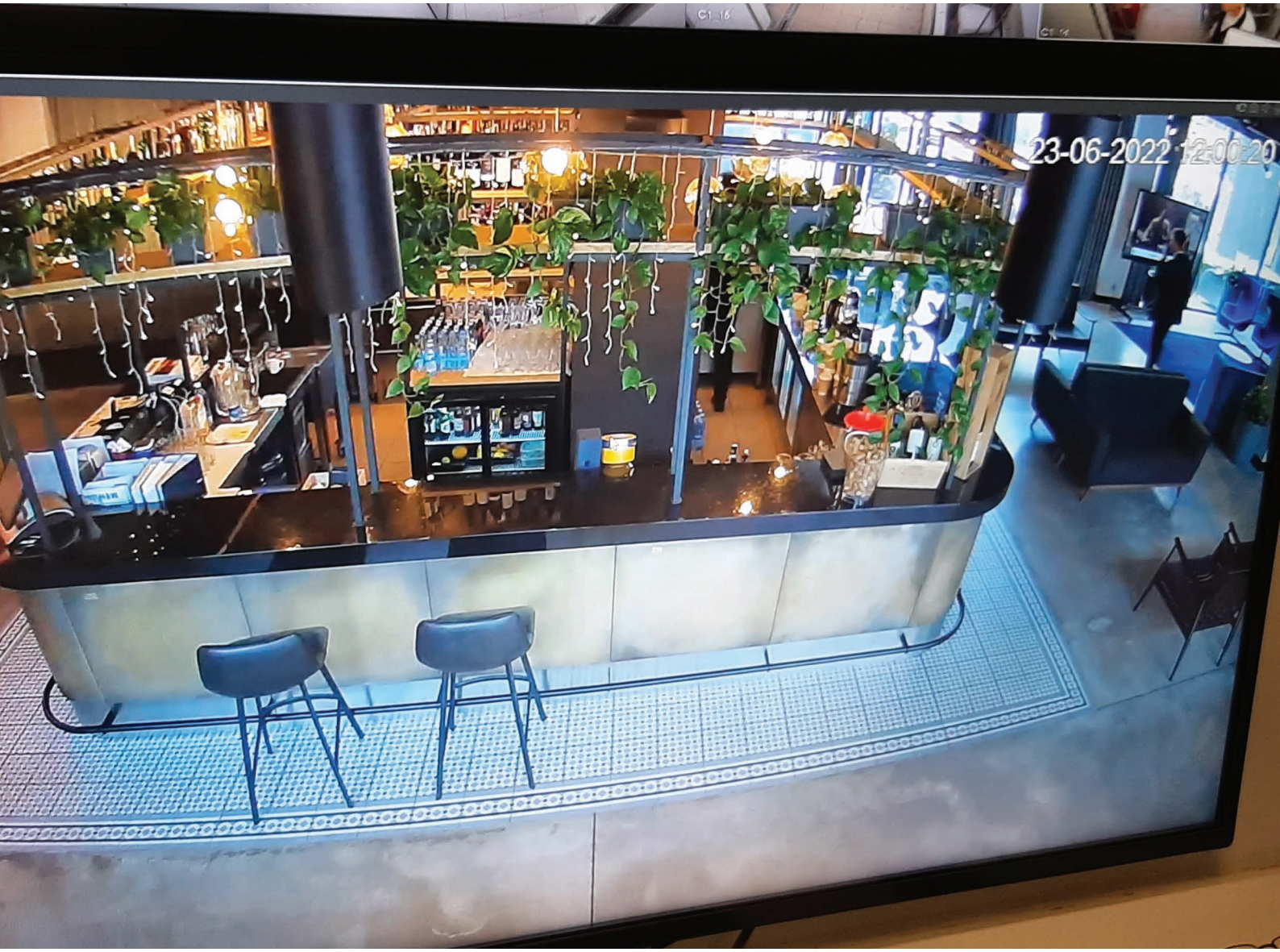


reached in the planned timeframe, the sample provided valuable insights from law enforcement and intelligence officers specialising in CBRNE terrorism. Due to the sensitive nature of this very narrow field, obtaining sufficient qualified experts for a statistical sample proved challenging.

Research results

Key findings revealed a lack of professional, empirical studies and standardised baselines for risk indicators, particularly for early detection of such crimes. Therefore the study addressed the need for empirical validation and enhanced training to reduce false positives and negatives. It noted the dynamic nature of baselines and emphasised their importance in identifying anomalies during public events or while performing security duties in critical infrastructure or public transportation. This foundational review informed subsequent phases of the research, focusing on operational and detection strategies despite limitations in existing literature.

The study draws attention to significant gaps in scientific research on CBRNE risk indicators, making the analysis of real world cases invaluable. The ISEMI Institute provided extensive case studies, security documents and court decisions to establish categories of risk indicators. CCTV footage from several high profile terrorist attacks, including the 9/11 and 2005 London bombings, the 2016 Brussels attacks, 2017 Manchester Arena explosive attack, and the 2018 Yperit attack, as well as lesser-known cases, helped identify behavioural, physiological and technological indicators across different stages of terrorist acts. These indicators covered the planning, execution and post attack phases, contributing to the



CCTV footage helped identify behavioural, physiological and technological indicators across different stages of terrorist acts ©M. Kolencik

Watching the indicators

development of a comprehensive risk assessment framework.

This research aims to evaluate the relevance and observability of various risk indicators used in threat detection. Analysis is based on responses to survey questions that assess the overall relevance of broad categories of risk indicators and the detailed relevance of subcategories. The findings highlight two key aspects; the prioritisation of risk indicators based on their perceived relevance, and the ease or difficulty of detecting or observing these indicators.

Regarding relevance, respondents ranked various categories of risk indicators. The first category to emerge as most relevant was Technological Detection/Air Sampling Alarm Risk Indicators, with a significant 93.6% of respondents considering it highly relevant. This was followed closely by Digital Indicators, with 89.4% of respondents highlighting its importance. Two categories, namely Items, Documents, Objects, and Other Belongings Detected on the Person (indicating signs of radicalisation or criminal activity), and Behaviour and Communication, tied for third place with 89.3% of responses indicating strong relevance. Other notable categories, like Specific Indicators of Previous Radicalisation and Insider Threat Risk Indicators, also ranked highly, with relevance percentages above 85%.

When examining subcategories within these broader categories, a shift in rankings occurred, revealing respondents' more detailed preferences. For instance, within the Digital Indicators category, the subcategory on Videos Containing Terrorist Propaganda garnered most support, with 91.3% relevance, while subcategories like Applications Detected by Covert Operational Activities ranked lower. Similarly, in the Technological Detection/Air Sampling Alarm Risk Indicators category, subcategories related to Explosive Detection Technology and Radiation Detector Alarms achieved the highest relevance, nearing 89.4%, while others, like Ionising Radiation Scanning Equipment, were still highly relevant but rated slightly lower at 82.6%.

Relying solely on behavioural detection might be insufficient and requires expertise across various fields ©M. Kolencik

The study also evaluated the ease of detecting or observing these indicators. Respondents indicated that Technological Detection/Air Sampling Alarm Risk Indicators were easiest to detect, with an average score of 67.1% across the subcategories. Specifically, subcategories like Ionising Radiation Scanning Equipment Alarm showed the highest detection potential, at 72.8%. On the other hand, categories like Behaviour and Communication, and Sound were rated harder to observe, with averages of 38.8% and 45.6%, respectively. Subcategories like Paralinguistics, and Other Suspicious Sounds scored lowest in terms of detectability, indicating challenges in observing such indicators in real world scenarios.

The survey then examined whether the identified risk indicators from the literature and case studies were useful for training security professionals. An overwhelming 82% of respondents agreed that these indicators were valuable for such purposes, emphasising their utility in preparing for preventive security operations. Some participants highlighted the list's comprehensiveness, stating that it provided crucial insights into identifying potential threats and should be used in security training, while several respondents suggested

Watching the indicators

additional risk indicators that could further improve threat detection. These related to specific means of transportation, financial transactions, the individuals' digital footprints, monitoring of AI search content, and unusual behaviours linked to mental health histories, like past suicidal tendencies or aggression. Incorporating these factors could enhance the ability to detect potential CBRNE threats beyond digital technologies and provide more comprehensive coverage for security operations.

Critical feedback from some participants raised concerns about the practical challenges of using these indicators. For example, one respondent pointed out that relying solely on behavioural detection might be insufficient and requires expertise across various fields. The need for a well trained behavioural specialist was emphasised, as the ability to interpret behavioural cues in the context of larger investigations is crucial. Again, the complexity of tracking multiple variables, as noted by a participant with law enforcement experience, suggested that while the list of indicators is extensive, real world operations often require integrating a broader range of factors, including environmental, psychological and contextual elements in connection to established baselines.

A police officer with over 15 years' experience highlighted the critical role that even seemingly minor indicators play in investigations, saying that every piece of information, no matter how small, can be vital in building a comprehensive picture of a potential threat. The officer emphasised the importance of using these indicators both individually and collectively, as a single indicator, when coupled with others, can raise professional suspicion and potentially prevent attacks.

Finally, respondents expressed overall support for the research and the risk indicators identified. Many found the list valuable for real world security operations, praising its potential to improve threat identification in diverse scenarios. Some participants also suggested linking the indicators to specific scenarios for practical application, which could further enhance the training process and real time threat detection.

Conclusion

The research reveals that the comprehensive risk indicators identified and defined baselines are highly relevant and useful for both threat detection and training purposes. While some indicators were more easily detected than others, the diversity of risk categories and subcategories allows security professionals to develop a more nuanced understanding of potential threats. Moreover, the feedback indicates that incorporating additional risk indicators and improving the practical application of behavioural detection could further enhance the effectiveness of security measures against a wide range of threats.

Following this research, ISEM Institute updated specific training programmes on Profiling in Protective Security and was accredited by the Slovak national authority using EU lifelong learning standards. It regularly conducts this type of training for various law enforcement and intelligence agencies worldwide.

ISEMI has already used the risk indication methodology in cooperation with law enforcement agencies in various mass gathering events, such as the South East Asia Games in 2023, airports, and criminal investigations.

The full research, including all categories and subcategories of risk indicators, will be published in a widely recognised security journal. Due to its sensitivity, the full list of indicators is available only for law enforcement and intelligence agencies.

[1] Binder, M. and Ackerman, G. (2021). Pick your POICN: Introducing the profiles of incidents involving CBRN and non-state actors (POICN) database. Studies in Conflict and Terrorism 44(9): 730–754.2. Cavusoglu, H., Kwark, Y., Mai, B., & Raghunathan, S. (2013). Passenger profiling and screening for aviation security in the presence of strategic attackers. Decision Analysis, 10(1), 63-81.
[3] European Parliament – TERR Committee (2018). Member states´ preparedness for CBRN threats. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604960/IPOL_STU(2018)604960_EN.pdf
[4] Feijoo-Fernández, M. C., Halty, L., & Sotoca-Plaza, A. (2023). Like a cat on hot bricks: The detection of anomalous behavior in airports. Journal of Police and Criminal Psychology, 38(1), 72-82.
[5] Fernández, M. D. C. F. (2021). Guardia Civil's ICARO teams: Behaviour analysis at airports and ports. Cuadernos de la Guardia Civil: Revista de seguridad pública, (66), 111-125. ISSN: 2341-3263.
[6] Granhag, P.A., Mac Giolla, E. (2014). Preventing future crimes. Eur Psychol 19(3):195–206. https://doi.org/10.1027/1016-9040/a000202
[7] Haggerty, K. D., & Gazso, A. (2005). Seeing beyond the ruins: Surveillance as a response to terrorist threats. Canadian Journal of Sociology/Cahiers canadiens de sociologie, 169-187.
[8] Koehler, D., & Popella, P. (2020). Mapping far-right chemical, biological, radiological, and nuclear (CBRN) terrorism efforts in the west: Characteristics of plots and perpetrators for future threat assessment. Terrorism and Political Violence, 32(8), 1666-1690.
[9] Kolencik, M. (2021). Criminal and Terrorist Profiling (Lecture I. – Law Enforcement in Central Asia – www.project.leica.eu, EU funded project). November 2021, ISEM Institute, www.isemi.sk. https://doi.org/10.52824/BMER5598
[10] Kolencik, M. (November 2021). National ToT on the identification of FTF and profiling techniques - Criminal and Terrorist Profiling, Law Enforcement In Central Asia (LEICA) funded by the EU. DOI: 10.52824/BMER5598
[11] Rudner, M. (2015). Intelligence-led air transport security: Pre-screening for watch-lists, no-fly lists to forestall terrorist threats. International Journal of Intelligence and Counterintelligence, 28(1), 38-63.
[12] Tin, D., Barten, D. G., De Cauwer, H., Mortelmans, L. J., & Ciottone, G. R. (2022). Terrorist attacks in Western Europe: a counter-terrorism medicine analysis. Prehospital and disaster medicine, 37(1), 19-24.
[13] Walsh, P. F. (2021). Evolving chemical, biological, radiological and nuclear (CBRN) terrorism: Intelligence community response and ethical challenges. In National Security Intelligence and Ethics (pp. 261-279). Routledge..
[14] Wigginton M. Jr., Jensen, C.J., Graves, M. & Vinson, J. (2014). What Is the Role of Behavioral Analysis in a Multilayered Approach to Aviation Security?, Journal of Applied Security Research, 9:4, 393-417, DOI: 10.1080/19361610.2014.942828