Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 317-322

Joint Information System Model Appliance in Man-Made Crisis Management

Laila Vaivode
State Police College
Department of Humanity Science;
Business University "TURĪBA"
Riga, Latvia
vaivode.laila@gmail.com

***Abstract*- Several crisis communication models can be applied in the discourse of man-made crises occurrence, such as terrorist attacks, cyber-attacks, or explosions caused by negligence and other similar events. However, one of the most comprehensive models in practical terms- and yet one of the least scientifically researched- is the Joint Information System (JIS) model. By nature, the resolution of such critical incidents, which are driven by human intention and action, requires the involvement of multiple actors, primarily state security institutions, as well as non-governmental organizations and possibly others. The JIS model thus provides a collaborative framework for crisis communication, involving multiple stakeholders, including government emergency responders, media representatives, community leaders and other actors depending on the type of incident. The JIS approach subsequently ensures that critical information dissemination is coordinated, consistent and effective in addressing the needs of all involved parties. The JIS model is based on five key principles: 1) Integrated communication, which requires collaboration among all stakeholders to ensure a unified message development and delivery, 2) Audience-focused communication, which prioritizes understanding the concerns and informational needs of different audiences to tailor messages accordingly, 3) Timely and accurate communication, which ensures that stakeholders receive reliable and up-to-date information throughout the various crisis phases, 4) Credible communication, which focuses on building trust and maintaining the credibility of information sources and 5) Continuous communication, which highlights the importance of sustained information-sharing in the precrisis stage and throughout both the crisis management and recovery phases. Recovery from a man-made crisis, including but not limited to terrorist incidents, is a complex and multifaceted process that encompasses physical, emotional, social, and economic dimensions. In the aftermath of such events, effective communication is crucial for maintaining public safety, disseminating critical information and mitigating the psychological and social impacts of the crisis on affected areas and citizens. This paper examines the application of the JIS model in man-made crisis scenarios, analysing its effectiveness in ensuring structured and transparent communication. The research employs a qualitative analysis of past crisis events where the JIS model has been implemented, drawing insights from case studies and best practices that are available online. The findings indicate that the JIS model significantly enhances crisis response by fostering coordination among stakeholders, reducing misinformation and improving public trust, consequently- maintaining reputational aspects of the state authorities high, that is one of the cornerstones of the successful crisis management. Overall, the JIS model is a highly effective approach to crisis communication, particularly in the context of man-made crises. By adhering to its principles, organizations can enhance their crisis management capabilities, minimize the adverse impacts on affected communities, and facilitate a more efficient recovery process.**

Keywords*- *Crisis communication, Joint Information System (JIS) model, man-made crisis management by state governed security authorities.

I. INTRODUCTION

This study aims to evaluate the role of Joint Information System model in enhancing crisis response mechanisms, with particular attention to their potential applicability within the newly developing Latvian Crisis Management Centre. It investigates how JIS can improve communication, ensure inter-agency coordination, and enhance public trust during man-made crisis events. By analysing real-world implementations and established best practices, the study highlights the effectiveness of JIS and provides practical recommendations for its adoption, especially valuable for emerging systems still in development,

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8503

A critical finding of the research is the notable scarcity of academic literature focused specifically on JIS. Existing studies often address broader crisis management topics or focus on technological dimensions (e.g., IT systems), despite JIS being a pivotal component in state-led security and emergency responses. It is routinely applied in real-world incidents that involve multi-agency collaboration, such as police, fire brigades, and emergency medical services.

Though extensively used in countries such as the United States, Australia, Canada, and the United Kingdom, scholarly attention to JIS remains limited. Regardless of the size and number of state or federal agencies involved, the JIS model has consistently demonstrated its value in delivering accurate, timely, and coordinated communication across entities. Over decades, it has proven its utility in practical applications, even though it has rarely been the central focus of academic inquiry.

One key research observation is that the JIS model has been adopted globally and is recognized as an effective and practical tool in managing both natural and man-made emergencies. For this study, a comparative analysis was conducted across four countries-Australia, the USA, the UK, and Canada-each representing a multilayered emergency governance structure across three continents. Although it is difficult to trace the exact origins of JIS in each country due to limited historical documentation available publicly, its universal appeal and practical value suggest that the model either developed independently in response to operational needs or was informally adopted based on its effectiveness (ref.: TABLE 1.).

TABLE 1. JIS SIMILARITIES AND DIFFERENCES

Feature	**Australia**	**USA**	**UK**	**Canada**
Structure	Decentra-lised, state- led	Federal interven-tion possible	Centralised national control	Provincial-led, federal support
Incident Command System	AIMS	ICS (NIMS)	JESIP (JDM)	IMS
Use of JIS/JIC	Forest fires, flood, security incidents	Hurricanes wildfires, terror events	Security threats, public health crisis	Wildfires, floods, pandemics
Public informa-tion coordina-tion	SES, EMA, BoM, Police	FEMA, JIC's	JESIP, COBR	Public Safety Canada

A coordinated information system like JIS plays a vital role in modern crisis management by enabling:

a) *Rapid information sharing*, ensuring that real-time updates on crisis developments reach both responders and the public efficiently [5].

b) *Consistency and accuracy*, preventing rumours, misinformation, and speculation by maintaining a single, verified source of truth [6].

c) *Public trust and engagement*, enhancing compliance and reducing panic by communicating transparently, clearly, and effectively [7].

d) *Efficient resource coordination*, helping emergency services deploy personnel and materials strategically while also activating volunteer or NGO support when needed [8].

Without a structured communication system like JIS, crisis responses risk fragmentation, misinformation, public confusion, and operational inefficiency.

II. MATERIALS AND METHODS

Timely and coordinated communication is fundamental in any emergency response. JIS is not just a helpful tool, it is a structured, scalable framework for managing and disseminating information across all involved parties, including government agencies, stakeholders, media, and the public.

Case studies from the United States reveal how JIS has been successfully integrated into the National Incident Management System (NIMS). By enabling a synchronized flow of verified information, JIS helps prevent misinformation and supports unified decision-making—central to the ultimate goal of saving lives.

The purpose and importance of JIS. The core function of JIS is to ensure relevant, accurate, and real-time communication during emergencies (see *Fig. 1: Information Dissemination Model in JIS*). Whether the crisis involves natural disasters, cyberattacks, or public health emergencies, efficient communication can determine the success of the response and the level of public cooperation.

A. The role of Joint Information System in crisis management

Whether dealing with natural disasters, public health crises, or cyberattacks, effective communication plays a decisive role in determining whether a crisis is managed efficiently or escalates into widespread panic. The Joint Information System (JIS) allows agencies across various levels- local, regional, national, and federal- to collaborate seamlessly. This coordination ensures that accurate and timely information reaches both the public, who may still be at risk during the incident (e.g., in ongoing situations such as an "active shooter" scenario) and decision-makers within Joint Information Centre (JIC), where access to precise, up-to-date information is essential for informed and effective decision-making.

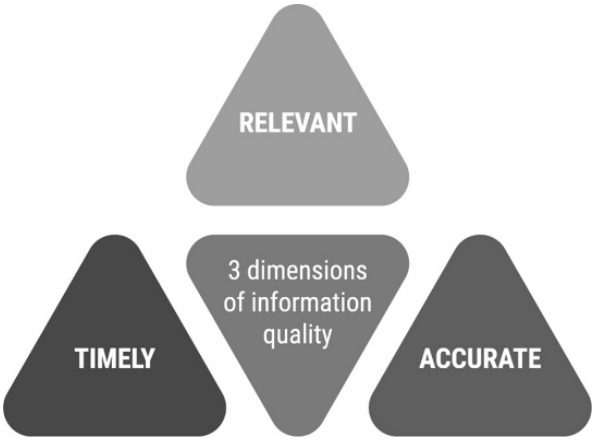

Fig.1. Information dissemination model in JIS.

By providing a centralized communication hub during multi-agency crisis responses, JIS significantly reduces the risk of confusion, misinterpretation, and misinformation, issues that frequently arise in complex emergencies. It ensures that messages are consistent, follow a unified strategy, and use standardized terminology, thereby avoiding contradictory statements that could hinder the crisis response and erode public trust. Maintaining public confidence is vital, as its absence can lead to reduced compliance in current and future emergency situations. Additionally, the system supports emergency personnel in making sound decisions based on real-time, verified data, ultimately strengthening the overall effectiveness of the crisis management process [9],[10].

Key Principles of JIS in Crisis Communication. JIS operates based on several core principles that ensure effective communication during emergencies:

- *Coordination and collaboration*: JIS promotes interagency coordination, even those under different ministries or jurisdictions, such as, emergency services, public health agencies, and law enforcement to share information and resources. This collaboration prevents duplication of efforts and ensures unified response. Importantly, it includes mechanisms for data protection and secure, controlled sharing of sensitive information and adhering to personal data protection rules.
- *Consistency in messaging:* one of the risk factors in crisis communication is possibility to operate with conflicting messages received from different agencies. To avoid public confusion, JIS ensures that all agencies use unified terminology and messaging strategies. This consistent communication is delivered across diverse platforms, including social media, to ensure clarity and avoid cognitive overload [11].
- *Timeliness and accuracy*: information in a crisis event must be rapidly disseminated while maintaining accuracy. JIS prioritizes real-time updates through multiple channels, which is especially vital for crisis managers at the different managerial levels and ensuring the public receives the latest developments, where possible, striving for even targeted message based on the community needs or territorial aspects of the incident.
- *Transparency and public trust*: keeping the public informed consequently fosters trust and compliance with emergency directives. Open communication reduces reliance also on unofficial sources and strengthens public confidence in official directives.
- *Flexibility and scalability*: JIS can be scaled up or down depending on the severity of the incident. It is flexible and adaptable to different crises, from local emergencies to national disasters as well as flexibility can be ensured by setting up the satellite or mobile centres as deemed necessary.

JIS as cross- Agency communication facilitator system. JIS comprises several structural and functional components:

- *Joint Information Centre (JIC)*: the JIC can be named as the central hub for coordinating public information efforts. It brings together Public Information Officers (PIOs) from multiple agencies to develop and distribute consistent messages. The JIC can operate physically being deployed on the spot or virtually, by coordinating and synchronising the content and delivering necessary messages depending on the crisis incidents' nature, manpower and other elements [12], [13].
- *Public Information Officers (PIOs)*: PIOs are responsible for gathering, verifying, tailoring and disseminating information to the media and public. These officials ensure that all messaging aligns with the overall crisis management strategy.
- *Interagency Briefings and Reports*: regular updates between all involved agencies ensures that all relevant actors have access to the latest information. Such briefings vary in frequency and length based on the stage of the incident. This prevents misunderstandings and allows for cohesive and coordinated decision-making.
- *Utilization of multiple communication channels*: JIS utilizes all available media-press, television, radio, websites, SMS alerts, and social platforms- to maximize outreach. The mobile messaging system is used in high-risk situations where are possible imminent threat. This ensures that messages reach diverse audiences effectively [14].

Real-world applications of JIS in crisis management. Historically the JIS has proven its effectiveness in various

high-risk situations, affecting safety and security of the society, including:

- *COVID-19 pandemic*: agencies like the FEMA, IMS and local health departments used JIS to coordinate public health messaging, ensuring consistent guidance on safety measures, vaccinations and response efforts.
- *Natural Disasters* (hurricanes, wildfires, earthquakes): in disasters such as Hurricane Katrina and California wildfires, JIS helped to streamline emergency alerts, evacuation orders and recovery updates, increasing solutions to ensure maximum safety [15].
- *Terrorism and security threats, including man-made crisis*: during events going back like the 9/11 attacks, JIS facilitated interagency communication between law enforcement, emergency responders, and governmental officials.

JIS remains one of the most practical, handy and effective tools for the crisis management as a process and interconnected communication aspects. The United Kingdom's JESIP (Joint Emergency Services Interoperability Principles) serves also as a model of publicly accessible training and decision-making tools. Dedicated website includes educational videos and structured communication guidelines (*see Fig. 2: Decision-Making Model in JESIP*).

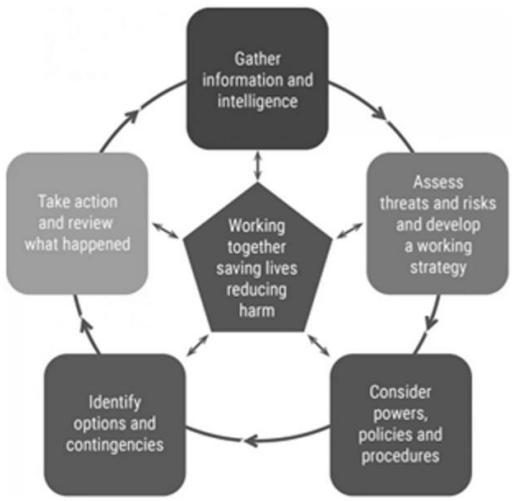

Fig.2 Decision making model in JESIP [2].

Applying JIS Models to Man-Made Crises. Following from the above findings and conclusions, it is evident that JIS is particularly relevant to the management of modern man-made crises, including:

- *Industrial accidents* (e.g., chemical spills, factory explosions and other accidents), by ensuring that affected communities receive also timely evacuation orders and safety instructions, followed by the psychological and medical care when required [16].
- *Cyber-Attacks.* Nowadays, when the number of cyber-incidents has significantly grown and continue to increase, JIS appliance allows to coordinate messaging between cybersecurity agencies, businesses, and the public to manage data breaches and minimize reputational [17].
- *Terrorism related incidents.* The JIS in terrorism situations is crucial mechanism, as it allows rapid managing public safety communications while preventing the spread of misinformation and panic as well as causing secondary damages [18].
- *Misinformation/Disinformation campaigns.* Often underestimated, but yet crucial from the security threats perspectives, especially when intentional disinformation campaigns can be causing significant impact both in short and long terms. By applying JIS, is possible to eliminate or minimise harmful narratives during elections, pandemics, or social unrest through consistent, fact-based messaging and proactive community engagement [19].

In each scenario, the JIS helps to ensure that all involved organizations are aligned in their messaging and response efforts.

B. Crisis management centralisation effort in Latvia

Latvia has recently undertaken significant structural reforms to strengthen its national crisis response capacity, notably through the establishment of a centralized Crisis Management Centre (CMC). This institutional innovation reflects a strategic shift towards more integrated and streamlined crisis management, with particular emphasis on improved inter-agency coordination, enhanced civil-military cooperation, and more effective public communication during emergencies [20].

As of January 28, 2025, the Latvian Government approved a series of draft legislative acts to create the Crisis Management Centre. The Centre is envisioned as a centralized hub responsible for managing various types of emergencies, including both natural and man-made crises. In line with global best practices, the CMC's mandate includes not only strategic oversight and decision-making, but also the operationalization of transparent and timely information flows- core components of an effective Joint Information System.

Structure and Functionality of the CMC. The CMC will operate under the direct authority of the Prime Minister [20], functioning as part of the State Chancellery. Its primary responsibilities include:

a. *Strategic Coordination during nation-wide threats.* The CMC will provide centralized coordination of crisis responses at the highest level, overseeing and synchronizing governmental actions across ministries and agencies during large-scale emergencies.

b. *Civil-Military cooperation*. Recognizing the increasing complexity of modern crises, the CMC will serve as a liaison platform to ensure seamless collaboration between civil authorities and the armed forces.

c. *Public communication.* A major responsibility of the CMC is to guarantee accurate, timely, and transparent public communication during crises. This reflects a core principle of the JIS model and is vital for maintaining public trust and compliance with emergency directives.

A particularly notable development is the planned establishment of a Situation Centre (SITCEN) within the CMC. This 24/7 operational unit will facilitate continuous monitoring, threat assessment, and real-time information exchange in cooperation with responsible institutions. SITCEN's role will mirror the intelligence-sharing and coordination functions typically embedded within the JIS framework in other countries.

To ensure the effective functioning of the CMC, the Latvian Government is concurrently implementing key structural and legal reforms:

- *Restructuring of the Crisis Management Council*. The Council has been expanded to include all Ministers, thereby institutionalizing cross-sectoral decision-making during national crises and aligning with comprehensive governance models seen in other advanced crisis management systems.
- *Empowerment of the Crisis Management Board*. This Board is now authorized to issue binding directives to state institutions, municipalities, legal entities, and individuals during declared civil crises. It also holds the statutory authority to declare a state of emergency, thereby enhancing Latvia's legal readiness for extraordinary situations [21].

The establishment of the CMC presents a critical opportunity to integrate the JIS model within Latvia's evolving crisis architecture. Key synergies include:

- *Institutional alignments.* With its centralized communication and coordination mandate, the CMC is structurally well-positioned to host or lead a JIS-style platform, including the creation of a Joint Information Center (JIC) or equivalent unit.
- *Operational readiness.* The SITCEN's continuous monitoring and threat assessment functions could serve as a backbone for a national JIS, facilitating real-time information flow to decision-makers, responders, and the public.
- *Public trust and transparency.* Given JIS's proven success in enhancing transparency and trust in crisis communication, its implementation in Latvia would significantly reinforce the country's efforts to ensure cohesive and coordinated messaging in emergencies.

In summary, Latvia's centralization of crisis management through the creation of the CMC demonstrates a forward-thinking approach grounded in international best practices. By integrating the JIS model into this new institutional framework, Latvia can further bolster its resilience against complex emergencies, particularly those of a man-made nature, and ensure that both decision-makers and the general public are equipped with the accurate and timely information necessary for effective response.

CONCLUSIONS

This research paper, along with prior practices, clearly indicates that the Joint Information System (JIS), both as a technical framework and as a decision-making process, is a critically important component of modern crisis management. It ensures that information shared across crisis management agencies is accurate, timely, and coordinated. By promoting collaboration, consistency, transparency and scalability, the JIS reduces confusion, builds public trust, and facilitates more effective emergency responses.

Mechanisms such as the Joint Information Center (JIC) and the role of Public Information Officers (PIOs) contribute significantly to streamlining communication between emergency management institutions and the public. These mechanisms enhance the overall responsiveness and resilience of crisis management efforts. As crises evolve in complexity, especially with the rise of hybrid threats, which are now more than just a theoretical concern, the role of JIS remains indispensable throughout all stages of crisis management: from the pre-crisis phase, through incident response, and into post-crisis recovery.

In light of these findings, it is important to emphasize that the establishment and ongoing development of Latvia's Crisis Management Centre (CMC) represents a major step forward. It reflects a clear commitment to advancing toward a joint European Union security management concept [22],[23],[24]. Within this framework, there is a strong need to develop and maintain a robust yet adaptable JIS model.

However, as Latvia embarks on this path, several challenges must be carefully addressed and prioritized-especially when considering JIS within the context of man-made crises:

- Data security and protection.
- Interoperability of systems already in use across various crisis management institutions [20].
- Legislative and administrative alignment.
- Public trust, reputational and ethical considerations.

Given that the Latvian CMC is still a relatively new institution and that it is expected to assume responsibilities not commonly centralized in other countries, such as enhanced civilian-military cooperation, there is significant scope for further research. Key areas for future study include:

- Integration of Artificial Intelligence (AI) and Big Data into the JIS, potentially leveraging models already developed within the European Union [25].
- Strengthening cross-border cooperation also in crisis communication and response aspects.
- Expanding public-private partnerships in the domain of security related emergencies.
- Enhancing training and capacity-building, including preparation for civil defence aspects.

In conclusion, the effective integration of the JIS into Latvia's evolving crisis management structure is not only a national priority but also a critical contribution to the broader European security architecture. It requires both strategic vision and ongoing adaptation to meet the dynamic challenges of today's threat landscape.

REFERENCES

[1] U.S. Department of Homeland Security, "National Response Framework," 4th ed., Oct. 2019. [Online]. Available: https://www.fema.gov/sites/default/files/2020-04/NRF_FINALApproved_2011028.pdf. [Accessed: Mar. 17, 2025].

[2] JESIP, "The Joint Decision Model (JDM)," 2025. [Online]. Available: https://www.jesip.org.uk/joint-doctrine/the-joint-decision-model-jdm/. [Accessed: Jan. 23, 2025].

[3] T Federal Emergency Management Agency, "National Incident Management System," 3rd ed., Oct. 2017. [Online]. Available: https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf. [Accessed: Feb. 17, 2025].

[4] European Commission, "EU Civil Protection Mechanism," Feb. 2025. [Online]. Available: https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/eu-civil-protection-mechanism_en. [Accessed: Jan. 20, 2025].

[5] Federal Emergency Management Agency, "NIMS Basic Guidance for Public Information Officers," Dec. 2020. [Online]. Available: https://www.fema.gov/sites/default/files/documents/fema_nims-basic-guidance-public-information-officers_12-2020.pdf. [Accessed: Feb. 17, 2025].

[6] National Response Team, "Joint Information Center Model," Apr. 2013. [Online]. Available: https://www.nrt.org/sites/2/files/Updated%20NRT%20JIC%20Model_4-25-13.pdf. [Accessed: Feb. 20, 2025].

[7] Pennsylvania Department of Health, "Joint Information System (JIS) and Joint Information Center (JIC)," 2016. [Online]. Available: https://www.pa.gov/content/dam/copapwp-pagov/en/health/documents/topics/documents/emergency-preparedness/Joint%20Information%20System%20and%20Joint%20Information%20Center%20-%20FEMA.pdf. [Accessed: Feb. 17, 2025].

[8] Federal Emergency Management Agency, "National Incident Management System," 3rd ed., Oct. 2017. [Online]. Available: https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf. [Accessed: Feb. 17, 2025].

[9] B. Van De Walle, M. Turoff, and S. R. Hiltz, *Information* Systems for Emergency Management. New York: M.E. Sharpe, 2010.

[10] J. C. Pine, Technology and Emergency Management, 2nd ed. Hoboken, NJ: Wiley, 2017.

[11] L. Vaivode, S. Ammar, "The role of social media during and in the aftermath of a terrorist attack," Acta Prosperitatis. *Journal of Turiba University*, no. 10, pp. 131-144, 2019. [Online]. Available: https://www.turiba.lv/storage/files/10-acta.pdf. [Accessed: Jan. 24, 2025].

[12] Sacramento County Office of Emergency Services, "Joint Information System Annex," Jun. 2019. [Online]. Available: https://sacoes.saccounty.gov/EmergencyManagement/Documents/Planning/JIS%20Plan%202019%20FINAL.pdf. [Accessed: Feb. 10, 2025].

[13] M. T. Kimour and D. Meslati, "Deriving objects from use cases in real-time embedded systems," Information and Software Technology, vol. 47, no. 8, p. 533, Jun. 2005. [Abstract]. Available: https://doi.org/10.1016/j.infsof.2004.10.003. [Accessed: Feb. 10, 2025].

[14] N. L. Le, J. Zhong, E. Negre, and M.-H. Abel, "CORec-Cri: How collaborative and social technologies can help to contextualize crises?" arXiv preprint arXiv:2310.02143, Oct. 2023. [Online]. Available: https://arxiv.org/abs/2310.02143. [Accessed: Feb. 12, 2025].

[15] Idaho Transportation Department, "State of Idaho Joint Information System/Center Operations Plan," Boise, ID, 2012. [Online]. Available: https://itd.idaho.gov/pop/assets/JISOperations.pdf. [Accessed: Jan. 10, 2025].

[16] U. Začs, "Security risk and crisis management: Analysis of survey results," presented at the SECUREU Project Conference, Turība University, Riga, Latvia, Apr. 2023. [Online]. Available: https://security.turiba.lv/wp-content/uploads/2023/05/Ugis-Zacs-paper-03.04.2023.pdf. [Accessed: Jan. 17, 2025].

[17] M. Auziņš, "Risk and crisis management in higher education institutions: The experience of the University of Latvia," Latvian Higher Education in Crisis, Riga: University of Latvia, 2011.

[18] M. Auziņš, "Risk and crisis management in higher education institutions: The experience of the University of Latvia," Latvian Higher Education in Crisis, Riga: University of Latvia, 2011.

[19] U.S. Department of Homeland Security, "National Response Framework," 4th ed., Oct. 2019.

[20] Ministry of the Interior of the Republic of Latvia, "Minister of the Interior of the Republic of Latvia: We are ready to strengthen crisis management across the European Union," European Social Fund, Mar. 9, 2025. [Online]. Available: https://www.esfondi.lv/en/about-eu-funds/news/minister-of-the-interior-of-the-republic-of-latvia-we-are-ready-to-strengthen-crisis-management-across-the-european-union. [Accessed: Mar. 9, 2025].

[21] Crisis Management Centre, "Crisis management centre to be set under the direct authority of the Prime Minister," Institute of Emergency Management, Mar. 25, 2025. [Online]. Available: https://www.iem.gov.lv/en/article/crisis-management-centre-be-set-under-direct-authority-prime-minister. [Accessed: Jan. 24, 2025].

[22] European Commission, "Artificial intelligence applied to disasters and crises management," Luxembourg, 2021. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/b2762bac-b839-11ef-91ed-01aa75ed71a1/language-en. [Accessed: Jan. 10, 2025].

[23] ResearchGate, "CRISIS: A System for Risk Management," 2012. [Online]. Available: https://www.researchgate.net/publication/304197313_CRISIS_A_System_for_Risk_Management. [Accessed: Feb. 20, 2025].

[24] European Commission, "Civil Protection," Feb. 2025. [Online]. Available: https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection_en. [Accessed: Feb. 17, 2025].

[25] GINA Software, "SmartCAD - Computer-Aided Dispatch System," 2025. [Online]. Available: https://www.ginasoftware.com/products/smart-cad/. [Accessed: Feb.16, 2025].