Scientific Advice Mechanism
to the European Commission

Framing the risks and opportunities of AI use in crisis management

Statement by the Group of Chief Scientific Advisors

December 2025

"I have always believed that Europe would be forged in crises, and that it would be the sum of the solutions we came up with to these crises."

Jean Monnet

The GCSA welcomes the publication of the Rapid Evidence Review Report on AI in emergency and crisis management[i], which moves towards filling an important knowledge gap in this area. In this short statement, our aim is to complement the Report with specific recommendations about **framing conditions** that should be put in place ahead of any widespread use of AI in crisis management in the EU. Our concern is that existence and availability of AI tools should not prevent or replace inclusive discussions about the potential consequences of their wider deployment. Similarly, AI cannot be a substitute for ambitious efforts in harmonisation between institutions, between different Member States, and about data preparedness across the Union. Our focus is on helping to ensure that the appropriate enabling conditions are in place to support the safe and responsible development of AI in crisis management situations and the ability of the EU to prevent and cope with crises, improving both safety and security.

Recommendations

The GCSA recommends

- A formal, technical assessment of the **risks associated with the use of crisis management AI tools**. We should consider in particular that AI tools, data storage and processing may be located and controlled outside the EU. Particular attention should be paid to cybersecurity and AI resilience (which should include infrastructural resilience, not only software robustness). The assessment should: (i) identify key infrastructure dependencies, (ii) emphasise the importance of local/edge AI and offline capacity, (iii) consider the use of EU-level investments for resilient compute, communications and data infrastructure, and (iv) clearly link these aspects to European strategic autonomy and cybersecurity.

- A thorough assessment of the **acceptability** of the risks associated with the use of AI in all stages of crisis management, ideally including a participatory democracy exercise[ii].
- The creation of an **inventory of AI tools** which may already be in use in Member States' environmental, health or other relevant agencies, and an assessment of the use of these tools in routine or crisis situations. If use is sufficiently far advanced, this could also include evaluations of performance, where appropriate.
- The systematic consideration of the **opportunity cost** of any recourse to AI solutions, with the creation of counterfactual scenarios that frame alternative futures[iii]. This should include one scenario with heavy reliance on AI tools for the management of crises, and another with significant investments in alternative approaches, such as greater coordination across institutions, more use of human resources in all areas including environmental sciences and data science, and the potential development and strengthening of EU environmental, health and other institutions in areas likely to be involved in crisis management. Such scenarios should include comparative estimates of all relevant financial and non-financial costs.
- Recourse to the **recommendations** set out in the 2022 GCSA scientific opinion on strategic crisis management, especially in areas like data-preparedness, and a stronger focus on crisis prevention through actions such as investment in harmonized monitoring studies, tools and institutions, with an understanding that crises are often not contained within national boundaries[iv].
- Ensuring that **humans remain at the centre of decision-making** in crisis management and remain accountable for moral and human implications. Efforts should be made to develop fit-for-purpose tools to support human deliberation and decision-making, without replacing it.
- **Training staff** to operate AI as well as non-AI tools in crisis situations and to act as guardians of shared ethical and moral standards. Capacity-building should prioritise critical thinking, situational awareness, and the ability to question and override AI outputs, so that any possible increasing reliance on AI does not lead to complacency, loss of expertise, or erosion of human judgement.

Risks and opportunities associated with AI use related to crises

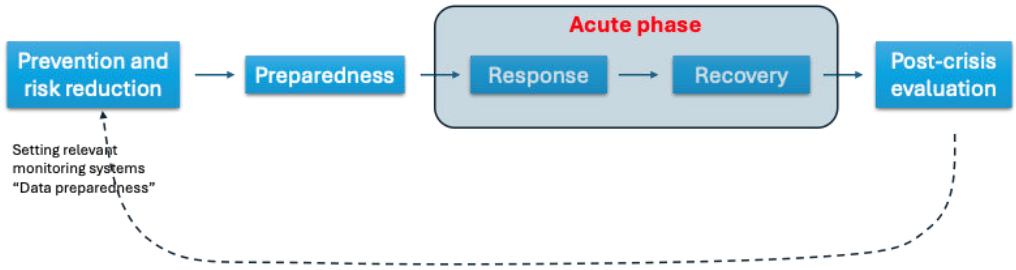

Figure: Key phases of crisis management

Crises are characterised by high uncertainty, limited or unreliable information, extreme time and social pressure, transboundary dynamics, cross-sectoral impacts, cascading failures, and complex coordination challenges. The best way to reduce the likelihood and severity of crises is sustained investment in prevention strategies across all sectors, complemented by robust preparedness, response, and recovery capacities.

Regarding the opportunities, when properly developed and deployed (see requirements below), AI can aid in prediction, prevention, and post-crisis evaluation, and such tools are already being developed in the European context by the EU's Joint Research Centre[v]. That said, major developmental issues remain and need to be addressed, including model overconfidence, reliance of models on trend stationarity, and constrains on data quality and availability.

To the best of our knowledge, there has not yet been a comprehensive, system-level assessment of the risks of AI for crisis management in the EU context. As a result, it cannot currently be stated with confidence that the benefits outweigh the risks. Moreover, even if such an assessment were to find that benefits outweigh risks, it is not known whether this conclusion would be acceptable to EU society.

Selected risks	Selected opportunities
Little suited to rare events and contexts of limited data availability	Faster detection of weather-, fire- and flooding-related hazards (at present)
Greater risk of data leakage compared to alternative approaches	Rapid processing of large volumes of heterogenous data
Reliance on AI may decrease trust in the decisions of public authorities	Real-time situational awareness
Over-emphasis on data analysis over data collection	Potential use in disinformation detection
Unfairness of AI tools due to bias in training data	Multilingual communication
Environmental impact of AI	Better scenario modelling and post event analysis
Decrease in human cognitive and moral expertise	
Risks associated with the use of non-sovereign AI systems	

Table: Some potential risks and opportunities of AI use related to crisis management (adapted from the SAPEA report).

Improving conditions for more efficient crisis prevention and management in the EU

We highlight here some conditions that need to be fulfilled before AI can be used for crisis management in the EU.

The usefulness of AI in any phase of disaster management depends on prior "data preparedness"[vi]; improving data preparedness is essential for both crisis prevention and management. This includes harmonised data collection, agreed standards for data formats and metadata, pre-negotiated protocols for secure data sharing across agencies and borders, clarity about lawful access and use, and provisions for traceability and audit. Data preparedness implies the development of data collection systems with increased equity and fairness, and monitoring systems where vulnerable or less favoured populations were underrepresented. Any investment in AI should go hand-in-hand with investments in the underlying data ecosystems and infrastructures, including provisions for their degradation, power outages, and analogue fall-backs when digital networks are disrupted. Moreover, research should examine weak aspects of past disaster responses in the EU, with a focus on the extent to which concrete AI tools could bring improvements in these domains.

The creation of AI-supported tools also opens additional attack surfaces which should become a matter of security and defence considerations. It should be recalled that even data and technologies for prevention and monitoring may be of use to ill-intended actors, including terrorists or inimical states, in their planning of attacks.

Decisions taken during a crisis should never be relegated to AI, because they are never purely technical. They carry profound moral, social, and legal weight, and typically have unforeseen outcomes that do not feature in data used to train AI models. This is why **decisions should remain firmly in human hands**. When making rapid decisions under conditions of uncertainty, crisis response teams should have access to strong analytical capacity but should refrain from asking AI to make the decision and tell them what to do[vii]. Instead, human decision-makers should remain accountable and consider how decisions can be justified in terms of moral and human experiences. As recalled in the SAPEA report[viii], 'moral deskilling' is a constant danger, and even the consultation of AI systems for morally charged decisions risks altering an operator's sense of agency and responsibility[ix].

More research and validation are needed into the added value and robustness of AI-related tools in the context of crisis prevention, preparedness, response or post-hoc evaluation. Relevant control conditions should be in place, enabling comparisons with human expertise guided by conventional monitoring or statistical approaches. Any AI system intended for crisis management should be subject to systematic evaluation before large-scale deployment, to avoid crisis-affected populations becoming inadvertent test beds for immature technologies. Wherever possible, such systems should be benchmarked against existing models, procedures and human expert performance in realistic scenarios, including stress tests under degraded data and infrastructure.

Conclusion

There are many opportunities – and many risks – associated with the use of AI for crisis management. This statement, and the reports it accompanies, do not allow for a formal appraisal of the benefit-risk balance. They show that AI can be used (and it is already being used), in particular during crisis preparedness for weather-related disasters. Implementation during the acute phases of a crisis requires the fulfilment of several conditions, including the development of sovereign AI systems, resilient data and communications infrastructure and clear guidance on boundaries in its use, especially as regards decision-making. Development should not come at the cost of other actions essential for improved prevention and management of crises in the EU, such as those related to European governance, data preparedness, cross-border collaborations in key sectors, the development of EU-wide harmonized monitoring systems, and investments in the training of human support.

The Group of Chief Scientific Advisors

Naomi Ellemers

Distinguished Professor of Social and Behavioral Sciences, Utrecht University, Netherlands.

Adam Izdebski

Professor of Human Ecology and Research Group Leader, Centre for Modern Interdisciplinary Technologies, Nicolaus Copernicus University in Toruń, Poland

Martin Kahanec

Professor, Central European University; University of Economics; Central European Labour Studies Institute in Bratislava, Slovakia

Rafał Łukasik

Director of Research & Innovation Department at Łukasiewicz Centre, The Łukasiewicz Research Network Presidential Plenipotentiary for International Relations in Warsaw, Poland

Dimitra Simeonidou

Professor of High-Performance Networks and Director Smart Internet Lab, University of Bristol, UK

Rémy Slama

Researcher in environmental health, senior investigator at Inserm (national institute of health and medical research), senior investigator at ENS-PSL (Ecole normale supérieure), Professor, IBENS, Paris.

Mangala Srinivas

Professor of Cell Biology & Immunology, Wageningen University and Research, Netherlands

References

[i] SAPEA. Artificial Intelligence in Emergency and Crisis Management. Brussels: Scientific Advice Mechanism to the European Commission, 2025.

[ii] Participatory democracy practices are efforts to involve citizens in the political decision-making process at different levels of governance.

[iii] 'Opportunity cost' is the value of the next best alternative given up when making a choice.

[iv] SAPEA, Science Advice for Policy by European Academies. (2022). Strategic crisis management in the European Union. Berlin: SAPEA. https://doi.org/10.26356/crisismanagement

[v] https://drmkc.jrc.ec.europa.eu/risk-data-hub#/

[vi] SAPEA (2022) op. cit., p. 206

[vii] Among the fast-growing body of literature in this field, see for example Jiang, L., Hwang, J. D., Bhagavatula, C., Bras, R. L., Liang, J. T., Levine, S., ... & Choi, Y. (2025). Investigating machine moral judgement through the Delphi experiment. Nature Machine Intelligence, 7(1), 145-160.

[viii] SAPEA 2025, p.35

[ix] Salatino, A., Prével, A., Caspar, E., & Bue, S. L. (2025). Influence of AI behavior on human moral decisions, agency, and responsibility. Scientific Reports, 15(1), 12329.

Publications Office of the European Union

Luxembourg: Publications Office of the European Union, 2025
© European Union, 2025

Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (https://creativecommons.org/licenses/by/4.0/). This means that reuse is allowed, provided appropriate credit is given and any changes are indicated.

The EU does not own the copyright in relation to the following elements: © Gorodenkoff_#1725140608. Source: stock.adobe.com

PDF ISBN 978-92-68-33391-4 doi: 10.2777/6187195 KI-01-25-226-EN-N