PRACTITIONER INSIGHTS & PERSPECTIVES

23rd International Conference on
INFORMATION SYSTEMS FOR CRISIS RESPONSE AND MANAGEMENT

"Building Stronger Futures"

Conference June 1st – 3rd, 2026

The Hague - Netherlands

https://iscram2026.com/

Organized by Leiden University and Netherlands Institute for Public Safety on behalf of ISCRAM association.

Interorganizational Collaboration for Event Safety: Addressing Challenges with Requirements for Technological Support

Moritz Aberle
City of Freiburg im Breisgau*
moritz.aberle@freiburg.de

Felix Märtin
City of Freiburg im Breisgau
felix.maertin@freiburg.de

Martin Kupper
Office for Fire and Disaster Protection
City of Freiburg im Breisgau
martin.kupper@freiburg.de

Hans-Christian Hegemann
Office for Public Order
City of Freiburg im Breisgau
hans-christian.hegemann@freiburg.de

ABSTRACT

Concerts, festivals, and other mass events contribute significantly to the cultural and economic life of any city. At the same time, however, large-scale events introduce various risks that need to be managed and addressed accordingly. We analyzed the interorganizational network of actors that safeguard events in the city of Freiburg im Breisgau, exemplarily for most municipalities in Germany. Through interviews and workshops, we identified recurring challenges and opportunities for improvement. Then, we elicitated requirements as a first step to design and implement a technological support system with the goal to address those shortcomings.

Keywords

Event Safety, Interorganizational Cooperation, Risk Management, Technological Support, Requirements Elicitation

INTRODUCTION

Every public event is unique based upon its format, organizers, duration, program, and composition of attendees as well as the environment in which it takes place (e.g., simultaneous events, weather, venue, or location). Large-scale events introduce risks beyond what is anticipated by the municipal emergency management, as seen by incidents in Germany (Helbing and Mukerji 2012) and internationally (Murray and Marvin 2024). The organizer, in cooperation with the authorities, must anticipate, mitigate and document these risks in safety plans.

We had the opportunity to reflect on this network of event safety actors in the city of *Freiburg im Breisgau*. The municipality is populated by about 240.000 and located in the south-west of Germany. It is characterized by a densely built-up city center and about 300 registered public events every year, of which many are large-scale.

CHALLENGES AND REQUIREMENTS

We conducted workshops and unstructured interviews with event organizers and authorities in Freiburg, including the Office for Public Order (2 representatives), State Police (6), and the Office for Fire and Disaster Protection (5). Thereby, we first analyzed the process from pre-planning to debriefing, with a focus on identifying recurring challenges therein. Then, we grouped these needs into themes (A to G) and elicitated functional requirements for a technological support system addressing these shortcomings.

*This work received funding from the German Federal Ministry of Research, Technology and Space (BMFTR) under grant number 13N16812.

Planning Phase

In this section, we describe the challenges and requirements elicited during the event planning phase (see table 1).

No	Requirement
A	**Digital Safety Plan**
A.1	Follow a guided process to create formalized safety plans
A.2	Document changes and view history
A.3	Import existing schematics and export documentation
B	**Evaluation of Safety Plan**
B.1	Identify deficiencies and plausibility mistakes
B.2	Audit plans based on standards and policies
B.3	Identify insufficient precautions and provide suggestions
C	**Crowd Simulations**
C.1	Simulate based on generated scenario parameters
C.2	Evaluate simulation results

Table 1. Functional requirements for a support system during the planning phase.

Digital Safety Plan (A) Safety plans document all preventive risk management measures and are currently composed as a PDF file. Details are often buried in lengthy documents that need to be distributed via e-mail. Organizers seek a digital solution to replace unstructured text, enabling imports of geospatial schematics like site maps and exports for workflow integration. A shared system is required as a single-source-of-truth and to maintain a universal change history for efficient version comparison.

Evaluation of Safety Plan (B) Our authorities emphasize that reviewing planning documents and site maps is time-consuming and requires expertise. They seek automated support to flag incorrect or missing information through plausibility analysis, e.g., detecting common deficiencies like missing emergency exits. Additionally, providing organizers with optimization suggestions could improve decision-making during the planing process.

Crowd Simulations (C) Agent-based computer simulations allow digital evaluation of venue layouts for evacuation. Our authorities recognize their potential but do not currently use them due to barriers like software availability, lack of specific training, and time constraints for setup. They aim to generate simulations from existing plans with minimal effort, customizing input parameters such as attendee numbers to test various scenarios through a ”what-if” framework. They also require quick visual overviews, such as heatmaps and videos of results, alongside statistical diagrams to support their case.

Execution Phase

In this section, we describe the requirements elicited for execution of events (see table 2).

Shared Real-time Situational Picture (D) Maintaining a clear and up-to-date situational overview during chaotic events is essential for effective response management. Users emphasized the need for a shared, map-based operational picture that displays real-time positions of units and personnel, with the ability to manually annotate elements such as assembly points or hazards. Information from control centers and on-site staff should be seamlessly integrated into a single map accessible by all authorized actors.

Crowd Behavior (E) Understanding and managing crowd flow and dynamics is essential for the prevention dangerous situations, as risks increase with rising density levels. Currently, assessments often rely on human spotters and subjective perception, which is particularly challenging during long-term or large-scale events such as Christmas markets where not all areas can be monitored continuously. Our actors therefore require systems that provide real-time measurements of crowd density and movement, enabling continuous monitoring of critical zones and automated warnings when configurable thresholds are exceeded. In addition, predictive capabilities are needed to forecast where and when critical levels may be reached, allowing authorities to intervene proactively.

Communication (F) Effective communication at events requires structured information sharing using chat and logbooks to document interruptions and decisions transparently. Our actors also seek tools to collect and analyze situational input via crowd-sourcing from pre-registered attendees and bystanders. Additionally, organizers want to alert staff via smartphone and convene ad-hoc crisis meetings, enabling faster coordination and decision-making in dynamic situations.

No	Requirement
D	**Shared Real-time Situational Picture**
D.1	View a dashboard with operation-specific data and prepared plans
D.2	Display and annotate geographic data on a map
D.3	Share information across organizations
D.4	Transfer information to and from command center systems
E	**Crowd Behavior**
E.1	Map the current density and flow of people
E.2	Receive warnings when configurable thresholds are reached
E.3	Obtain forecasts how critical values could be exceeded
F	**Communication**
F.1	Use a cross-organizational multi-modal chat
F.2	Write and read event logbook
F.3	Inquire situational information through crowd-sourcing

Table 2. Functional requirements during the execution of large-scale events.

Debriefing Phase

Finally, we describe our software needs to support the debriefing of large-scale events (see table 3).

Analysis of Past Events (G) Accessing the documentation after events allows capturing decisions, actions, and outcomes, to enable the organizations to learn and improve future planning. Our practitioners value data-supported, cross-organizational analyses, and structured post-incident reports. They require a survey function to systematically record and evaluate the perspectives of all actors involved in the event.

No	Requirement
G	**Analysis of Past Events**
G.1	Create well-structured debriefing reports
G.2	Access all event data retrospectively
G.3	Compare recent events and evaluate them using a quantitative metric

Table 3. Functional requirements during the debriefing phase.

LIMITATIONS AND CONCLUSION

Our participants emphasized that many needs extend beyond technological support, requiring policy adjustments, organizational changes, or enhanced training. At the same time, we realize that overcoming these obstacles and resolving the listed challenges using system support enables more resources to be dedicated to these tasks.

REFERENCES

Helbing, D. and Mukerji, P. (2012). "Crowd disasters as systemic failures: analysis of the Love Parade disaster". In: *EPJ Data Science* 1.1, p. 7.

Murray, M. A. and Marvin, A. (2024). "The Astroworld tragedy as an argument for proactive crisis management". In: *Corporate Communications: An International Journal* 29.4, pp. 516–532.

From a Pandemic Patch to National Infrastructure: Scaling Automation Under Crisis Constraints

Parag Bhatnagar
Health New Zealand
Parag.Bhatnagar@tewhatuora.govt.nz

ABSTRACT

Process and workflow automation capabilities in public health systems are often introduced as efficiency tools, yet their role can shift quickly under crisis conditions. This paper reflects on practitioner experience scaling automation from pandemic-driven deployment through to national consolidation within a unified health system. It examines how governance, organisational structure, support models, and process suitability behave when automation becomes operational infrastructure rather than discretionary technology. The paper offers practical insights for practitioners and researchers concerned with crisis readiness, digital resilience, and the safe scaling of automation during sustained system stress.

Keywords

Crisis readiness; Automation governance; Health systems resilience; Digital infrastructure; Public sector operations.

INTRODUCTION

Automation in public health and emergency response environments is often framed to improve efficiency or offset workforce shortages. But the conditions under which automation is first adopted can shape its long-term role. In this case, automation did not emerge from a planned transformation programme. It accelerated during a pandemic response, when workforce availability was disrupted and continuity became paramount.

In this paper, "automation" refers specifically to digital process automation across organisational systems, including rule-based and semi-structured workflows supporting administrative and clinical operations.

This paper adopts a reflective practitioner perspective based on direct involvement in the design, deployment, and scaling of automation capabilities within a large public health system. Insights are derived from longitudinal operational experience across multiple implementations and incident scenarios during and following crisis conditions, rather than from a formal evaluative methodology. The intent is not to generalise statistically, but to surface recurring patterns and lessons observed in practice that may inform both practitioners and researchers.

CONTEXT / BACKGROUND

In the northern part of New Zealand's health system, automation accelerated during the COVID-19 pandemic. Workforce availability was constrained as staff were redeployed to frontline roles, worked remotely, or were unable to attend workplaces. Automation was introduced to support continuity in essential administrative and clinical support activities, such as credentialing and compliance checks, where delays would have immediate downstream impacts. Under crisis conditions, automation was valued less for cost efficiency and more for operating independently of physical presence and absorbing workload volatility.

Following the pandemic, structural reform amalgamated multiple regional and district entities into a single

national health system. Automation capabilities that had developed regionally, often with local tools, processes, and governance, were required to scale nationally. This transition introduced complexity: differing risk tolerances, overlapping platforms, evolving governance controls, and shared support responsibilities. As automation moved from a regional crisis response capability to a national service expected to operate reliably at scale, it entered a prolonged transition state. The observations in this paper are situated within this period of crisis-born automation meeting system-wide consolidation.

WHAT WE OBSERVED WHEN AUTOMATION BECAME INFRASTRUCTURE

As automation volumes increased and processes became embedded in time-critical pathways, four recurring patterns were identified across implementations and incident scenarios that were not visible in early pilots.. Under crisis conditions, these patterns were less about individual use-cases and more about how automation behaved once it became operational infrastructure.

Governance collided with urgency

Controls around access, identity, security reviews, and change approvals were designed for steady-state delivery. Under crisis conditions, these mechanisms became runtime dependencies. Expired access, delayed approvals, or unclear ownership could halt automation even when the workflow logic remained valid.

Insight: governance shifted from background assurance to an operational determinant of response speed.

Failure modes multiplied at scale

As automation expanded nationally, failures shifted from isolated defects to systemic fragility. Processes reliant on stable interfaces, predictable data, or informal human intervention proved vulnerable during surge demand. Failures outside business hours were especially disruptive, exposing gaps in monitoring, escalation, and recovery.

Insight: scaling exposed hidden assumptions about availability and resilience, not just capacity limits.

Organisational boundaries re-emerged during incidents

The transition to a national capability blurred responsibility during automation failures. While prioritisation and delivery were increasingly centralised, operational dependencies remained distributed across infrastructure teams, application owners, and local services. During incidents, fragmentation complicated diagnosis and resolution, especially where automated workflows crossed organisational boundaries.

Insight: incident-time accountability must be designed, not assumed, in federated operating models.

Limits to what should be automated became clearer

Crisis conditions amplified the risks of automating workflows lacking stable decision anchors. Processes involving judgement, interpretation, or evolving clinical context were more likely to fail or require ad-hoc intervention. Automation could assist with data movement or preparation but attempts to replace judgement increased error risk when pressure was highest.

Insight: under crisis conditions, boundary-setting on suitability is a safety and resilience function.

REFLECTION AND LESSONS LEARNED

These experiences prompted a shift in how automation was understood and governed. Automation had initially been treated as a delivery activity: processes were identified, built, and deployed. Under crisis conditions, this framing proved insufficient. Automation supporting critical workflows behaved less like discrete solutions and more like shared infrastructure with system-wide dependencies, consistent with prior work on information systems in crisis contexts (Walle & Turoff, 2006). While many organisations deploy automation during crises, fewer reflect on how crisis-born automation reshapes long-term governance, support, and risk.

One lesson was that governance must be designed for crisis conditions, not only compliance. Mechanisms that function adequately in steady state can become sources of operational risk when rapid response is required. Without pre-authorised pathways and clear ownership, automation cannot adapt at the pace demanded by system stress.

A second lesson concerned resilience and support. Early assumptions about predictable operating hours and

available human oversight did not hold at scale. Failures during peak demand or outside standard hours exposed the need to invest in monitoring, escalation, and recovery arrangements as first-class design requirements.

Finally, crisis conditions sharpened judgement around suitability. Automation delivered the most value when applied to well-defined, rule-based work with stable anchors. Exercising restraint—deciding what not to automate—became critical to maintaining safety and reliability under pressure.

IMPLICATIONS / TAKEAWAY MESSAGE

When automation becomes embedded in crisis critical operations, it must be treated as operational infrastructure rather than a collection of projects. Crisis ready automation requires preauthorised governance, resilient support models, and clear boundaries around suitability. Without these conditions, scaling automation during disruption can amplify systemic fragility rather than strengthen resilience.

REFERENCES

Walle, B. V. D., & Turoff, M. (2006). ISCRAM: Growing a global R&D community on information systems for crisis response and management. *International Journal of Emergency Management*, *3*(4), 364. https://doi.org/10.1504/IJEM.2006.011302

Decision Latency in Cybersecurity Incident Response

Martijn Dekker
University of Amsterdam
m.dekker4@uva.nl

ABSTRACT

In large organizations, the speed of incident response is constrained by the delay between incident detection and responsive decision making and subsequent action. This decision latency is due to, for example, organizational structure, risk governance and accountability distributions. Most of these are optimized for authority but not for speed. As cybersecurity incidents can evolve very quickly, the solution space of possible responsive actions can diminish quickly, and decision latency should be minimized. In this paper we explore some trade-offs that can be made to reduce decision latency during cybersecurity incident response.

Keywords

Decision latency, cybersecurity, governance.

INTRODUCTION

Organizations are faced with cybersecurity incidents at increasing frequency and impacts. Often, these incidents start by end-user reporting or detection of anomalous system behavior. Typically, the situational awareness of what is happening, or what can happen next, is low due to high levels of uncertainty and lack of data. Some of the possible incident response measures involve system shutdowns, public disclosure or paying ransom, with significant business impact. Impact of cybersecurity incidents can grow quickly, and quick decision making is necessary. Due to the significant business impact, these decisions normally can only be taken by decision makers with executive authority, which are organizationally far removed from the security teams. In the financial industry, organizations include advanced risk governances including risk policies and processes. This includes risk committees for decisions about risk treatments. The operating models in these organizations heavily rely on approval processes and regulatory scrutiny in the sector can even lead to avoiding making decisions due to fear. Even the crisis- and business continuity processes are characterized by strict processes and high escalation overhead, which is not suited for time-compressed cybersecurity incidents. Therefore organizations need to prepare new agreements that better balance authority and speed.

ACCELLERATION OF CYBERSECURITY INCIDENTS

Organizations realize that cybersecurity incidents have become inevitable, not very predictable, with high uncertainty and evolving quickly. Security professionals observe time-compression of the kill-chain because of automation by attackers. Defenders in organizations deal with legacy IT-estates that often have little segmentation or isolation of vulnerable (legacy) systems. This can increase the threat of lateral movements. After the start of an incident, the options available to the security team therefore quickly diminish as the intrusion spreads. Once attackers reach their target, exfiltration of data can occur at speed, leading quickly to data theft and privacy breaches. The impact of cybersecurity incidents can quickly become irreversible, while they start almost opaque. Time-compression, information asymmetry and high uncertainty have become an operational reality for many organizations.

THE LATENCY DILEMMA

As cybersecurity incidents evolve, decisions need to be taken to execute actions. Responses can include shutting down systems, disconnecting networks, communicating with stakeholders and paying or refusing ransom. These decisions are financially material, legally binding and reputational sensitive. Regulations like the EU regulation Digital Operational Resiliency Act (DORA) stipulate that executive management plays a pivotal role in these and put personal liability on senior leaders. Therefore, operational teams cannot make these decisions autonomously unless clear guardrails are agreed before, creating a "speed versus authority" dilemma. In the financial industry, sophisticated risk governances are put in place to address this dilemma in normal conditions, and business continuity processes for addressing it under stress conditions, balancing several risk types. In practice, the rise of cyber-risks is now shifting this balance.

For example, a cybersecurity risk that is classified as "high" requires decision making in the senior management risk committee that convenes once a month and requires extensive documentation and preparation. An operational incident can start small with code "yellow" and activation of a local business continuity team. But it can escalate to code "red" requiring activation of the central crisis management team at almost board-level. This escalation can take hours or even days. This decision latency is not inefficiency, but a structural dilemma in regulated organizations that are used to applying rigorous mechanisms to manage risk and liability. For example, mandatory cybersecurity incident reporting to regulatory bodies, often requires senior management sign-off. The processes and governances that are put in place are often designed to verify information, align legal and communication aspects, to mitigate regulatory risks. The decision latency can be further compounded by cultural aspects like risk-averseness and over-reliance on formal approval procedures.

IMPROVED RESILIENCY THROUGH LOWER DECISION LATENCY

Cybersecurity incident response requires strong technical controls to slow down incident development. It requires lowering decision latency by agreeing delegation of authorizations under defined conditions, and with agreed transparency and reporting. This needs to be explicitly agreed at executive management level, as those managers need to feel comfortable with delegation while being personally liable. Practitioners in the financial industry have adopted five ways to improve the resiliency of their organization by addressing the decision latency dilemma.

Firstly, agree, *a priori*, priorities and mandates during incident responses. Delegate decision autonomy under clearly defined conditions. For example, many Chief Information Security Officers now have the mandate to shut down systems, in case they see imminent threat.

Secondly, maintain good, shared understanding of cyber threats and business implications through asset management and scenario analysis.

Thirdly, implement technical measures, like network segmentation, to slow down incident development. Invest in optionality to ensure choices for decision makers during incidence response.

Fourthly, define risk appetites and tolerances, that include time-to-decide metrics to ensure the speed of response is aligned with the time-compressed cyber incidents.

Fifthly, improve decision making by regular training and simplifying management information during an incident.

CONCLUSION

As cybersecurity incidents become more time-compressed, decision latency in the defending organization becomes a concern. Digital resilience can be improved by measures that make incidents develop more slowly plus measures that reduce decision latency. Delegation of decision authority is possible, by agreeing clear conditions and possible actions. By balancing the risk of responding too slowly (by not delegating enough) and the risk of making wrong decisions or, reporting inaccurate information (by delegating too much) a new risk optimum can be reached.

Lessons for Netcentric Information Management In and Around Black-Out Areas

Emma de Weger
Trimension
deweger@trimension.nl

Steven van Campen
Trimension
vancampen@trimension.nl

Martijn van der Kolk
Stedin
Martijn.vanderkolk@stedin.net

ABSTRACT

This paper explores the necessity and feasibility of Netcentric Information Management (NIM) during large-scale black-outs, even when telecom fails. Drawing on lessons from grid operators, it argues that NIM principles - creating shared situational awareness and effective coordination - can be maintained using alternative communication methods, if possible assembling tactical/ strategic crisis teams at back-up locations outside the area, and most importantly using a "NIM-ring" around this black-out area. These principles and the NIM-ring allow for modern, effective crisis management, rather than reverting to old-fashioned hierarchical structures and periodic reports. Governmental and critical entities should plan and exercise for this.

Keywords

black-out, power cuts, crisis management, information management, netcentric coordination, grid operators, ISCRAM 2026 conference

INTRODUCTION, RATIONALE AND AIM

Large-scale power black-outs lasting several days are becoming more likely, due to electrification, net congestion and geo-political developments. (Analistennetwerk Nationale Veiligheid, 2022) Within 2 to 12 hours of a power failure, the telecommunication grids will also fail causing the digital infrastructure used by crisis organisations to disappear. Based on the experience of authors, working for and as crisis coordinators at a Dutch grid operator, these operators have valuable experience in crisis management (CM) when telecom has failed.

Netcentric Information Management (NIM; in Dutch: Netcentrisch Werken or NCW) is based on the principle that all CM-actors involved can access the same, shared, real-time depiction of the crisis, in text, images and/or maps: a shared situational overview (SSO) shown in **Figure 2**. NIM is a proven, method to facilitate highly effective CM. (Treurniet, Korpel, Suitela, & van Dijk, 2023) Although for NIM mostly web-based ICT systems are used – e.g. a dedicated MS Teams channel, or the highly secure website LCMS (Nederlands Instituut Publieke Veiligheid, 2026) - NIM itself is an organisational principle, not a technology.

As many (Dutch) crisis organisations rely on web-based NIM tools, it is tempting to conclude that when electricity and thus telecom black out, one reverts to traditional, hierarchical CM-structures, with old-fashioned situation reports (SITREPs; see **Figure 1**). However, this is neither realistic nor necessary. Today's complexity and time pressure make sequential information chains unworkable.

For effective CM, operators keep using NIM also during outages, to fix the black-out and mitigate its effects as quickly as possible. Accustomed to operating in and around the black-out area, they rely on alternative communication methods and backups to maintain netcentric coordination. The principles of NIM remain intact; only the means change.

In this paper we therefore argue, first, that NIM is both possible and necessary without regular ICT, and second, that organisations can learn from grid operators to remain effective during black-outs.

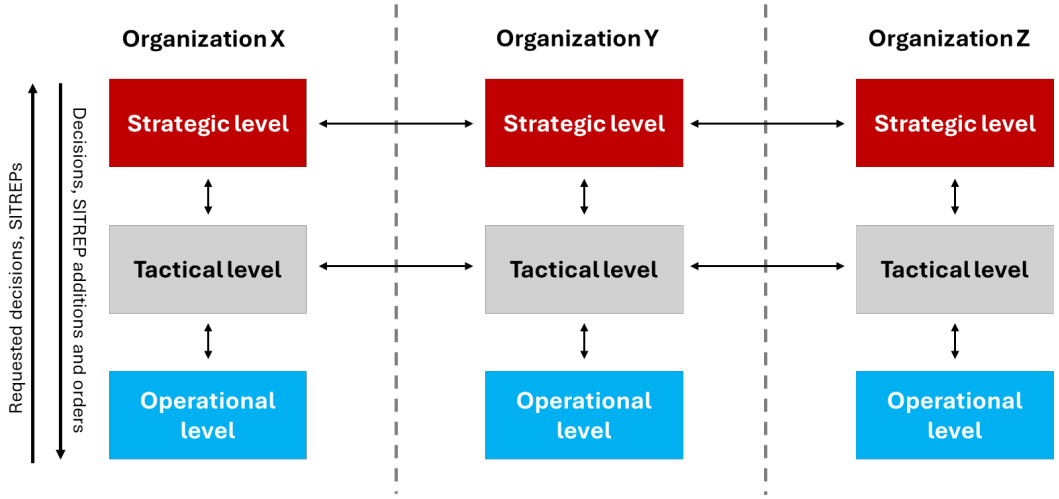

Figure 1: Traditional information management – hierarchal internal processing causes delays

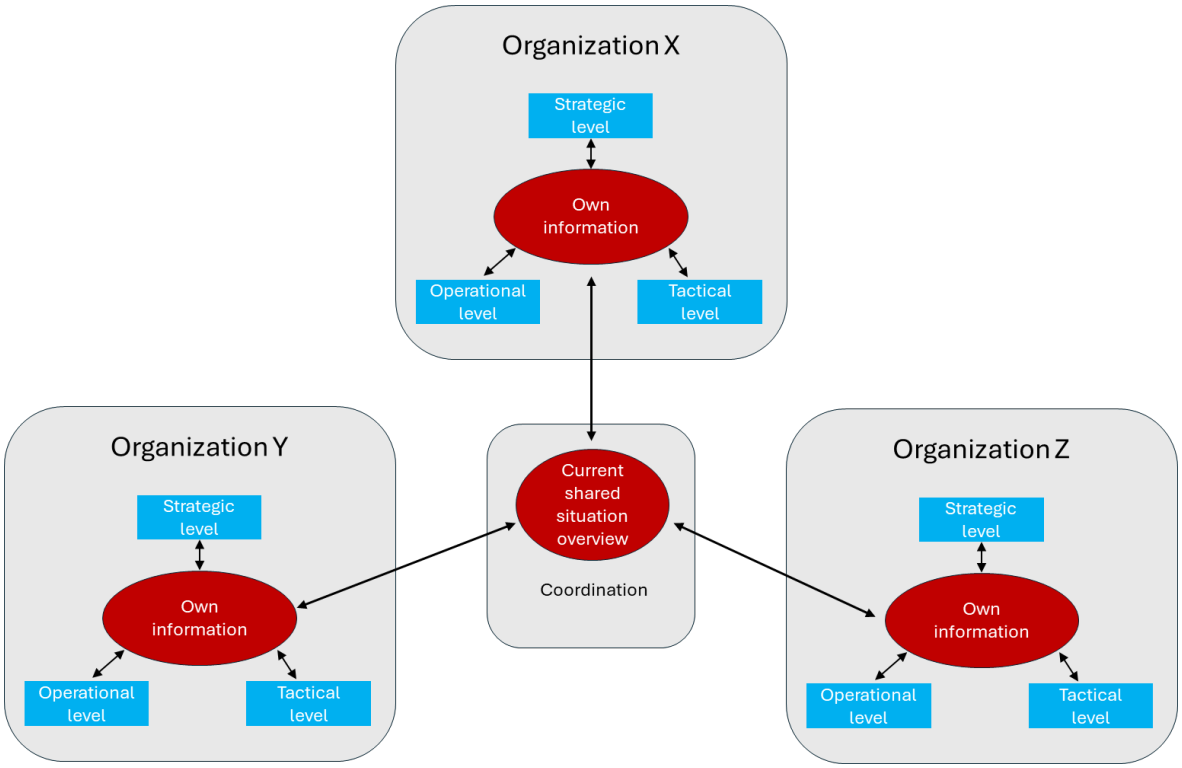

Figure 2: NIM - information is shared instantly and openly across teams and organizations, providing all one up-to-date situation overview, minimizing delays.

GRID OPERATORS AS REFERENCE

Based on the experience of authors, operators of electricity and gas networks face local disruptions daily and regional outages occasionally. Their CM-approach is netcentric, robust, and adaptive, as the whole of society depends on them to swiftly resolve the black-out. To mitigate societal unrest, emergency services and governments also depend on information from the operator about the duration.

Continuity is built through redundancy and segmentation: proprietary glass fibre networks with emergency power for operational technology (OT), satellite communication for communication and data-transfer backup, and

backup locations for control centres and crisis teams. The result is a modular system with backups, that can lose components without collapsing.

A communication pyramid guides information exchange. Voice communication remains essential for coordination and decision-making. Digital data transfer is preferred for NIM, as it makes sharing an SSO much easier and thereby reduces voice communication. Voice communication and data transfer are both possible via back-ups, e.g. VoIP over the operator's OT-network or satellite communication. Physical transport of messages is a last resort, because time-consuming. All channels are preconfigured, trained, and supported by checklists and scheduled contact windows. Resilience lies in their combination.

CM is organised "outside-in": positioning essential CM-teams at the outside and operational teams at the edges of the black-out area and at stations with back-up communication devices. Given the complexity of energy grids, information is shared as context-rich units—outage reports, switching schemes—rather than reduced summaries, preserving granularity and improving decision-making.

Operational teams are empowered to act independently within clear boundaries, reducing response times and reliance on constant connectivity. This requires a clear commander's intent outlining objectives, priorities and constraints. Feedback from operational level updates the SSO, on which the commander's intent is adjusted. Tactical and strategic crisis teams are preferably positioned outside the affected area for stability and full-time connectivity.

IMPLICATIONS FOR CRISIS ORGANISATIONS

The lessons from grid operators are highly relevant for other crisis organisations, like governments, emergency services and water safety organisations; all less experienced with black-outs. Instead of relying on a single digital platform, NIM-procedures should be designed to function under different levels of disconnectivity.

An innovative approach is to create a "NIM ring" around the black-out area (**Figure 3**). Operational teams, technical hubs and local command posts inside the area are structurally connected to information management cells and other crisis teams outside; preferably via back-up communication lines and worst-case by sectorized messengers in vehicles. This structure ensures information relay-times are minimized and the system can lose components without failing as a whole.

This preferably requires a backup digital data grid, independent of regular telecom infrastructure. E.g. by satellite connections, OT networks or autonomously powered communication points. The goal is to minimise relay-time. Even with limited bandwidth, digital and real-time information exchange remains preferable over periodic SITREPs.

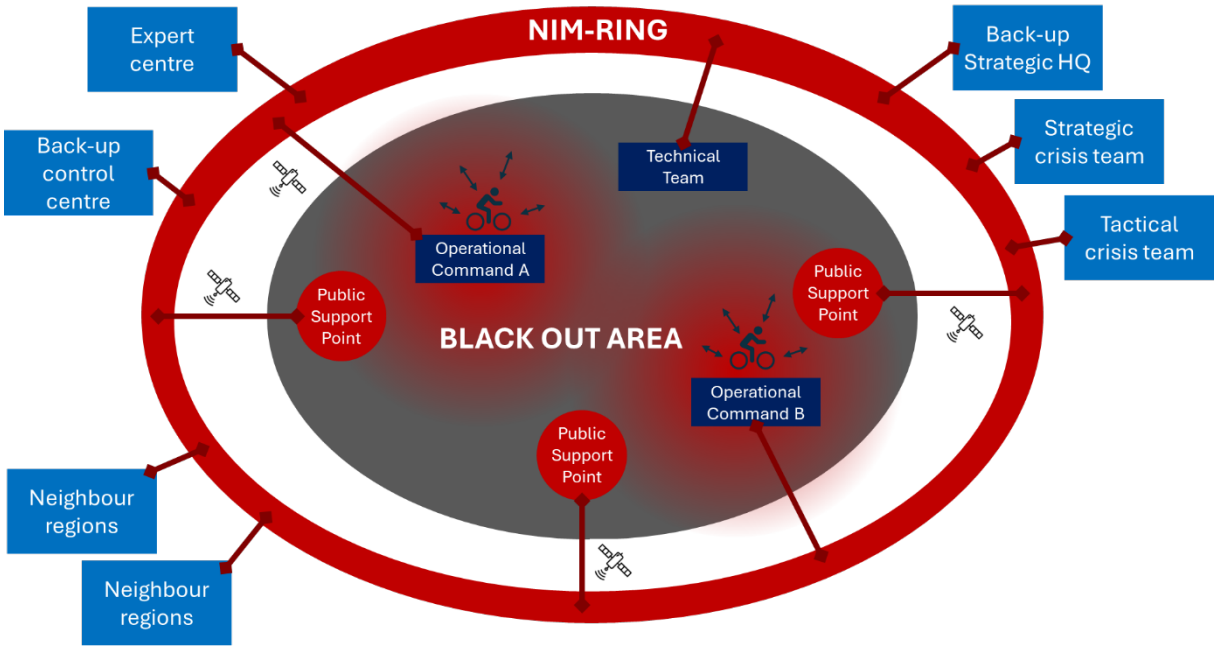

Figure 3: A NIM-ring around and command or support hotspots within the black-out area

Control centres, tactical and strategic crisis teams should, where possible, be positioned outside the black-out area and must have a direct, zero-delay-link with the NIM-ring. If strategic leaders (e.g. mayor) have to remain inside the black-out area for visibility and legitimacy, a hybrid model can be used: information officers connect the inner hubs and outer ring, ensuring the SSO remains robust.

Structural cooperation with neighbouring crisis partners is needed to erect a NIM-ring. Blackouts cross administrative borders, so pre-established links with neighbouring regions, grid operators and even international coordination centres are essential. Standardised minimal datasets and fixed communication formats are essential to enable effective exchange under constrained conditions.

Crucially, organisations must remain committed to the core principles of NIM. While SITREPs can provide useful summaries, they should not replace parallel, real-time and source-based information flows. The key distinction lies not in the communication medium, but in the design of the process.

Finally, this approach requires regular training. The ability to work netcentric without regular ICT does not emerge automatically during a crisis; it must be practised. Exercises should include long-term energy and telecom outages, satellite communication, narrowband data exchange, physical data transfer and hybrid inside–outside command structures. Only through repetition and joint training can the network become resilient enough to function effectively under degraded conditions.

A prolonged blackout is therefore not a reason to abandon netcentric information management, but a test of how deeply it is embedded as organisational principle.

REFERENCES

Analistennetwerk Nationale Veiligheid. (2022). *Rijksbrede Risicoanalyse Nationale Veiligheid.* ANV.

Nederlands Instituut Publieke Veiligheid. (2026, April). *Landelijk Crisis Management Systeem (LCMS)*. Retrieved from LCMS.nl: https://nipv.nl/informatievoorziening/voorzieningen/landelijk-crisis-management-systeem/

Treurniet, W., Korpel, M., Suitela, V., & van Dijk, E. (2023). *Referentiekader Netcentrische Crisisbeheersing 2023.* Arnhem: NIPV.

Cyber Crisis Consulting Beyond Deliverables

Rosa Edema
Bureau Veritas
rosa.edema@bureauveritas.com

Max Tijmann
Bureau Veritas
max.tijmann@bureauveritas.com

ABSTRACT

Cybersecurity and cyber crisis management (CCM) are fundamental to safeguarding public organizations against evolving digital and hybrid threats. However, many public organizations remain reliant on the consultancy sector for expertise, which is costly and diminishes internal capability and accountability. This Practitioner Insights & Perspectives (PiP) paper reflects on experiences from a recent engagement with a public organization and uses this case to operationalize the insights gained. While many consultancy engagements consist of a singular assessment or report, this paper argues they should be designed to transfer capabilities. These projects should have long-term effects by embedding ownership to strengthen resilience and reduce dependency.

Keywords

Practitioner insights; cybersecurity consultancy; public sector; capability building; crisis management.

INTRODUCTION

Public organizations operating in critical sectors carry a responsibility to deliver essential services to society, such as electricity grid operations or maritime safety. Traditionally, crisis management in these organizations has focused on the physical domain to ensure continuity, as this was considered the highest risk area. However, with rising digital and hybrid threats, there is a greater reliance on cyber response, which is often insufficiently integrated into crisis management practices. Bridging physical crisis management with cyber crisis response remains a challenge, particularly as the cyber response domain is relatively new and continues to evolve rapidly. While digital threats become more sophisticated, public organizations often struggle to retain internal cyber expertise due to limited budgets and competition from the private sector. As a result, external consultants are frequently engaged for CCM support.

While public-private partnership and collaboration with external expertise brings significant value, many consultancy engagements in CCM are focused on singular exercises or assessments, rather than approaches that build lasting internal capability. This PiP paper reflects on this difference through an example case from the Dutch public sector, illustrating how the approach to consultancy engagements can significantly influence long-term organizational knowledge and resilience. Though this is a singular example, we have experienced similar patterns across various public organizations. In our experience, a cyber crisis consultancy engagement that focuses on shared capacity building and identifying clear roles, responsibilities and ownership within the organization increases the lasting effect and return on investment for almost all public organizations. However, these projects may be shaped in various ways depending on factors like organization size, its primary purpose or the goals of the engagement.

BACKGROUND

Existing academic research consistently illustrates that an organization's resilience benefits much more from investments in internal capacity rather than fully outsourcing critical knowledge and capabilities. Research on public sector "dynamic capabilities" emphasizes the need for governmental organizations to develop the ability to adapt, learn, coordinate, and govern digital systems internally, rather than outsourcing these capacities, particularly in the case of crises (Mazzucato & Kattel, 2020). Additionally, Miller (2024) argues that factors like

internal learning routines, cross-functional coordination, and adaptive governance (which he calls dynamic capabilities) are essential for effective cyber response in the public sector. He posits that public organizations can benefit from collaboration with the private sector to learn how to apply these capabilities. Looking at cyber crises, Mahmood et al. (2024) underscore defined roles, strengthened internal structures, and structured crisis management processes as key components of organizational preparedness. This again points to the importance of internal capacity. Of course, an organization may need support in establishing this crucial internal capability. This is where consultants can play a vital role, if projects are shaped the right way.

The above-described dynamics are also reflected in practice. In this case, a water management organization was struggling to integrate their cyber crisis response with their 'traditional' physical crisis response. Their internal IT experts were not experienced with cybersecurity and internal crisis management experts were insufficiently aware of digital threats, risks, and related organizational impact. Additionally, most people with knowledge about cybersecurity were external consultants who were only involved with the organization for a limited time. As a result, there was insufficient internal expertise and ownership for CCM, leaving it underdeveloped.

INSIGHT

The engagement started as a standard consultancy assignment, supporting the client in developing and executing exercises. However, we soon noticed that this familiar approach was insufficient. Cyber crises differ fundamentally from traditional ones, and those responsible for crisis management within the organization were not familiar with the nuances of these distinctions. We treated the topic as a deliverable until we realized the desired results required knowledge and ownership to be embedded within the organization.

Therefore, we switched from drafting and executing exercises to collaboration on an internal governance structure for CCM. With relevant stakeholders, we identified internal ambassadors for the topic, active within incident management, IT, and 'traditional' crisis management. We explained to these ambassadors what CCM entailed, what this meant for their roles, and which (shared) responsibilities they held for ensuring an effective response. This helped break with the misconception that CCM is entirely separate or overly complex, and showed that by combining internal expertise, meaningful progress could be made.

Next, we worked with internal stakeholders to create response plans, scenarios, and (technical) work instructions, to minimize dependence on external expertise. With this documentation framework, ambassadors and stakeholders were educated and trained in the materials and broader CCM concepts. After this foundational work, we shifted to exercises by developing and performing various cyber crisis exercises, establishing an ongoing exercise program, and helping the stakeholders to design and organize exercises internally. This tested the plans and ensured that knowledge of exercising was present and shared internally.

REFLECTION AND LESSONS LEARNED

Through the engagement at the water management organization, two main insights were gained.

First, CCM projects should focus on the long term and ensure ownership and capability within. While external cyber crisis expertise can enhance planning and response, organizations should ensure a strong internal foundation. By taking joint ownership, developing initial plans, and identifying where external expertise adds most value, the topic can be addressed, internally owned, and progress without external parties in the lead. This also results in more cost-effective use of consultants. At least one internal owner or ambassador should be embedded in each project to retain ownership and knowledge, and success should be partially measured by whether the organization can continue independently after consultants leave.

Second, consultants themselves carry a professional and ethical responsibility: to avoid reinforcing dependency and to prevent consultancies from taking over core internal expertise, helping strengthen public resilience with evolving digital threats. While it may be easier, and at times more profitable in the short term, for consultancy firms to take on ownership, this engagement showed the opposite was needed. By enabling the organization to independently run a Plan-Do-Check-Act cycle and embedding expertise internally, resilience increased, and consultants shifted toward a meaningful validating and advisory role rather than creating operational dependence.

IMPLICATIONS

To help public organizations effectively progress, CCM should be seen as a long-term activity. Consultancies and public organizations have a shared responsibility to ensure that engagements are aimed at internal ownership, active involvement, and combining existing expertise to enable real progress and reduce dependency.

CONCLUSION

The case of the water management organization demonstrates that effective CCM in the public sector requires a shift in how consultancy engagements are structured. Rather than delivering isolated assessments or exercises, consultants must prioritize capability building and internal ownership. This approach strengthens organizational resilience and ensures critical knowledge remains in the organization, even after external support ends. By establishing governance structures, identifying internal ambassadors, and transferring knowledge, organizations can prevent dependency and progress their cyber response capabilities. Both the consultants and the public organizations have the responsibility to operationalize this approach. Consultancies must prioritize long-term improvement within the public organization over short-term revenue, ensuring project designs serve public value, even when that does not maximize commercial profits. Public organizations must commit to active participation and ensure internal owners drive initiatives forward. Only through this collaborative approach to public-private partnerships can the public sector develop lasting internal cyber crisis capabilities.

ACKNOWLEDGMENTS

We thank all colleagues who helped in forming this paper in one way or another. Without their expertise and insights, both during the writing of the paper and during the execution of the project described, we would not have been able to develop this reflection. Artificial Intelligence was used to structure internal conversation notes and link them to the headers determined in the PiP template, to critically review specific sentence structures and internal discussions about some of the concepts described, to help draft ideas for a title, and to perform final spellchecks. An internally developed and managed AI tool was used to do so.

REFERENCES

Mahmood, S., Mehmood Chadhar, & Firmin, S. (2024). Digital resilience framework for managing crisis: A qualitative study in the higher education and research sector. *Journal of Contingencies and Crisis Management*, *32*(1). https://doi.org/10.1111/1468-5973.12549

Mazzucato, M., & Kattel, R. (2020). COVID-19 and public-sector capacity. *Oxford Review of Economic Policy*, *36*(1). https://doi.org/10.1093/oxrep/graa031

Miller, M. S. (2024), *Essays on Innovation and Dynamic Capabilities: Evidence from Public Sector Operations and Cybersecurity* [Doctoral dissertation, Virginia Tech]. VTechworks. https://hdl.handle.net/10919/120950

Combining Aerial and Ground Unmanned Assets in Multi-aspect Search and Rescue Operations

Harris Georgiou
Hellenic Rescue Team of Attica (HRTA)
harris@xgeorgio.info

Alexios Vlachopoulos
Hellenic Rescue Team of Attica (HRTA)
nosailor01@gmail.com

Anastasia Andriopoulou
Hellenic Rescue Team of Attica (HRTA)
aandriop2@gmail.com

ABSTRACT

In Search & Rescue (SAR) operations, both speed and efficiency are equally important when it comes to timely, optimized deployment of technical resources. This report describes and analyzes a real-world large-scale SAR exercise, involving Unmanned Aerial Vehicles (UAV), Unmanned Ground Vehicles (UGV) and Tactical Field Communications (TFC). Command-level decisions determine search coverage, detection accuracy and effective support of First Responder teams through coordinated deployment and situational awareness. Important lessons are drawn for combined dispatching and the need for multi-purpose technological solutions in the field.

Keywords

Search & Rescue, crisis management, remote sensing, drones, rescue robotics.

BACKGROUND & CONTEXT

First Responders (FR) operate in diverse Search & Rescue (SAR) environments, as defined by terrain, weather, accessibility, victim location, available resources, access routes, etc. In terms of prioritization and planning, there are three interconnected factors:

1) **safety**, ensuring protection of FRs through hazard awareness and monitoring;

2) **speed**, maximizing search efficiency and victim rescue;

3) **situational awareness**, including informed decisions, damage and risk assessment, worksite triage, logistics.

In robot-assisted SAR operations, there are several additional challenges in mission planning. These include technological limitations, tradeoffs between speed and accuracy, possible risks to victims and/or FRs (e.g. heavy-duty UGVs), data privacy issues (remote sensing), as well as increased logistics support (e.g. recharging stations).

This paper evaluates three key technologies in SAR operations: UAV, UGV and TFC. The use case presented here provides a real-world test regarding their practical value, advantages and limitations.

EXPERIENCE

A large-scale SAR exercise evaluated UAV, UGV and TFC deployment in a maritime disaster scenario, involving sinking of a tourist boat during severe thunderstorm and rough sea conditions. Survivors were scattered across coastline, islands and open sea. Access routes were limited and restrictions applied for drone flights.

Mission objectives included rapid deployment, coordinated search and victim detection across land and sea. Resources included small boats (RIB), UAV teams, a transport-capable UAV, a UGV, scuba divers, medical teams and ground search teams, supported by a portable Base of Operations (BoO).

Parallel deployment enabled rapid area coverage. UAVs conducted aerial sensing and mapping of inaccessible

coastline and sea areas. The transport UAV deployed the UGV on a nearby island for autonomous ground search. Ground teams searched accessible coastal areas, while boats conducted surface search operations. Coordination through the BoO ensured efficient tasking in parallel.

Real-time communication provided continuous situational awareness. TFC enabled transmission of imagery and video from UAVs, UGVs and FRs to command staff. Specifically for remote sensing employed in area searching in both sea and land, RGB and thermal/IR cameras were extensively used; the first provides better spatial resolution in good visibility conditions, while the second is better for colder background (sea) and more resilient to limited visibility (night, water vapor, smoke).

Figure 1 shows the exercise area, roughly 2 x 1 km^2 in actual size. The colored numbers indicate locations of interest.

Figure 1. Exercise area and the most important locations of interest for the scenario.

Due to the urgency of the situation, multiple SAR aspects where activated in parallel, even while the BoO was being set up. One RIB was tasked for coastal search around the islands (#5, #6) and the other for wide area surface search (#7) and along the main wind drift (#8). One UAV was tasked for wide area search along the main coastline (#2). The transportation UAV was tasked for carrying and dropping the UGV at the smallest island (#5) for rapid area search. A FR team was immediately dispatched for land search towards (#2). The scuba diving team remained on standby.

LESSONS LEARNED

UAV deployment proved critical for rapid wide-area search, particularly during early mission phases. Their sensing capabilities reduced response time and improved detection probability via combined and supplementary use. Transport UAVs provided additional value by deploying UGVs quickly to otherwise inaccessible locations, eliminating the need for full responder deployment.

UGVs provided localized ground-level sensing while minimizing responder risk. However, terrain and environmental constraints limited their operational range. Their effectiveness was highest when deployed via aerial transport to targeted areas.

Reliable TFC were essential for coordination, safety, and decision-making. Continuous transmission of sensor data enabled command staff to maintain operational awareness and optimize deployment strategy, while extended communication coverage ensured operational continuity.

Operational planning required balancing UAV deployment risks with coverage priorities. Multi-role UAV platforms equipped with sensing payloads improved flexibility and efficiency. Future improvements can include UAV launch capability from mobile platforms (boats) and deployment of airborne communication repeaters to extend network coverage.

TAKEAWAY MESSAGE

Combined deployment of UAVs, UGVs, and TFC technologies improves SAR effectiveness in major ways:

UAVs provide rapid sensing and deployment capability; UGVs enhance localized search while reducing responder risk; robust communications ensure coordination and situational awareness. Appropriate use of these technologies and multi-purpose design can improve operational efficiency even more in the future.

ACKNOWLEDGEMENTS

This work is funded by the EU Horizon Europe for projects CARMA (GA n.101168355) and 6G-VERSUS (GA n.101192633); and jointly by the EU Horizon Europe, SSERI Switzerland, STA Japan, SICT Ministry & KETRI Korea, under project SYNERGISE (GA n.101121321).

REFERENCES

Chrysanthopoulos, S., Kapetanakis, T., Chaidemenos, G., Vernardos, S., Georgiou, H., & Rossi, C. (2020). Emergency response in recent urban/suburban disaster events in Attica: Technology gaps, limitations and lessons learned. *17th ISCRAM Conference (ISCRAM 2020), 24-27 May 2020 @ Blacksburg, USA [Best Paper / Murray Turoff Award].*

Georgiou, H., Andriopoulou, A., & Vlachopoulos, A. (2024). Evolution of Urban Search & Rescue (USAR) operations with remote sensing and information management via emerging ICT and robotics technologies for field deployment. *Information Technology in Disaster Risk Reduction (ITDRR 2024), 14-16 Oct 2024 @ Krems, Austria.*

Steinhausler, F., & Georgiou, H. (2022). Detection of victims with UAVs during wide area Search and Rescue operations. *IEEE Intl. Symposium on Safety, Security and Rescue Robotics (SSRR 2022), 8-10/11/2022 @ Seville, Spain.*

Professionalizing Liaison Roles for Civil Protection

Katharina Kahl
Research Assistant
Katharina.Kahl@idf.nrw.de

Dr. Monika Rode
Research Coordinator
Monika.Rode@idf.nrw.de

Frank Cools
Researcher
Frank.cools@nipv.nl

ABSTRACT

Cross-border emergencies in Europe require cooperation between neighboring countries but often remain below the activation threshold of EU coordination mechanisms. In such cases, response effectiveness depends on informal networks. This paper reflects on experiences from the Civil Protection Liaison Network Concept (CivPro-LiNC) project, which aims to professionalize cross-border liaison functions in civil protection. It is based on qualitative insights from stakeholder meetings, semi-structured practitioner interviews, and iterative training development. Drawing on stakeholder engagement, interviews, and training development, the paper highlights challenges and lessons learned regarding communication, role clarity, and sustainability. The paper discusses implications for information systems and blended learning approaches in line with the ISCRAM community's focus. The insights offer implications for improving preparedness and operational coordination in border regions.

Keywords: Cross-border cooperation, civil protection, liaison officers, preparedness, practitioner insights

INTRODUCTION

Disasters do not respect administrative or national borders. While the EU provides coordination instruments for major crises, such as UCPM, many incidents remain below the threshold for its activation. These smaller yet operationally demanding events must be managed at regional or local levels, often under time pressure.

In such situations, cross-border cooperation depends on personal contacts, informal agreements, and the experience of practitioners. Differences in legal frameworks, organizational structures, terminology, and professional cultures complicate coordination. The CivPro-LiNC project was initiated to address this gap by strengthening and professionalizing cross-border liaison functions in civil protection.

This paper reflects on practical insights gained during the phases of CivPro-LiNC, focusing on stakeholder engagement, role definition, and training design. The paper follows a qualitative, practice-based research approach and aims to increase methodological transparency by outlining data collection and analysis procedures. Rather than presenting a methodological study, the paper shares lessons learned that may be relevant for practitioners and decision-makers involved in cross-border disaster management.

CONTEXT AND BACKGROUND

CivPro-LiNC is an EU–funded project. Launched in March 2025 with a duration of 18 months, the project is led by the District Government of Cologne in cooperation with partners from Germany, the Netherlands, and Belgium. Its objective is to improve cross-border disaster response by professionalizing the role of liaison officers.

Liaison officers act as bridges between organizations and jurisdictions. Their task is to facilitate communication, translate procedures, clarify responsibilities, and support mutual understanding between teams. Liaison roles across Europe are diverse, often informal, and rarely supported by standardized training.

Early project activities revealed that many border regions rely on a small number of experienced individuals who "know how things work across the border." While effective in the short term, this approach is vulnerable to staff turnover and changing organizational structures.

EXPERIENCE AND INSIGHTS

A central element of the project has been the involvement of practitioners. Two stakeholder meetings brought together participants from public administration, emergency services, research institutions, and European networks. Participants were invited to reflect key actors in cross-border civil protection, particularly those directly involved in operational coordination and decision-making. However, the selection was purposive and may not fully represent all relevant perspectives. These meetings provided insights into operational needs. The stakeholder meetings were designed using the World Café method, enabling structured yet open discussions across rotating groups, with systematic documentation of key themes. Several recurring themes emerged.

There was strong agreement that liaison roles need clearer definition. In practice, expectations toward liaison officers vary: some are expected to advise command staff, others to translate language and procedures, and still others to resolve administrative issues. This ambiguity can lead to misunderstandings during operations.

Stakeholders emphasized the importance of physical presence. Liaison officers embedded within partner teams were seen as more effective than those operating remotely. This perceived effectiveness is based on qualitative assessments reported by participants during stakeholder meetings and interviews. It may reflect factors such as improved informal communication, faster feedback loops, and increased trust. Further research with systematic evaluation methods would be needed to validate this observation.

Training was identified as a critical gap. While some regions offer informal briefings or ad hoc learning through exercises, there is little systematic preparation for liaisons. Stakeholders stressed that training should include cultural understanding, communication skills, and network-building. In response, the project explores blended learning approaches that combine digital learning environments with in-person exercises, aligning with ISCRAM's focus on the integration of information systems in crisis management training.

REFLECTIONS AND LESSONS LEARNED

For cross-border cooperation personal commitment remains essential, it must be supported by institutional structures. Professionalizing liaison roles does not mean standardization, but rather creating a shared baseline of understanding, competencies, and expectations.

Border regions differ significantly in governance models and operational practices. A "one-size-fits-all" approach would not work. Stakeholders favor modular tools that can be adapted to local contexts while maintaining a common conceptual framework.

Many liaison systems depend on a few motivated individuals. Without formal recognition, and organizational support, these capacities risk eroding over time. Embedding liaison roles within organizational structures was therefore seen as essential.

It is important to involve practitioners in defining training formats. Their operational perspective proved invaluable in distinguishing what is theoretically useful from what seems sensible for the practice. Curriculum development should unite pedagogical, didactic concepts. This synthesis results in a spiral curriculum to develop skills for professional activities (Tramm & Naeve-Schoß, 2020).

IMPLICATIONS AND TAKEAWAY MESSAGE

CivPro-LiNC demonstrates that strengthening cross-border disaster response starts with investing in people, roles, and relationships. Liaison officers are a critical yet often overlooked resource in European civil protection. Clear role definitions, practice-oriented training, and sustainable networks can enhance coordination in everyday cross-border incidents. Effective cooperation needs to be prepared, practiced, and supported long before the next crisis occurs. Furthermore, strengthening methodological rigor, integrating digital tools and information systems will be essential to align future work with ISCRAM's agenda.

ACKNOWLEDGEMENT

CivPro-LiNC is funded by the European Union from 2025 to 2026.

REFERENCES

Tramm, T., & Naeve-Schoß, N. (2020). Curricula für die berufliche Bildung – Lernfeldstrukturen zwischen Situations- und Fächerorientierung. In R. Arnold, A. Lipsmeier, & M. Rohs (Eds.), *Handbuch Berufsbildung* (3rd ed., pp. 309-324). Springer VS.

Digitization in Civil Protection in a Federal Country – A Practitioner's View on Chances and Challenges

Christoph Lamers
Ministry of the Interior of the State North Rhine Westphalia
christoph.lamers@im.nrw.de

ABSTRACT

German civil protection is defined by a complex federal structure where responsibilities are divided between the federal government for civil defense and the 16 federal states for "peacetime" disaster control. While this decentralization allows for localized expertise and resilience, it has resulted in a fragmented digital landscape characterized by incompatible IT systems, a lack of standardization, and tedious procurement processes. This paper examines the current state of digitization in situation awareness systems and tactical training. By analyzing the national "GeKoB" platform and Berlin's real-time situation report, the paper highlights the tension between regional autonomy and the need for nationwide interoperability. The findings suggest that while modern technology like virtual reality is being integrated into training, significant synergy effects remain inhibited by the lack of shared standards and systems.

Keywords

Digitization, Situation Pictures, Training

INTRODUCTION

Whereas the use of the internet for sharing information and exchanging data, especially by using smartphones, has drastically changed our daily life in the past 25 years, the working methods of the fire service and other relief organizations are not so different from those of the 1990s. Modern information technology has also found its way in there to some extent, but it still does not play a vital role.

A study carried out by the "Safety innovation center", a German private research center, in cooperation with Paderborn university, commissioned by the German Fire Protection Association (vfdb) in 2020[1] revealed a low level of satisfaction with digital transformation among the emergency services. A lack of financial resources and tedious procurement processes as well as a lack of standardization leading to an inconsistent, difficult-to-access IT market were identified as the key obstacles in the process of digitization. Thus, the authors requested the creation of standardized interfaces and networked IT systems combined with clear guidelines, responsibilities and framework conditions German civil protection.

LEGAL SITUATION

The German civil protection system is characterized by a historically developed federal structure based on a strict division of responsibilities between the federal government and the federal states. Under this dual architecture, the federal government is solely responsible for civil defense, i.e. the protection of the population in the event of a defense situation, in accordance with the German constitution. In contrast, responsibility for 'peacetime' disaster control – for example, in the event of natural disasters, large-scale accidents or pandemics – lies solely with the 16 federal states.

A key advantage of this decentralized structure is the close proximity and detailed knowledge of those responsible on the ground. In addition, the distribution of resources across many shoulders ensures a high level of resilience

[1] Safety innovation center, 2020.

of the overall system against selective failures.

However, this fragmentation also poses considerable challenges, which become particularly apparent in large-scale cross-border situations. A major hurdle is the lack of standardization: since each federal state issues its own organizational and equipment guidelines, tactical units of fire brigades and aid organizations are often defined differently. In addition, different communication channels, command systems and alert procedures in large-scale crises affecting several federal states at the same time lead to enormous coordination efforts and potential friction losses at the interfaces between responsibilities.

DIGITAL SITUATION AWARENESS SYSTEMS

The fact that the federal states are primarily responsible for civil protection also has an impact on digital situation awareness systems. There is a heterogeneous landscape of systems in use, which are generally not compatible with each other. Two of them are presented below.

The "Lagebild Berlin" (Berlin Situation Report)[2] was established due to the urgent information requirements of Berlin's disaster control authorities, recognized aid organizations and critical infrastructure operators in light of the growing Covid-19 situation. It has been active since mid-March 2020 and has been continuously developed in consultation with the parties involved.

The ELD-BS, German acronym for "Electronic situation display for civil protection" is a tool that has been used for years in staff work and crisis management by authorities in the state of Baden-Württemberg[3]. The platform was developed by Fraunhofer IOSB, a research center for optronics, systems engineering and image analysis, in collaboration with the Baden-Württemberg Ministry of the Interior. It is used extensively in operational and training scenarios at all administrative levels.

This fragmentation of situation reports, especially the lack of a situation report at national level, was identified as a problem several years ago. For this reason, the "Joint Competence Centre for Civil Protection" (GeKoB), a cooperation platform between the federal government and the states founded in 2022, was tasked with creating a national digital situation report. Following a thorough analysis of existing requirements and systems, a pilot system is currently being developed.

TRAINING

The use of virtual reality (VR) also offers a wide range of applications in tactical training for the fire service. Since 2018, the State Fire Service Institute North Rhine Westphalia, the fire academy of this state, has therefore started to use VR in part of the practical leadership training for platoon leaders and incident commanders in medical rescue.[4] The avatars of the platoon and group leaders move around in virtual space and can only see the parts of the operation site that would be actually visible from their respective positions. The three-dimensional representation of the environment offers the opportunity to practice the initial phase of an operation in a very realistic manner as part of the reconnaissance.

An obstacle for a wider use of VR in the tactical training is the fact that the development of scenarios has turned out to be rather tedious and time-consuming. The fact that firefighting is the responsibility of the federal states, with each state operating its own firefighting academy, has a negative impact here. Even though the fire service academies are in contact with each other and regularly exchange information on their teaching content and methods, no significant synergy effects have yet been achieved in the use of virtual reality.

CONCLUSION

The digital transformation of German civil protection faces systemic hurdles rooted in its constitutional architecture. The autonomy of federal states and municipalities has led to a "digital patchwork" where essential information often stops at administrative borders, complicating large-scale cross-border operations. While initiatives like the national digital situation report currently developed by the joint federal-state GeKoB platform represent vital steps toward networking information, the overall level of satisfaction with digitization among emergency services remains low.

Ultimately, for German civil protection to remain effective in the digital age, it must balance its successful

[2] Senatsverwaltung für Inneres und Sport, n.d.
[3] Fraunhofer IOSB, 2025.
[4] Speth, 2021.

principle of local subsidiarity with a mandatory commitment to nationwide technical interoperability and standardized interfaces.

REFERENCES

Fraunhofer IOSB (2025). Elektronische Lagedarstellung Bevölkerungsschutz, https://www.iosb.fraunhofer.de/de/projekte-produkte/elektronische-lagedarstellung-bevoelkerungsschutz.html

Safety innovation center (2020). Digitale Transformation in der zivilen Gefahrenabwehr, https://www.blaulicht.digital/wp-content/uploads/sites/6/2020/09/Studie-Digitale-Transformation-in-der-zivilen-Gefahrenabwehr.pdf.

Senatsverwaltung für Inneres und Sport (n.d).: Lagebild Berlin, https://www.berlin.de/katastrophenschutz/organisation/lagebild-berlin/artikel.1332384.php

Speth, H. (2021). Digitalisierung der Feuerwehr- Aus- und Fortbildung: Von Möglichkeiten und Grenzen, *Proceedings of the 67th Annual Conference of the vfdb*.

Experiments with AI Decision Support in Operational Contexts

McEwan-Verver
Veiligheidsregio Noord- en Oost Gelderland
S.McEwan@vnog.nl

Van Balen-de Greef
Veiligheidsregio Midden- en West Brabant
Jolande.van.Balen@vrmwb.nl

ABSTRACT

We present initial lessons learned from two experiments with AI Decision Support Systems (AI DSS) in an operational setting. The systems, based on multiple LLMs and a RAG architecture, were developed and tested to explore their potential for supporting operational decision-making and to identify key implementation preconditions. The resulting proof-of-concepts were evaluated as promising by operational decision makers. Key insights highlight the importance of high-quality training data, algorithmic transparency and explainability, and the ability to collaborate with new and diverse partners as critical preconditions for successful development and deployment of such systems.

Keywords

AI, LLM, crisis decision making, knowledge, data.

INTRODUCTION

Three Dutch crisis management organizations have experimented with the use of AI for crisis decision support in 2025. The AI technologies used were mainly a combination of several Large Language Models (LLM) with a Retrieval Augmented Generation (RAG) architecture. Two experiments were done to support operational decision support:

1. CoCommander, where incident specific advice is generated based upon training documentation, using incident and building characteristics as input parameters. The resulting recommendations are integrated into the standard operational information systems used by the fire commander.
2. MultAI, where crisis specific advise is generated for the crisis manager based upon knowledge documents that describe the administration governance of the different crisis types based upon incident characteristics and geographic location.

SHORT DESCRIPTION OF THE TWO AI MODELS

The CoCommander experiment is a collaboration between a start-up and a Dutch crisis management organization, aimed at supporting less experienced fire commanders. Due to demographic aging, most Dutch crisis organization find themselves faced with a high staff turnover from highly experienced fire commanders to more recently trained commanders. In addition, this model aims to detect 'hidden' patterns that are not quickly or easily detected, also by more experienced fire commanders. The added value of this algorithm lies mostly for more complex incidents, and not for relatively easy situations. The algorithm consists of three separate LLM's. The main logic resides in the LLM that evaluates incident characteristics, the other LLM's process, search or summarize based upon building and training documentation. Outputs are integrated into existing operational systems for usability. Special measures were taken with regards to transparency, explainability and hallucinations, and to prevent the model from "over advising".

The MultAI experiment is a collaboration of several organizations including two Dutch crisis management organizations and a Dutch university. The aim is to develop an AI tool that supports crisis managers by reducing

the time required to identify which organizations should be called in during a crisis. Instead of manually reviewing multiple documents for at least 30 minutes, MultAI is designed to provide an answer within approximately 45 seconds. Generic generative AI was insufficient because the crisis documentation includes both text and highly specific diagrams, leading to the development of a custom Python-based algorithm. Students implemented several LLM components and conducted initial technical tests on the demonstrator. Crisis managers also evaluated the system in multiple user tests, resulting in improvements to the frontend interface. The tool was demonstrated at a symposium on decision support for crisis managers in September last year.

EXPERIENCE AND INSIGHT

The operational decision-makers from both experiments concluded that the results from the Proof of Concepts are promising. Some of the main insights were:

1) **Communication** proved challenging. Dutch crisis management organizations mainly operate in Dutch and rely on Dutch-language documentation, while both experiments involved non-Dutch-speaking partners. In addition, in contrast to traditional IT projects, which typically start with fixed requirements specifications, AI development followed a more iterative and organic process in which all disciplines needed continuous involvement and mutual understanding.
2) A lot of the effort needed to be allocated to **data quality.** Traditional software engineering primarily involves designing, implementing, and debugging code. In contrast, machine learning starts with collecting data and training of a function on the data. (Whang et al., 2023, p. 791). We found that some of our datasets were of insufficient quality to be used in the finetuning of the machine learning model, because the manner in which these datasets are perceived by humans differs significantly from the manner in which AI is using these documents.
3) During the tests, the future users (fire commanders and information managers) indicated that they found it important that it is **clearly visible** that the advice output is AI generated. They also expressed the importance of transparency and explainability of the outcomes.

REFLECTION AND LESSONS LEARNED

1. Working with new partners such as students and start-ups deliver. They have the latest knowledge and broaden our horizon.
2. The development process differs from traditional non-AI systems development and has more focus on finding common ground between AI en operational practitioners. The development process depends on a mutual understanding of how AI works and how it deals with data.
3. RAG based LLM's can work on selected organization-specific datasets. This has however only been tested in an experimental setting and the necessary checks and balances for operational use are not followed through yet. Operational use of these systems require careful ethical and legal reflections on the impact of these systems on the operational decision-maker.
4. We observed that certain datasets were overrepresented in the system's outputs. For instance, training materials related to aircraft incident response were initially disproportionately reflected in CoCommander's results. Further understanding of the underlying algorithmic processes is needed to explain this effect.
5. The introduction of AI DSS needs to be carefully considered. Legally, the decision-maker is required to be aware that this is AI, and the decision-maker needs to be AI literate.

CONCLUSION

RAG based LLM's offer great opportunities to access large (amounts of) datasets in support of decision-making. It can also lead to unexpected insights into our (traditional) ways of working. It is important to embrace the opportunities in how this can disrupt our current ways of working.

REFERENCES

Whang, S. E., Roh, Y., Song, H., & Lee, J. G. (2023). Data collection and quality challenges in deep learning: a data-centric AI perspective. *VLDB Journal*, *32*(4), 791–813. https://doi.org/10.1007/s00778-022-00775-9

Which Insights from Cyber Crisis Exercises Survive Contact with Reality?

Stefan Nelwan
National Cyber Security Centre (NCSC-NL)
Stefan.Nelwan@ncsc.nl

Michael Meijerink
National Cyber Security Centre (NCSC-NL)
Michael.Meijerink@ncsc.nl

ABSTRACT

National cyber crisis exercises are vital to collaborative preparedness for public and private organisations, but from a practitioner's perspective the transferability of exercise lessons to real-world incidents remains underexamined. Based on experience from several national-level cyber exercises and real-world incidents, this paper identifies several recurring patterns between exercises and reality. Exercises aim to build trust among participants and provide an opportunity to rehearse and refine procedures, but real-world incidents may introduce political pressure and uncertainty.

Keywords

cyber crisis exercises; cyber preparedness; cyber resilience; public-private collaboration; national coordination.

INTRODUCTION

As society has become increasingly dependent on the ubiquitous availability of information and communication technologies, exposure to cyber risks has grown accordingly. These risks are not only increasing in frequency and impact, but are also characterised by high levels of uncertainty. Cyberspace is inherently uncertain: decision-makers must act without access to a complete and coherent picture. As Van Den Berg (2024) argues, organisations respond to such uncertainty through combinations of risk management, resilience-building, regulation, and trust. These strategies shape how organisations manage digital crises.

Investigations into real-world incidents further highlight the persistent nature of uncertainty and the challenges it poses for coordination and decision-making. For example, the Dutch Safety Board has emphasised that during large-scale digital disruptions, organisations struggle with incomplete information, unclear responsibilities, and difficulties in achieving a shared operational picture (Dutch Safety Board 2021).

National cyber crisis exercises are widely used to strengthen collaborative preparedness, test incident response plans, improve collective sense-making, coordination, and decision-making. These exercises bring together ministries, critical infrastructure, law enforcement, and public and private-sector partners to test coordination and escalation procedures. However, repeated experience across exercises and real incidents suggests that not all lessons survive contact with reality. The way uncertainty is experienced and acted upon may differ substantially between cyber crisis exercises and real-world incidents. It is important to understand these differences for assessing the applicability of lessons learned from cyber exercises to real-world incidents.

EXPERIENCES

The presented insights are based on practitioner experience across several national cyber crisis exercises and multiple real-world incidents over the past years. These include large-scale national exercises such as ISIDOOR IV (2023), as well as operational involvement in incidents with national impact, including the Log4Shell vulnerability (2021) and preparedness activities for international events such as the NATO Summit 2025 in The Hague. Even though this is not a formal comparative study, the observations reflect recurring patterns identified across both exercises and operational practice.

Tempo and synchronisation dynamics. Cyber exercises operate within a structured and coordinated timeline. Participants are informed in advance of the exercise period, and participation is typically limited to a predefined subset of actors. Injects and escalation paths are designed beforehand, and even simulated time pressure remains bounded and synchronised across organisations. These characteristics reflect established design principles for crisis exercises. For example, Grunnan and Fridheim (2017) emphasise the importance of clear exercise objectives, realistic scenarios, and the involvement of diverse participants to support effective decision-making. This structured approach was also observed in the evaluation of ISIDOOR IV (Rijksoverheid 2023), where coordination moments and information exchange were aligned across participants.

In real cyber crises, events unfold asymmetrically. Periods of uncertainty may abruptly shift into operational overload. Media, political and managerial timelines may diverge from technical investigation timelines. These divergences introduce cognitive and political stressors that are difficult to replicate in an exercise setting. Crisis leadership research shows that decision-makers frequently need to operate under pressure to act before full information is available (Boin et al. 2017).

Exercises tend to reward adherence to processes and procedures, but real incidents demand decision-making under uncertainty.

Information Ambiguity. Exercises are built around predefined objectives and scenario-driven events. Although participants lack complete visibility, the scenario itself remains internally and logically coherent. Real incidents rarely offer such a coherent and complete picture. Indicators may conflict or may be spread across multiple organisations. Root causes and attribution may be uncertain. Intelligence can be incomplete or too sensitive to share. External narratives can evolve independently of verified facts. Experience shows that collective sense-making and information sharing between organisations are often more challenging than scarcity of information. Information exchange does not automatically produce shared understanding.

In high-pressure environments, organisations must engage in collective sense-making under conditions where meaning is unstable and contested (Weick 1993).

Information Management. In exercises, information flows are typically designed and bounded within the scenario. In real incidents, data may arrive simultaneously from multiple, often unexpected sources with no guarantee of relevance or reliability. The organisational and cognitive burden of processing large volumes of information can be underestimated. During real incidents, unclear reporting lines and parallel communication channels can lead to duplication, delays, or even loss.

Furthermore, available information may not be actionable. Actors at the strategic level may lack operational detail, while technical teams may not fully grasp broader societal impact. Without structured integration mechanisms, situational awareness remains fragmented and unevenly distributed.

The challenge is therefore not only ambiguity in the external environment, but the internal management of information flow. Ineffective information architecture may amplify uncertainty, slow decision-making, and increase friction between organisational layers. This is a dimension that is difficult to stress-test in exercises.

REFLECTIONS AND LESSONS LEARNED

Exercises are a means of preparing organisations for the unexpected. Their purpose is to validate plans, procedures, and escalation mechanisms. A well-rehearsed plan reduces the time required to organise an appropriate response. Feedback from real incidents should be incorporated into the subsequent iterations of cyber exercises.

Lessons from exercises that transfer to real-world incidents in addressing tempo, synchronisation, and information ambiguity are most effective when organisational trust, structured communication, and role clarity are already established. Crises are ultimately managed by people. Personal and organisational trust and mutual understanding are cultivated in the preparation phase and reinforced during real incidents. Structured communication formats at scheduled times reinforce trust in the reliability and predictability of the coordination process.

In addition to these relational and procedural elements, structural investments in information architecture appear to transfer effectively. In response to recurring challenges in information integration and role clarity, a tailored crisis information management system at NCSC-NL was developed and refined during exercises before being deployed in real-world cyber incidents. Its use in both exercises and real-word incidents suggests that improvements in information management may transfer more reliably than scenario-specific learning. Rather than eliminating uncertainty, such systems help actors function within it.

Preparedness is therefore less about rehearsing a specific cyber attack and more about fostering and improving adaptive capacity across organisational and governance boundaries.

CONCLUSION

National cyber exercises are foundational for rehearsing processes and procedures in the public-private ecosystem. To enhance transferability, exercises should deliberately incorporate cognitive and political stressors, rather than focusing only on technical complexity. In cyber ecosystems characterised by structural uncertainty, preparedness ultimately depends on the cultivation of adaptability and agility within the crisis organisation. These observations align with crisis leadership and sense-making theory, which emphasise that structure and trust stabilise action under conditions of uncertainty.

REFERENCES

Boin, A., Hart, P., Stern, E., and Sundelius, B. (2017). *The Politics of Crisis Management: Public Leadership Under Pressure*. 2nd ed. Cambridge: Cambridge University Press.

Dutch Safety Board (2021). *Vulnerable through Software*. Tech. rep. Dutch Safety Board.

Grunnan, T. and Fridheim, H. (Nov. 2017). Planning and conducting crisis management exercises for decision making: the do's and don'ts. In: *EURO Journal on Decision Processes* 5.1, pp. 79–95.

Rijksoverheid (2023). *Evaluatie Isidoor IV*. Technical report. Ministerie van Justitie en Veiligheid.

Van Den Berg, B. (2024). Dealing with uncertainty in cyberspace. In: *Computers & Security* 144, p. 103939.

Weick, K. E. (1993). The Collapse of Sensemaking in Organizations: The Mann Gulch Disaster. In: *Administrative Science Quarterly* 38.4, pp. 628–652.

Organisational Resilience through Business Continuity Management: Exciting or Stressful?

Megin Reijnders
Trimension
reijnders@trimension.nl

Max Mutsaers
IND
m.j.l.mutsaers@ind.nl

ABSTRACT

Organisations face increasingly frequent and complex disruptions. While business continuity management (BCM) is sometimes approached as a compliance-driven activity, its real value lies in how it supports faster, more focused crisis management by clarifying priorities before disruption occurs. This paper expands on the importance of determining strategic intent in order to optimise the gains of BCM. When grounded in strategic intent, supported organisation-wide, and updated regularly, a business continuity management system (BCMS) becomes more than compliance: it strengthens resilience and enables faster, more effective crisis management.

Keywords

Business continuity management (BCM), Preparedness, Resilience, Strategic priorities

INTRODUCTION

Organisations today face disruptions in many forms, with an ever-increasing frequency and level of complexity. From technical failures and geopolitical tensions to sudden electrical outages, the question is no longer *if* something will interrupt operations, but *when* and for how long. There is therefore growing pressure to strengthen resilience. EU directives such as NIS2[1] and CER[2], designed to help ensure vital services continue, provide an additional incentive for organisations to take a fresh, honest look at their resilience. Business Continuity Management (BCM) offers a way to prepare for the effects of disruption through structured, proactive planning rather than last-minute improvisation. It specifically looks at the impact of disruptions, rather than the causes, to help prioritise essential activities. When approached thoughtfully, it increases the effectiveness of crisis management and helps organisations clarify what truly matters to keep their mission intact when disruptions occur. This article discusses activities and lessons learned in the preparation, or pre-incident, phase.

DEFINING DIRECTION

Business Continuity Management (BCM) is a structured approach to ensure the "capability of an organisation to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption" (ISO, 2019, p.2). It is not about high-pressure decision-making. Its value lies in prior strategic choices, determining what is essential. If those choices are not made at the strategic level, crisis teams end up debating priorities while services are already under pressure. BCM therefore starts at the strategic level. Senior management must define the goal, scope and direction, and acceptable impact before BCM is taken into departments or the operational level. Without explicit decisions and leader's intent, choices are implicitly pushed down to operational teams, resulting in siloed outcomes based on local assumptions. In other words: if you didn't agree on where your goal is during a football match, where do you put the goalkeeper?

[1] EU Network & Information Systems Directive 2
[2] EU Critical Entities Resilience Directive

Starting a BCM system (BCMS) without a defined goal leads to inefficient use of resources, overloaded staff, and unmet expectations due to misaligned requirements and missing elements.

SOLUTIONS FROM EXPERIENCE: EFFECTS AND AWARENESS

BCM is not a guarantee against crises but does improve preparedness. When business continuity plans are not prepared or a crisis exceeds their scope, crises can quickly escalate and crisis management becomes the response mechanism. BCM therefore makes crisis management quicker and more effective and is a key driver of crisis prevention and de-escalation. It is important to have a function dedicated to facilitating and coordinating this effort as well as allocating time to involved personnel.

The critical elements and practical insights to initiate a BCMS listed below are based on experience facilitating the implementation of BCM in several sectors ranging from government to healthcare and energy.

1) Creating urgency and moving to action mode

Determining scope and goals often takes more than a single meeting. Organisations need to be ready to take on BCM, consider it sufficiently important and dedicate time and resources. Therefore, it is important to take time to address BCM in several (informal) conversations to gain insight into concerns of strategic leadership. Even in the absence of recent incidents, there is often a substantial 'gut feeling' which will form the basis for the 'why' of the BCMS. Addressing this before formally setting scope helps build shared understanding, commitment, and the move to 'action mode'.

2) A clear leader's intent through a strategic vision

Setting a leader's intent at the strategic level clarifies organisational priorities and principles, such as impact categories or essential services for the organisation's mission at a high-level. These scope all further BCM efforts and focus business impact analyses (BIAs). A BIA distils the essence of an organisation's business, at departmental, process or activity level. However, without leader's intent, BIAs risk becoming fragmented and undermine the effectiveness of BCM measures.

Because BCM focuses on impact first, a meeting or workshop based on discussing the severity of impact on high level tasks can help leadership make trade-offs explicit. Experiences in the field highlight the importance of starting with a proposal for critical services and impact categories, to facilitate the flow of the workshop. This proposal should be pre-agreed upon with a BCM manager or high-level person in the organisation. The conversations during such workshops provide a means to distil business essential processes and recovery strategies. Discussions are likely to arise and are often characterised by a mix of functional, political, and personal considerations. These discussions may otherwise happen during a crisis itself. Those facilitating the workshop and supporting the organisation's strategic team should be prepared adequately, by guiding the participants through a process based on clear goals as predefined with the head of the strategic team. It is essential to officially validate the results. This gives the operational layer of the organisation direction and mandate to execute BIAs and develop and implement continuity plans.

3) Broad organisational support for the BCMS

Using the leader's intent, departments should be involved in developing and implementing BCM based on their own expertise. When the various organisational departments understand the business impact of possible disruptions, as well as internal and external dependencies, it creates cohesion and promotes ownership. This supports personnel in the development of integral measures while at the same time making the benefits of a BCMS tangible. For example, encouraging departments with heavily IT dependent business processes to formulate alternative workflows in case of IT disruptions.

BCMS AS A PREPARATORY TOOL FOR DISRUPTIONS

By setting clear priorities at the strategic level, fostering broad organisational support, and revisiting plans as conditions evolve, having a BCMS becomes more than a compliance exercise. It becomes a practical tool for resilience, helping organisations manage crises more effectively and achieving quantifiable reductions in the impact of disruptions.

REFERENCES

International Organisation for Standardisation. (2019). *Security and resilience — Business continuity management systems — Requirements* (ISO Standard No. 22301:2019). https://www.iso.org/standard/75106.html

Beyond Generic Courses: How Self-Evaluation Tools Can Drive Custom Training for Municipal Crisis Staff

Malte Schönefeld
State Fire Institute of North-Rhine Westphalia
malte.schoenefeld@idf.nrw.de

Monika Rode
State Fire Institute of North-Rhine Westphalia
monika.rode@idf.nrw.de

ABSTRACT

Municipalities increasingly face overlapping crises that strain staff, structures and coordination capacities. This paper reports from the KRISENFIT project, which links an innovative municipal crisis fitness self-evaluation tool (SET) with a modular, learning field-oriented training concept for crisis staff. Indicator-based self-assessment results are used to prioritize locally relevant competencies and scenarios, which then drive tailored blended learning and exercise modules. Utility analysis of existing concepts, practitioner workshops and trainer expertise inform curriculum design and a scenario catalogue. The approach aims to improve municipal crisis fitness through targeted, practice-driven and evaluable learning interventions rather than generic courses.

Keywords

Municipal crisis management, crisis fitness, self-evaluation, scenario-based training, coordination in emergencies.

INTRODUCTION

Under potentially overlapping and mutually reinforcing "multiple crises", local governments must maintain core services while coordinating complex crisis responses, stressing people, processes and structures (Schönefeld et al. 2023). Many municipalities invest in training their crisis staff but often rely on generic courses only loosely connected to their own structures, risk landscape and organizational culture. Such training conveys important baseline knowledge yet often fails to address municipality-specific gaps in cooperation, communication and role clarity that become visible in real crises.

The KRISENFIT project addresses this challenge by combining a self-evaluation tool (SET) for municipal crisis fitness[1] with a modular, learning-field-oriented training concept. Such approaches have been called for by research and public institutions (Bralewski et al. 2024). The SET is an Excel-based application that embeds an indicator catalogue and scoring ranges for municipal crisis management. Municipal staff enter assessment data on structures, processes, resources and cooperation; the tool then generates profiles of strengths and weaknesses. These digital profiles feed into blended learning and exercise modules that reflect local priorities and strengthen both individual skills and institutional crisis fitness. From an information systems perspective, the SET structures qualitative and quantitative information on municipal crisis management into configurable indicators, scales and reports and integrates self-evaluation results into existing documentation and learning practices.

WHY SELF-EVALUATION MUST FEED TRAINING

The SET can reveal strengths and needs in municipal crisis management, but without a dedicated training pathway it rarely leads to sustained capability development. In KRISENFIT, the SET is explicitly designed to identify entry points for concrete exercise and learning modules. Key reasons to link self-evaluation with custom training

[1] In the project, municipal 'crisis fitness' denotes the ability of administrations to maintain essential services and coordinate crisis responses under stress, based on robust structures, clear roles, practiced procedures and sufficient resources.

are:

Targeted capacity building: The results of the indicator-based self-evaluation are used to prioritize learning needs (e.g. debriefing skills, communication with the public, maintaining essential services) rather than offering generic crisis seminars.
Organizational ownership: When municipalities see their own data translated into specific modules and scenarios, the training may be perceived as "ours" and not as an external standard course, which may increase participation and willingness to implement changes.
Efficient use of scarce time: Municipal staff have limited time for training and exercises; using SET results to prioritise indicators and scenarios helps administrations focus the available hours on the most pressing gaps instead of broad but only loosely relevant standard courses.

CURRICULUM DESIGN

To ensure high didactic quality, the project analyses existing education and exercise concepts for municipal crisis management staff. The resulting curriculum is modular and learning-field-oriented: discrete building blocks (e.g. communication in crisis staff, cross-departmental coordination, documentation, evaluation) can be combined into tailored learning paths that correspond to specific SET indicators and municipal priorities. This involves:

Developing a weighted evaluation schema with criteria such as contribution to crisis fitness indicators, time requirements, suitability for blended learning, scalability, and alignment with process-oriented crisis management.
Interviewing providers and experts from institutions such as State Fire Institute of North-Rhine Westphalia, universities and national agencies (e.g. German Federal Office for Civil Protection) about strengths and weaknesses of their concepts for the municipal target group.

On this basis, an integrative curriculum is developed that links required competencies (e.g. communication, stress management) with appropriate methods (e.g. tabletop exercise, serious gaming) and learning levels (introductory, advanced, expert). Training is tied to the SET dimensions so that low scores in a specific indicator (e.g. cross-departmental communication) trigger clear recommendations for specific modules and exercise types rather than a vague 'more training' recommendation.

ROLE OF MUNICIPAL WORKSHOPS AND TRAINER EXPERTISE

The *input of practitioners for designing the link between self-evaluation and training* is crucial to ensure feasibility and acceptance. KRISENFIT's partner municipalities Duisburg and Landkreis Vorpommern-Rügen participated in workshops where scenarios and capacity gaps were prioritized. By combining the municipal input, an analysis of exercise requests to the State Fire Institute of North-Rhine Westphalia and expert knowledge, *a catalogue of frequent and high-impact scenarios* is developed and prioritized with municipalities. This catalogue anchors both SET items and training scenarios.

Experienced crisis management trainers contribute practical insights on typical failure patterns in staff work (e.g. unclear roles, communication breakdowns, weak documentation) and on methods that work with administrative staff. Their expertise informs both the design of SET indicators and the selection of methods in the *utility analysis*.

In a later step, selected municipalities implement customized exercise modules based on their SET profiles, supported by *a directing script* that describes scenarios, injects and expected learning processes. These exercises are evaluated through participant and trainer feedback, observation and a pre/post comparison of SET results.

PRACTICAL IMPLICATIONS FOR MUNICIPAL CRISIS PROFESSIONALS

For municipal crisis managers and trainers, this integrated approach offers several concrete advantages:

Clear line of sight from diagnosis to intervention: SET findings inform which competencies, scenarios and roles are to be addressed in training, avoiding generic priorities.
Evidence-informed iteration: By repeating the SET after training cycles and comparing results, municipalities can see whether competence levels and perceived crisis fitness have improved and where the curriculum needs adjustment.
Transferability with tailoring: The SET and modular training architecture are designed to be transferable to other municipalities, while prioritization of scenarios, modules and learning fields is locally negotiated via workshops and stakeholder engagement.

Linking a self-evaluation scheme to a custom-tailored training concept allows municipal administrations not only

to measure their "crisis fitness", but to systematically improve it through targeted, practice-driven and evaluable learning interventions.

ACKNOWLEDGMENTS

KRISENFIT is funded by the Federal Ministry of Research, Technology and Space from 2024 to 2027.

REFERENCES

Bralewski, A., Bralewska, K., Gawroński, W., Zwęgliński, T., & Gikiewicz, M. (2024). Key aspects that make decision-making training in the field of crisis management tailored to identified gaps and needs. *Scientific Reports of Fire University (ZN SGSP)*, *1*(92), 25–56. https://doi.org/10.5604/01.3001.0054.8383

Schönefeld, M., Schütte, P. M., Schulte, Y., & Fiedrich, F. (2023). Critical infrastructure and crisis affected actor? Investigating the double role of municipal administrations. In J. Radianti, I. Dokas, N. Lalone, & D. Khazanchi (Eds.), *Proceedings of the 20th International ISCRAM Conference* (pp. 88–95). University of Nebraska at Omaha. https://idl.iscram.org/files/radianti/2023/2601_Radianti_etal2023.pdf

Lessons from Planning a Whole-of-Society Digital Cross-Border CBRNe Drill

Heejun Shin
SCH Disaster Medicine Center
Soonchunhyang University Bucheon Hospital
World Association for Disaster and Emergency Medicine (WADEM)
79819@schmc.ac.kr

Niklas Tschäschke
TH Köln – University of Applied Sciences
niklas.tschaeschke@th-koeln.de

Anina Felicia Dennhardt
TH Köln – University of Applied Sciences
anina.dennhardt@th-koeln.de

Ompe Aimé Mudimu
TH Köln – University of Applied Sciences
ompe_aime.Mudimu@th-koeln.de

ABSTRACT

Cross-border chemical, biological, radiological, nuclear, and explosive (CBRNe) response requires tight coordination, yet conventional exercises are costly, hard to repeat, and often miss semantic interoperability gaps until late deployment. This practitioner paper shares lessons from planning a digital drill platform linking European and Korean emergency actors. We used a simulation-first design principle that tested interfaces, message exchange, and triage translation before any live session through role-specific dashboards, standardized schemas, degraded-network scenarios, and integrated after-action review. Governance and semantics, more than software alone, drove coordination risk. We highlight reusable planning artefacts for cross-border drills beyond CBRNe.

Keywords

Crisis exercises, Digital training platforms, Medical interoperability, CBRNe preparedness

CONTEXT & AIM

CBRNe incidents require cross-border multi-agency coordination, yet breakdowns often arise from interorganizational and semantic failures rather than technical defects alone. We use “whole-of-society” to describe the full response chain, from field triage and dispatch to hospital allocation, involving fire services, EMS, public-health actors, and critical-infrastructure stakeholders across two national systems.

Conventional exercises are costly and logistically complex, limiting repetition and access. We therefore planned a digital platform for repeatable joint drills without travel. The European-Korean pairing served as a stress test by exposing wider semantic and procedural distance. We defined “simulation-first” as testing interfaces, message schemas, decision points, and translation rules with synthetic scenarios before any live drill, consistent with experiential learning principles (Kolb, 1984).

Scope and Evidence Level

This paper is a practitioner design note from the pre-pilot planning stage of an upcoming exercise series. It reports planning lessons rather than post-exercise outcomes. The evidence base consists of requirements workshops with European fire services, EMS, and dispatch personnel, comparison of Korean DMAT field protocols, and joint architectural design sessions. No live exercise, participant outcome, or measured interoperability result is claimed here; those are reserved for later pilot evaluation.

What Worked in Planning

Clear role definition and technical responsibility assignment improved planning from the outset. The European side mapped fire, EMS, dispatch, and critical-infrastructure operators to command, operations, and support layers, while the Korean side aligned equivalent functions through shared decision points in triage, hazard-zone management, transport, and strategic command. Across workshops, the most important problems were organizational and semantic rather than technical.

We therefore prioritized interoperability-by-design. Standardized message formats were favored over point-to-point adapters, and role-specific interfaces reduced overload by showing only task-relevant information. The platform was designed as a cloud-hosted, web-based drill environment with filtered dashboards for dispatch, on-scene command, and hospital coordination. A central message broker enforced common schemas, controllers injected scenario events and degraded-network conditions, and an AAR module captured timestamped decision logs for debriefing.

Transfer to Real-World Practice

The semantic gap between European "Critical" and Korean DMAT "Red" was not hypothetical. It emerged during side-by-side comparison of DIN 13050 triage categories and Korean DMAT field protocols in bilateral workshops with active-duty EMS personnel. Three fire-service incident commanders independently judged that this mismatch could delay patient handover in a real cross-border deployment. The workshops also informed command-layer mappings, and network degradation profiles came from failure modes seen in earlier bilateral communication exercises.

An important trade-off was how to standardize multinational display without erasing local practice. We resolved this by preserving local triage labels at the source while translating them for shared dashboard visibility. These insights matter in practice because they address handover, dashboard interpretation, and authority rules that also apply in real operations. We acknowledge that psychological and organizational fidelity cannot be fully validated until live pilot testing.

Pitfalls and Mitigations

Planning identified four recurring pitfalls. Information overload threatened situational awareness, so interfaces were restricted to role-relevant information. Adapter fragility risked schema drift, so standardized message models, versioned schemas, and explicit interface contracts were preferred. Semantic interoperability problems reduced trust and consistency, so translation rules and approval gates were incorporated. Cross-border governance issues around authority, visibility, and data ownership required role-based access control and predefined governance rules. Together, these findings linked governance, semantics, and digital architecture as a single design problem (Wolbers & Boersma, 2013).

Minimal Artifacts to Reuse

Three artefacts were especially reusable. First, a scenario matrix linked hazard, sector, task, and inject; for example: chemical release / EMS triage / mass-casualty triage / "50 casualties, wind shift NE, second hot zone declared." Second, a compact metrics catalogue included triage-to-dashboard latency, measured from field triage tag assignment to dashboard display, with a target of ≤90 seconds under nominal connectivity. Third, a medical semantics mapping layer translated urgency categories across systems: European "Critical" had no direct Korean DMAT equivalent and was mapped to "Immediate" with an operational flag. Figure 1 shows the resulting medical data flow.

Illustrative Vignette

A hypothetical chemical-terror walkthrough showed the value of these artefacts. When European fire-service protocols were mapped to Korean DMAT guidance, the "Critical" category lacked a direct Korean equivalent. That failure led directly to the medical semantics mapping rule and confirmed that translation tables must be defined before platform coding begins.

Transparency and Ethics

All rehearsals used simulated data, so no identifiable patient information was processed. Before any live pilot, institutional approvals will be obtained and privacy-by-design controls will be applied.

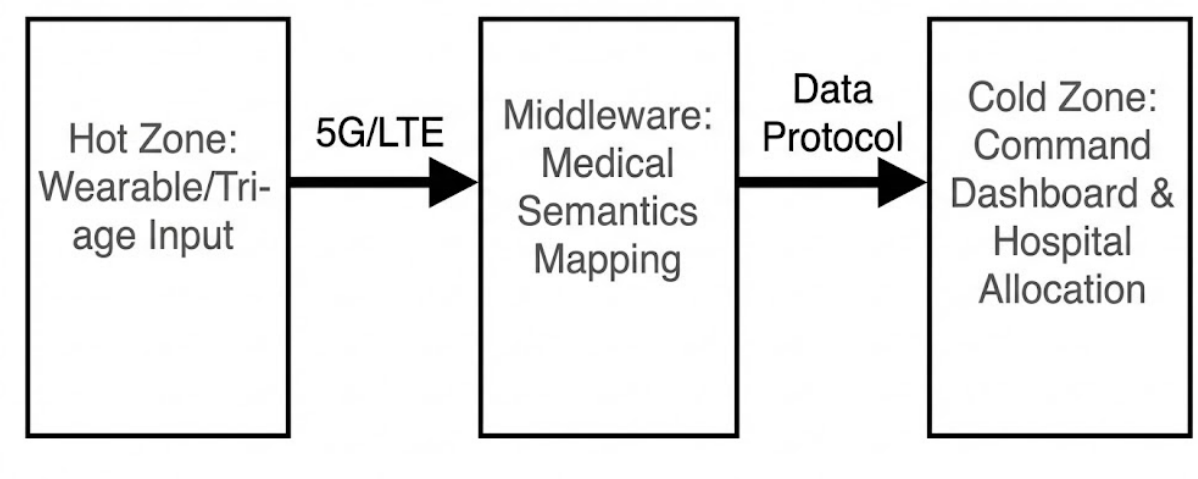

Figure 1. Medical Data Flow from Hot Zone (Field Triage) to Cold Zone (Transport/Hospital Allocation) via Semantics Mapping Layer

Practitioner Checklist

1. Confirm governance and approval gates.
2. Freeze shared vocabulary and triage terms.
3. Instrument key timestamps across the workflow.
4. Rehearse degraded-network conditions before pilot deployment.
5. Verify bilingual medical and operational terminology.

CONCLUSION

Planning a cross-border digital drill requires governance, semantic alignment, and technical architecture to be developed together. A simulation-first approach can expose handover and coordination failures before costly live deployment and generate reusable artefacts for multi-agency exercise design beyond the immediate CBRNe context.

REFERENCES

Kolb, D. A. (1984). *Experiential learning: Experience as the source of learning and development.* Prentice-Hall.

Wolbers, J., & Boersma, K. (2013). The common operational picture as collective sensemaking. *Journal of Contingencies and Crisis Management, 21*(4), 186-199. https://doi.org/10.1111/1468-5973.12027

Learning from a Planned Contingency Event: Using Translational Simulation for Organizational Learning in a Hospital Relocation

Une Elisabeth Støm er
Stavanger University Hospital
une.elisabeth.stomer@sus.no

Benedicte Skjold-Ødegaard
Stavanger University Hospital
benedicte.skjold-odegaard@sus.no

Riana Steen
University of South-Eastern Norway
riana.steen@usn.no

Jørgen Hustadnes Hagen
Stavanger University Hospital
jorgen.hustadnes.hagen@sus.no

Oda Cecilie Langfeldt-Omre
Stavanger University Hospital
oda.cecilie.langfeldt-omre@sus.no

Elisabeth Farbu
Stavanger University Hospital
elisabeth.farbu@sus.no

Geir Haakonsen
Stavanger University Hospital
geir.haakonsen@sus.no

ABSTRACT

This paper describes how a large hospital used system-focused simulation to prepare for transition into a new facility. Over a ten-week period, clinical units tested scenarios in their future work areas to explore workflows and identify hazards. The simulations generated 127 reports and revealed key practical issues, supporting early detection of risks and a safer activation of the new hospital.

KEYWORDS

Simulation, hospital transition, organisational readiness, latent safety threats, workflow testing

INTRODUCTION

Stavanger University Hospital is one of the largest hospitals in Norway with more than 9000 employees and a catchment area of approximately 390,000 inhabitants. In November 2025 the hospital relocated into a new hospital building. Maintaining emergency preparedness throughout the transition was essential, and the move was approached as a planned contingency event.

A training project was established to ensure patient safety, identify latent safety threats, and prepare staff for unfamiliar environments, workflows, and operational systems. Several training modalities were used, and simulation was identified as a useful tool to ensure preparedness during the planned contingency event.

THEORETICAL BACKGROUND

Simulation is defined as a technique that recreates real-world situations for practice, evaluation, and system understanding (Healthcare Simulation Dictionary, 2024). In this project, simulation was designed not as individual skills training, but as a system-level diagnostic tool to support organizational learning during transition. The approach draws on three theoretical perspectives. First, experiential learning theory (Kolb, 2014) conceptualizes learning as a cycle where experience is transformed through reflection and experimentation. Scenarios provided structured experience, and debriefing supported reflection and adjustment. Second, team learning theory

emphasizes psychological safety, defined as a shared belief that the team is safe for interpersonal risk-taking (Edmondson, 1999), as a condition for identifying weaknesses and uncertainty. Third, organizational learning theory highlights how insights become institutionalized across levels (Crossan et al., 1999). Translational simulation operationalizes this by linking frontline observations to leadership follow-up and structural change.

METHODS

As part of the training project, translational simulation (Brazil et.al 2017, Nickson et.al. 2021) was employed, with an emphasis on system-level diagnosis and improvement rather than individual skills training. The method was selected due to its documented ability to reveal safety and performance issues, test planned infrastructure, and support organizational readiness. At the hospital, the simulation team adapted the Summarize, Anchor, Facilitate, Explore, Elicit (SAFEE) debriefing model (Coleman et al. 2017) to better align with local needs. The adapted model was named Summarize, Anchor, Facilitate, Explore and Report (SAFE(E)-R), reflecting the added focus on reporting findings to leadership and supporting the Organizational Development Unit in systematic follow-up and improvement efforts.

Over a 10-week period prior to the transition, all hospital units were allocated 2–6 days each in the unfinished building to run predefined scenarios in their designated clinical areas. The purpose was to explore new workflows, identify hazards, and test environmental and logistical arrangements before clinical operations commenced.

All simulationists/facilitators received targeted training to ensure consistent delivery of structured briefings and debriefings. Each scenario focused on identifying *"what is new"* and conducting a +/Δ (plus/delta) analysis. When latent safety threats or improvement opportunities were identified, the scenario was repeated incorporating proposed adjustments. After each simulation, facilitators submitted a short digital report to both the unit leadership and the organizational development department to enable rapid follow-up and system-level learning.

Digital reports from each run scenario constitute the data material in this study. All reported improvement areas were extracted as originally phrased by the units and then categorized into overarching themes based on semantic similarity. This entailed grouping together variant formulations referring to the same underlying issue. Only improvement needs were included in the thematic count. Positive observations and solution suggestions were excluded from the thematic frequency analysis but retained separately for organizational follow-up.

RESULTS

A total of 3,082 healthcare professionals from 18 departments participated in the simulation activities over the 10-week period. The translational simulations generated a substantial body of system-focused information that resulted in 127 reports submitted to leaders and organizational development team.

The six most frequently reported improvement areas (with number of occurrences) were:

Nr.	Improvement area	Results
1.	Wayfinding and Signage (153 occurrences)	The need for clearer or more consistent signage emerged as the most dominant theme. Staff frequently reported difficulties navigating between rings, corridors, clusters, and floors, distinguishing bed elevators from personnel elevators, and locating correct routes across interconnected buildings. These issues represent critical barriers to efficient workflow, patient movement, and emergency response in a new facility.
2.	Equipment, Medical Technical Equipment (MTE) Access Points, Niches, and Outlets (66 occurrences)	Units noted inconsistencies or uncertainties around the placement, accessibility, and configuration of equipment and utilities. This included recessed niches, supply closets, wall outlets, and device docking areas. Such issues risk workflow slowdowns or safety hazards if not corrected prior to activation.
3.	Door and Elevator Functionality (55 occurrences)	Multiple units reported problems with automatic door timing, elevator response times, and door–bed alignment. These concerns directly impact patient transport, emergency logistics, and staff efficiency.

4.	Alarm Systems and Communication Infrastructure (55 occurrences)	Several scenario phases uncovered issues with alarm routing, calling systems, notification clarity, and the integration of communication technology with actual workflow. Robust alarm and communication systems are vital for safe operation, making these findings particularly important.
5.	Workflow, Roles, and Reporting (42 occurrences)	Challenges were identified in how roles, responsibilities, and workflow steps aligned within the new environment. Simulations revealed points of friction during handovers, interdisciplinary coordination, and role clarity.
6.	Transport and Patient Flow (33 occurrences)	Participants identified logistical bottlenecks in patient movement, supply transport, and coordination between units. These are especially important in a large new facility where distances, routes, and interdependencies may differ significantly from the previous hospital.

INTERPRETATION OF FINDINGS AND CONCLUSION

The high number of participants made this the largest system-focused simulation effort conducted at the hospital. The 487 proposed solutions indicate high staff engagement and support the value of simulation as a participatory design method, enabling frontline employees to directly shape the operationalization of the new hospital.

The system-focused data demonstrate that translational simulation functioned as a powerful organizational diagnostic tool. The identification of 263 improvement areas—many of them highly practical, infrastructural, or logistical—shows that the simulations enabled early detection of latent safety threats and operational inefficiencies that could have compromised safety and workflow at the time of go-live.

These findings show that the majority of issues identified were *environmental, infrastructural, or workflow-based*, rather than clinical in nature. This aligns with the purpose of translational simulation as a method for testing new environments, workflows, and organizational interfaces. The dominance of environmental and workflow themes reinforces the conclusion that large-scale hospital transitions cannot be safely managed through documentation and training alone. Instead, embodied, scenario-based testing in the unfinished environment provides a uniquely effective method for surfacing system vulnerabilities and testing operational readiness.

REFERENCES

Brazil, V. (2017). Translational simulation: not ‘where?’but ‘why?’A functional view of in situ simulation. *Advances in Simulation*, *2*(1), 20.

Colman, N., Dalpiaz, A., Walter, S., Chambers, M. S., & Hebbar, K. B. (2020). SAFEE: a debriefing tool to identify latent conditions in simulation-based hospital design testing. *Advances in Simulation*, *5*(1), 14.

Crossan, M. M., Lane, H. W., & White, R. E. (1999). An organizational learning framework: From intuition to institution. Academy of management review, 24(3), 522-537.

Edmondson, A. (1999). Psychological safety and learning behavior in work teams. Administrative science quarterly, 44(2), 350-383.

Kolb, D. A. (2014). Experiential learning: Experience as the source of learning and development. FT press.

Lioce, L., Lopreiato, J., Downing, D., Chang, T. P., Robertson, J. M., Anderson, M., ... & Terminology and Concepts Working Group. (2020). Healthcare simulation dictionary. *Rockville, MD: Agency for Healthcare Research and Quality*, *2020*, 20-0019.

Nickson, C. P., Petrosoniak, A., Barwick, S., & Brazil, V. (2021). Translational simulation: from description to action. *Advances in Simulation*, *6*(1), 6.

Speedrunning a Crisis: Building a Robust Cyber Crisis Response Capability

Renzo Stoppelenburg
Ministry of Infrastructure and Water Management
Renzo.stoppelenburg@minienw.nl

Jeroen Gaiser
Ministry of Infrastructure and Water Management
Jeroen.gaiser@minienw.nl

ABSTRACT

The ministry of Infrastructure and Water Management has a very robust and proven crisis management capability, but it was built for the physical domain. In preparation for the 2025 NATO summit this capability needed to be extended to the digital domain. This paper shares the main differences like the high volatility of evolving events and need for split second decision-making in an environment with a high level of uncertainty. We present our lessons learned in creating clear governance, team composition and facilitating decision-making by high-level management on an unfamiliar topic like cyber.

Keywords

Cybersecurity, Cyber Crisis, Capability building

INTRODUCTION

A safe and secure society rests on a diverse number of critical sectors; from manufacturing, energy to transport and water management. The Ministry of Infrastructure and Water Management is responsible for a great number of critical sectors. Responsibilities are both externally focused on the societal functions of these sectors as internally focused on the business operations of the ministry itself. These two are intertwined, especially in the digital domain.

The cyber domain, including Operational Technology (Chitadze 2018), is firmly established as target for exercising geopolitical power, criminal activities and societal influence campaigns. Therefore, as host nation of the 2025 NATO summit, the ministry needed to be ready for a digital crisis.

BUILDING THE CYBER CAPABILITY

The starting point was to see how the existing crisis management process handled under real world incident conditions. This was done in both one-on-one discussions and tabletop exercises. These showed that actors in 'traditional' crisis roles were overwhelmed by unknown technical aspects/jargon, speed of developments, role boundaries and lack of certainty. Additionally, previous work at Rijkswaterstaat on cyber crisis management gave us focus areas for improvements. These improvements were then tested in tabletop exercises and implemented as changes in our cyber crisis management manual. For example, experts were trained on explaining events in layman terms without jargon, reporting was supported by subject matter experts to increase quality and trust was built between decision makers and experts. By creating small targeted events, e.g. a session focused on the sensemaking phase, a rapid iterative process was possible. Each event resulted in an update of the main crisis management manual which was shared for review to all roles.

Key in this approach was selecting the appropriate composition of event participants. Aspects considered were

group size, diversity (both in expertise and seniority), knowledge level and organizational role. The crisis management approach was also tested as part of larger exercises like the NATO CMX25 and by using past cyber crises as testcases. This approach addressed the pitfall of creating an event-specific capability.

Two main differences between regular crises and cyber crises emerged:

1. The speed of developments and informational dynamics of the crisis are significantly higher than a regular crisis (e.g. impact is known at a physical location like a bridge). This had profound impact on how/when to organize the crisis team meetings and how to handle receiving new relevant information while decision makers are in closed meetings.
2. Mandate for taking action is difficult in a digital crisis due to digital systems crossing boundaries between teams, departments or even organizations. Impact assessment is diffuse (e.g. cascade effects vs root-cause) and impact containment to a physical location or process is often impossible. This leads to the need for rapid escalation to top-level of management not supported by traditional crisis management decision making.

The result was a thoroughly tested process codified in a central crisis management manual in which all roles involved have a clear perspective on action which was well tested in realistic exercises.

LESSONS LEARNED

The iterative approach of improving the capability was essential in creating both quick progress and stakeholder buy-in. Small changes were more readily accepted than combining them into a larger change. Small iterations gave a manageable focus for participants with recognizable dilemmas. The many interactions during table tops, especially with higher management, created confidence in the crisis roles in general in both the process as expertise involved. This confidence in the advice given enabled timely decision making by mandated upper management, directly addressing the highly volatile decision-making environment of a cybercrisis.

Due to the complex system of the supply chain and involved partners, we included a diverse mix of personnel and organizations in creating the capability. The resulting intensive and broad interaction slowed the process somewhat, but created a more robust approach. At the beginning of the exercises, it was emphasized as a learning experience with no wrong or right answers, which helped create an open and honest discussion.

Including decisionmakers from upper management resulted in a clearer sense of urgency at that level and a trust in the crisis management process to support their responsibility. Through this approach, we created an agile core cyber crisis team for quick triage (director level chairperson with 3 experts) and assessment with a larger flexible ‘shell’ that is scaled up based on the type of crisis and area of impact.

Finally, we realized that ‘cyber’ is a very abstract field for most. This created a challenge of finding a balance in what knowledge level is required for each role to be effective. Exercises not only helped to educate on digital risk, but also forced experts to develop the skills to communicate complex digital concepts to lay(wo)men. Enabling an atmosphere where people feel safe to ask clarifying questions and challenge each other on clarity was an unexpected bonus we did not see as relevant beforehand.

TAKEAWAY

You never know if you’re ready for a cyber crisis until it’s done. The next best thing is to exercise and communicate, both during creation of a capability and in maintenance of it. Have a plan, test, improve, repeat.

REFERENCES

Chitadze, N. (2022). Cyber warfare – New threat for national and international security and transformation of the conflicts under the conditions of the new geopolitical order. *Journal of Social Sciences*, *7*(2), 70–76. https://doi.org/10.31578/jss.v7i2.120

Demonstrating Value of Disaster Management Programs

Magda Sulzycki
Principal Consultant
Business Continuity Management Canada Inc.
magda@resiliency.help

ABSTRACT

As disruptive events become more frequent and complex, disaster management (DM) costs are rising, drawing more attention to their funding. Drawing on practitioner experience from the Canadian electricity sector, this paper examines how DM investments are scrutinized by regulators, specifically the Ontario Energy Board's (OEB) rate filing process. It suggests that DM programs can be vulnerable if their value is poorly evidenced. The paper proposes a performance management approach that uses structured indicators and methods to translate risk and trends into program-supporting evidence.

KEYWORDS

Program management, program financing, data management

INTRODUCTION

DM programs are expected to deliver continued mitigation and response readiness over long periods, often in the absence of major events, while operating under increasing financial and organizational pressure. In regulated sectors, this challenge is amplified by the need to regularly justify operating costs through formal review processes.

In Ontario, Canada's energy sector, utilities must demonstrate that their operating expenditures are necessary and reasonable; DM activities are part of these expenditures and are therefore assessed alongside all operational priorities. This creates a practical management challenge: while preparedness requires ongoing investment, its benefits may only become visible during infrequent but high-impact events, making it more vulnerable to funding clawbacks.

This case provides a useful lens for examining how clearer performance reporting and program management discipline can help decision-makers better understand the value of sustained disaster management investment.

CONTEXT & BACKGROUND

Energy utilities in Ontario are required to submit applications to the OEB when seeking approval for changes to customer rates, which ultimately fund in-house DM programs. By mandate, the OEB must set rates that are just and reasonable, and utilities bear the burden of demonstrating that the costs they seek to recover meet this standard (Ontario Energy Board, 2016, 2025). This requires utilities to clearly explain what activities, in this case DM programs, are being funded, why they are required, and how investments contribute to improved services and risk management.

DM presents a particular challenge within this model, as many of its benefits are realized unevenly over time, often only following infrequent but high-impact events. While planning, training, system maintenance, and coordination require continuous investment, disruptive events such as extreme weather or large-scale cyber incidents do not occur on predictable schedules. This makes sustained DM difficult to justify using traditional, event-based measures alone.

The challenge is heightened when DM programs are framed using broad or abstract indicators, without clearly linking risk trends to operational workload, resource demands, or performance outcomes; this weakens the ability to assess whether costs are reasonable or proportionate. When the connection between investment and observable outcomes is unclear, DM programs are more likely to face funding constraints during rate review cycles.

PRACTICAL INSIGHTS

The approach described here is a response to recurring challenges in resourcing and sustaining DM programs in the Canadian disaster management industry. In the Ontario example, experience across multiple rate review cycles suggests that these programs are not vulnerable because they do not bring value, but rather that this value is poorly articulated, as performance metrics fragmented or weakly connected to operational realities.

To address this, a more deliberate performance management approach is proposed, one that treats DM as a coherent and measurable program. Central to this approach is a structured performance framework that translates risk trends into program objectives and performance indicators that are meaningful to decision-makers. The goal is to support a defensible narrative linking risk, workload, capability development, and outcomes.

A key element of this approach is the distinction between leading and lagging indicators. Leading indicators address pressures before major incidents occur, while lagging indicators capture performance during and after events. Together, these measures are intended to support focused discussions with decision-makers about where disaster management programs deliver value (see Table 1).

LONGITUDINAL PERFORMANCE MANAGEMENT DATA

One of the most underutilized assets a DM program can build is a structured, maintained database of its own performance over time. When program funding must be justified over multi-year cycles, directional trends are considerably more persuasive than point-in-time figures presented without context, and they allow programs to demonstrate relevance: that gaps identified in one period were addressed in the next, and that investment produced measurable change.

A well-designed performance database does not need to be complex to be effective. It requires consistent indicator definitions that do not change between cycles, a defined collection cadence, clear data ownership, and version control so that methodology changes are documented rather than quietly absorbed. Structurally, options range from purpose-built solutions designed around program-specific requirements, to configured instances of enterprise risk management platforms that may already exist within the organization's technology environment, to well-governed spreadsheet or database environments that can support rigorous longitudinal reporting without significant technology investment.

The gap most programs face is not the absence of data, but the absence of a deliberate structure for aggregating and retaining it across time. Treating the performance database as a living program asset rather than something assembled in the months before program budget justifications begin is what separates programs that can speak credibly to their own track record from those that cannot.

TABLE 1 – SAMPLE DISASTER MANAGEMENT PROGRAM PERFORMANCE INDICATORS

Impact Domain	*Leading Indicators*	*Lagging Indicators*
Prevention & Mitigation	• Percentage of high-risk assets or systems with completed vulnerability assessments • Proportion of identified mitigation actions funded and implemented within planned timelines • Rate of infrastructure hardening or risk-reduction investments relative to identified hazard exposure	• Reduction in frequency or severity of damage to critical assets over successive events • Cost avoidance achieved through mitigation investments compared to modelled scenarios • Decrease in service interruptions attributable to known hazards
Preparedness	• Percentage of response plans reviewed and updated within defined cycles • Training coverage rate for staff in critical roles • Exercise participation rate across internal teams and external partners	• Availability of required response resources and stockpiles • Readiness gaps identified during exercises or audits • Degree to which preparedness objectives are met during real events

	• Percentage of preparedness deficiencies resolved within target timeframes	
Response & Recovery	• Average time to activate emergency response structures during simulations/real events • Availability and reliability of response systems during peak demand periods • Proportion of updated, pre-established, and documented recovery priorities, strategies, and decision criteria	• Duration and scale of customer or service disruption • Time to restore critical services relative to event severity • Recovery costs and timelines compared to prior events and forecasts • Effectiveness of coordination during real-time response, as reported by Incident Management Teams, stakeholders, and/or communities
Program Management	• Percentage of program initiatives/projects with defined objectives, success criteria, and owners • Stability of program staffing and leadership roles over time • Regularity of program-level performance reviews and updates	• Delivery of program objectives within approved scope, schedule, and budget • Incidence of scope creep or unfunded mandates over time • Funding stability or growth across review cycles • Reduction in repeat findings from audits or reviews

IMPLICATIONS

Disruptive events are becoming more frequent, complex, and attention-drawing, and funding for DM programs is under increasing scrutiny. In communities and industries where resources are tight and non-essential programs are vulnerable, DM program managers will need to clearly show the value of their work with strong, credible evidence. Clear and well-chosen performance indicators complemented by well structured, longitudinal DM program management data will be key to doing this effectively.

REFERENCES

1. Ontario Energy Board. (2025, December 16). *Filing Requirements For Electricity Distribution Rate Applications - 2026 Edition for 2027 Rate Applications*. Ontario Energy Board. https://www.oeb.ca/sites/default/files/OEB%20Filing%20Req_ED%20Rate%20Applications_2027_Chapter%201_2027_20251216.pdf
2. Ontario Energy Board. (2016). *Handbook for Utility Rate Applications*. Ontario Energy Board. https://www.oeb.ca/sites/default/files/uploads/documents/regulatorycodes/2019-01/Handbook-Utility-Rate-Applications-20161013.pdf

Towards a National Guideline on Recovery: A Whole-of-Society Approach to Strengthen Resilience in The Netherlands

Sam ter Horst
Netherlands Institute for Public Safety
Sam.terhorst@nipv.nl

Michel Dückers
Netherlands Institute for Public Safety
Netherlands Institute for Health Services
ARQ National Psychotrauma Centre
University of Groningen
m.duckers@nivel.nl

Marije Bakker
Netherlands Institute for Public Safety
Marije.Bakker@nipv.nl

Imco Janssen
Netherlands Institute for Public Safety
Imco.Janssen@nipv.nl

Paul Gelton
Netherlands Institute for Public Safety
Paul.Gelton@nipv.nl

Amy Matser
Netherlands Institute for Public Safety
Amy.Matser@nipv.nl

ABSTRACT

In an era of escalating geopolitical tensions and increasingly frequent large-scale crises, strengthening societal resilience has become essential. In the Netherlands, the recovery phase remains underdeveloped, with limited practical implementability of existing guidelines and insufficient integration of societal capacities. This project addresses these gaps by co-creating a national framework for disaster and crisis recovery using a data-driven, whole-of-society approach. Through literature review, case analysis, scenario development, and stakeholder co-creation, the project identifies key recovery factors and develops tools to assess needs, mobilize capacities, and coordinate support. The resulting guideline aims to enhance effective, equitable, and future-proof crisis recovery nationwide.

Keywords

Crisis recovery; Societal resilience; Whole-of-society approach; Guideline development; Data-driven framework

BACKGROUND

In today's context of rising geopolitical tensions, armed conflict, and increasingly frequent large-scale crises, building a resilient society is more urgent than ever. Governments cannot achieve resilience alone; it requires coordinated action from public authorities, private partners, civil society organizations, and citizens. Mobilizing society's full capacity strengthens prevention, response, and recovery efforts. A holistic and inclusive Whole-of-Society approach is essential to address today's challenges and ensure long-term societal resilience.

EXPERIENCE AND INSIGHT

Despite increasing attention to preparedness and response, the recovery phase after a crisis remains the least developed component of crisis management in the Netherlands (Bas et al., 2017). An example of this is the handling of earthquake damage in Groningen. Due to bureaucracy and cumbersome procedures, the repair of homes is progressing slowly, and citizens' distrust and stress are increasing. And although acute assistance got underway relatively smoothly after the flooding disaster in Limburg, we also see here that longer-term support is fragmented, surrounded by bureaucracy, and that policy and practice do not seem to align well. Although recovery continues long after an acute crisis, public and institutional focus often declines quickly. Furthermore, existing recovery guidelines insufficiently reflect today's complex challenges, including risks to critical infrastructure and scenarios of armed conflict that may strain national capacities.

Even though substantial knowledge exists concerning the expectations of affected populations and the challenges they face during the recovery process, much of this knowledge has been embedded in protocols and operational guidelines, and tasks and responsibilities are clearly assigned to national (e.g. National Institute for Public Health and the Environment) and sub-national civil protection authorities (i.e. safety regions and public health services), as well as to other public and private parties (e.g. insurance companies), it has been demonstrated that the practical implementability of many of these guidelines remains a weak and insufficiently developed component (Berger et al., 2019). Insight into the capacities available within society is also limited, leading to underuse of societal resources and incomplete integration of non-governmental and community actors.

REFLECTION AND LESSONS LEARNED

The project aims to strengthen resilience in the Netherlands by co-creating and implementing a national framework for disaster and crisis recovery, using a data-driven and whole-of-society approach. We do this as follows:

1) We identify key factors (e.g. crisis characteristics, demographics, health-related factors, and financial/economic factors) that shape disaster and crisis recovery. Using these insights and the needs of end-users, we develop structured scenarios that capture uncertainties, cascading effects, and societal vulnerabilities.
2) We develop a data-driven framework to assess the type, scale, and duration of support that will be needed, as well as to identify which groups within the affected population are most likely to require support. This model will inform more effective, equitable, and evidence-based recovery interventions. Data sources used for this might include, e.g. Statistics Netherlands microdata, general practitioner records, and data from insurance companies. A proof-of-concept will be developed that leverages data-driven methods to facilitate the timely and accurate building of networks, matching needs and capabilities, thereby enhancing operational effectiveness during crisis recovery
3) Results will be consolidated and shared with stakeholders. Through co-creation sessions, these stakeholders, the end-users from diverse societal backgrounds, will collaboratively contribute to the design of the guideline.

During the presentation, we will discuss the (preliminary) results of objectives 1 and 2, and outline the approach for objective 3.

IMPLICATIONS

Societal resilience can be strengthened through a whole-of-society approach that incorporates data-driven strategies, as this enables more accurate identification of needs, faster mobilisation of capacities and more efficient coordination of support. An integrated and evidence-based collaboration is therefore a key enabler for becoming more efficient, effective and future-proof in managing the recovery phase of crises. However, the successful implementation of such a framework may be constrained by factors such as data availability and quality, interoperability, data-sharing barriers and institutional fragmentation. Addressing these constraints through clear governance arrangements and shared standards is essential for the framework to deliver its intended impact.

REFERENCES

Bas, M. de, Helsloot, I., & Dückers, M. (2017). De preparatie op de nafase binnen veiligheidsregio's: Een verkennend onderzoek. *Tijdschrift voor Veiligheid, 16*(1), 3–16. https://doi.org/10.5553/TvV/187279482017016001001

Berger, E., Domrose, J., & Van der Varst, L. (2019). *Maatschappelijk herstel na grootschalige overstromingen.* Instituut Fysieke Veiligheid, Lectoraat Crisisbeheersing. https://nipv.nl/wp-content/uploads/2022/02/20191017-IFV-Wave2020-Maatschappelijk-herstel-na-grootschalige-overstromingen.pdf

Interpreted information vs. Raw Data: How the Netherlands Approaches Crisis Information Sharing and the Dilemmas We Face

Jochem van Heek
Information Architect, Netherlands Institute for Public Safety (NIPV)
jochem.vanheek@nipv.nl

ABSTRACT

Crisis management depends on raw data and professional interpretation, which operate at different speeds and scales. In the Netherlands, domain specialists interpret data and share assessments through a shared crisis management system. This paper describes the Dutch approach, illustrated by innovations in drone integration, wildfire prediction, and multi-agency coordination during a major public event. The method proved its value but raises dilemmas about the pace of human interpretation in an era of real-time data, and the boundary between professional judgment and automated business rules. I argue that rather than a trade-off, these can be designed to reinforce each other.

Keywords

crisis information sharing, net-centric crisis management, interpreted information, data driven insights

INTRODUCTION

Crisis professionals have never had more data at their fingertips. Drones deliver live aerial footage, sensors monitor water levels around the clock, and AI-generated analyses arrive faster than any human could. Yet more data does not automatically lead to better decisions. In the Netherlands, we have made a deliberate choice in how we share information during crises: we exchange interpreted information rather than raw data. It is a method that works — but comes with dilemmas.

THE DUTCH APPROACH: NET-CENTRIC CRISIS MANAGEMENT

In the Netherlands, crisis response organisations follow a shared doctrine called Net-Centric Crisis Management (Treurniet, 2022). The idea is straightforward: every partner in the crisis network contributes its piece of the puzzle. A water authority interprets hydrological data. A fire department assesses the risk of hazardous material exposure. A public health agency evaluates the impact on vulnerable populations. Each of these partners shares its professional interpretation through the nation-wide crisis management system (LCMS), building a common operational picture that all parties can act upon.

During large-scale flooding, a military liaison or healthcare coordinator does not receive raw river water level readings. Instead, they receive the water authority's assessment of what those readings mean — where levees are at risk, which areas may need to be evacuated, and on what timeline. The specialist translates data into meaning. Others build on that meaning to make their own decisions.

CONNECTING NEW DATA SOURCES

We have expanded this method by integrating new data sources into our nation-wide crisis management platform (LVCb). For example, we connected a national drone operations platform to our data environment. Drone imagery is now accessible directly on the shared operational map, allowing crisis professionals to view live aerial footage alongside other available information.

We are now taking this a step further by connecting drone operations to a wildfire spread prediction model.

Traditionally, an incident commander would send out teams to physically walk or drive around the fire perimeter to identify the head, flanks, and tail of the fire. Today, teams from our Digital Reconnaissance Unit are dispatched to fly drones to map that information. They mark key points and lines directly on the drone controller, and through an API connection, this data feeds straight into the wildfire spread prediction model — turning a time-consuming and risky field reconnaissance into a near real-time digital process. Automation and human interpretation work together: technology accelerates what was once a slow manual process, but the judgment of what to mark — where the fire is heading, which flanks are most critical — remains a professional call.

During large-scale events, this integrated approach is put to the test. At SAIL Amsterdam 2025 — Europe's largest public event, with over 2.5 million visitors and 10,000 ships — around 20 partners worked together under the coordination of the Safety Region Amsterdam-Amstelland. Data from 180 sources was exchanged and combined through a data platform: from live ship locations and congestion measurements to drone detection and public atmosphere. To make this volume of data manageable, the safety region and its partners developed an open-source Digital Twin that visualises data through 3D simulations and provides tailored insights per user role. In a dedicated 'boiler room', analysts conducted real-time research during the event, interpreting incoming information and refining data sources on the fly. The interpretations and consequences of these analyses were shared through the nation-wide crisis management system (LCMS). A key takeaway: technology only truly works when there is collaboration and trust. This was possible through the willingness of 20 partners to share their information openly and act on each other's interpretations. However, this volume of data demanded careful design: user profiles provided tailored information per role to prevent data overload, and automated thresholds filtered what warranted attention. But thresholds only work when partners agree in advance on what counts as 'too busy' — a judgment that differs per context and role.

THE DILEMMAS WE FACE

These examples illustrate both the promise and the tensions of our approach. We continue to wrestle with fundamental questions.

How do we keep up with the speed of new information sources? Drones, AI-generated analyses, real-time sensor networks — the volume and velocity of data continue to grow. Our method depends on human professionals interpreting and contextualising information before sharing it. But when drone footage arrives in real time and predictive models update every few minutes, the question becomes: can human interpretation keep pace? And if it cannot, what do we lose by slowing things down?

Where is the boundary between human interpretation and automated business rules? We have started implementing automated business rules that can flag certain conditions or trigger alerts without human intervention. When sensor data crosses a threshold, the system generates a warning automatically. This introduces tension: automated rules are consistent and fast, yet they lack the contextual judgment that human experts bring. How far should we push automation before we lose the professional nuance that makes our method valuable?

RECONCILING THE DILEMMA

These two questions are variations of the same tension: speed and scale on one side, human judgment and context on the other. Hampden-Turner and Trompenaars' (2000) dilemma theory offers a useful lens here. Rather than treating opposing values as a trade-off where one must come at the expense of the other, they argue that the real challenge and opportunity lies in reconciling them so that both sides are strengthened.

Applied to our practice, the question is not whether crisis information sharing should be driven by automation or by human judgment. It is how we design systems where both reinforce each other: where automation handles speed and volume, freeing up experts to provide context, meaning, and nuanced interpretation.

Our examples show that this integration is already taking shape in practice. There is still much to explore in how we scale and refine it. But I believe this is where the conversation between practitioners and researchers becomes essential. Not to choose between the two ends of the spectrum, but to investigate under what conditions automated and human-interpreted information reinforce each other. Let's have that conversation.

REFERENCES

Hampden-Turner, C., & Trompenaars, F. (2000). *Building cross-cultural competence: How to create wealth from conflicting values*. Yale University Press.

Treurniet, W. (2022). *Between chaos and continuity: A common operational picture in support of emergency response networks*. [PhD-Thesis - Research and graduation internal, Vrije Universiteit Amsterdam]. s.n.