



How advanced information technologies help and hurt adaptation in crisis-response supply chains[☆]

Yvonne Lont^{a,*,}, Patrick Steinmann^a, Jan Kwakkel^a, Tina Comes^{a,b}

^a Delft University of Technology, Jaffalaan 5, Delft 2628 BX, The Netherlands

^b DLR Institute for the Protection of Terrestrial Infrastructures, Bonn, 53227, Germany

ARTICLE INFO

Dataset link: <https://doi.org/10.4121/5676067d-e852-4bf8-a346-0dac8379a9bd>

Keywords:

Information sharing
Supply chain
Exploratory modeling
Crisis response
Adaptation process
Supply chain resilience
Advanced information technologies
Maladaptation

ABSTRACT

Climate change and geopolitical tensions demand increased adaptability from crisis-response supply chains. Advanced information technologies, such as Artificial Intelligence and Blockchain, have been proposed as tools for increased adaptability. However, recent evidence shows that such technologies can also lead to new vulnerabilities and risks, a phenomenon we refer to as *technology-induced maladaptation*. This paper analyzes the effects of information technologies on resource allocation in crisis-response supply chains and identifies the conditions under which technology-induced maladaptation emerges. We develop an agent-based discrete-event simulation model in which managers adapt their resource allocations and coordination structures in response to climate shocks and geopolitical emergencies, using different information technologies. Using exploratory modeling and rule induction, we examine a sequential and a convergent supply chain configuration. Both configurations use different information technologies and are exposed to disruption patterns representing climate shocks and geopolitical emergencies. Rule induction reveals technology-disruption combinations under which technology-enabled efforts to reduce information delays and accelerate recovery may inadvertently decrease performance. The findings reveal two technology-induced maladaptation profiles: conditional and broad maladaptation. Conditional maladaptation refers to underperformance restricted to specific disruption duration windows, whereas broad maladaptation is distributed across the full range of disruption durations. The disruption pattern and supply chain configuration jointly moderate which profile a technology exhibits. Identifying these profiles advances understanding of maladaptation in crisis-response supply chains as a condition-specific phenomenon.

1. Introduction

Advanced information technologies are being rapidly deployed in crisis-response supply chains [1–3]. Artificial Intelligence tools are proposed as means to accelerate situational awareness, anticipate demand, and support allocation decisions across heterogeneous, degraded information environments [3,4]. Blockchain-based tools are presented as solutions to the trust and traceability problems in multi-agency response [5]. Real-time common operational pictures and remote sensing are argued to reduce the information delays and gaps that slow response [6]. Taken together, these information technologies are framed as enablers of adaptation in the face of intensifying climate shocks and geopolitical emergencies.

[☆] This article is part of a Special issue entitled: 'IS for Emergency Response' published in International Journal of Disaster Risk Reduction.

* Corresponding author.

E-mail address: y.l.lont@tudelft.nl (Y. Lont).

<https://doi.org/10.1016/j.ijdr.2026.106342>

Received 31 March 2026; Received in revised form 17 June 2026; Accepted 25 July 2026

Available online 12 September 2026

2212-4209/© 2026 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

Information technologies do not merely speed up existing supply chain processes, they also shift how organizations perceive and act on crisis situations [7]. In crisis response, this reshaping role acts on two levels simultaneously: information technologies alter the volume and speed of information available to decision-makers, and they change the coordination structures through which organizations share and act on information [8,9]. Yet this role is not neutral, and its effects are not guaranteed to improve performance. For example, research on the productivity paradox of Artificial Intelligence establishes that information technology implementations do not automatically translate into performance gains; their effects depend on complementary organizational conditions that are slow to develop and difficult to sustain [10]. In crisis-response supply chains, where organizational and coordination structures are temporary and established ad-hoc, these complementary conditions are particularly hard to implement. Beyond implementation, information technologies act as lenses that shape which aspects of an evolving crisis become visible and actionable to decision-makers [11,12]. By filtering and prioritizing certain information over others, information technologies determine what the lens renders visible and what it leaves out. When the resulting picture is misaligned with the actual situation, adaptive actions can systematically lead to outcomes worse than those achieved without the technology, a phenomenon we refer to as *maladaptation* [13,14]. Such maladaptation can take different forms, for example, automation and decision-support tools can introduce automation biases, that is, where decision makers overrely on algorithmic recommendations [15,16]. Furthermore, shared platforms may create new bottlenecks when multiple organizations converge on the same information channel [17], and accelerated information flows can propagate local distortions across echelons before decision-makers can verify them [18].

The crisis-response supply chain literature has not systematically investigated the conditions under which technology-enabled, well-intended adaptive actions reduce rather than enhance supply chain performance. Empirical studies document cases where well-intended adaptive actions led to unintended performance degradation. For instance, material convergence overwhelming logistics capacity [19], information complexity weakening the positive effects of agility and resilience on humanitarian supply chain performance [3], or that well-intended coordination adjustments can lead to unintended performance degradation (e.g., [20]). These cases of unintended performance degradation are often described as operational failures rather than theorized as structurally emerging maladaptation, leaving the conditions that trigger them unexamined.

The aim of this paper is to determine the conditions and information technologies under which maladaptation in crisis-response supply chains may emerge. Our central research question is: *For which combinations of information technologies and disruption patterns do adaptive actions in crisis-response supply chains lead to maladaptive outcomes?*

To address this question, we build on a previous simulation model of information sharing in crisis response [21]. The model focuses on information-driven adaptation in crisis-response supply chains: how supply chain actors perceive evolving crisis situations and adapt their actions accordingly. We conceptualize maladaptation as a pattern of individual adaptive actions and decisions aimed at enhancing performance, but with an adverse effect. To examine maladaptation, we apply exploratory modeling to systematically vary information technology parameters and disruption patterns across many plausible scenarios. From these scenarios, we identify the conditions under which maladaptive outcomes emerge.

This study is situated at the intersection of information technologies and crisis-response supply chain management, where supply chains act and adapt to crises. The study contributes to this intersection by examining how technology-enabled supply chain coordination shapes maladaptation in crisis response. First, we advance understanding of crisis-response maladaptation by explaining under what conditions information technologies can turn out maladaptive. Second, we demonstrate the use of exploratory modeling to uncover such maladaptive dynamics over time.

The remainder of this paper is structured as follows. Section 2 introduces maladaptation as the central concept and reviews the role of information technologies in crisis-response supply chains. Section 3 introduces the research approach. Section 4 describes the model development and the agent-based simulation model. Section 5 details the experimental design. Section 6 presents the approach used to analyze the results. Section 7 reports the findings, highlighting conditions under which maladaptive outcomes emerge. Section 8 positions the findings against the literature and reflects on methodological contributions and limitations. Section 9 concludes the paper with implications for research and practice.

2. Background

2.1. Adaptation in crisis-response supply chains driven by information technologies

Adaptation in crisis-response supply chains is an information- and decision-driven process. In these supply chains, multiple organizations are linked through flows of supply needs and resources. Adaptation can be understood as the adjustment of an existing supply chain in response to actual or expected disruptions [22]. For crisis-response organizations, this adaptation aims to preserve the ability to deliver critical supplies where and when they are needed [23,24]. Adaptive actions can be performed at multiple, interacting levels: At the operational level, thus internally, actors reallocate resources in response to evolving needs [23]. At the structural level, organizations adapt their coordination structures in response to sustained overload [8]. In addition, adapting by implementing new policies like information technologies, adapts the information-processing environment within which these endogenous adaptations unfold. Together, the levels and technologies shape how adaptation dynamics evolve over time and ultimately determine system performance. Recent studies view adaptation in crisis-response contexts as an ongoing process [9,25]. This process, which unfolds in response to evolving disruptions, can be understood as an information–decision–action loop [9]. In this loop, actors collect, process, analyze, and share information. Information activities shape what decision makers can perceive and interpret. Decisions then trigger operational and coordination actions that adapt the operational situation and the subsequent information environment. Hence, information and coordination co-evolve during crises.

Information technologies can shift the dimensions of the information-sharing and decision-making loop through which coordination takes place [9]. Across crisis-response settings, technologies can be understood as shifting five recurring coordination-relevant dimensions: (i) *delays* in peer coordination (after how much time cross-manager reallocations can be executed), (ii) *information staleness* across hierarchical levels (how current decision makers' situational views are), (iii) *sharing frictions* (how likely actors are to post and accept information across organizational boundaries) [26], (iv) *decision-right allocation* [27] and (v) *observational coverage* — the fraction of the operational situation directly visible to decision makers [28,29]. These dimensions matter because crises compress decision time, while information is highly uncertain and information is volatile [30]. The dimensions govern how quickly and accurately organizations reallocate resources to where supply needs arise; coordination failures therefore translate directly into delayed or unmet supply deliveries. Information flows are a prerequisite for coordination and adaptation within and across organizations [26,31,32]. Both the quality and timeliness of information influence whether decisions translate into effective adaptive actions [30,33]. At the same time, decision-making in crises is constrained by cognitive biases that are typical under uncertainty and time pressure [30,34]. Other constraints that influence how and by whom information activities are performed include the bureaucratic, hierarchical structures that characterize many humanitarian and military organizations. These constraints can slow or channel adaptation in particular directions [9]. While information technologies have the potential to improve crisis-response supply chain performance, they can also have negative effects. For example, when many actors respond to the same indicators, overreaction or herding can occur, especially under noisy signals [35]. These effects occur across technologies. Therefore, the following paragraphs describe each technology and its expected effects on the coordination dimensions defined above.

Artificial intelligence. Artificial Intelligence comprises heterogeneous tools [4]. Each tool affects different information management activities. For example, Artificial Intelligence functions in crisis response are associated with faster collecting, sensing, processing, and analyzing of heterogeneous information flows [4,7,36,37].

Artificial intelligence-drone. In disaster logistics, drones (Artificial Intelligence-enabled flying sensors) primarily serve as mobile sensing platforms that expand the capacity for collecting crisis information. They are deployed to rapidly capture and transmit field observations on damage and evolving needs. This capture improves the coverage of the operational picture [28,38,39]. The distinctive information-management contribution of drones is therefore faster and broader information collection. In some deployments, drones collect information in areas that would otherwise remain unobserved or be observed only with substantial delay [28,40]. Drone literature also discusses surveillance ethical concerns, privacy concerns, and information overload from excessive unfiltered imagery [40,41].

Artificial intelligence-intake standardization. Artificial Intelligence-intake standardization automatically converts incoming supply and demand updates into a structured signal. Without such standardization, each state change requires a clarification loop. Crisis information research demonstrates the feasibility of extracting structured, actionable information from heterogeneous streams. By reducing semantic ambiguity and formatting heterogeneity, standardization lowers interpretation effort [42,43] and reduces errors and noise. Standardization, therefore, functions as a coordination mechanism [44].

Prediction-enhanced common operational picture. A Common Operational Picture (COP) is a shared representation of the operational situation for participating actors [6,45–47]. A COP can support collective sense-making and reduce misunderstanding and fragmentation, while still allowing interpretive differences to persist [45,46,48]. A COP is framed as mechanisms across hierarchical echelons and horizontal levels [6,47]. In a crisis-response logistics setting, the COP covers operational states of warehouse stock levels, queue backlogs at locations, transport capacity, and projected shortfalls. Prediction-enhanced decision support extends the COP with Artificial Intelligence-generated forecasts of those shortfalls, improving early risk detection in crisis management settings. However, this type of Artificial Intelligence can also lead to automation biases [15,16].

Blockchain-traceability and -compliance. Blockchain establishes a shared ledger of transaction events (e.g., dispatch, receipt, inventory update). In a crisis-response supply chain context, such a ledger records, for example, transfers between agencies or units and confirms delivery, increasing trust in the accuracy of recorded transactions [49]. Systematic reviews emphasize these potential benefits, transparency, traceability, and accountability, but also highlight adoption barriers and a lack of evidence in the field [5,49–52]. These barriers include engagement issues, a lack of technical skills and resources, privacy concerns, and governance challenges [49]. The governance and access-control requirements can increase organizational rigidity, slowing adaptation when rapid reconfiguration is required [5,49]. Importantly, blockchain strengthens validation and accountability rather than perceptual alignment: it does not alter how allocations are decided, but increases the verifiability of executed allocations [49]. By contrast, a Common Operational Picture constructs a shared representation of system state to support perceptual alignment. Empirical work reports that crisis-response blockchain solutions are often used indirectly via intermediaries. Furthermore, permissioned implementations can restrict visibility [49].

Satellite internet. Satellite internet provides resilient long-range connectivity [29]. In disaster response operations, satellite internet enables sustained cross-level reporting and coordination even when terrestrial communication infrastructure is damaged or congested [53,54].

In sum, technologies can both improve and degrade coordination and system performance. Evaluating whether a given adaptation improved or worsened system performance requires metrics and a method to investigate adaptation and maladaptation over time.

2.2. Maladaptation in crisis-response supply chains

Maladaptation was first described in ecology and climate change adaptation research [14,55,56]. In ecology and evolutionary biology, maladaptation arises when adaptive responses become misaligned with a changing environment, for example, because the environment shifted faster than the adaptation evolved, or because adaptive actions that were once appropriate are no longer suited to the actual situation [57]. In climate change research, the same logic extends to social-ecological systems: well-intended adaptive actions can inadvertently increase vulnerability, shift vulnerability, or lead to externalities [58]. In supply chains, maladaptation refers to purposeful adaptive actions aimed at improvement, yet lead to unintended adverse consequences [13]. In crisis-response supply chains, maladaptation is driven by time pressure to adapt to highly dynamic changing situations [13].

Information technologies can trigger maladaptation through several mechanisms. Increasingly, crises are not observed directly, but are mediated via technologies, ranging from satellite imagery to social media feeds [59]. As such, information technologies determine what aspects of an evolving crisis become visible and actionable [12]. When the resulting mental model is misaligned with the actual situation, adaptive actions, even if well-intended, can systematically lead to adverse outcomes. While human decisions in crises are subject to a range of biases [60], information technology introduces new biases, ranging from algorithmic or data bias [30] to automation bias, where decision makers over-rely on algorithmic recommendations [15].

In crisis-response supply chains, maladaptation can manifest by shifting vulnerabilities, costs, or delays over time or across organizations. Temporally, short-term recovery actions intended to fix immediate shortcomings may increase vulnerability to long-term [35] or subsequent disruptions. Across organizations, improvements in one organization can shift delays or costs onto partners [13]. Both manifestations are difficult to detect because the adverse consequences only become visible over time or when a downstream actor's performance degrades. Information technologies can amplify both manifestations. By filtering or prioritizing information, information technologies determine how actors understand the situation and, therefore, what they respond to [12]. If the information is incomplete or delayed, individual responses can systematically lead to maladaptive outcomes at the system level. This is the mechanism this paper investigates.

Evaluating whether crisis-response supply chain adaptation improves or degrades system performance requires metrics. Reviews of supply chain adaptation metrics indicate that most indicators fall into one of three categories: performance-, time-, or cost-based [61–63]. These metrics usually evaluate performance during and immediately after a single disruptive event, or they characterize static capabilities and capacities (e.g., redundancy, flexibility, collaboration) presumed to support future performance. Recently, Sardesai and Klingebiel [64] proposed a process capability index to rapidly detect whether supply chain adaptations keep the system within an acceptable performance range. Detecting maladaptation similarly requires a process view: adverse outcomes accumulate over time and across disruptions.

2.3. Agent-based modeling studies in information technology-driven adaptation in crisis-response supply chains

Agent-based models are suited to studying adaptation and maladaptation in crisis-response supply chains because they capture how local coordination and allocation decisions interact over time, leading to emergent system-level outcomes [65]. The combination of agent-based and discrete-event techniques enables modeling both coordination behavior and physical supply flows within the same framework [66]. The modeling literature established two findings. First, information quality and timeliness are critical determinants of response effectiveness. Models of post-disaster information diffusion establish that information quality shapes whether coordination improves or degrades performance [26]. Willingness to share information interacts with meeting structures so that regular meetings can partly substitute for individual sharing willingness [67]. Delayed or incorrect information during evolving events can undermine planning even when physical resources are available [68]. Second, coordination structure shapes response speed and allocation. Common operational pictures that mediate coordination between autonomous agents can reduce response times compared to purely decentralized coordination [69]. Allowing multiple information-sharing channels outside a central coordination system reduces inter-organizational response times [70]. Agent-based simulation has been used to optimize resource allocation across concurrent incident sites under capacity constraints [71].

The studies described above establish that information flows and coordination structures matter, but existing models share important limitations. Most of these studies evaluate a single information technology as a binary intervention and expose the system to a single disruption event [68–71]. None examines whether faster or more complete information sharing can lead to adverse system-level effects. Outside the supply chain domain, an agent-based study demonstrated that individual crisis-response adaptive actions can lead to maladaptive outcomes at the population level [72]. This study confirms the value of agent-based approaches for studying maladaptation, but does not address supply chain coordination or information technologies.

2.4. Summary and gap

Information technologies shift coordination in crisis-response supply chains by shifting delays, staleness, sharing frictions, decision-right allocation, and coverage. These shifts improve or degrade supply chain performance. When adaptive responses become misaligned with an evolving crisis, this degradation constitutes maladaptation. Existing agent-based models confirm that information quality and timeliness shape coordination effectiveness, but no model compares multiple information technologies or identifies the conditions under which technology-enabled adaptation becomes maladaptive (Section 2.3).

Three knowledge gaps limit our understanding of when crisis response becomes maladaptive. First, it is unknown whether different information technologies lead to distinct maladaptation vulnerabilities. Current studies evaluate technologies in isolation

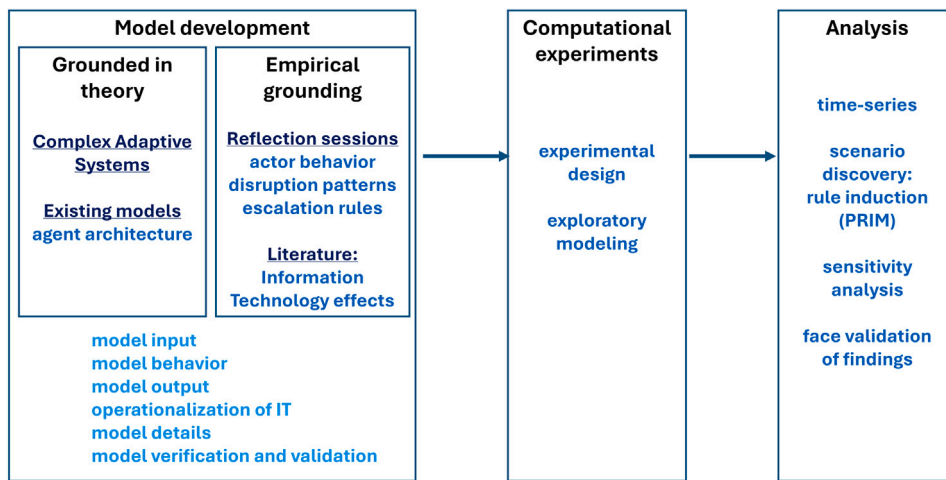


Fig. 1. Research approach.

and therefore cannot compare their failure modes. Second, it is unclear whether technology-enabled adaptations to an initial disruption increase or decrease vulnerability to subsequent ones. Current models allocate resources within a single event or across concurrent sites [71], but do not examine whether these adaptations become liabilities when the next disruption arrives. Third, the specific disruption conditions under which adverse technology effects emerge have not been identified. Without such identification, maladaptation remains a theoretical concern rather than guidance for technology implementation. This study addresses all three gaps by comparing multiple technology configurations across evolving crises and identify the conditions under which each technology becomes maladaptive.

3. Research approach

We conducted the research in three steps (see Fig. 1): Model development, computational experiments, and analysis.

3.1. Model development

We developed the model in two complementary ways. We grounded its agent architecture in theory on complex adaptive systems and existing agent-based models. We grounded the model behavior and the operationalization of information technologies empirically through reflection sessions and the literature.

3.1.1. Grounded in theory

We developed a model building on the theoretical foundations of complex adaptive systems and existing agent-based models established in Section 2. We conceptualized crisis-response supply chains as complex adaptive systems [73–76]. In such systems, system-level outcomes emerge from the interaction of multiple locally adaptive decisions under delays and feedback. Capturing these interactions requires a model that represents individual decision rules and their propagation over time [65]. Therefore, we employed an agent-based model [77].

We followed a pattern-oriented modeling approach [77,78]: A pattern-oriented model derives its validity not from calibration against a single case, but from its ability to generate the types of dynamics that are recognized as structurally realistic [77]. The model should accordingly be read as a representation of information-sharing and adaptation dynamics, not as an empirical prediction of crisis-response performance.

The present agent-based discrete-event model builds on a previously published crisis-response model [21]. This model introduced the core entities (responsibility areas, supply needs, managers/logistics officers, workers), the team-meeting coordination mechanism, and the rules for upward and downward authority transfer. We extend the model in two ways: (i) we represent information technologies as portfolios of parameters; (ii) we move from a single organization to three organizations arranged in a sequential or convergent configuration. The second extension is the supply chain configuration. In crisis-response supply chains, supply needs typically traverse multiple organizational boundaries (e.g., from warehousing to last-mile distribution, from the processing of supply information to a regional organization, and identifying that it has to be solved by the national organization). Each organization processes supply needs before passing them to the next, introducing inter-organizational dependencies. Through these dependencies delays in one organization propagate downstream.

3.1.2. Empirical grounding

We held reflection sessions with a national defense organization involved in crisis-response training and operational preparedness. These sessions informed the model's disruption patterns. The behavioral mechanisms for information use and sharing, and the escalation and de-escalation rules, were subsequently assessed for plausibility by practitioners from the same organization. The parameter shifts used to operationalize the information technologies were informed by the literature of technology effects on information management activities. The operationalization is described in Section 4.5.

3.2. Computational experiments

We conducted computational experiments by varying the disruption patterns and technologies. Crisis-response supply chains face uncertain disruption patterns and technology effects, and the relationships and their interdependencies in the model cannot be predicted with confidence. We therefore adopted an exploratory modeling approach [79,80]. Exploratory modeling treats the model as a computational experiment across a large number of systematically varied conditions. The exploratory modeling and analysis (EMA) workbench provides software for running and analyzing the experiments [81].

3.3. Analysis

The outcomes of the experiments were then analyzed using time-series analysis and scenario discovery [80,82]. Scenario discovery is a way to sift through many simulation runs and describe, in plain thresholds, the kinds of situations in which a specific outcome occurs more often (e.g., 'failure tends to occur when X is high and Y is low') [82,83]. In this paper, we use scenario discovery to pinpoint the operating conditions under which a technology improves performance and those under which it may lead to maladaptation. The Patient Rule Induction Method (PRIM) focuses on finding a small set of conditions, defined by a few straightforward cut-offs, where the class of outcomes that we are interested in is concentrated [83,84]. Therefore, PRIM is useful to isolate 'worst-case' sets of conditions.

4. Model development

4.1. Model overview

The model's purpose is to understand and analyze the role of information technology in maladaptation. To conduct this analysis, we connect the virtual layer (information collection, analysis, decisions) with the physical reality of crisis-response supply chains. The model abstracts from physical transportation, inventory positioning, and routing decisions. Instead, the model represents a pooled operational capacity problem: supply needs queue at responsibility areas, and workers are reallocated across responsibility areas to process them. This representation enables isolation of the information–decision–adaptation mechanisms.

Our model combines agent-based and discrete event processes. The agent-based processes represent how managers coordinate and allocate resources using fixed decision rules. Furthermore, these processes enable endogenous adaptation of the decision-making structure. The discrete event processes govern the flow of supply needs across responsibility areas and efficiently handle timing and delays.

The model includes decision-making Managers, and operational Workers, supported by four main entities: Supply needs, Responsibility areas (each with a queue), Team meetings, and Organizations (see Fig. 2). Each organization contains a set of responsibility areas and a hierarchy of managers (up to five echelons), and schedules team meetings for same-echelon coordination. Supply needs flow in the model in these responsibility areas. We model exogenous disruptions as either abrupt peaks or structural shifts in supply needs. Demand peaks in the model reflect two compounding effects: a volume surge in supply needs and simultaneous activation of previously idle responsibility areas. These compounding effects capture the characteristic pattern of disaster-driven demand, where crises expand the breadth of operational domains under pressure. Supply needs are generated exogenously in batches and routed to responsibility areas. The responsibility areas queue the supply needs until a worker is pushed to process a supply need. Each responsibility area represents, for example, a geographic zone or a functional domain assigned to a processing unit within the organization. Workers process supply needs at their assigned responsibility areas; they do not choose which responsibility area to serve. Supply needs that exceed an acceptable queue time are marked as unmet and removed from the queue.

Managers' decision authority is defined by their span of control: the number of responsibility areas a manager oversees doubles at each higher echelon. At any time, each responsibility area is under the authority of exactly one active manager (with inactive managers serving as potential decision makers if authority is transferred upward or downward).

4.2. Model input

Disruptions and crises differ in onset speed and duration [86,87]. Some disruptions lead to temporary demand peaks with a short duration that strain existing capacity, while others trigger structural shifts. For example, structural shifts alter the location, or priority of supply needs in ways not immediately legible to decision makers [19]. These differences imply distinct adaptation challenges, for example, structural shifts require recognizing that existing orientations may no longer fit the evolving pattern of supply needs. Therefore, we model it using batches of supply needs. At each time step, the model generates a new batch of supply needs. This batch enters a subset of the responsibility areas of the first organization. The batch size follows an exogenous disruption pattern (e.g., stable, peak, regime shift), see Fig. 3. Within each time step, the batch size varies stochastically. Supply needs enter the responsibility area queues. When a disruption occurs, the newly created supply needs are more urgent than those created earlier.

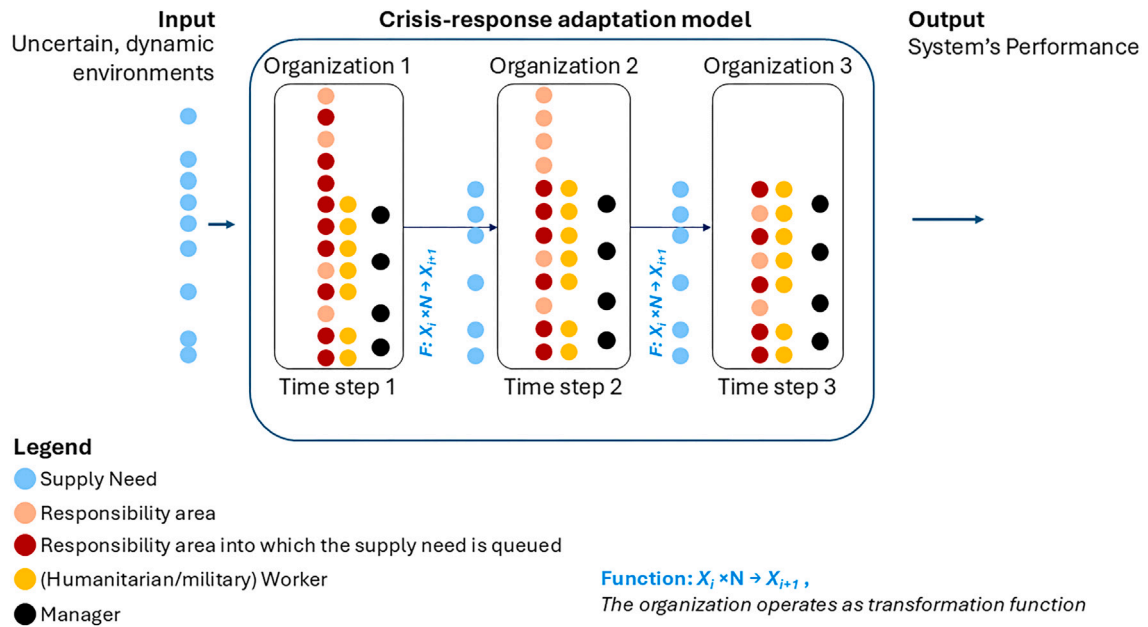


Fig. 2. A schematic overview of the Organizations in the crisis-response model, the Workers and Managers within the Organization and the Supply Needs flowing through the Organizations.

Source: Adapted from [85]

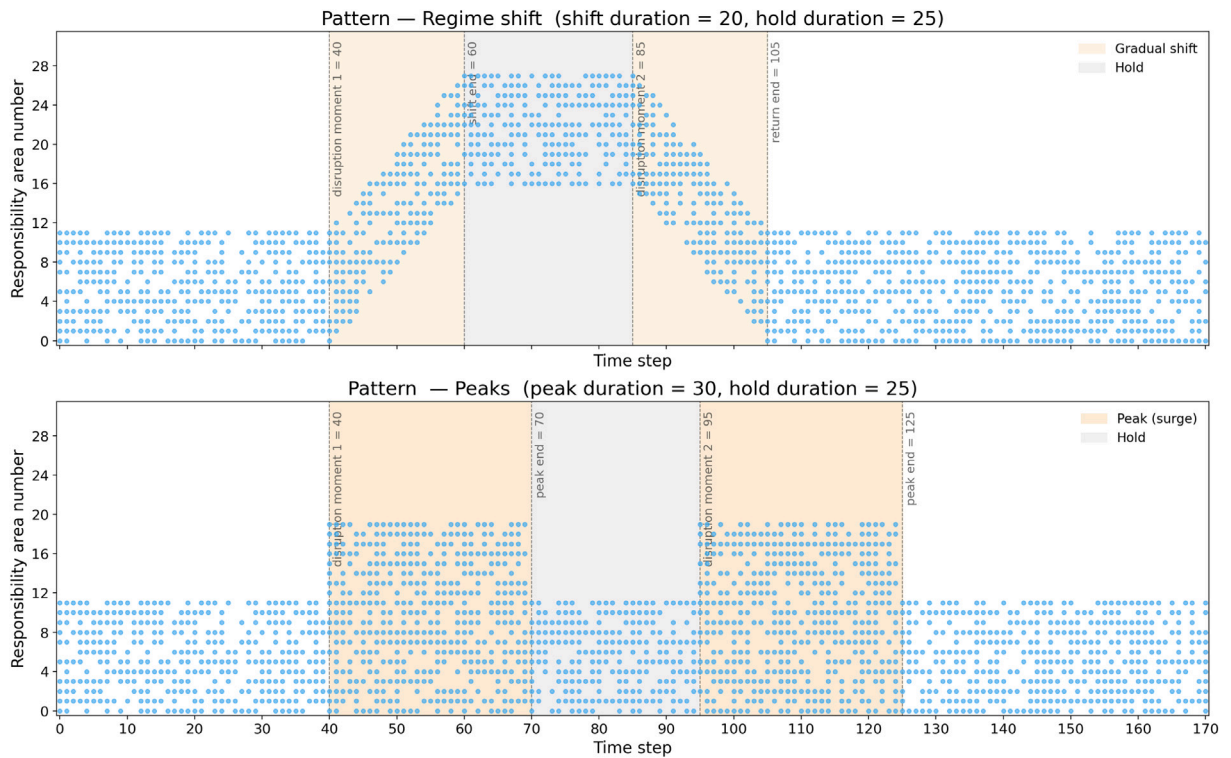


Fig. 3. Input Supply need patterns at Organization 1. At each time step, an exogenous batch of Supply Needs (a vertical column of blue dots) is assigned to the queues of the responsibility areas. Subsequent Organizations receive the SupplyNeeds only after they are processed at the preceding one, so their Responsibility Areas are not shown. This figure is conceptual: the model is non-spatial and queues are not visualized. Blue dots (Supply Needs) persist across time solely to reveal temporal patterns.

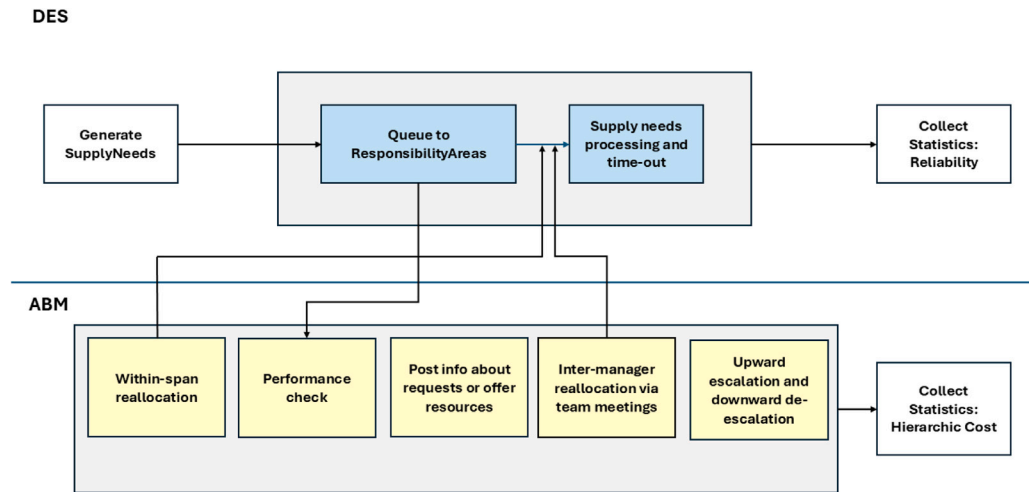


Fig. 4. DES and ABM key processes within 1 organization. The gray areas mark the processes discussed in the subsection ‘Model behavior’. The DES area (top) shows how supply needs queue at responsibility areas and are processed or timed out. The ABM area (bottom) shows the manager’s decision processes. Arrows between the two areas indicate where decisions are made on the responsibility area states (performance check), and allocations are made. The white blocks show the model input and output processes. In the multi-organization configurations, supply need generation occurs only at the first organization, and the statistics are recorded for the final organization. For intermediate organizations, the white input and output blocks represent the supply needs received from and passed to the adjacent organization.

4.3. Model behavior

The model evolves through repeated processes of supply need generating and inflow (see Fig. 4), local reallocation, information sharing, and supply need processing. Each process is governed by one or more parameters that technologies can shift (Table 2). The behavioral rules themselves remain constant across technologies; only the parameter values change. Besides the supply need generating and inflow, the most important processes are:

Within-span reallocation. Each active manager periodically evaluates the states of responsibility areas and workers within their span of control and reallocates available workers to responsibility areas with queued supply needs. This reallocation decision is executed immediately. However, the input for the reallocation is the manager’s information, which can be vertically delayed (that is, higher-echelon managers can act on outdated state information). Higher-echelon managers act on state information that is echelon $\times$ vertical delay steps old. Technologies that reduce vertical delay (e.g., prediction-enhanced COP, blockchain-traceability) make this evaluation more current. Technologies that increase span (e.g., drones, satellite internet) expand the set of responsibility areas a manager can observe directly.

Performance check. Each manager monitors performance by calculating a shortfall rate SR_i over a memory window. At each time step, the manager counts the supply needs that were removed from the queue unprocessed within their span of control and averages these missed counts over the memory window. Higher-echelon managers compute SR_i from state information that is echelon $\times$ vertical delay steps old, introducing staleness into the trigger.

Post info about requests or offer resources. Each manager compares its shortfall rate against the echelon-specific thresholds (T_{min} and T_{max}). Above T_{max} , the manager posts a request for workers; below T_{min} , posts an offer of surplus workers to the queue of the next team meeting, and in between, nothing happens. Posting is subject to each manager’s barrier to sharing information (modeled probabilistically).

Inter-manager reallocation via team meetings. The requests and offers are pooled and matched at the next team meeting at that echelon, producing reallocations across spans of control. The interval between team meetings introduces a horizontal delay between recognizing a supply need (a request) and executing cross-manager reallocations. Technologies that reduce horizontal delay (e.g., Artificial Intelligence-intake) shorten the coordination cycle. Technologies that lower barriers (e.g., Blockchain-based traceability) increase the likelihood that managers share information across organizational boundaries.

Upward escalation and downward de-escalation. A sustained overload measured by a shortfall rate above an upper threshold (for a specified inertia period) triggers escalation: decision authority is transferred to the superior. This superior has an expanded span of control and coordination. Therefore, coordination occurs at a changed echelon. A shortfall rate below a lower threshold for a specified inertia period (i.e., sustained underload) triggers de-escalation, with authority returning to subordinates. Thus, escalation and de-escalation lead to endogenous changes in hierarchy over time. Technologies that shorten the memory length (e.g., prediction-enhanced COP) cause the escalation trigger to respond more quickly to recent disruptions.

Supply needs processing and time-out. Workers process the first supply need in the queue of their assigned responsibility area. Supply needs exceeding the maximum acceptable waiting time are marked as unmet, contributing to the shortfall rate that managers use to calculate their performance. This process is not directly affected by any technology parameter.

4.4. Model output

The key processes yield two time-series metrics: reliability $R(t)$ and hierarchical structure cost $Hm(t)$. These metrics capture how the system adapts to a changing environment along two dimensions: reliability and cost of the hierarchy. Both metrics are recorded per time step, enabling comparison between the first and second disruption response. Maladaptation can be inferred from these time-series metrics and is therefore explained in the analysis phase (see Section 6). The metrics are calculated as follows: Note that we use the metric and term reliability here in the operational sense of a fill rate rather than in the engineering sense of a time-dependent probability of component non-failure [88].

(a) Reliability (R) — the fraction of performed over created supply needs (Eq. (1)):

$$R(t) = \frac{\text{processed supply needs at time } t}{\text{processed and unmet supply needs at time } t} \times 100\% \quad (1)$$

(b) Hierarchy metric (Hm) — a cost-based metric that increases with the number and echelon of active managers (and thus makes escalation visible) (Eq. (2)):

$$Hm(t) = \sum_{o \in \mathcal{O}} \sum_{m \in \mathcal{M}_o(t)} \left(\mathbf{1}_{\{m \text{ active at } t\}} C_{\text{echelon}(m)}^{\text{Active}} + \mathbf{1}_{\{m \text{ inactive at } t\}} C_{\text{echelon}(m)}^{\text{Inactive}} \right) \quad (2)$$

where $\mathcal{O}$ is the set of Organizations, $\mathcal{M}_o(t)$ the set of Managers in Organization o at time t , and $\text{echelon}(m) \in \{0, 1, 2, \dots\}$ the echelon of Manager m . The costs of an active Manager at echelon $m+1$ are exponentially higher than those at echelon m , and active Managers have higher costs than inactive ones within the same echelon. The hierarchy metric is reported in euros.

4.5. Operationalization of the information technologies

The model entails five parameters that are used in the operationalization of the technologies: (i) horizontal delay (time between cross-manager reallocation opportunities). Horizontal delay is implemented through the team-meeting interval: managers may submit requests and offers at each step, but matching and reallocation occur only at the next meeting (i.e., meeting interval-1). Horizontal delay is expressed in whole time steps; (ii) vertical delay (information staleness across echelons). Vertical delay is implemented by basing selected managerial assessments on delayed state information, with effective staleness increasing by echelon. The vertical delay also takes integer values: the effective staleness is used as the memory length across echelons, which must be an integer; (iii) barrier to share information (friction in posting and accepting requests and offers). This barrier reflects the extent to which information is shared and influenced by (i) heterogeneity (e.g., formats and semantics), (ii) overload, and (iii) trust concerns across intra- and inter-organizational boundaries. The barrier is implemented as a probabilistic gate (on $[0,1]$) that determines whether managers post requests or offers outside their span of control; (iv) coverage (span_level1), represents the effective operational reach of a manager, defined as the proportion of responsibility areas for which state information can be obtained. For span, only powers of two are feasible, since each echelon- k manager oversees $\text{span_level1} \times 2^{k-1}$ responsibility areas. Technologies may expand coverage either by generating new field observations (e.g., drones) or by restoring direct connectivity under infrastructure disruption (e.g., satellite internet) and (v) length of memory (the rolling window of recent state observations used in assessment), expressed in whole time steps. These parameters map onto distinct activities. Collecting and processing information draws on coverage: the span over responsibility areas from which a manager gathers state information. Performance checks rely on vertically delayed state information and a rolling memory. Peer-level exchange (sharing information) is governed by the barrier to sharing information. Peer-supported reallocations occur during periodic team meetings, so the lag between recognizing a supply need and executing a cross-manager reallocation is governed by horizontal delay.

For each information technology, we identified its primary effect on information management activities from the literature and translated this effect into a directional shift in one or more model parameters relative to a baseline configuration (see Table 1). This baseline represents a crisis response operating without any of the described information technologies. The baseline is therefore not frictionless, but a configuration in which delays and the information-sharing barrier are present at their unimproved levels. The baseline does have technology parameter values, which are motivated below. All other parameters remain fixed, isolating the technology's effect. To translate a technology into a parameter portfolio, we follow three steps. We identify, based on the literature, the technology's effects on the information or decision-making activities affected. Next, we assess whether each effect or activity has a direct counterpart in the model. Finally, when no one-to-one match exists, we translate the technology's effects into the closest model activities and behavioral rules, selecting the corresponding parameter shifts. The Table 1 details the translation.

The magnitude of each parameter shift of a technology is determined by the difference between technologies rather than by an absolute calibration. The shifts are thus specified relative to one another, measured from a baseline configuration. The baseline parameter values of the horizontal and vertical delay are set to 2, because these parameters are integer-valued and a baseline of 2 is the smallest value that distinguishes a single step reduction (to 1) from full elimination (to 0). The baseline barrier to sharing information is centered at 0.5, the midpoint of its $[0,1]$ range. A shift of equal magnitude in either direction (to 0.25 or 0.75) remains symmetric and avoids the extremes of complete openness or obstruction. The baseline values for the memory length and span parameters follow Epstein [89].

Table 1

Technology implementations mapped to parameter portfolios.

Technology implementation	Affected IM step(s)	Technology type	What it improves	Model mechanism it impacts	Parameter direction	Refs
AI-enabled flying sensors (drones)	Collect	UAV sensing and imagery	Faster and broader field observation; reduces unobserved areas	Coverage of responsibility areas with direct state visibility	Span ↑	[28,38]
Artificial Intelligence-intake standardization	Collect and Process	From unstructured to structured request fields	Reduces manual interpretation	State evaluation	Horizontal delay ↓ Vertical delay ↓	[42,43]
Prediction-enhanced COP	Analyze and Share	Real-time dashboard with predictive highlighting	Highlights areas approaching thresholds before formal crossing	Escalation and de-escalation trigger based on rolling memory and thresholds	Vertical delay ↓; Length of memory ↓	[3,90]
Blockchain-traceability (broad permissioned trusted ledger)	Store/Verify/Share	Permissioned shared ledger for transaction traceability	More traceability; increased trust in posted requests/offers	Cross-manager information posting	Barrier ↓; Vertical delay ↓	[5,50]
Blockchain-compliance (segmented access)	Store/Verify/Share	Permissioned ledger used indirectly via intermediaries; added procedural verification	Reduced practical visibility across levels; capability constraints; extra steps before information usable	Cross-manager information posting; Horizontal coordination cadence	Barrier ↑; Vertical delay ↑; Horizontal delay ↑	[5,49,50]
Satellite internet	Share	Resilient long-range connectivity	Improves reliability of cross-level transmission; extends reachable areas	Direct operational reach; Delayed situational assessment	Vertical delay ↓; Span ↑	[29,91]

Table 2

Information technologies operationalized as information-sharing and decision-making parameters.

Information technologies	Horizontal delay	Vertical delay	Barrier to share info	Span_level1	Memory length
Baseline	2	2	0.50	2	10
Artificial Intelligence - drones	2	2	0.50	4	10
Artificial Intelligence - intake	1	1	0.50	2	10
Prediction-enhanced COP	2	0	0.50	2	5
Blockchain – traceability	2	1	0.25	2	10
Blockchain – compliance	3	3	0.75	2	10
Satellite internet	2	1	0.50	4	10

From the baseline, each technology shifts one or more parameters. The size of each shift follows from the nature of the parameter: the discrete parameters shift in integer or power-of-two steps, while the continuous barrier to share information shifts in symmetric increments. For the delay parameters, a shift of 1 reduces the delay; a shift to 0 removes it entirely. The span parameter admits only powers of two, so the smallest upward shift from the baseline of 2 is to 4. The barrier to sharing information shifts by 0.25, dividing its [0,1] range symmetrically around the baseline of 0.5. We assume this shift is large enough to alter sharing behavior yet short of complete openness or obstruction. The resulting parameter values per technology are shown in Table 2. The design choices and parameter details are described per technology in Appendix A.

4.6. Model details

A complete specification of the model is provided in the Supplementary Material, using the ODD (Overview, Design concepts, Details) protocol [92]. The ODD includes all parameter definitions and decision rules of the behavioral mechanisms and the discrete-event logic. At $t=0$, the model is initialized with 8 workers and 32 responsibility areas. We start with 8 or 16 managers at the lowest echelon, depending on the current technology that defines the coverage per manager at echelon-1. Workers are initially allocated to responsibility areas in the subset with the lower responsibility area numbers; the initial supply-need pattern directs supply to the same specified subset of responsibility areas, with stochasticity controlled by a creation probability of 0.70. Each organization employs eight workers who each process one supply need per time step, yielding a system-wide capacity of 24 needs per step. With a baseline creation probability of 0.7 and a batch size of 12, the expected demand for capacity per step is 25.2, which structurally exceeds the available capacity of 24 under stable conditions. The model is implemented in Python using the pydsol-model and pydsol-core packages [93].

Table 3
Experimental parameters: uncertainties and technologies.

Uncertainty	Description	Values
supply_need_pattern	Disruption pattern governing how supply needs evolve over time.	[Peaks, Regime shift]
peak_duration	Length (time steps) of a peak episode during which supply need arrivals exceed the baseline.	[10, 50]
shift_duration	Length (time steps) of the transition from one stable supply need distribution to another; controls how gradual the regime shift is.	[0, 30]
hold_duration	Length of the stable inter-disruption period between the end of the first disruption episode and the onset of the second. Under the peaks pattern, this length is a return to the baseline supply needs; under the regime shift pattern, this is a period of a stable supply needs pattern within the newly established set of responsibility areas.	[10, 50]
<i>Technologies — Policy lever</i>		
technology	Information technology applied to the organization (see Table 1 for parameter portfolios).	[Baseline, Artificial Intelligence-drone, Artificial Intelligence-intake, Blockchain-compliance, Blockchain-traceability, Prediction-enhanced COP, Satellite internet]

4.7. Model verification and validation

We evaluated the model in two ways: verification of individual components against theoretical expectations with peer review from academic colleagues and face validation with practitioners. For verification, we tested model components incrementally, starting with a single-organization setup. We compared the model's logic and outputs with the frameworks of Epstein [89] and Lont et al. [21]. The model led to expected outcomes: reliability declined after disruptions, and the hierarchy expanded when performance fell short. A full replication of Epstein [89] was not possible because the original paper does not fully specify its initialization and because our hierarchical escalation works differently. However, the core mechanisms, reallocation behavior, de-escalation, and escalation, matched between the two implementations. For face validation, employees from our collaborating organization assessed whether the model's stylized organizational structure and behavioral mechanisms matched their practice. They confirmed that the model captures the main mechanisms of how information-sharing for decision-making is structured.

The purpose of the model is to explore under what conditions of different disruption patterns and information technologies, maladaptation in crisis-response supply chains may emerge. The model is fit for this purpose: its core elements, technologies, disruption patterns, and managers, workers, team meetings represent the adaptive actions and decisions through which maladaptation may occur. The model does not reproduce all empirical aspects of real crisis-response supply chains, but it leads to the two outcomes we investigate: reliability and hierarchical expansion [77].

5. Computational experiments

5.1. Experimental design

We use the exploratory modeling and analysis workbench [81] to run the model across a range of disruptive patterns and across the information technologies. The scenarios vary the values of the experimental parameters, see Table 3. We performed 40 replications per scenario, each with a different seed. Each replication spans 220 time steps. We used Latin Hypercube Sampling to ensure even coverage of parameter values across the parameter range with a limited number of scenarios. The total number of scenarios was 7007 (500 regime shift patterns, 500 peak patterns, and 1 stable pattern). We have two supply chain configurations, a sequential structure of the organizations and a convergent one. The experiments described above are carried out for both configurations.

The ranges of the disruption parameters reflect the variety of temporal profiles observed in real-world crises. Peak duration spans short-lived surges (10 steps), comparable to a sudden infrastructure failure or flash flood, to prolonged demand peaks (50 steps) characteristic of a protracted conflict. Shift duration ranges from an instantaneous regime change (0 steps), such as an earthquake that immediately alters the operational landscape, to a gradual transition (30 steps) in which access restrictions and coordination structures evolve over weeks. The broad ranges are chosen deliberately: we let the scenario discovery analysis (see Section 6.2) identify the critical thresholds from the simulation output. Hold duration governs the interval between two successive disruptions. Short intervals (10 steps) represent cascading crises in which the supply chain has barely stabilized before the next disruption arrives. Longer intervals (up to 50 steps) allow the organizations to complete their adaptive response.

We also kept certain parameters fixed in the model. Fixed parameters follow the values established by Epstein [89] unless stated otherwise (see the complete overview in the Appendix). Fixed parameters include the number of organizations (3), the number of workers (8), the maximum number of echelons (5), and the number of responsibility areas per organization (32). The input side

generates batches of 12 possible supply needs per time step with a creation probability of 0.7; during peaks, a surge of up to 70% additional needs is generated, split equally between medium- and high-priority needs. Manager thresholds for escalation ($T_{\max}$) and de-escalation ($T_{\min}$) follow Epstein's echelon-dependent schedule [0.7, 1.4, 2, 4, 10] [89]. Each echelon's $T_{\min}$ equals the $T_{\max}$ of the echelon above it. In the responsibility area, each area requires one time step per supply need and removes unprocessed needs after a delay of 1.05 steps. The small offset above 1.0 prevents race conditions in the discrete-event scheduler.

6. Analysis

6.1. Time-series analysis

Before applying scenario discovery, we visually inspect the reliability and hierarchy cost time series for two selected scenarios, one for the peak pattern and one for the regime shift pattern. The visualization is meant for illustrative purposes and is presented in Section 7.

6.2. Scenario discovery with PRIM

To apply scenario discovery, the model's outputs must be translated into a binary classification of maladaptive or non-maladaptive. The model already contains internal endogenous forms of adaptation (reallocation and structural change), and the technology levers represent an exogenous one. As maladaptation is inferred from adaptation, we evaluate for maladaptation both externally and internally. Following the recommendation of Steinmann et al. [63] to use multiple conceptually distinct resilience metrics, we define an indicator for internal and external evaluation. Each indicator serves as a binary target for a separate PRIM analysis [84], applied per technology to identify the smallest set of duration combinations (peak duration/shift duration, and hold duration) that contains a disproportionately high share of maladaptive experiments. For each experiment, the reliability time series is smoothed with a moving average (window of 5 time steps) to reduce per-step stochastic noise; metrics are averaged across the 40 replications per scenario.

Resilience loss. The resilience loss indicator captures external maladaptation: it compares a technology's cumulative performance loss against the Baseline under the same scenario conditions (Eq. (3)). This indicator measures the cumulative shortfall from perfect reliability over the evaluation window [61]. The resilience loss integral captures both the depth and duration of performance decline, which means that slower recovery directly increases the metric even when the eventual reliability level is the same. An experiment is classified as maladaptive when the technology's resilience loss exceeds the Baseline's at identical disruption parameters. The Baseline thus serves as the reference for comparing each technology against operating without any of these technologies.

$$R_{\text{loss}} = \frac{100}{t_{\text{end}} - t_1} \sum_{t=t_1}^{t_{\text{end}}} \max(0, 1 - R(t)) \quad (3)$$

where $R(t) \in [0, 1]$ is the reliability at time step t , t_1 is the onset of the first disruption, and $t_{\text{end}} = t_{\text{early}_2}^{\text{end}} + \tau$ is the end of the evaluation window, defined as $\tau = \text{maxhold_duration}$ time steps after the end of the second disruption's unstable phase ($t_{\text{early}_2}^{\text{end}}$). Hence, the evaluation window is different for peak and regime shifts. An experiment is classified as maladaptive when $\Delta_{\text{loss}} > 0$: The resilience loss exceeds Baseline's resilience loss. A larger difference in losses indicates greater loss of functionality during and after the disruption.

Cross-disruption. The cross-disruption indicator captures internal maladaptation: it compares mean reliability during the first and second disruption episodes. A positive ΔR indicates that the system performed worse on the second disruption despite having experienced the first, capturing situations in which adaptive actions triggered by the first disruption (e.g., an expanded hierarchy or reallocated workers) leave the system more vulnerable when the next disruption arrives. The indicator extends single-disruption resilience metrics to a cross-disruption comparison, which Steinmann et al. [63] identify as absent from the multi-disruption resilience literature. Both episodes are evaluated over a window hold_duration time steps following the unstable phase of each disruption ($d_k = \text{peak_duration}$ for the peaks pattern; $d_k = \text{shift_duration}$ for the regime-shift pattern), ensuring that the two windows are directly comparable (Eq. (4)). An experiment is classified as maladaptive when ΔR falls in the top 20% of its pattern-technology group. The quantile threshold was chosen following Bryant and Lempert [83], who applied the same value to define cases of interest in a policy analysis context. This threshold aims to balance a stringent worst-case criterion with sufficient cases for stable box-finding.

$$\Delta R = \bar{R}_1 - \bar{R}_2, \quad \bar{R}_k = \frac{1}{\text{hold_duration}} \sum_{t=t_k+d_k}^{t_k+d_k+\text{hold_duration}-1} R(t) \quad (4)$$

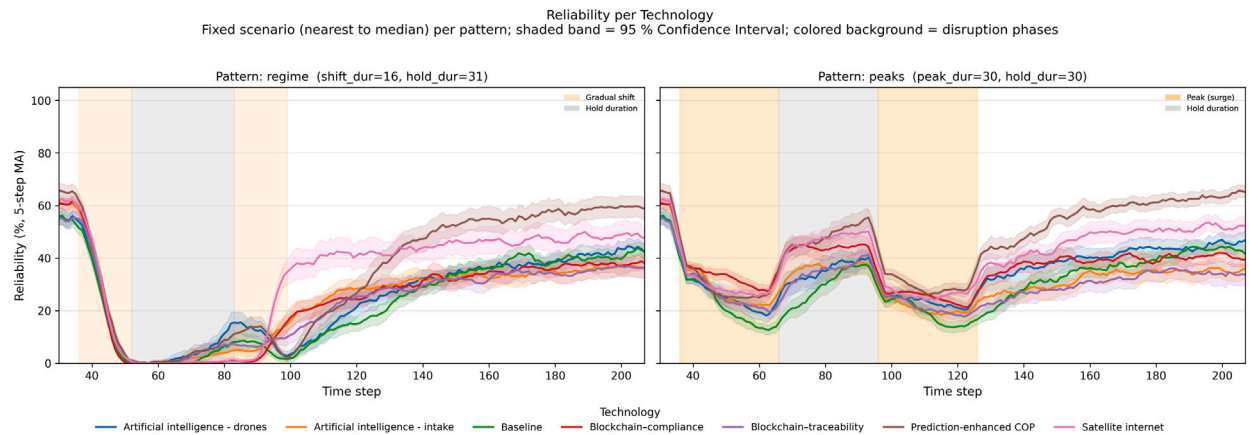


Fig. 5. Reliability time series per technology for representative scenarios, sequential configuration: regime shift pattern (left figure), with peaks pattern (right figure).

7. Findings

7.1. Sequential configuration

7.1.1. Time-series analysis — technology effects over time for the sequential configuration

We first illustrate how the model output evolves over time under a scenario of the disruption pattern with peaks and a scenario with the disruption patterns with the regime shift. Figs. 5 and 6 show, respectively, the reliability and cost of the hierarchy for each technology over time. These time-series plots serve two purposes. First, they make visible the adaptive dynamics that the indicators used in scenario discovery summarize: the initial reliability decline after the first disruption, the recovery trajectory, the second decline, and the degree to which recovery is slower or incomplete. Second, they illustrate the structural cost dimension: the hierarchy expands as managers escalate decision authority, and the speed and extent of subsequent contraction differ across technologies. The information technologies do not alter system capacity; they modify the speed of supply need detection and intra-organizational allocation. The performance differences between technologies, therefore, reflect differences in how effectively the fixed worker capacity is utilized. One of these technology configurations is the baseline, which represents operation without any of the described information technologies and serves as the reference against which each technology is compared.

In the regime shift pattern (left figure), a single prolonged trough appears. The trough follows from the nature of regime shifts, see Fig. 3: a regime shift changes which responsibility areas receive supply needs. The first shift, starting $t=36$, gradually redirects the supply needs to different responsibility areas over 15 time steps. By the time the system begins to adapt to the new situation, the second shift back begins. The system is therefore continuously in transition, with no stable intermediate period in which recovery can occur. This transition explains the extended period of low performance. A further observation is that, during a regime shift, all technologies experience an initial reliability decline at virtually the same rate. The decline is driven by the structural mismatch between where workers are allocated and where supply needs arrive. This mismatch is purely positional: no technology can prevent workers from being stationed at responsibility areas that no longer receive supply needs when supply needs shift. Differences between technologies thus become mainly visible during recovery.

In the peaks pattern (right figure), two distinct reliability declines are visible. After the first decline, technologies recover at different speeds. For example, Artificial Intelligence-drone and Satellite internet seem to recover fastest, whereas Artificial Intelligence-intake recovers the slowest. After the second decline, the Artificial Intelligence-drone is again the fastest in recovery. However, for several technologies, the recovery is slower or less complete than after the first disruption. This difference between first and second recoveries is a candidate signal of maladaptation: the adaptive actions triggered by the first disruption (e.g., hierarchy expansion) may not have been fully performed before the second disruption arrives. These ‘unfinished’ adaptive actions leave the system more vulnerable. During peak durations, the expected demanded capacity rises to approximately 43 supply needs per step, exceeding the available worker capacity by a factor of 1.7. This difference between demanded and available capacity creates an upper bound on reliability of approximately 56%, independent of the technology. Appendix Fig. 7 provides the reliability range across all scenarios per technology for both disruption patterns.

In both the regime shift pattern and the peaks pattern, the two information technologies with the highest coverage, Artificial Intelligence-drone and Satellite internet, have a lower hierarchy cost over the whole period. In the regime shift pattern (left figure), the technologies exhibit different profiles. Prediction-enhanced COP leads to the highest hierarchy cost, whereas Artificial Intelligence-drone seems not to respond by escalating at all. In the peaks pattern (right figure), two hierarchy cost increases are visible. Here, Prediction-enhanced COP leads again to the highest hierarchy cost.

The illustrative time series shows that information technologies differ in how quickly reliability recovers and how quickly hierarchy costs increase. Furthermore, the figures indicate that information technologies may differ depending on whether the first

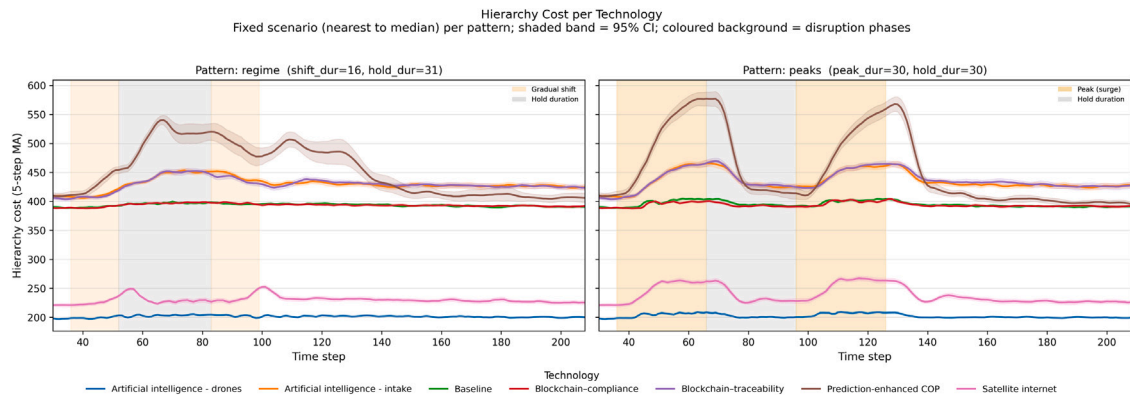


Fig. 6. An example of active hierarchy cost over time per technology for the same scenario, sequential configuration. Higher values indicate that more management echelons are active: regime shift pattern (left figure), with peaks pattern (right figure).

Table 4

PRIM analysis for the sequential configuration: input conditions under which a technology accumulates greater resilience loss than the Baseline (7007 experiments, each 40 replications). n_{mal} : number of target experiments; — : no maladaptive cases; *no discriminating conditions*: criterion triggered but PRIM found no restricting parameter region.

Regime-shift pattern			
Technology	n_{mal}	Shift duration	Hold duration
Baseline	N/A		
Artificial intelligence – drones	26	<i>no discriminating conditions</i>	
Artificial intelligence – intake	30	<i>no discriminating conditions</i>	
Blockchain-compliance	66	[18, 30]	[46, 50]
Blockchain-traceability	47	[1, 12]	[10, 18]
Prediction-enhanced COP	0	–	–
Satellite internet	0	–	–
Peak pattern			
Technology	n_{mal}	Peak duration	Hold duration
Baseline	N/A		
Artificial intelligence – drones	0	–	–
Artificial intelligence – intake	81	<i>no discriminating conditions</i>	
Blockchain-compliance	0	–	–
Blockchain-traceability	121	[10, 22]	[18, 50]
Prediction-enhanced COP	0	–	–
Satellite internet	0	–	–

recovery is complete before the next disruption arrives. When recovery from the first disruption is still ongoing, the system enters the second disruption with a partially expanded hierarchy or misallocated workers, which may impact second-disruption performance.

7.1.2. The PRIM analyses for the sequential configuration

Resilience loss compared to the baseline. Table 4 summarizes the duration conditions under which each technology accumulates greater resilience loss than the baseline. Two technologies, Prediction-enhanced COP and Satellite internet, show no maladaptive cases under either pattern, indicating that neither technology leads to worse outcomes than the baseline across any tested duration condition. The remaining technologies exhibit distinct maladaptation profiles. Under the regime shift pattern, Artificial Intelligence-drone and Artificial Intelligence-intake each lead to maladaptive cases, but PRIM finds no discriminating conditions for either. The absence of discriminating conditions means that maladaptive outcomes are distributed uniformly across the full range of shift and hold durations: these technologies underperform the baseline under regime shifts, regardless of how gradual the shift is or how long the inter-disruption interval hold_duration lasts. Blockchain shows conditional maladaptation, concentrated within specific shift and hold duration windows. Under the peak pattern, the picture is different. Artificial Intelligence-intake leads to 81 maladaptive cases with no discriminating conditions, confirming broad maladaptation independent of peak and hold duration. Blockchain-traceability is conditionally maladaptive, with underperformance concentrated in a peak-duration window of [10,22] steps: maladaptation is restricted to relatively short peaks and does not emerge under longer ones.

Table 5

PRIM analysis for the sequential configuration: disruption conditions under which the second disruption episode leads to lower mean reliability than the first (7007 scenarios, each 40 replications). n_{mal} is the number of target experiments; — : no maladaptive cases; *no discriminating conditions*: criterion triggered but PRIM found no restricting parameter region.

Regime shift pattern			
Technology	n_{mal}	Shift duration	Hold duration
<i>Baseline</i>	N/A		
Artificial intelligence – drones	100	<i>no discriminating conditions</i>	
Artificial intelligence – intake	100	<i>no discriminating conditions</i>	
Blockchain-compliance	100	<i>no discriminating conditions</i>	
Blockchain-traceability	100	<i>no discriminating conditions</i>	
Prediction-enhanced COP	100	[7, 26]	[48, 50]
Satellite internet	100	[23, 28]	[10, 50]
Peak pattern			
Technology	n_{mal}	Peak duration	Hold duration
<i>Baseline</i>	N/A		
Artificial intelligence – drones	100	<i>no discriminating conditions</i>	
Artificial intelligence – intake	100	<i>no discriminating conditions</i>	
Blockchain-compliance	100	<i>no discriminating conditions</i>	
Blockchain-traceability	101	<i>no discriminating conditions</i>	
Prediction-enhanced COP	100	<i>no discriminating conditions</i>	
Satellite internet	100	<i>no discriminating conditions</i>	

Cross-disruption. Beyond comparing technologies against the baseline, we examine the disruption dynamics that drive maladaptation from within: specifically, whether the adaptive response to the first disruption leaves the system more vulnerable when the second begins. Table 5 summarizes the conditions under which the second disruption episode leads to lower mean reliability than the first. By construction, the top 20% of experiments per pattern-technology group constitutes the target class, so n_{mal} is about 100 for every technology. The informative result is therefore not the count but whether the worst deterioration between disruptions concentrates in a specific region of the parameter space or is spread uniformly across it.

Under the regime shift pattern, PRIM identifies discriminating conditions for only two technologies. For Prediction-enhanced COP, the smallest improvements concentrate at shorter shift durations combined with the longest hold durations (shift [7, 26], hold [48, 50]). For Satellite internet, these improvements concentrate on upper-middle to long shift durations across the full hold range (shift [23, 28], hold [10, 50]), so only shift duration discriminates. For the remaining technologies, PRIM finds no discriminating conditions: the smallest improvements between disruptions are spread across the full range of shift and hold durations. Under the peaks pattern, no technology shows discriminating conditions. The classification in Table 17 (in the Appendix) confirms that all top-20% target cases under peaks are genuine cross-disruption deterioration ($\Delta R > 0$ for 100% of cases across every technology). The second peak leaves the system in a worse settled state than the first, regardless of peak and hold durations, a structural property shared across the information technologies under peak disruptions.

The interpretation of the within-group criterion differs between the two disruption patterns. For the peaks pattern, the target cases represent scenarios in which disruption 2 left the system in a worse steady state than disruption 1. For the regime-shift pattern, the system consistently improves between the two disruptions regardless of disruption conditions (see Table 17). The discriminating conditions reported for regime shifts in Table 5 should therefore be read as the conditions under which this inter-disruption learning effect is smallest, not as conditions under which the system deteriorates. Table 17 confirms that this directional pattern already holds for the Baseline: each technology therefore amplifies or dampens an effect that is present independent of the technology.

7.2. Convergent configuration

7.2.1. PRIM analysis for the convergent structure

Resilience loss compared to the baseline. Table 6 summarizes the duration conditions under which each technology performs worse than the baseline in the convergent configuration. Prediction-enhanced COP again shows no maladaptive cases under either pattern. Satellite internet similarly shows no maladaptive cases under the peak pattern, though it does exhibit maladaptive cases under the regime shift pattern.

Under the regime shift pattern, Artificial Intelligence-drone, Artificial Intelligence-intake, Blockchain-compliance, and Blockchain-traceability each show several hundred maladaptive cases. Artificial Intelligence-drones and Blockchain-compliance show conditional vulnerability, with maladaptive cases concentrated in shift durations of [8, 28] and [6, 30] combined with hold durations of [14, 50] and [22, 50], respectively. Blockchain-traceability shows no discriminating conditions despite 491 maladaptive cases, indicating that its underperformance under regime shifts is distributed broadly across all duration combinations. Satellite internet

Table 6

PRIM analysis for the convergent configuration: input conditions under which a technology accumulates greater resilience loss than the Baseline (7007 experiments, each 40 replications). n_{mal} : number of target experiments; — : no maladaptive cases; *no discriminating conditions*: criterion triggered but PRIM found no restricting parameter region.

Technology	Regime-shift pattern		
	n_{mal}	Shift duration	Hold duration
<i>Baseline</i>	N/A		
Artificial intelligence – drones	350	[8, 28]	[14, 50]
Artificial intelligence – intake	496	<i>no discriminating conditions</i>	
Blockchain-compliance	427	[6, 30]	[22, 50]
Blockchain-traceability	491	<i>no discriminating conditions</i>	
Prediction-enhanced COP	0	–	–
Satellite internet	274	[16, 30]	[26, 50]

Technology	Peak pattern		
	n_{mal}	Peak duration	Hold duration
<i>Baseline</i>	N/A		
Artificial intelligence – drones	104	<i>no discriminating conditions</i>	
Artificial intelligence – intake	491	<i>no discriminating conditions</i>	
Blockchain-compliance	135	[44, 48]	[10, 50]
Blockchain-traceability	499	<i>no discriminating conditions</i>	
Prediction-enhanced COP	0	–	–
Satellite internet	0	–	–

is more conditionally vulnerable: its maladaptation is restricted to shift durations of [16, 30] combined with longer hold durations ([26, 50]), suggesting sensitivity to sustained regime shifts paired with prolonged inter-disruption intervals.

Under the peak pattern, the picture is more differentiated. Artificial Intelligence-intake and Blockchain-traceability both show broad vulnerability across the full range of peak and hold durations, with case counts close to the maximum (491 and 499, respectively). Artificial Intelligence-drone is more moderately affected (104 cases, *no discriminating conditions*). Blockchain-compliance is the exception: maladaptation concentrates in a narrow window of long peaks ([44, 48]) combined with hold durations of [10, 50], indicating a conditional vulnerability restricted to near-maximum peak duration. This contrasts with Blockchain-compliance in the sequential configuration, where no maladaptive cases were found under peaks, confirming that the convergent structure introduces peak-pattern vulnerability for this technology. Blockchain-traceability similarly shifts from conditional maladaptation in the sequential configuration (restricted to peaks of [10, 22] steps) to *no discriminating conditions* here. This contrast with the sequential configuration confirms that the convergent one amplifies and generalizes vulnerability.

Cross-disruption. Table 7 summarizes the conditions under which the second disruption episode leads to lower mean reliability than the first in the convergent configuration. Under the regime shift pattern, the convergent configuration yields a discriminating condition for only one technology. Where the sequential configuration identifies discriminating conditions for two technologies (Prediction-enhanced COP and Satellite internet), the convergent configuration retains a box only for Prediction-enhanced COP, whose cross-disruption indicator values concentrate at short shift durations ([1, 16]) and longer hold durations ([42, 50]) — consistent in direction with its sequential counterpart. Under the peak pattern, no technology yields discriminating conditions. The absence of discriminating conditions mirrors the sequential finding for peaks and confirms the structural property that is independent of disruption patterns.

7.3. Sensitivity analysis

A sensitivity analysis on the demand–capacity ratio varied the number of workers below (6) and above (10) the main value. We examined how sensitive maladaptation is to capacity and whether technologies still diverge when capacity is fixed. In the sequential configuration, maladaptation is low and only weakly sensitive to capacity, yet technologies differ at a fixed worker level: under peaks, Blockchain-traceability is maladaptive in most configurations, while Prediction-enhanced COP is never maladaptive. In the convergent configuration under regime shifts, the span- and delay-shifting technologies (e.g., Artificial Intelligence-drone, Satellite internet) become less maladaptive as workers rise from 6 to 10. Here, the needs are more rapidly visible, so additional capacity directly serves the mismatched areas. For Artificial Intelligence-intake and Blockchain-traceability, the opposite holds: under convergent peaks, maladaptation intensifies toward near-universal as capacity grows. A capacity interpretation, under which extra workers relieve maladaptation uniformly, cannot account for this. The mechanism is that capacity governs whether the coordination and escalation response is ever triggered. Escalation activates only when the shortfall rate exceeds its threshold, but ample capacity keeps local performance below that threshold. Hence, managers escalate and reallocate less, while the technology continues to act on a partially stale picture. This aligns with the productivity paradox [10]: a technology yields gains only when the conditions

Table 7

PRIM analysis for the convergent configuration: disruption conditions under which the second disruption episode leads to lower mean reliability than the first (7007 scenarios, each 40 replications). n_{mal} is the number of target experiments; *no discriminating conditions*: criterion triggered but PRIM found no restricting parameter region. — : no maladaptive cases.

Regime shift pattern			
Technology	n_{mal}	Shift duration	Hold duration
<i>Baseline</i>	N/A		
Artificial Intelligence – drones	100	<i>no discriminating conditions</i>	
Artificial Intelligence – intake	100	<i>no discriminating conditions</i>	
Blockchain-compliance	100	<i>no discriminating conditions</i>	
Blockchain-traceability	100	<i>no discriminating conditions</i>	
Prediction-enhanced COP	100	[1, 16]	[42, 50]
Satellite internet	100	<i>no discriminating conditions</i>	
Peak pattern			
Technology	n_{mal}	Peak duration	Hold duration
<i>Baseline</i>	N/A		
Artificial Intelligence – drones	100	<i>no discriminating conditions</i>	
Artificial Intelligence – intake	100	<i>no discriminating conditions</i>	
Blockchain-compliance	100	<i>no discriminating conditions</i>	
Blockchain-traceability	101	<i>no discriminating conditions</i>	
Prediction-enhanced COP	100	<i>no discriminating conditions</i>	
Satellite internet	100	<i>no discriminating conditions</i>	

that activate it are present, and capacity can remove them. Because the response to added capacity differs across technologies with identical worker counts, the outcome reflects each technology's information-processing behavior. Mean resilience-loss differences from the baseline for every technology and capacity level are reported in [Appendix E.1](#).

A sensitivity analysis was also conducted on the technology parameters. First, to identify which technology parameters drive the magnitude of maladaptation, we applied random forest feature scoring (500 trees) to the resilience-loss difference relative to the baseline. *Vertical delay* emerged as the most influential parameter, followed by *length_memory* and *span_level1*. Detailed parameter importances are reported in [Appendix E.2](#). Second, we assessed robustness of the maladaptation profiles by varying each technology's defining parameters one at a time. We assessed whether the type of maladaptation profile was preserved across parameter variations. For the sequential configuration, the majority of information technology–pattern combinations, the profile type remained stable. For the convergent configuration, stability was lower, consistent with the greater sensitivity of convergent chains to information technology parameters. Detailed results per technology and variation are reported in the same subsection of the Appendix.

A sensitivity analysis was also conducted on an alternative baseline. Because every technology's maladaptation is defined relative to the baseline, raising the baseline's barrier to share information tests whether the profiles depend on the specific reference rather than on the technology itself. We changed the baseline barrier_share_info from 0.50 to 0.75 and re-derived each profile. Across both configurations, 12 of the 24 technology–pattern combinations retain their profile. Prediction-enhanced COP, Blockchain-traceability, and Satellite internet are most robust (3 of 4 combinations each), shifting only under regime shift. Artificial Intelligence-intake and Blockchain-compliance are most sensitive, moving toward *none* under most patterns. Artificial Intelligence-drone alternates between broad and no maladaptation under peaks. The sequential configuration is more stable (8 of 12) than the convergent one (4 of 12). The main findings are therefore partially sensitive to the baseline sharing barrier, with sensitivity concentrated in the convergent configuration. Detailed results are reported in [Appendix E.3](#).

8. Discussion

8.1. Synthesis: maladaptation profiles and conditions

This study explores conditions when information technologies lead to maladaptive outcomes in crisis-response supply chains. To explore, we developed an agent-based model to perform computational experiments under different disruption conditions and information technologies. The study operationalized maladaptation as a condition-specific phenomenon. By applying scenario discovery with PRIM, we concluded that maladaptive outcomes are not uniformly distributed across all disruption durations and information technologies. We identify two distinct maladaptation profiles: broad and conditional maladaptation. The broad profile refers to information technologies that exhibit maladaptive cases spread across disruption durations rather than confined to a window. The conditional profile refers to information technologies whose maladaptation is triggered only within specific duration windows. A further finding is that the disruption pattern moderates which profile an information technology exhibits: technologies that avoid maladaptation under the peaks pattern can lead to broadly maladaptive outcomes under regime shifts, as shown for

Artificial Intelligence-drone in the sequential configuration. The configuration of the organizations, sequential or convergent, further moderates maladaptation: the convergent configuration amplifies the number of maladaptive cases and reduces the discriminating conditions observed in the sequential configuration. The absence of discriminating conditions makes maladaptation more pervasive and less diagnosable when organizations process supply needs simultaneously. The sensitivity analyses show that the maladaptation findings are partially sensitive to the technology-parameter specification and to the assumed baseline information-sharing barrier. This sensitivity is itself a finding: it shows that the value of an information technology in crisis-response supply chains cannot be assessed as a property of the technology, but only as a property of the technology under specific conditions.

Prior studies in other knowledge domains have defined maladaptation as adaptive actions that degrade system performance [14,55,72], but have not investigated the concept as a structurally emergent outcome in crisis-response supply chains. Because the disruption pattern is not known in advance, a technology whose maladaptation is confined to a narrow window is the more robust choice.

The two profiles can be understood through theoretical arguments established in the literature on information technologies in crisis response. Artificial Intelligence-intake exhibits broad maladaptation under supply need peaks across the full range of disruption durations. This finding is consistent with the productivity paradox of Artificial Intelligence [10]: introducing Artificial Intelligence does not automatically translate into performance gains. Under peak disruptions, Artificial Intelligence-intake carries a systematic but unpredictable maladaptation risk: in a minority of scenarios, it underperforms the no-technology baseline, and no disruption duration conditions have been identified that predict when this occurs. Organizations cannot, therefore, rely on timing to avoid this risk. Artificial Intelligence-drone as technology avoids maladaptation under supply need peaks, but leads to broadly maladaptive outcomes under regime shifts. This finding is consistent with the lens argument: information technologies shape which aspects of an evolving crisis become visible and actionable [12].

The two Blockchain implementations lead to complementary maladaptation conditions in the sequential configuration. This complementarity is consistent with the blockchain literature, which recognizes both the benefits and barriers to coordination resulting from blockchain implementations [5,49]. Each of the two implementations operationalizes a different balance between these benefits and barriers. The complementary maladaptation conditions confirm that both sides matter: the implementation that realizes more benefits is maladaptive under different disruption conditions than the implementation that suffers more from the barriers.

Prediction-enhanced COP has the fewest maladaptive cases among the technologies, indicating that it is the most robust technology. This finding aligns with the literature on Common Operational Pictures and predictive capabilities that overall claim that prediction supports crisis-response operations [3,4]. The robustness of Prediction-enhanced COP follows from the interaction between zero vertical delay and escalation. Escalation transfers authority to a manager with a broader span who, operating on current information, can reallocate more accurately. Satellite internet is robust in the sequential configuration and under peaks. In the convergent configuration under a regime shift, Satellite internet shows conditional maladaptation. Following the lens argument [12], Satellite internet broadens the scope of the available information, which may explain its relative robustness. This finding contrasts with the prevailing assumption in the literature, that a broader scope improves the response to a crisis.

For crisis-response supply chain theory, our findings extend coordination research. Coordination research has documented the structural difficulty of aligning actors through coordination in crisis-response supply chains [94–96]. Coordination operates as an information–decision–action loop: actors gather information, decide, and act, and their actions reshape the situation the next cycle observes [9]. We contribute to coordination research by showing that introducing information technologies into this loop does not guarantee improvement. Whether an information technology leads to maladaptive outcomes depends on how its effects interact with the disruption pattern, not on the technology alone.

Information-processing theory holds that coordination performance depends on the fit between an organization's information-processing needs and its information-processing capacity [8,97]. Introducing information technology is a common adaptation response in crisis-response supply chains, premised on the assumption that added capacity improves coordination. Our findings qualify this assumption by showing that added capacity becomes maladaptive when a disruption pattern shifts processing needs out of alignment with the technology's capabilities. That information technologies can become maladaptive has been identified as a concern in crisis-response supply chain contexts [12,98]. Our findings give this concern a structural form: maladaptation is sometimes broad, and sometimes conditional. For information technology design and evaluation, these findings imply that technologies should be assessed on their maladaptation risk profile. A technology that performs well on average but exhibits broad maladaptation under a specific disruption pattern may be less suitable than an information technology with a narrower but predictable vulnerability window. For some of the technologies examined, the Baseline outperforms adoption under specific disruption conditions; thus, sometimes, no such technology is better than introducing one.

The findings on maladaptation can be positioned against existing agent-based models of crisis-response supply chain coordination. These agent-based models have established that information quality and timeliness shape coordination effectiveness [26,68,69]. The present findings extend this modeling literature by showing that exploratory modeling with PRIM detects maladaptive outcomes that single-case evaluations or average-performance metrics would miss. This approach is, in addition, a first step toward stress-testing information technologies for crisis-response supply chains before deployment. Supply chain stress-testing evaluates whether a system withstands extreme yet plausible disruptions [99,100]. The supply chain stress-testing literature is largely commercial and imposes predefined crises and disruptions. We extend this literature to crisis-response supply chains.

8.2. Face validation of findings

Practitioner input supports our findings. Six practitioners and domain experts with backgrounds in crisis response and crisis information systems assessed the findings for recognizability and plausibility. The findings that deploying a technology can actively degrade performance and that its effect is conditional on the type of crisis were recognized and considered plausible. One respondent illustrated the conditional profile, noting that tools performing well in data-rich, slower-moving crises are less effective in sudden-onset events where data quality and time are scarce. Another respondent found the claim that some technologies never perform worse implausible. This claim is where our model's findings and practitioner intuition diverge most clearly. In the model, Prediction-enhanced COP never performs worse under any tested crisis conditions. The role of the supply chain configuration was considered plausible by some and hard to judge by others.

8.3. Limitations and future research

This study has some limitations, which also provide directions for future research. First, the model does not include an explicit attribute for information accuracy, nor does it model noise or distortion in information flows. Technologies are assumed to function without intrinsic failure or performance variability. For example, drones do not malfunction, and satellite internet connections do not experience outages or bandwidth constraints. Incorporating technology failure modes and information distortion would allow future research to examine whether maladaptation intensifies under the conditions that already strain coordination. Second, information availability during disruptions and the availability of technologies are not modeled. Satellite internet, for example, is conceptually valuable because it provides connectivity when other technologies fail. However, our model does not capture temporary breakdowns in information sharing. Future research could examine whether technology-specific information availability alter which maladaptation profile emerges. Third, operational routing and flow reconfiguration are exogenous. The routing of supply needs is predefined in the model structure. Thus, information technologies cannot dynamically reconfigure information routes other than the fixed escalation rules. This fixity constrains the model's ability to represent adaptive information-routing mechanisms such as automated filtering or role-based information sharing. Extending the model to incorporate adaptive information routing could bring the study closer to what we observe in practice.

Overall, these limitations imply that the model emphasizes structural coordination dynamics and capacity and resource reallocation. Consequently, the results should be interpreted as reflecting coordination and allocation mechanisms under idealized functioning of information technologies, not as a comprehensive representation of information technologies.

9. Conclusions

This paper addresses the question *For which combinations of information technologies and disruption patterns do adaptive actions in crisis-response supply chains lead to maladaptive outcomes?* The findings show that whether and when a technology leads to maladaptation depends on the specific technology and that maladaptation concentrates in two distinct profiles: broad maladaptation, refers to a technology whose underperformance is distributed across disruption durations, and conditional maladaptation, where underperformance is restricted to specific duration windows. Furthermore, the findings show that the disruption pattern moderates which profile that technology exhibits. The configuration of organizations, sequential or convergent, further moderates maladaptation.

The technology-specific findings show that each technology exhibits a distinct maladaptation profile. Artificial Intelligence-intake is broadly maladaptive under peaks. Artificial Intelligence-drone avoids maladaptation under peaks but is broadly maladaptive under regime shifts. The two Blockchain implementations result in complementary maladaptation conditions in the sequential configuration, confirming that the implementation design, not the technology itself, determines where maladaptation concentrates. Prediction-enhanced COP never accumulates more resilience loss than the Baseline under any tested condition. Satellite internet is robust in the sequential configuration but conditionally maladaptive in the convergent configuration under regime shifts. The convergent configuration amplifies the number of maladaptive cases and eliminates discriminating conditions, making maladaptation more pervasive and less diagnosable.

This study makes two contributions. Conceptually, we advance understanding of how information technologies can lead to maladaptation in crisis-response supply chains. The study operationalizes maladaptation as a condition-specific phenomenon with identifiable boundaries. The findings pertain to the information and coordination processes of crisis-response supply chains, specifically the reallocation decisions that govern what gets allocated, where, and when. Methodologically, this study demonstrates that the combination of exploratory modeling with rule induction can detect maladaptive outcomes across repeated disruptions and information technologies. The contributions are based on a model with idealized assumptions about technology functioning. The model abstracts from technology failures, information quality and availability, and dynamic information routing. Future research could relax these assumptions.

For practitioners, this study can provide guidance for selecting information technologies for crisis-response supply chains. Because the stylized disruption patterns map onto real-world crisis profiles (peaks correspond to sudden-onset events such as flash floods, regime shifts to structural changes such as prolonged conflict or earthquake aftermath), the maladaptation profiles can inform technology selection for the type of crisis an organization is most likely to face. An information technology that exhibits broad maladaptation under a given disruption pattern should be avoided under that pattern, regardless of how disruptions are timed. A technology with conditional maladaptation can be deployed with greater confidence outside its identified maladaptation duration

windows. However, specific implementations, such as a particular drone system or blockchain platform, may differ from the stylized portfolios modeled here and would benefit from dedicated analysis.

Understanding how information technologies help, but also when and why they hurt, is a necessary condition for implementing them effectively in crisis-response supply chains. This study provides a first step toward that understanding.

CRediT authorship contribution statement

Yvonne Lont: Writing – original draft, Software, Methodology, Conceptualization. **Patrick Steinmann:** Writing – original draft, Visualization, Validation, Supervision, Methodology, Formal analysis, Conceptualization. **Jan Kwakkel:** Validation, Supervision, Software, Methodology, Conceptualization. **Tina Comes:** Writing – review & editing, Supervision, Methodology, Conceptualization.

Use of AI

Claude (Anthropic) and Copilot were used to assist with debugging and refactoring analysis code. After using these tools, the author reviewed, edited, and validated all content and code as needed. The authors take full responsibility for the final publication.

Funding

This research was supported by the Netherlands Ministry of Defence.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Yvonne Lont reports financial support was provided by the Netherlands Ministry of Defense. The other authors declare that they have no competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The authors are grateful to the employees of the Netherlands Ministry of Defence who provided insights on their processes and behavior, and whose involvement informed both the model design and the face validation of the findings. We also thank the practitioners in crisis response who shared their judgments on the plausibility of our findings. Any remaining errors are the responsibility of the authors.

Appendix A. - Operationalization of the information technologies — details

This subsection describes the details of the operationalization per technology

Artificial intelligence-drones. In our model, we operationalize the contribution of *Artificial Intelligence-drones* as a coverage effect. The coverage, is operationalized by the fraction of responsibility areas for which operational managers have direct state visibility (proxy: higher *span*), increasing the availability of timely local observations. Span increases from 2 to 4, the smallest valid step-change given the model's hierarchical structure and algorithm. Vertical and horizontal delays, as well as information-sharing barriers, are held constant because drone (sensing) technologies do not inherently alter reporting structures [28]. Drones do not change decision rules.

Artificial intelligence-intake standardization. In our model, we define *Artificial Intelligence-intake* as an enrichment function at the point of observation (*collect/process*) that automatically converts incoming updates into a structured signal. In the model, this conversion is represented as a reduction in horizontal and vertical delay: when signals arrive already structured, the coordination cycle at team meetings is shorter. The standardization reduces vertical delay by faster interpretation of the responsibility area states. A single-step reduction reflects partial improvement. This reduction is relative to the real-time Common Operational Picture in which we assume a full elimination of the vertical delay.

Prediction-enhanced common operational picture. In our model, we define *Prediction-enhanced COP* as a shared real-time dashboard enhanced with automated predictive highlighting. In the model, a COP affects two parameters. First, it reduces vertical delay: managers have current situational assessments. Vertical delay reduces to zero, reflecting real-time situational awareness. Second, a Prediction-enhanced COP earlier detects threats. We model this by reducing the memory length managers use as a performance window to evaluate shortfall rates. Length_memory shortens from 10 to 5, representing a halving of the baseline, which is a natural midpoint choice. As a result, the escalation trigger responds more quickly to recent disruptions. The team meeting cadence and information-sharing barriers remain unchanged.

Blockchain-traceability. In our model, we define blockchain not as a ledger technology itself. Instead, we translate the benefits and barriers to the model parameters. We define *Blockchain-traceability* as an implementation in which a permissioned shared ledger is broadly accessible to relevant operational actors and used as a trusted reference, such that *store* and *verify* improve cross-echelon visibility and confidence in shared information. These improvements imply that observations of states become less stale because higher echelons can consult the same operational updates (we assume here a reporting layer as part of the blockchain system). Thus, vertical delay decreases by a single step. Beyond vertical delays, peer-to-peer information sharing is more likely, as traceability increases trust in requests and offers. Thus, the barrier to sharing decreases by 0.25, reflecting increased trust without removing the barrier entirely. Because this implementation does not assume smart-contract automation of reallocations, it does not alter the team-meeting cadence of cross-manager reallocations and thus leaves horizontal delay unchanged.

Blockchain-compliance. We define *Blockchain-compliance* as an implementation in which participation and access are restrictive, intermediated, or segmented, and in which additional procedural steps are required before updates become broadly usable. The restricted access conditions reverse the practical benefits of *store* and *verify* in three ways. First, information becomes less broadly usable across levels (increasing the staleness of the inputs for higher echelons). Vertical delay increases by one step, from 2 to 3. Second, *sharing* becomes less likely because posting and accepting information is conditional on governance, privacy, and capability constraints. In addition, ledger-based verification can introduce additional verification steps before updates are usable [5,49]. Because our model does not represent such verification effort as an explicit time-consuming activity, we proxy these additional steps as a longer peer-coordination cycle. Thus, horizontal delay increases by one step, from 2 to 3. We emphasize that these settings are proxies consistent with the current evidence base rather than claims of deterministic effects in practice [5,50].

Satellite internet. In our model, we proxy the effect of *Satellite internet* by assuming that it expands coverage by extending the reach of direct communication [29]. In the model, this is represented as an increase in span. Span increases from 2 to 4, the smallest valid step-change given the model's hierarchical structure and algorithm. In addition, satellite internet connectivity reduces vertical delay by improving the reliability and speed of cross-echelon reporting. Horizontal coordination cadence and information-sharing barriers remain unchanged.

Appendix B. - Additional figures

B.1. Sequential configuration — the reliability range per technology

Fig. 7 shows how various technologies affect the system's reliability vis-à-vis the baseline under two different disruption patterns. For both disruption patterns, the baseline is shown in gray in the topmost row, with dashed vertical lines extending downwards to aid comparison. For each considered technology, the reliability (expressed as the 20–80 quantile range) is shown for both disruption patterns. It is evident that, for some technologies such as *Prediction-enhanced Common Operational Picture (COP)* or *Artificial Intelligence (AI)-enabled drones*, a wide gap emerges between the reliabilities under the two different disruption patterns, indicating the usefulness of these technologies (at least in terms of reliability) is conditional on the experienced disruption. Furthermore, certain technologies (e.g., *Blockchain-traceability* experiencing a Peaks-type disruption) do not or only barely improve reliability compared to the baseline, raising questions about their suitability and effectiveness.

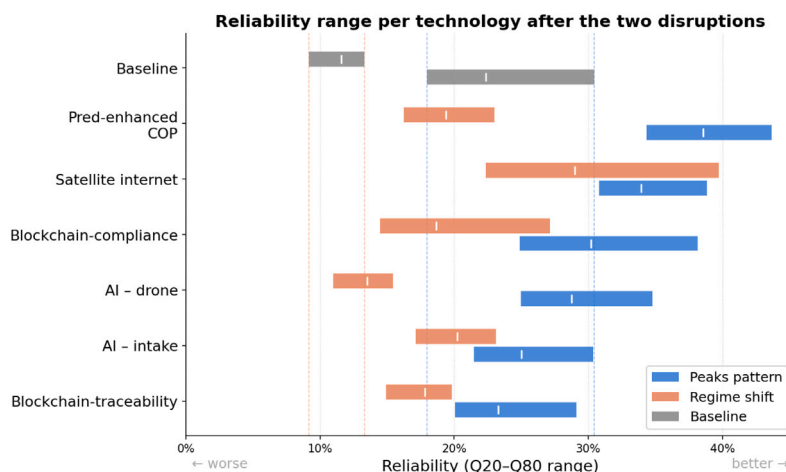


Fig. 7. Sequential configuration — The reliability range (20–80 quantile) per technology.

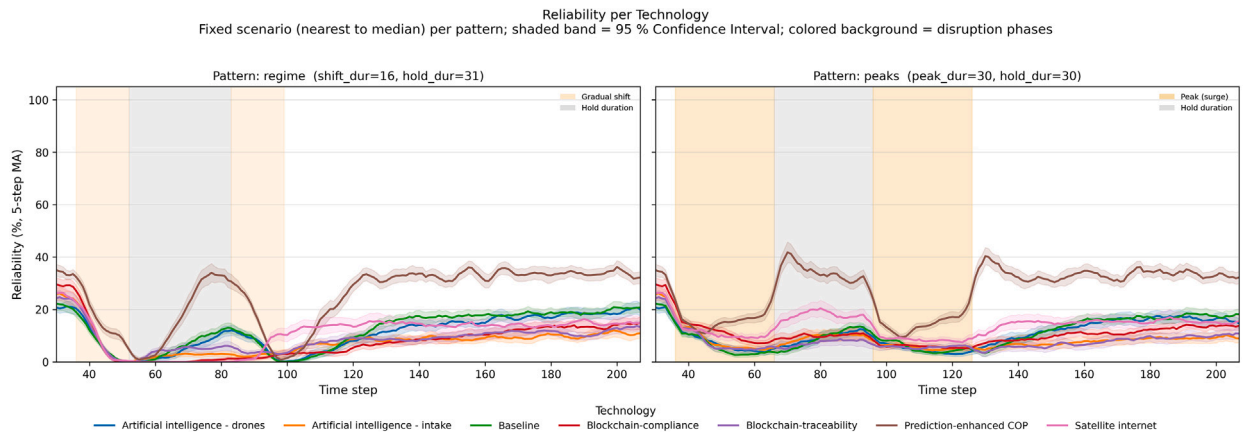


Fig. 8. Reliability time series per information technology for representative scenarios in the convergent configuration: (a) regime-shift pattern, (b) peaks pattern.

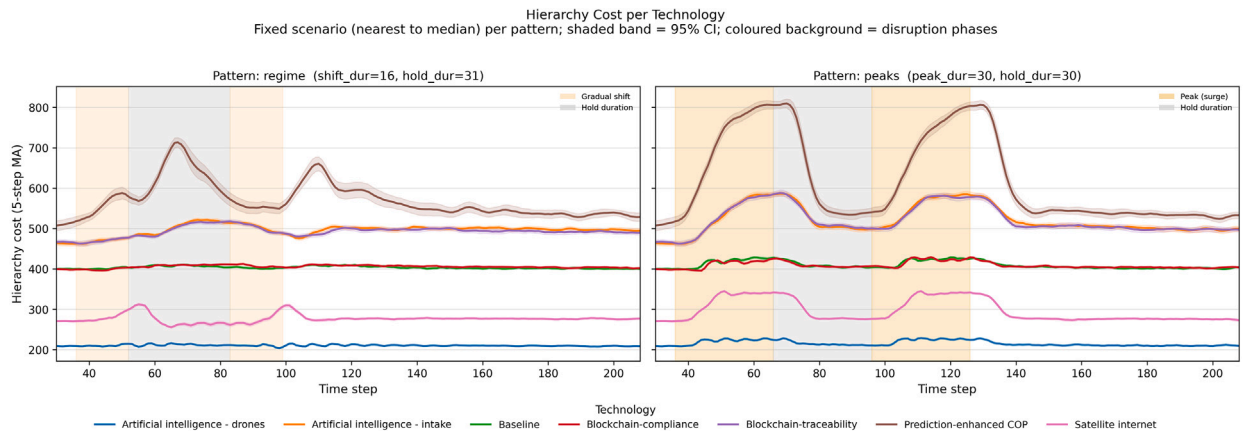


Fig. 9. Hierarchical cost time series per information technology for representative scenarios in the convergent configuration: (a) regime-shift pattern, (b) peaks pattern.

B.2. Time-series analysis — technology effects over time for the convergent configuration

Figs. 8 and 9 show the reliability and hierarchy cost per technology for the convergent configuration. The overall impression is consistent with the sequential configuration presented in Section 7. We observe that the ordering of technologies is preserved across both disruption patterns and the initial reliability also declines. Two quantitative differences are worth noting. First, absolute reliability levels are lower throughout in the convergent configuration: pre-disruption reliability starts around 20%–35% compared to around 60% in the sequential condition, and post-disruption recovery reaches at most 30%–35% for the information technologies. Second, hierarchical escalation is more pronounced in the convergent configuration: the Prediction-enhanced COP hierarchy cost peaks around 700–800, compared to approximately 530–570 euros in the sequential condition. These differences suggest that a convergent configuration triggers stronger hierarchical escalation while simultaneously leads to lower reliability. Therefore, these differences point to a less efficient system response under this condition. Despite these quantitative differences, the technology-level conclusions are unchanged. Prediction-enhanced COP consistently leads to the highest hierarchy cost and highest reliability; Artificial Intelligence-drone has the lowest hierarchy cost and does not escalate.

Appendix C. - Overview of parameter tables

See Tables 8–11.

Table 8

Event priorities used by the simulation scheduler (higher value is earlier execution of the event).

Event type	Method name	Priority	Notes
Manager events	manager_step	3	Reallocation, posting, (de)-escalation
Team Meeting	meeting	1	Executes finally, after all other activities that are scheduled at the same time
Worker state check	worker_step	4	Runs after any high-priority events (helper function)
Supply need generation	exit_source, enter_output_node	10	Generator forwards Supply needs promptly
Pattern engine	enter_output_node, exit_output_node	10	Routes batches promptly
Queue timeout	exit_from_queue	1	Timeouts executed after other scheduled events at the same time
Start Worker processing	start_at_area	10	Runs immediately after a Team Meeting or when no Team Meeting occurs after Manager events
All other events	(unset)	5	Simulation engine default

Table 9

Team Meeting parameters of the model.

Parameter	Description	Value	Reference
meeting_interval	the interval between team meetings	varies	this study
horizontal_delay	meeting_interval - 1, delay between inter-manager coordination moments	varies	this study

Table 10

Manager parameters of the model.

Parameter	Description	Value	Reference
T_max	when the shortfall rate exceeds the T_max threshold, the Manager will demand for worker(s)	see 'threshold'	Epstein [89]
T_min	when the shortfall rate is lower than T_min, the Manager will supply worker(s)	see 'threshold'	Epstein [89]
threshold	threshold[Manager_echelon]	[0.7, 1.4, 2, 4, 10]	Epstein [89]
length_memory	the number of time steps a Manager uses to calculate their shortfall rate	10	Epstein [89]
upward_inertia	Determines the number of time steps the maximum Threshold (T_max) must be met or exceeded before the Manager reverts their decision rights to a higher management echelon	3	Wu et al. [101]
downward_inertia	Determines how many time steps the minimum Threshold (T_min) has not been met before the Manager reverts their decision rights to their subordinates	3	Wu et al. [101]
barrier_ask_labor	probability barrier to announcing a demand for labor (sharing probability = 1 - barrier)	varies	Epstein [89]
barrier_give_labor	probability barrier to announcing a surplus of labor (sharing probability = 1 - barrier)	varies	Epstein [89]
vertical_delay	the delay time of the information between Manager echelons	varies	

Table 11

Responsibility area parameters of the model.

Parameter	Description	Value	Reference
processing time	The Responsibility area takes this duration to process a supply need, Set to 1 so that observed performance differences reflect coordination dynamics instead of processing delays.	1	this study
maximum accepted delay	the maximum time a Supply Need is in the queue of the Responsibility area before it is removed. This time is slightly higher than the Manager step, to avoid race conditions	1.05	this study

Table 12
PRIM algorithm settings.

Parameter	Value	Description
peel_alpha	0.05	Fraction of cases removed per peeling step
paste_alpha	0.05	Fraction of cases restored per pasting step
mass_min	0.05	Minimum fraction of all cases the box must contain
threshold	0.80	Minimum density required for box selection

Table 13

PRIM diagnostics for the resilience loss metric: selected box per information technology, sequential configuration. Coverage, density, mass, and res_dim are reported for the selected box on the peeling trajectory. Boxes classified as non-discriminating in the main results are included here for completeness; their diagnostics (e.g., res_dim = 0, mass = 1.00) confirm the absence of any restricting sub-region. See [Table 4](#).

Regime-shift pattern					
Technology	n_{mal}	Coverage	Density	Mass	res_dim
Baseline	—	—			
Artificial intelligence – drones	26	1.00	0.05	1.00	0
Artificial intelligence – intake	30	1.00	0.06	1.00	0
Blockchain-compliance	66	0.38	0.96	0.05	2
Blockchain-traceability	47	0.77	0.82	0.09	2
Prediction-enhanced COP	0	—			
Satellite internet	0	—			
Peak pattern					
Technology	n_{mal}	Coverage	Density	Mass	res_dim
Baseline	—	—			
Artificial intelligence – drones	0	—			
Artificial intelligence – intake	81	1.00	0.16	1.00	0
Blockchain-compliance	0	—			
Blockchain-traceability	121	0.75	0.83	0.22	2
Prediction-enhanced COP	0	—			
Satellite internet	0	—			

Appendix D. - PRIM configuration and diagnostics

[Table 12](#) reports the algorithm settings used in all scenario discovery analyses, following the approach of Kwakkel et al. [80]. The selected box corresponds to the last non-empty entry in the peeling trajectory returned by `find_box()`. When no box on the trajectory reaches the density threshold, the last non-empty box spans the full sampled range and is therefore classified as non-discriminating. Coverage, density, mass, and res_dim are reported following ter Horst et al. [102]. A box is classified as non-discriminating when all dimensions span at least 99.9% of their sampled range. Thus, non-discrimination indicates that PRIM found no meaningful concentration of maladaptive cases. Such boxes have res_dim = 0 and mass = 1.00. The 20% quantile threshold for the internal maladaptation indicator is motivated in [Section 6](#).

D.1. Resilience loss metric

[Tables 13](#) and [14](#) report the values of the algorithm settings for the resilience loss metric for the selected box per technology and disruption pattern.

D.2. Cross-disruption indicator

[Tables 15](#) and [16](#) report the values of the algorithm settings for the cross-disruption indicator for the selected box per technology and disruption pattern. [Tables 17](#) and [18](#) report the 80th-percentile deterioration value and the fraction of target cases with $\Delta R > 0$ for each pattern–technology group in the sequential configuration. The same pattern holds for the convergent configuration. A sensitivity analysis across thresholds of 10%, 15%, 20%, and 25% confirms that the results are stable across almost all tested values. The underlying analysis is provided in the Supplementary material.

Table 14

PRIM diagnostics for the resilience loss metric: selected box per information technology, convergent configuration. Coverage, density, mass, and res_dim are reported for the selected box on the peeling trajectory. Boxes classified as non-discriminating in the main results are included here for completeness; their diagnostics (e.g., res_dim = 0, mass = 1.00) confirm the absence of any restricting sub-region. See Table 6.

Regime-shift pattern					
Technology	n_{mal}	Coverage	Density	Mass	res_dim
<i>Baseline</i>	–	—			
Artificial intelligence – drones	350	0.72	0.84	0.60	2
Artificial intelligence – intake	496	1.00	0.99	1.00	0
Blockchain-compliance	427	0.64	1.00	0.55	2
Blockchain-traceability	491	1.00	0.98	1.00	0
Prediction-enhanced COP	0	—			
Satellite internet	274	0.49	1.00	0.27	2
Peak pattern					
Technology	n_{mal}	Coverage	Density	Mass	res_dim
<i>Baseline</i>	–	—			
Artificial intelligence – drones	104	1.00	0.21	1.00	0
Artificial intelligence – intake	491	1.00	0.98	1.00	0
Blockchain-compliance	135	0.44	0.97	0.12	1
Blockchain-traceability	499	1.00	1.00	1.00	0
Prediction-enhanced COP	0	—			
Satellite internet	0	—			

Table 15

PRIM diagnostics for the cross-disruption indicator: selected box per information technology - sequential configuration.

Regime-shift pattern					
Technology	n_{mal}	Coverage	Density	Mass	res_dim
<i>Baseline</i>	–	—			
Artificial intelligence – drones	100	1.00	0.20	1.00	0
Artificial intelligence – intake	100	1.00	0.20	1.00	0
Blockchain-compliance	100	1.00	0.20	1.00	0
Blockchain-traceability	100	1.00	0.20	1.00	0
Prediction-enhanced COP	100	0.29	0.97	0.06	2
Satellite internet	100	0.82	0.82	0.20	1
Peak pattern					
Technology	n_{mal}	Coverage	Density	Mass	res_dim
<i>Baseline</i>	–	—			
Artificial intelligence – drones	100	1.00	0.20	1.00	0
Artificial intelligence – intake	100	1.00	0.20	1.00	0
Blockchain-compliance	100	1.00	0.20	1.00	0
Blockchain-traceability	101	1.00	0.20	1.00	0
Prediction-enhanced COP	100	1.00	0.20	1.00	0
Satellite internet	100	1.00	0.20	1.00	0

Appendix E. - Sensitivity analysis

E.1. Sensitivity to capacity (nr of workers)

This subsection provides the per-configuration results underlying the capacity sensitivity reported in the main text. Each cell in Tables 19 and 20 reports two numbers for a given combination of a technology, disruption pattern, and number of workers. The first is the mean resilience-loss difference relative to the baseline organization facing the identical scenario, expressed in reliability percentage-points. A positive value means the technology performs worse than the baseline (maladaptive), and a negative

Table 16

PRIM diagnostics for the cross-disruption indicator, selected box per information technology - convergent configuration.

Technology	Regime-shift pattern		Density	Mass	res_dim
	n_{mal}	Coverage			
<i>Baseline</i>	–	—			
Artificial intelligence – drones	100	1.00	0.20	1.00	0
Artificial intelligence – intake	100	1.00	0.20	1.00	0
Blockchain-compliance	100	1.00	0.20	1.00	0
Blockchain-traceability	100	1.00	0.20	1.00	0
Prediction-enhanced COP	100	0.47	0.90	0.10	2
Satellite internet	100	1.00	0.20	1.00	0

Technology	Peak pattern		Density	Mass	res_dim
	n_{mal}	Coverage			
<i>Baseline</i>	–	—			
Artificial intelligence – drones	100	1.00	0.20	1.00	0
Artificial intelligence – intake	100	1.00	0.20	1.00	0
Blockchain-compliance	100	1.00	0.20	1.00	0
Blockchain-traceability	101	1.00	0.20	1.00	0
Prediction-enhanced COP	100	1.00	0.20	1.00	0
Satellite internet	100	1.00	0.20	1.00	0

Table 17

Cross-disruption indicator: target classification per pattern and technology group. n : number of experiments per group. Deterioration (p_{80}): the 80th-percentile ΔR value that defines the top-20% target class; a positive value indicates that the within-group criterion selects cases of cross-disruption deterioration. $\Delta R > 0$ (%): percentage of the top-20% target cases with strictly positive ΔR . Sequential configuration.

Technology	Regime-shift pattern		$\Delta R > 0$ (%)
	n	Deterioration (p_{80})	
<i>Baseline</i>	500	−0.088	0
Artificial intelligence – drones	500	−0.093	0
Artificial intelligence – intake	500	−0.229	0
Blockchain-compliance	500	−0.215	0
Blockchain-traceability	500	−0.171	0
Prediction-enhanced COP	500	−0.142	0
Satellite internet	500	−0.313	0

Technology	Peak pattern		$\Delta R > 0$ (%)
	n	Deterioration (p_{80})	
<i>Baseline</i>	500	+0.022	100
Artificial intelligence – drones	500	+0.015	100
Artificial intelligence – intake	500	+0.087	100
Blockchain-compliance	500	+0.085	100
Blockchain-traceability	500	+0.084	100
Prediction-enhanced COP	500	+0.029	100
Satellite internet	500	+0.061	100

value means it performs better. The second value in parentheses is the share of sampled configurations in that cell that are flagged maladaptive. Columns vary the number of workers around the value of 8 used in the main experiments, thus varying the demand-capacity ratio.

From Tables 19 and 20, two patterns emerge. First, maladaptation is only weakly sensitive to capacity: within each row the maladaptive share shifts modestly as workers move from 6 to 10. In addition, for several technologies, maladaptation changes little. Capacity is therefore not the primary driver of the resilience loss. Second, at any fixed number of workers the technologies diverge. For example, in the convergent configuration, the maladaptive share spans the full 0%–100% range at every capacity level. Since this divergence occurs while capacity is held constant, it cannot be a capacity effect.

Table 18

Cross-disruption indicator: target classification per pattern and technology group. n : number of experiments per group. Deterioration (p_{80}): the 80th-percentile ΔR value that defines the top-20% target class; a positive value indicates that the within-group criterion selects cases of cross-disruption deterioration. $\Delta R > 0$ (%): percentage of the top-20% target cases with strictly positive ΔR . Convergent configuration.

Technology	Regime-shift pattern		
	n	Deterioration (p_{80})	$\Delta R > 0$ (%)
Baseline	500	+0.002	100
Artificial intelligence – drones	500	+0.007	100
Artificial intelligence – intake	500	−0.049	100
Blockchain-compliance	500	−0.035	0
Blockchain-traceability	500	−0.025	0
Prediction-enhanced COP	500	−0.014	21
Satellite internet	500	−0.103	0

Technology	Peak pattern		
	n	Deterioration (p_{80})	$\Delta R > 0$ (%)
Baseline	500	+0.007	100
Artificial intelligence – drones	500	+0.007	100
Artificial intelligence – intake	500	+0.031	100
Blockchain-compliance	500	+0.038	100
Blockchain-traceability	500	+0.023	100
Prediction-enhanced COP	500	+0.013	100
Satellite internet	500	+0.034	100

Table 19

Capacity sensitivity of maladaptation (sequential configuration, $n = 500$ per cell). Each cell reports the mean resilience-loss difference versus the same-scenario baseline (reliability percentage-points; positive = maladaptive), with the share of sampled configurations flagged maladaptive in parentheses. Columns vary the number of workers, i.e. the demand–capacity ratio, around the value of 8 used in the main experiments.

Pattern	Technology	Workers (demand–capacity ratio)		
		6	8	10
Regime	Artificial intelligence – drones	−1.4 (3%)	−1.7 (5%)	−2.1 (6%)
	Artificial intelligence – intake	−1.9 (7%)	−3.7 (6%)	−4.9 (9%)
	Blockchain-compliance	−2.6 (20%)	−4.0 (13%)	−6.0 (5%)
	Blockchain-traceability	−1.8 (8%)	−2.6 (9%)	−3.5 (12%)
	Prediction-enhanced COP	−6.8 (0%)	−8.2 (0%)	−8.0 (0%)
	Satellite internet	−6.5 (0%)	−10.1 (0%)	−10.8 (2%)
Peaks	Artificial intelligence – drones	−7.0 (0%)	−5.2 (0%)	−2.3 (12%)
	Artificial intelligence – intake	−1.9 (7%)	−2.7 (16%)	+0.2 (41%)
	Blockchain-compliance	−7.0 (0%)	−8.8 (0%)	−11.4 (0%)
	Blockchain-traceability	+1.1 (86%)	−1.2 (24%)	+1.8 (63%)
	Prediction-enhanced COP	−7.1 (0%)	−15.1 (0%)	−14.8 (0%)
	Satellite internet	−11.9 (0%)	−11.5 (0%)	−5.2 (1%)

E.2. Sensitivity to technology parameters

This subsection provides the per-configuration results underlying the sensitivity to technology parameters reported in the main text. To assess the relative influence of the technology parameters, we computed feature importances. These importance values were calculated by random-forest regression (500 trees), using the EMA Workbench [81]. The regression scores each parameter against the resilience-loss difference from the same-scenario baseline. This baseline serves as the continuous target, so that higher scores identify the parameters governing the magnitude of departure from it. Random forest scores parameter importance directly on the existing Latin hypercube sample. Our analysis reuses the existing primary sample because the technology parameters were already varied across their ranges (e.g., *vertical delay* from 0 to 3). Fig. 10 reports the resulting values. Higher values indicate that the parameters governing the magnitude of the deviation from the baseline are more influential.

To assess the robustness of the maladaptation profiles, each technology's defining parameters were varied one at a time. For each variant, the maladaptation profile type (e.g., conditional) was determined using the same procedure as the main analysis. The robustness fraction reported in Tables 22 and 23 indicates how many variants, including the original specification, resulted in the same profile type as the original. The parameter settings are presented in Table 21.

For the sequential configuration, the profile type was preserved in the majority of technology–pattern combinations. Counting each technology–pattern cell as stable when the original profile type recurred in at least half of its parameter variants, 9 of the

Table 20

Capacity sensitivity of maladaptation (convergent configuration, $n = 300$ per cell). Each cell reports the mean resilience-loss difference versus the same-scenario baseline (reliability percentage-points; positive = maladaptive), with the share of sampled configurations flagged maladaptive in parentheses. Columns vary the number of workers, i.e. the demand–capacity ratio, around the value of 8 used in the main experiments.

Pattern	Technology	Workers (demand–capacity ratio)		
		6	8	10
Regime	Artificial intelligence – drones	+0.2 (71%)	+0.2 (70%)	−0.2 (40%)
	Artificial intelligence – intake	+1.4 (100%)	+2.1 (100%)	+2.6 (98%)
	Blockchain-compliance	+1.7 (86%)	+2.6 (85%)	+2.5 (72%)
	Blockchain-traceability	+0.8 (98%)	+1.6 (99%)	+2.3 (98%)
	Prediction-enhanced COP	−10.6 (0%)	−12.3 (0%)	−14.4 (0%)
	Satellite internet	+0.7 (77%)	−0.1 (51%)	−0.0 (49%)
Peaks	Artificial intelligence – drones	−0.8 (0%)	−0.4 (25%)	−1.4 (10%)
	Artificial intelligence – intake	+0.5 (82%)	+1.3 (98%)	+3.6 (100%)
	Blockchain-compliance	−1.5 (7%)	−1.5 (29%)	−3.6 (9%)
	Blockchain-traceability	+0.8 (95%)	+1.7 (100%)	+4.2 (100%)
	Prediction-enhanced COP	−12.9 (0%)	−16.1 (0%)	−15.3 (0%)
	Satellite internet	−4.0 (0%)	−4.2 (0%)	−2.4 (7%)

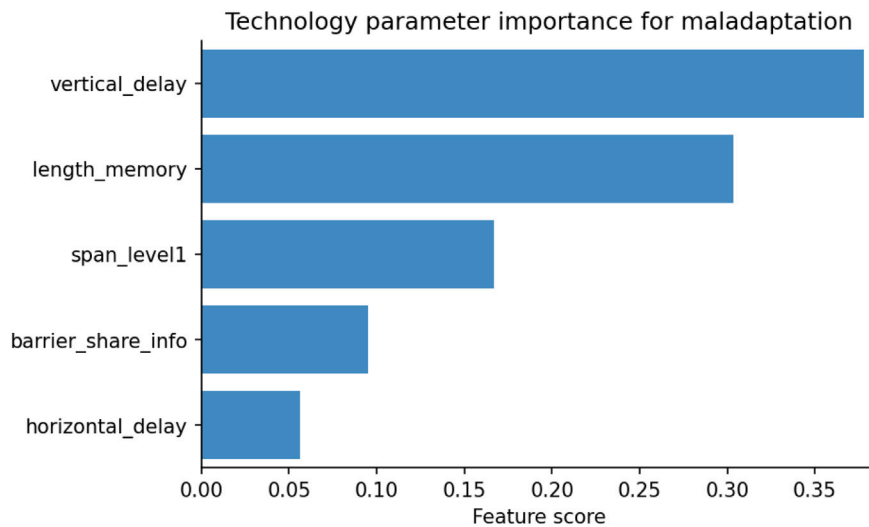


Fig. 10. Technology-parameter importance for maladaptation, from random-forest regression (500 trees) on the resilience-loss difference from the baseline.

12 cells were stable. Stability was strongest for Satellite internet, the only technology robust under both patterns (2/2 peaks, 2/2 regime), and for Prediction-enhanced COP (3/3 peaks) and Blockchain-compliance (4/4 peaks, 3/4 regime). The least stable were AI-intake under peaks (1/4) and Blockchain-traceability under both patterns (1/2 peaks, 1/2 regime), where small parameter changes flipped the profile between conditional, broad, and none. For the convergent configuration, stability was lower, consistent with the greater sensitivity of convergent chains to the information-technology parameters reported in the main findings. Where profiles were unstable, parameter variations shifted maladaptation between conditional maladaptation, broad maladaptation (without discriminating conditions), and no maladaptation.

E.3. Sensitivity to alternative baseline organizations

We conducted a sensitivity analysis on alternative baseline organizations. We assessed whether the maladaptation profiles depend on the specific baseline organization we assumed. We therefore reran the experiments with the baseline barrier_share_info raised from 0.50 to 0.75. The higher barrier value represents a baseline organization with substantially more friction in sharing information. We then re-derived each technology's barrier value under this higher baseline. For technologies whose defining parameters did not include the barrier, the new baseline value also became 0.75. For technologies whose defining parameters included the barrier, the original shift relative to the baseline was preserved. This shift places Blockchain-traceability at 0.50. For Blockchain-compliance, preserving the original +0.25 shift would have placed the barrier at 1.0, the extreme value at which information sharing at the same horizontal level is entirely blocked. Therefore, the shift was reduced to +0.20, placing the barrier at 0.95 and avoiding the boundary case. We re-applied the same PRIM analysis, using the identical maladaptation resilience loss criterion ($\Delta Loss_{vs_Baseline} > 0$).

Table 21

Technology parameter portfolios used in the one-at-a-time (OAT) robustness analysis, sequential configuration. Each group lists the original specification first, followed by its single-parameter perturbations. The perturbed parameter is highlighted in bold. Values are read directly from `run_config.yaml`: barrier=barrier_ask_labor, barrier_give_labor; hdelay=horizontal_delay, vdelay=vertical_delay; mem=length_memory; span=span_level1.

Technology (variant)	barrier	hdelay	mem	span	vdelay
<i>Baseline</i>					
Baseline	0.50	2	10	2	2
<i>AI-intake</i> (vary hdelay, vdelay)					
AI-intake (original)	0.50	1	10	2	1
perturbed hdelay=0	0.50	0	10	2	1
perturbed hdelay=2	0.50	2	10	2	1
perturbed vdelay=2	0.50	1	10	2	2
<i>AI-drones</i> (vary span)					
AI-drones (original)	0.50	2	10	4	2
perturbed span=8	0.50	2	10	8	2
perturbed span=16	0.50	2	10	16	2
<i>Satellite internet</i> (vary span)					
Satellite internet (original)	0.50	2	10	4	1
perturbed span=8	0.50	2	10	8	1
perturbed span=16	0.50	2	10	16	1
<i>Blockchain-traceability</i> (vary barrier)					
Blockchain-traceability (original)	0.25	2	10	2	1
perturbed barrier=0.40	0.40	2	10	2	1
<i>Blockchain-compliance</i> (vary hdelay, vdelay, barrier)					
Blockchain-compliance (original)	0.75	3	10	2	3
perturbed hdelay=4	0.75	4	10	2	3
perturbed vdelay=4	0.75	3	10	2	4
perturbed barrier=0.95	0.95	3	10	2	3
<i>Prediction-enhanced COP</i> (vary vdelay, mem)					
Prediction-enhanced COP (original)	0.50	2	5	2	0
perturbed vdelay=1	0.50	2	5	2	1
perturbed length_memory=7	0.50	2	7	2	0

Table 22

Robustness fractions for the sequential configuration. Fractions indicate the number of parameter variants (including the original specification) for which the maladaptation profile type matched the original, out of the total number of variants tested. Profile labels: *none* = no maladaptation detected; *broad* = maladaptation with no discriminating conditions; *conditional* = maladaptation specific for restricted durations.

Technology	Peaks		Regime shift	
	Fraction	Profiles	Fraction	Profiles
AI-intake	1/4	broad, conditional, none	3/4	broad, conditional
Blockchain-traceability	1/2	conditional, none	1/2	broad, conditional
Prediction-enhanced COP	3/3	none	2/3	broad, none
Blockchain-compliance	4/4	none	3/4	conditional, none
Satellite internet	2/2	none	2/2	none
AI-drones	3/3	none	2/3	broad, none

Table 23

Robustness fractions for the convergent configuration. Fractions indicate the number of parameter variants (including the original specification) for which the maladaptation profile type matched the original, out of the total number of variants tested. Profile labels: *none* = no maladaptation detected; *broad* = maladaptation with no discriminating conditions; *conditional* = maladaptation specific for restricted durations.

Technology	Peaks		Regime shift	
	Fraction	Profiles	Fraction	Profiles
AI-intake	4/4	broad	2/4	broad, conditional
Blockchain-traceability	1/2	broad, conditional	1/2	broad, conditional
Prediction-enhanced COP	2/3	broad, none	2/3	conditional, none
Blockchain-compliance	1/4	broad, conditional, none	3/4	conditional, none
Satellite internet	3/3	none	2/3	conditional, none
AI-drones	1/3	broad, none	2/3	conditional, none

and the same classification into broad, conditional, and no maladaptation profiles. We then compared the resulting profiles against those from the original baseline (see [Tables 24](#) and [25](#)).

Table 24

Sensitivity of maladaptation findings to the baseline information-sharing barrier (sequential configuration). Fractions indicate the number of barrier variants (including the main body specification at barrier = 0.5) for which the maladaptation profile type matched the main body profile, out of 2 variants tested. Profile labels: *robust* = no maladaptation detected; *broad* = maladaptation with no discriminating conditions; *conditional* = maladaptation within a specific disruption-parameter region.

Technology	Peaks		Regime shift	
	Fraction	Profiles	Fraction	Profiles
AI-drones	1/2	broad, robust	2/2	broad
AI-intake	1/2	broad, robust	2/2	broad
Blockchain-compliance	2/2	robust	1/2	conditional, robust
Blockchain-traceability	2/2	conditional	2/2	conditional
Prediction-enhanced COP	2/2	robust	1/2	conditional, robust
Satellite internet	2/2	robust	2/2	robust

Table 25

Sensitivity of maladaptation findings to the baseline information-sharing barrier (convergent configuration). Fractions indicate the number of barrier variants (including the main body specification at barrier = 0.5) for which the maladaptation profile type matched the main body profile, out of 2 variants tested. Profile labels: *robust* = no maladaptation detected; *broad* = maladaptation with no discriminating conditions; *conditional* = maladaptation within a specific disruption-parameter region.

Technology	Peaks		Regime shift	
	Fraction	Profiles	Fraction	Profiles
AI-drones	1/2	broad, robust	1/2	broad, conditional
AI-intake	1/2	broad, robust	1/2	broad, robust
Blockchain-compliance	1/2	conditional, robust	1/2	conditional, robust
Blockchain-traceability	2/2	broad	1/2	broad, conditional
Prediction-enhanced COP	2/2	robust	2/2	robust
Satellite internet	2/2	robust	1/2	conditional, robust

Across both configurations, 12 of 24 technology–pattern combinations retain the same maladaptation profile when the baseline barrier is raised from 0.50 to 0.75. Stability differs between configurations. The sequential configuration preserves 8 of 12 technology-disruption pattern combinations, whereas the convergent configuration preserves only 4 of 12 combinations. Peaks and regime-shift patterns have 7 and 5 of 12 combinations unchanged. Prediction-enhanced COP, Blockchain-traceability, and Satellite internet are the most robust technologies (3 of 4 combinations show the same maladaptation profile). These results indicate that the main body findings are partially sensitive to the baseline information-sharing barrier.

E.4. Summary

The results from these three sensitivity analyses show that the results are partially condition-dependent. This condition-dependence is itself a finding that information technology has no fixed value in crisis-response supply chains. That value depends on the crisis's disruption pattern. An earthquake, a wildfire, and a flood each impose a different pattern. The value of the technology is therefore tied to the pattern of crisis it meets.

Appendix F. Supplementary data

Supplementary material related to this article can be found online at <https://doi.org/10.1016/j.ijdr.2026.106342>.

Data availability

The model code and analysis notebooks are available at: <https://doi.org/10.4121/5676067d-e852-4bf8-a346-0dac8379a9bd>.

References

- [1] S. Bag, M.S. Rahman, G. Srivastava, M. Giannakis, C. Foropon, Data-driven digital transformation and the implications for antifragility in the humanitarian supply chain, *Int. J. Prod. Econ.* 266 (2023) 109059, <http://dx.doi.org/10.1016/j.ijpe.2023.109059>.
- [2] N. Altay, G. Heaslip, G. Kovács, K. Spens, P. Tatham, A. Vaillancourt, Innovation in humanitarian logistics and supply chain management: a systematic review, *Ann. Oper. Res.* 335 (3) (2024) 965–987, <http://dx.doi.org/10.1007/s10479-023-05208-6>.
- [3] R. Dubey, D.J. Bryde, Y.K. Dwivedi, G. Graham, C. Foropon, Impact of artificial intelligence-driven big data analytics culture on agility and resilience in humanitarian supply chain: a practice-based view, *Int. J. Prod. Econ.* 250 (2022) 108618, <http://dx.doi.org/10.1016/j.ijpe.2022.108618>.
- [4] S. Lythreathis, F. Acikgoz, N. Yassine, Artificial intelligence in humanitarian aid: A review and future research agenda, *Technovation* 151 (2026) 103415, <http://dx.doi.org/10.1016/j.technovation.2025.103415>.

- [5] K. Hunt, A. Narayanan, J. Zhuang, Blockchain in humanitarian operations management: A review of research and practice, *Socio-Econ. Plan. Sci.* 80 (2022) 101175, <http://dx.doi.org/10.1016/j.seps.2021.101175>.
- [6] G.H. Hwang, W.C. Yoon, A new approach to requirement development for a common operational picture to support distributed situation awareness, *Saf. Sci.* 125 (2020) 104569, <http://dx.doi.org/10.1016/j.ssci.2019.104569>.
- [7] D. Fischer-Prefßler, D. Bonaretti, D. Bunker, Digital transformation in disaster management: A literature review, *J. Strat. Inf. Syst.* 33 (4) (2024) 101865, <http://dx.doi.org/10.1016/j.jsis.2024.101865>.
- [8] J.R. Galbraith, Organization design: An information processing view, *Interfaces* 4 (3) (1974) 28–36, <http://dx.doi.org/10.1287/inte.4.3.28>.
- [9] T. Comes, B. Van de Walle, L. Van Wassenhove, The coordination-information bubble in humanitarian response: Theoretical foundations and empirical investigations, *Prod. Oper. Manage.* 29 (11) (2020) 2484–2507, <http://dx.doi.org/10.1111/poms.13236>.
- [10] E. Brynjolfsson, D. Rock, C. Syverson, Artificial intelligence and the modern productivity paradox: A clash of expectations and statistics, in: A. Agrawal, J. Gans, A. Goldfarb (Eds.), *The Economics of Artificial Intelligence: An Agenda*, University of Chicago Press, 2019, pp. 23–57, <http://dx.doi.org/10.7208/chicago/9780226613475.003.0001>.
- [11] K.B. Sandvik, *Humanitarian Extractivism: The Digital Transformation of Aid*, Manchester University Press, 2023, pp. 1–153, <http://dx.doi.org/10.7765/9781526165831>.
- [12] K.B. Sandvik, Calibrating AI/d talk: framing perceptions, reframing policy, and deframing knowledge, *J. Int. Humanit. Action* 10 (11) (2025) <http://dx.doi.org/10.1186/s41018-025-00173-0>.
- [13] Y. Lont, P. Steinmann, J. Kwakkel, T. Comes, Maladaptation in supply chains: the unintended consequences of adaptive actions aimed at enhancing resilience, *J. Supply Chain Manag.* (2026) <http://dx.doi.org/10.1111/jscm.70031>.
- [14] E.L.F. Schipper, Maladaptation: When adaptation to climate change goes very wrong, *One Earth* 3 (4) (2020) 409–414, <http://dx.doi.org/10.1016/j.oneear.2020.09.014>.
- [15] S. Alon-Barkat, M. Busuioc, Human-AI interactions in public sector decision making: ‘automation bias’ and ‘selective adherence’ to algorithmic advice, *J. Public Adm. Res. Theory* 33 (1) (2023) 153–169, <http://dx.doi.org/10.1093/jopart/muac007>.
- [16] M.C. Horowitz, L. Kahn, Bending the automation bias curve: a study of human and AI-based decision making in national security contexts, *Int. Stud. Q.* 68 (2) (2024) sqae020, <http://dx.doi.org/10.1093/isq/sqae020>.
- [17] S.R. Hiltz, L. Plotnick, Dealing with information overload when using social media for emergency management: Emerging solutions, in: T. Comes, F. Fiedrich, S. Fortier, J. Geldermann, T. Müller (Eds.), *Proceedings of the 10th International Conference on Information Systems for Crisis Response and Management (ISCRAM 2013)*, Baden-Baden, Germany, 2013, pp. 823–827, URL https://idl.iscram.org/files/hiltz/2013/582_Hiltz_et_al2013.pdf.
- [18] J.D. Sterman, *Business Dynamics: Systems Thinking and Modeling for a Complex World*, Irwin/McGraw-Hill, Boston, 2000.
- [19] J. Holguín-Veras, M. Jaller, L.N. Van Wassenhove, N. Pérez, T. Wachtendorf, On the unique features of post-disaster humanitarian logistics, *J. Oper. Manage.* 30 (7–8) (2012) 494–506, <http://dx.doi.org/10.1016/j.jom.2012.08.003>.
- [20] J. Collier, S. Balakrishnan, Z. Zhang, Comparing actions and lessons learned in transportation and logistics efforts for emergency response to hurricane Katrina and hurricane Harvey, *J. Homel. Secur. Emerg. Manag.* 17 (3) (2020) 20190022, <http://dx.doi.org/10.1515/jhsem-2019-0022>.
- [21] Y. Lont, J. Kwakkel, T. Comes, An agent-based exploration of information sharing for adaptation in crisis response, in: *Proceedings of the International ISCRAM Conference, Vol. 22: 22nd International ISCRAM Conference*, Halifax, Canada, 2025, <http://dx.doi.org/10.59297/h0rgwd57>.
- [22] A. Wieland, M. Stevenson, S.A. Melnyk, S. Davoudi, L. Schultz, Thinking differently about supply chain resilience: what we can learn from social-ecological systems thinking, *Int. J. Oper. Prod. Manag.* 43 (1) (2023) 1–21, <http://dx.doi.org/10.1108/IJOPM-10-2022-0645>.
- [23] L.N. Van Wassenhove, Humanitarian aid logistics: Supply chain management in high gear, *J. Oper. Res. Soc.* 57 (5) (2006) 475–489, <http://dx.doi.org/10.1057/palgrave.jors.2602125>.
- [24] M. Jahre, N. Fabbe-Costes, How standards and modularity can improve humanitarian supply chain responsiveness: The case of emergency response units, *J. Humanit. Logist. Supply Chain Manag.* 5 (3) (2015) 348–386, <http://dx.doi.org/10.1108/jhlsm-06-2015-0026>.
- [25] N. Altay, R. Pal, Coping in supply chains: a conceptual framework for disruption management, *Int. J. Logist. Manag.* 34 (2) (2023) 261–279, <http://dx.doi.org/10.1108/IJLM-05-2021-0305>.
- [26] N. Altay, R. Pal, Information diffusion among agents: Implications for humanitarian operations, *Prod. Oper. Manage.* 23 (6) (2014) 1015–1027, <http://dx.doi.org/10.1111/poms.12102>.
- [27] N. Bloom, L. Garicano, R. Sadun, J. Van Reenen, The distinct effects of information technology and communication technology on firm organization, *Manag. Sci.* 60 (12) (2014) 2859–2885, <http://dx.doi.org/10.1287/mnsc.2014.2013>.
- [28] E. Yusecoy, B. Balci, E. Coban, The role of drones in disaster response: A literature review of operations research applications, *Int. Trans. Oper. Res.* 32 (2025) <http://dx.doi.org/10.1111/itor.13484>.
- [29] Q. Wang, W. Li, Z. Yu, Q. Abbasi, M. Imran, S. Ansari, Y. Sambo, L. Wu, Q. Li, T. Zhu, An overview of emergency communication networks, *Remote. Sens.* 15 (6) (2023) 1595, <http://dx.doi.org/10.3390/rs15061595>.
- [30] D. Paulus, R. Fathi, F. Fiedrich, B. Van de Walle, T. Comes, On the interplay of data and cognitive bias in crisis information management: An exploratory study on epidemic response, *Inf. Syst. Front.* 26 (2024) 391–415, <http://dx.doi.org/10.1007/s10796-022-10241-0>.
- [31] B. Van de Walle, T. Comes, On the nature of information management in complex and natural disasters, *Procedia Eng.* 107 (2015) 403–411, <http://dx.doi.org/10.1016/j.proeng.2015.06.098>.
- [32] D. Zhang, L. Zhou, J.F. Nunamaker, A knowledge management framework for the support of decision making in humanitarian assistance/disaster relief, *Knowl. Inf. Syst.* 4 (3) (2002) 370–385, <http://dx.doi.org/10.1007/s10150200012>.
- [33] J.E. Bailey, S.W. Pearson, Development of a tool for measuring and analyzing computer user satisfaction, *Manag. Sci.* 29 (5) (1983) 530–545, <http://dx.doi.org/10.1287/mnsc.29.5.530>.
- [34] A. Tversky, D. Kahneman, Judgment under uncertainty: Heuristics and biases, *Science* 185 (4157) (1974) 1124–1131, <http://dx.doi.org/10.1126/science.185.4157.1124>.
- [35] I. Palagara Sigala, M. Sirenko, T. Comes, G. Kovács, Mitigating personal protective equipment (PPE) supply chain disruptions in pandemics – a system dynamics approach, *Int. J. Oper. Prod. Manage.* 42 (13) (2022) 128–154, <http://dx.doi.org/10.1108/IJOPM-09-2021-0608>.
- [36] E.X. Wood, AI and big data in disaster response: Ethical and practical challenges, *J. Dyn. Disasters* 1 (4) (2025) 100041, <http://dx.doi.org/10.1016/j.jdd.2025.100041>.
- [37] P. Kolivand, S. Azari, A. Bakhtiari, P. Namdar, S.M. Ayyoubzadeh, S. Rajaie, M. Ramezani, AI applications in disaster governance with health approach: A scoping review, *Arch. Public Health* 83 (2025) 218, <http://dx.doi.org/10.1186/s13690-025-01712-2>.
- [38] M. Erdelj, E. Natalizio, UAV-assisted disaster management: Applications and open issues, in: *2016 International Conference on Computing, Networking and Communications (ICNC)*, 2016, pp. 1–5, <http://dx.doi.org/10.1109/ICNC.2016.7440563>.
- [39] M. Ozbiltekin-Pala, V. Yavas, Y.D. Ozkan-Ozen, Drivers and barriers of unmanned aerial vehicles in emergency logistics operations, *Technol. Soc.* 82 (2025) 102894, <http://dx.doi.org/10.1016/j.techsoc.2025.102894>.
- [40] K.B. Sandvik, K. Lohne, The rise of the humanitarian drone: Giving content to an emerging concept, *Millenn.: J. Int. Stud.* 43 (1) (2014) 145–164, <http://dx.doi.org/10.1177/0305829814529571>.
- [41] F. Greenwood, E.L. Nelson, P.G. Greenough, Flying into the hurricane: A case study of UAV use in damage assessment during the 2017 hurricanes in Texas and Florida, *PLoS One* 15 (2) (2020) e0227808, <http://dx.doi.org/10.1371/journal.pone.0227808>.

- [42] S. Fekih, N. Tamagnone, B. Minixhofer, R. Shrestha, X. Contla, E. Oglethorpe, N. Rekabsaz, HUMSET: Dataset of multilingual information extraction and classification for crisis response, in: Findings of the Association for Computational Linguistics: EMNLP 2022, Association for Computational Linguistics, Abu Dhabi, United Arab Emirates, 2022, pp. 4379–4389, <http://dx.doi.org/10.18653/v1/2022.findings-emnlp.321>.
- [43] M. Imran, C. Castillo, F. Diaz, S. Vieweg, Processing social media messages in mass emergency: A survey, *ACM Comput. Surv.* 47 (4) (2015) 67:1–67:38, <http://dx.doi.org/10.1145/2771588>.
- [44] T.W. Malone, K. Crowston, The interdisciplinary study of coordination, *ACM Comput. Surv.* 26 (1) (1994) 87–119, <http://dx.doi.org/10.1145/174666.174668>.
- [45] J. Wolbers, K. Boersma, The common operational picture as collective sensemaking, *J. Contingencies Crisis Manag.* 21 (4) (2013) 186–199, <http://dx.doi.org/10.1111/1468-5973.12027>.
- [46] K. Steen-Tveit, B.E. Munkvold, From common operational picture to common situational understanding: An analysis based on practitioner perspectives, *Saf. Sci.* 142 (2021) 105381, <http://dx.doi.org/10.1016/j.ssci.2021.105381>.
- [47] H. van Dijk, Situation awareness in crisis situations: Development of a user defined operational picture, in: *Proceedings of the ISCRAM 2015 Conference*, Kristiansand, Norway, 2015.
- [48] W. Treurniet, *Between chaos and continuity: A common operational picture in support of emergency response networks* (Ph.D. thesis), Vrije Universiteit Amsterdam, 2022.
- [49] H. Baharmand, A. Maghsoudi, G. Coppi, Exploring the application of blockchain to humanitarian supply chains: insights from humanitarian supply blockchain pilot project, *Int. J. Oper. Prod. Manage.* 41 (9) (2021) 1522–1543, <http://dx.doi.org/10.1108/IJOPM-12-2020-0884>.
- [50] H. Baharmand, N. Saeed, T. Comes, M. Lauras, Developing a framework for designing humanitarian blockchain projects, *Comput. Ind.* 131 (2021) <http://dx.doi.org/10.1016/j.compind.2021.103487>.
- [51] R. Dubey, A. Gunasekaran, D.J. Bryde, Y.K. Dwivedi, T. Papadopoulos, Blockchain technology for enhancing swift-trust, collaboration and resilience within a humanitarian supply chain setting, *Int. J. Prod. Res.* 58 (11) (2020) 3381–3398, <http://dx.doi.org/10.1080/00207543.2020.1722860>.
- [52] P. Dutta, T.-M. Choi, S. Somani, R. Butala, Blockchain technology in supply chain operations: Applications, challenges and research opportunities, *Transp. Res. Part E: Logist. Transp. Rev.* 142 (2020) 102067, <http://dx.doi.org/10.1016/j.tre.2020.102067>.
- [53] P.-Y. Beauchemin, E. Grusd, E.E. Noste, A. Cook, J.-E. Larsen, A. Poblete Alonzo, M. Enkhdalai, S.T. Casey, Satellite communications in health emergencies: no longer a luxury, *West. Pac. Surveill. Response J.* 16 (1) (2025) 1–2, <http://dx.doi.org/10.5365/wpsar.2025.16.1.1217>.
- [54] S. Shaffiee Haghsheenas, V. Astarita, S. Shaffiee Haghsheenas, G. Martino, G. Guido, The potential of satellite internet technologies for crisis management during urban evacuation: A case study of starlink in Italy, *Information* 16 (10) (2025) 840, <http://dx.doi.org/10.3390/info16100840>.
- [55] J. Barnett, S. O'Neill, Maladaptation, *Glob. Environ. Chang.* 20 (2) (2010) 211–213, <http://dx.doi.org/10.1016/j.gloenvcha.2009.11.004>.
- [56] D.L. Lofflin, S.R. Kephart, Outbreeding, seedling establishment, and maladaptation in natural and reintroduced populations of rare and common *Silene douglasii* (caryophyllaceae), *Am. J. Bot.* 92 (10) (2005) 1691–1700, <http://dx.doi.org/10.3732/ajb.92.10.1691>.
- [57] S.P. Brady, D.I. Bolnick, A.L. Angert, A. Gonzalez, R.D.H. Barrett, E. Crispo, A.M. Derry, C.G. Eckert, D.J. Fraser, G.F. Fussmann, F. Guichard, T. Lamy, A.G. McAdam, E.M. Newman, A. Paccard, G. Rolshausen, A.M. Simons, A.P. Hendry, Causes of maladaptation, *Evol. Appl.* 12 (7) (2019) 1229–1242, <http://dx.doi.org/10.1111/eva.12844>.
- [58] J. Barnett, S.J. O'Neill, Minimising the risk of maladaptation: A framework for analysis, in: *Climate Adaptation Futures*, 2013, pp. 87–93, <http://dx.doi.org/10.1002/9781118529577.ch7>.
- [59] T. Comes, Sensemaking AI: Introducing a research and design agenda for human-ai networks, *EPJ Data Sci.* 15 (1) (2026) 42, <http://dx.doi.org/10.1140/epjds/s13688-026-00634-5>.
- [60] T. Comes, Cognitive biases in humanitarian sensemaking and decision-making lessons from field research, in: *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, IEEE, 2016, pp. 56–62, <http://dx.doi.org/10.1109/COGSIMA.2016.7497786>.
- [61] M. Bruckler, L. Wietschel, L. Messmann, A. Thorenz, A. Tuma, Review of metrics to assess resilience capacities and actions for supply chain resilience, *Comput. Ind. Eng.* 192 (2024) 110176, <http://dx.doi.org/10.1016/j.cie.2024.110176>.
- [62] S. Hosseini, K. Barker, J.E. Ramirez-Marquez, A review of definitions and measures of system resilience, *Reliab. Eng. Syst. Saf.* 145 (2016) 47–61, <http://dx.doi.org/10.1016/j.res.2015.08.006>.
- [63] P. Steinmann, H. Tobi, G.A.K. van Voorn, Resilience metrics for socio-ecological and socio-technical systems: A scoping review, *Systems* 12 (9) (2024) 357, <http://dx.doi.org/10.3390/systems12090357>.
- [64] S. Sardesai, K. Klingebiel, Maintaining viability by rapid supply chain adaptation using a process capability index, *Omega* 115 (2023) 102778, <http://dx.doi.org/10.1016/j.omega.2022.102778>.
- [65] C.M. Macal, Everything you need to know about agent-based modelling and simulation, *J. Simul.* 10 (2) (2016) 144–156, <http://dx.doi.org/10.1057/jos.2016.7>.
- [66] C.C. Krejci, Hybrid simulation modeling for humanitarian relief chain coordination, *J. Humanit. Logist. Supply Chain Manag.* 5 (3) (2015) 325–347, <http://dx.doi.org/10.1108/JHLSCM-07-2015-0033>.
- [67] L. Bateman, E. Gralla, Evaluating strategies for intra-organizational information management in humanitarian response, in: *Proceedings of the 15th International Conference on Information Systems for Crisis Response and Management (ISCRAM 2018)*, Rochester, NY, USA, 2018, pp. 145–157, URL <https://idl.iscram.org/show.php?record=2096>.
- [68] C. Fikar, P. Hirsch, P.C. Nolz, Agent-based simulation optimization for dynamic disaster relief distribution, *Central Eur. J. Oper. Res.* 26 (2) (2018) 423–442, <http://dx.doi.org/10.1007/s10100-017-0518-3>.
- [69] R.A. Gonzalez, *A Framework for ICT-Supported Coordination in Crisis Response* (Ph.D. thesis), Delft University of Technology, Delft, The Netherlands, 2010.
- [70] S.K. Aros, D.E. Gibbons, Exploring communication media options in an inter-organizational disaster response coordination network using agent-based simulation, *European J. Oper. Res.* 269 (2) (2018) 451–465, <http://dx.doi.org/10.1016/j.ejor.2018.02.013>.
- [71] G.I. Hawe, G. Coates, D.T. Wilson, R.S. Crouch, Agent-based simulation of emergency response to plan the allocation of resources for a hypothetical two-site major incident, *Eng. Appl. Artif. Intell.* 46 (2015) 336–345, <http://dx.doi.org/10.1016/j.engappai.2015.06.023>.
- [72] M. Sirenko, A. Verbrack, T. Comes, On urban maladaptation in times of epidemics, *Sci. Rep.* 16 (2026) <http://dx.doi.org/10.1038/s41598-025-33158-5>.
- [73] B.R. Tukamuhawa, M. Stevenson, J. Busby, M. Zorzini, Supply chain resilience: Definition, review and theoretical foundations for further study, *Int. J. Prod. Res.* 53 (18) (2015) 5592–5623, <http://dx.doi.org/10.1080/00207543.2015.1037934>.
- [74] T.Y. Choi, K.J. Dooley, M. Rungtusanatham, Supply networks and complex adaptive systems: control versus emergence, *J. Oper. Manage.* 19 (3) (2001) 351–366, [http://dx.doi.org/10.1016/S0272-6963\(00\)00068-1](http://dx.doi.org/10.1016/S0272-6963(00)00068-1).
- [75] J.M. Day, Fostering emergent resilience: The complex adaptive supply network of disaster relief, *Int. J. Prod. Res.* 52 (7) (2014) 1970–1988, <http://dx.doi.org/10.1080/00207543.2013.787496>.
- [76] S. Schiffling, C. Hannibal, M. Tickle, Y. Fan, The implications of complexity for humanitarian logistics: a complex adaptive systems perspective, *Ann. Oper. Res.* 319 (1) (2022) 1379–1410, <http://dx.doi.org/10.1007/s10479-020-03658-w>.
- [77] V. Grimm, E. Revilla, U. Berger, F. Jeltsch, W. Mooij, S.F. Railsback, H.H. Thulke, J. Weiner, T. Wiegand, D.L. DeAngelis, Pattern-oriented modeling of agent-based complex systems: Lessons from ecology, *Science* 310 (5750) (2005) 987–991, <http://dx.doi.org/10.1126/science.1116681>.

- [78] V. Grimm, S.F. Railsback, Pattern-oriented modelling: a 'multi-scope' for predictive systems ecology, *Phil. Trans. R. Soc. B* 367 (1586) (2012) 298–310, <http://dx.doi.org/10.1098/rstb.2011.0180>.
- [79] S. Bankes, Exploratory modeling for policy analysis, *Oper. Res.* 41 (3) (1993) 435–449, <http://dx.doi.org/10.1287/opre.41.3.435>.
- [80] J.H. Kwakkel, E. Pruyt, Exploratory modeling and analysis, an approach for model-based foresight under deep uncertainty, *Technol. Forecast. Soc. Change* 80 (3) (2013) 419–431, <http://dx.doi.org/10.1016/j.techfore.2012.10.005>.
- [81] J.H. Kwakkel, The exploratory modeling workbench: An open source toolkit for exploratory modeling, scenario discovery, and (multi-objective) robust decision making, *Environ. Model. Softw.* 96 (2017) 239–250, <http://dx.doi.org/10.1016/j.envsoft.2017.06.054>.
- [82] P. Steinmann, W.L. Auping, J.H. Kwakkel, Behavior-based scenario discovery using time series clustering, *Technol. Forecast. Soc. Change* 156 (2020) 120052, <http://dx.doi.org/10.1016/j.techfore.2020.120052>.
- [83] B.P. Bryant, R.J. Lempert, Thinking inside the box: A participatory, computer-assisted approach to scenario discovery, *Technol. Forecast. Soc. Change* 77 (1) (2010) 34–49, <http://dx.doi.org/10.1016/j.techfore.2009.08.002>.
- [84] J.H. Friedman, N.I. Fisher, Bump hunting in high-dimensional data, *Stat. Comput.* 9 (2) (1999) 123–143, <http://dx.doi.org/10.1023/A:1008894516817>.
- [85] Y. Lont, P. Steinmann, T. Comes, J. Kwakkel, Modelling supply chain maladaptation: How delay and misalignment undermine adaptive actions, 2026, *Under revision at Journal of Artificial Societies and Social Simulation*.
- [86] J. Mackay, A. Munoz, M. Pepper, A disaster typology towards informing humanitarian relief supply chain design, *J. Humanit. Logist. Supply Chain Manag.* 9 (1) (2019) 22–46, <http://dx.doi.org/10.1108/JHLSCM-06-2018-0049>.
- [87] K.P. Scheibe, J. Blackhurst, Supply chain disruption propagation: a systemic risk and normal accident theory perspective, *Int. J. Prod. Res.* 56 (1–2) (2018) 43–59, <http://dx.doi.org/10.1080/00207543.2017.1355123>.
- [88] R.E. Barlow, F. Proschan, *Mathematical Theory of Reliability*, John Wiley & Sons, New York, 1965.
- [89] J.M. Epstein, Growing adaptive organizations: An agent-based computational approach, in: J.M. Epstein (Ed.), *Generative Social Science: Studies in Agent-Based Computational Modeling*, in: *Princeton Studies in Complexity*, Princeton University Press, Princeton, NJ, 2006, pp. 309–344.
- [90] A. Khan, S. Gupta, S.K. Gupta, Multi-hazard disaster studies: Monitoring, detection, recovery, and management, based on emerging technologies and optimal techniques, *Int. J. Disaster Risk Reduct.* 47 (2020) 101642, <http://dx.doi.org/10.1016/j.ijdrr.2020.101642>.
- [91] S. Waring, L. Alison, G. Carter, C. Barrett-Pink, M. Humann, L. Swan, T. Zilinsky, Information sharing in interteam responses to disaster, *J. Occup. Organ. Psychol.* 91 (3) (2018) 591–619, <http://dx.doi.org/10.1111/joop.12217>.
- [92] V. Grimm, S.F. Railsback, C.E. Vincenot, U. Berger, C. Gallagher, D.L. Deangelis, B. Edmonds, J. Ge, J. Giske, J. Groeneveld, A.S.A. Johnston, A. Milles, J. Nabe-Nielsen, J.G. Polhill, V. Radchuk, M.S. Rohwäder, R.A. Stillman, J.C. Thiele, D. Ayllón, The ODD protocol for describing agent-based and other simulation models: A second update to improve clarity, replication, and structural realism, *J. Artif. Soc. Soc. Simul.* 23 (2020) <http://dx.doi.org/10.18564/jasss.4259>.
- [93] P. Jacobs, *The DSOL simulation suite: Enabling multi-formalism simulation in a distributed context* (Ph.D. thesis), Delft University of Technology, Delft, The Netherlands, 2005.
- [94] B. Balcik, B.M. Beamon, C.C. Krejci, K.M. Muramatsu, M. Ramirez, Coordination in humanitarian relief chains: Practices, challenges and opportunities, *Int. J. Prod. Econ.* 126 (1) (2010) 22–34, <http://dx.doi.org/10.1016/j.ijpe.2009.09.008>.
- [95] B. Adsanver, B. Balcik, V. Bélanger, M.-È. Rancourt, Operations research approaches for improving coordination, cooperation, and collaboration in humanitarian relief chains: A framework and literature review, *European J. Oper. Res.* 319 (2024) 384–398, <http://dx.doi.org/10.1016/j.ejor.2023.11.031>.
- [96] M. Jahre, L.-M. Jensen, Coordination in humanitarian logistics through clusters, *Int. J. Phys. Distrib. Logist. Manage.* 40 (2010) 657–674, <http://dx.doi.org/10.1108/09600031011079319>.
- [97] C. Posey, Using organizational information processing theory to examine the relationship between information sharing and supply chain performance, in: J. Wang (Ed.), *Supply Chain Optimization, Management and Integration: Emerging Applications*, IGI Global, Hershey, PA, 2011, pp. 230–240, <http://dx.doi.org/10.4018/978-1-60960-135-5.ch016>.
- [98] A. Behl, S. Bhardwaj, N. Jayawardena, V. Pereira, M. Roohanifar, Grass is always dark(er) on the other side: Exploring the dark side of artificial intelligence humanitarian supply chain operations, *Technol. Forecast. Soc. Change* 224 (2026) 124484, <http://dx.doi.org/10.1016/j.techfore.2025.124484>.
- [99] D. Simchi-Levi, E. Simchi-Levi, We need a stress test for critical supply chains, *Harv. Bus. Rev.* (2020) URL <https://hbr.org/2020/04/we-need-a-stress-test-for-critical-supply-chains>, Published online April 28, 2020.
- [100] D. Ivanov, A. Dolgui, Stress testing supply chains and creating viable ecosystems, *Oper. Manag. Res.* 15 (2) (2022) 475–486, <http://dx.doi.org/10.1007/s12063-021-00194-z>.
- [101] J. Wu, H. Bin, Z. Yu, C. Spence, S.B. Hall, K. Carley, An agent-based simulation study for exploring organizational adaptation, *Simulation* 85 (6) (2009) 397–413, <http://dx.doi.org/10.1177/0037549709105267>.
- [102] J.T. ter Horst, P. Steinmann, J.H. Kwakkel, Evaluating rule induction algorithms for scenario discovery, *Environ. Model. Softw.* 203 (2026) 107006, <http://dx.doi.org/10.1016/j.envsoft.2026.107006>.