

North American Actuarial Journal

ISSN: 1092-0277 (Print) 2325-0453 (Online) Journal homepage: www.tandfonline.com/journals/uaaj20

The Economic Impact of Extreme AI Scenarios

Martin Eling

To cite this article: Martin Eling (24 Mar 2026): The Economic Impact of Extreme AI Scenarios, North American Actuarial Journal, DOI: 10.1080/10920277.2026.2638235

To link to this article: https://doi.org/10.1080/10920277.2026.2638235

© 2026 The Author(s). Published with license by Taylor & Francis Group, LLC.

Published online: 24 Mar 2026.

Submit your article to this journal

Article views: 1737

View related articles

View Crossmark data

Citing articles: 1 View citing articles

Full Terms & Conditions of access and use can be found at https://www.tandfonline.com/action/journalInformation?journalCode=uaaj20

North American Actuarial Journal, 0(0), 1–15, 2026
© 2026 The Author(s). Published with license by Taylor & Francis Group, LLC.
ISSN: 1092-0277 print / 2325-0453 online
DOI: 10.1080/10920277.2026.2638235

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

The Economic Impact of Extreme AI Scenarios

Martin Eling
Institute of Insurance Economics, University of St. Gallen, St. Gallen, Switzerland

We use the dynamic inoperability input–output model—presented in this journal to analyze cyber risk scenarios—to evaluate the economic impact of seven plausible, potentially high-consequence artificial intelligence (AI) risk scenarios. The scenarios span a diverse range of AI-related disruptions, including failures of widely used business software, breakdowns in AI-enabled transport systems, or targeted AI-based attacks on critical infrastructure. Each scenario is modeled based on sectoral inoperability, recovery dynamics, and cascading effects across the economy. Estimated losses for the U.S. economy range from US$11 billion to US$85 billion. While most scenarios fall within insurable limits, some might exceed the risk-bearing capacity of private insurers and require public–private risk-sharing mechanisms, especially for AI-based attacks on critical infrastructure. This study presents a structured, scenario-based approach to assessing the insurability of emerging AI risks in the absence of historical data and thus assists decision-makers in better understanding this emerging type of risk.

MOTIVATION AND AIM

The rapid adoption of artificial intelligence (AI) across nearly all sectors of the economy—from finance and healthcare to transportation and government—has transformed AI from a niche technology into a foundational infrastructure (World Economic Forum 2025). As AI systems become deeply integrated into critical processes and decision-making, concerns about the potential economic consequences of their failure or misuse are rising (Brundage et al. 2018). However, unlike other risks, data on AI-related incidents is scarce. This absence of data and empirical analysis is partly due to the intensified use of the technology in recent years, and partly due to the lack of incentives for transparent reporting of near misses or system failures.

In the absence of reliable data, scenario-based stress testing has emerged as a useful tool to raise awareness among policymakers, insurers, and regulators. Several organizations and think tanks have begun discussing hypothetical worst-case AI scenarios, such as systemic model failures or rogue use of generative AI (e.g., Hendrycks et al. 2023). A particular concern with relevance to the insurance sector lies in the "monoculture" associated with the widespread deployment of a few dominant AI models and providers. This could lead to large-scale accumulation risk if a single technical vulnerability or governance failure cascades across sectors.

In this article, we adapt a dynamic inoperability input–output model (DIIM) to consistently assess the macroeconomic impact of seven potential AI risk scenarios. Each scenario is filtered through a common lens, parameterized using sectoral exposure, estimated inoperability, and recovery time. The result is a standardized, scalable framework for quantifying the economic effects of emerging AI risks at both macro and micro levels. We also provide a taxonomy to classify the different types of AI risk from an insurance perspective.

Our findings show that estimated losses from AI risk scenarios for the U.S. economy range from US$11 billion to US$85 billion. While several scenarios fall clearly within the realm of private insurability, others may exceed insurers' capacity and necessitate alternative forms of societal risk governance—such as public–private risk-sharing arrangements, regulatory interventions, or dedicated risk pools. For instance, a general-purpose AI system failure affecting business software results in an

Address correspondence to Martin Eling, Institute of Insurance Economics, University of St. Gallen, Girtannerstr. 6, 9010 St. Gallen, Switzerland. E-mail: martin.eling@unisg.ch

Supplemental data for this article can be accessed online at https://doi.org/10.1080/10920277.2026.2638235.
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

estimated loss of US$11 billion, whereas an AI-based attack on critical infrastructure leads to losses of US$85 billion. These figures are benchmarked against historical catastrophes such as Hurricane Katrina (US$125 billion) and the 2011 Japanese tsunami (US$210 billion). Even the most severe AI scenarios remain well below 1% of U.S. gross domestic product (GDP), offering perspective on loss magnitudes and for insurability assessments. The proposed framework provides a replicable foundation for future AI risk modeling and a valuable decision-support tool for policymakers, insurers, and regulators seeking to understand and manage this emerging class of risk.

After definitions and literature review, we briefly introduce the methodology to make the article self-contained. Then we identify relevant AI risk scenarios and measure their potential economic impact. Finally, we present our conclusions.

DEFINITIONS AND LITERATURE REVIEW

AI Risk

An unambiguous and universally accepted definition of AI risk does not yet exist. The term is used to describe a wide range of potential harms associated with the development, deployment, or failure of AI systems. These include operational disruptions, data leakage, discriminatory outcomes, systemic misalignment, loss of human oversight, and in extreme cases, catastrophic failures in critical infrastructure or social systems (European Union 2024; Uuk et al. 2025). From an operational perspective, AI risks can be understood as risks arising from the use of AI systems that lead to unintended, harmful consequences for individuals, organizations, or society. These may result from errors in training data, flawed model design, poor implementation, adversarial manipulation, or the misuse of general-purpose models (Brundage et al. 2018). AI risks can be classified by domain of impact (e.g., healthcare, finance, public administration), origin (e.g., state-sponsored actors, rogue developers), and intentionality (e.g., unintentional misuse, malicious deployment). A broader taxonomy of AI risk—building upon existing taxonomies for cyber risk—is presented in Appendix A (available upon request). Compared to other operational risks covered by insurers, AI risks share characteristics with cyber risk, such as accumulation potential, high correlation, and loss verification difficulties. For example, a single flawed model update could propagate across hundreds of organizations using the same underlying AI system. What distinguishes AI risks from other operational risks is the autonomous, adaptive, and opaque nature of many AI systems, which can lead to novel failure modes, delayed detection, and cascading effects that are difficult to anticipate or control. AI systems learn and evolve over time, making their behavior less predictable and more difficult to audit.

For the purpose of this article, we use the term AI to refer to computational systems capable of performing tasks that typically require human intelligence, such as pattern recognition, prediction, and autonomous decision-making, based on statistical learning from data (adapted from OECD et al. 2025; European Union 2024). In this context AI risk is defined as the potential for unintended or harmful outcomes arising from the design, development, deployment, or failure of AI systems, which may lead to operational, financial, legal, or societal consequences (adapted from Uuk et al. 2025; Brundage et al. 2018). It is important to distinguish between AI as a continuous, systemic background risk—reflecting the general dependency of modern economies on AI—and AI disruption events, which denote discrete, high-impact failures or malfunctions that temporarily disable critical AI functions across sectors. The present study focuses on these acute AI disruption events and quantifies their macroeconomic impact using dynamic inoperability input–output models.

AI risk is amplified by its widespread integration into critical infrastructures—such as transportation, energy, healthcare, and finance. As with cyber risk, growing interdependencies between sectors mean that the failure or exploitation of one AI system can lead to cascading consequences, potentially crossing national and sectoral boundaries (Bryson et al. 2017; Rahwan et al. 2019). Given the complexity and opacity of many AI systems, traditional risk assessment tools are often insufficient. This has led to a growing body of work focused on scenario-based analysis, AI governance, and resilience modeling, which aim to understand not only technical failure but also societal and economic consequences (e.g., Heaven 2019; Falco et al. 2021).

Scenario Analysis

Scenario analysis is a strategic planning tool used across different disciplines to explore plausible future developments based on coherent assumptions (Mahmoud et al. 2009), particularly valuable where historical data are unreliable predictors—such as risk from AI. Unlike forecasts, scenarios are structured, internally consistent narratives that support decision-making through phases including definition, construction, analysis, assessment, and risk management (Mahmoud et al. 2009). Risk scenarios, often presented as qualitative narratives, help evaluate the likelihood and consequences of devastating, correlated incidents. However, most quantitative loss models neglect scenario context. This article addresses that gap by integrating

qualitative scenario elements into quantitative assessments through sensitivity analysis and proposes a standardized typology to enable comparison and classification of AI risk scenarios, which to the best of our knowledge currently does not exist in either academic or practitioner literature.

Economic Impact Analysis

The economic impacts of AI-related risk scenarios remain underexplored in academic literature, especially compared to debates on AI insurability and regulation (Brundage et al. 2018; OECD 2021). One reason is the lack of data on past AI failures and the absence of standardized, transparent methods for scenario construction. Similar to cyber risk, the field is shaped by practitioner reports and case studies (e.g., Novelli et al. 2024), which often highlight a few examples without offering generalizable frameworks. Existing studies also vary widely in impact estimates, with limited disclosure of assumptions and methods.

This article addresses these gaps by proposing a replicable scenario typology and modeling framework to assess the economic consequences of severe AI risk events. We apply the dynamic inoperability input–output model (DIIM), which effectively captures short-term shocks and sectoral interdependencies (Rose et al. 2016; Wei et al. 2018). Unlike complex equilibrium models, DIIM offers transparency and is suitable where data are scarce—such as in emerging AI risks. Focusing on seven plausible AI scenarios, we integrate qualitative narratives with quantitative modeling. Scenario parameters are drawn from literature and expert input, improving comparability and avoiding arbitrary assumptions. Our approach also allows for sensitivity analysis, helping to address uncertainty and advance the understanding of AI-related risk.

METHODOLOGY

Leontief Input–Output Model

The Leontief (1951, 1966, 1974) input–output model captures the equilibrium behavior of economies by analyzing interdependent sectors. Originally developed to quantify economic shifts (e.g., changes in consumption), it is now widely used to assess the impact of disruptions (e.g., Dietzenbacher and Miller 2015). Since each sector relies on inputs from others, interdependencies emerge. Its basic form is (Lian and Haimes 2006; Santos 2006)

$$\boldsymbol{x} = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{c} \Longleftrightarrow \left\{ x_i = \sum_j a_{ij} x_j + c_i \right\} \forall i. \tag{1}$$

where x_i represents the total output of sector i, a_{ij} is the input from sector i to sector j, and c_i the final demand of the ith sector, defined as the portion of sector i's total output for final consumption by end-users.

Inoperability Input–Output Model

The inoperability input–output model developed by Haimes and Jiang (2001) extends the traditional Leontief model. Both are deterministic linear equilibrium models using the same data set (Santos 2006), but differ structurally: The inoperability model replaces the technical coefficient matrix with an interdependency matrix (Jung et al. 2009). It captures how a sector's reduced functionality impacts the broader economy via interdependencies (Panzieri and Setola 2008), making it a useful tool for ripple effect analysis. In the inoperability input–output model the inoperability vector is formulated as

$$\boldsymbol{q} = \boldsymbol{A}^* \boldsymbol{q} + \boldsymbol{c}^* = \left[\boldsymbol{I} - \boldsymbol{A}^*\right]^{-1} \boldsymbol{c}^* \tag{2}$$

where $\boldsymbol{q}$ represents the demand-based inoperability vector, $\boldsymbol{A}^*$ the demand-based interdependency matrix derived from the technical coefficient matrix $\boldsymbol{A}$, $\boldsymbol{I}$ the identity matrix, and $\boldsymbol{c}^*$ the demand-based perturbation vector. These are defined as $\boldsymbol{q} = \hat{\bar{\boldsymbol{x}}}^{-1} \delta \boldsymbol{x}$, $\boldsymbol{A}^* = \hat{\bar{\boldsymbol{x}}}^{-1} \boldsymbol{A} \hat{\bar{\boldsymbol{x}}}$, $\boldsymbol{c}^* = \hat{\bar{\boldsymbol{x}}}^{-1} \delta \boldsymbol{c}$, with $\partial \boldsymbol{x} = \bar{\boldsymbol{x}} - \tilde{\boldsymbol{x}}$, $\partial \boldsymbol{c} = \bar{\boldsymbol{c}} - \tilde{\boldsymbol{c}}$, where $\hat{\bar{\boldsymbol{x}}}$ is the diagonal matrix generated by the vector $\bar{\boldsymbol{x}}$ (which is the baseline industry total production vector), $\tilde{\boldsymbol{x}}$ is the degraded industry total production vector,[1] $\bar{\boldsymbol{c}}$ is the baseline final uses vector, and $\tilde{\boldsymbol{c}}$ is the degraded final uses vector. The elements of matrix $\boldsymbol{A}^*$ are defined as $a^*_{ij} = a_{ij} \frac{x_j}{x_i}$, where x_i and x_j are the outputs of sectors i and j, respectively, and a_{ij} corresponds to the elements of the original technical coefficient matrix A (Ali and Santos 2015).

[1]The baseline final production refers to the volume of production in the absence of economic disturbance. Degraded is the reduced production volume with economic disturbance.

Haimes et al. (2005) extended the inoperability input–output model to its dynamic form, incorporating time-varying (in)operability and the discrete-time postshock resilience of sectors. It is defined as follows:

$$\boldsymbol{q}(t+1) = \boldsymbol{K}\boldsymbol{A}^*\boldsymbol{q}(t) + \boldsymbol{K}\boldsymbol{c}^*(t) + (\boldsymbol{I} - \boldsymbol{K})\boldsymbol{q}(t) \tag{3}$$

where $\boldsymbol{q}(t)$ represents the inoperability vector at time t, $\boldsymbol{K}$ the sectoral resilience matrix, $\boldsymbol{A}^*$ the interdependency matrix, $\boldsymbol{c}^*(t)$ the perturbation vector at time t, and $\boldsymbol{I}$ the identity matrix. The initial inoperability value $q_i(0)$ of a sector ranges between 0 and 1 and can be estimated, for example, through expert judgment. The resilience factor k_i of a particular sector i depicts its recovery rate from the external shock and the resulting inoperability and is defined as (Lian and Haimes 2006)

$$k_i = \frac{ln\left[\frac{q_i(0)}{q_i(T)}\right]}{T_i} * \left(\frac{1}{1 - a_{ii}^*}\right) \tag{4}$$

where T_i is the recovery time of sector i, and a_{ii}^* is the technical coefficient from the input–output matrix. Resilience is defined as the ability or capability of a system to absorb or cushion against damage or loss (Holling 1973). The recovery period T is the time a sector needs to return to an acceptable operability level relative to its preshock state and is typically estimated from historical data or expert judgment (Ali and Santos 2015). Since historical data on AI risks do not exist, the AI risk scenarios are based on expert opinions in this respect. Following Ali and Santos (2015), we assume that the inoperability at T corresponds to the state when all sectors have recovered to 1% of their initial inoperability values (i.e., $q_i(T) = 0.01q_i(0)$). The ratio of the initial inoperability with respect to the inoperability at T is

$$\frac{q_i(0)}{q_i(T)} = 100 \tag{5}$$

The actual recovery rate k_i of sector i depends on both its own recovery rate and its interdependence with the other sectors. The term $1 - a_{ii}^*$ represents the interdependency index of sector i, denoted as θ_i:

$$\theta_i = 1 - a_{ii}^* \tag{6}$$

The interdependency between two sectors is captured by

$$\rho_{ij} = \frac{\theta_i}{\theta_j} = \frac{1 - a_{ii}^*}{1 - a_{jj}^*} \tag{7}$$

For sectors not directly impacted by an event, it is assumed their production quickly adapts; hence, their resilience coefficient k_i is set to 1.

Inoperability values are derived from the initial inoperability vector $\boldsymbol{q}(0)$ and evolve through iterative applications of Equation (3). Because sectors influence each other via interdependencies, the resulting inoperability curves can take various forms (see, e.g., Figure 1). The speed of recovery depends on the affected sectors, the interdependency matrix, and the resilience matrix. Recovery curves—the inverse of inoperability curves—may follow linear, trigonometric, or exponential patterns (Cimellaro et al. 2010). For the scenarios considered, an exponential recovery is most plausible, as an intense initial response to the AI disruption is followed by gradually diminishing recovery efforts. Accordingly, the inoperability curves typically exhibit a convex shape with a decreasing slope. The expected total economic loss for a given scenario is calculated as (Lian et al. 2007)

$$E[\boldsymbol{Q}_s] = diag(\boldsymbol{x})(\boldsymbol{I} - \boldsymbol{A}^*)^{-1}E[\boldsymbol{K}]^{-1}\boldsymbol{q}(0) \tag{8}$$

where $E[\boldsymbol{Q}_s]$ represents the expected value of the total economic loss in scenario s and $\boldsymbol{x}$ is the nominal sector output vector for the time period considered.

For the analysis of different AI risk scenarios, minimum and maximum values were estimated for recovery time and inoperability. This approach enables a sensitivity analysis that reflects the uncertainty and fuzziness of key input parameters, without introducing additional assumptions. While more sophisticated methods exist—such as the fuzzy dynamic input–output inoperability model by Panzieri and Setola (2008), which expresses both inoperability and interdependencies as fuzzy numbers—we

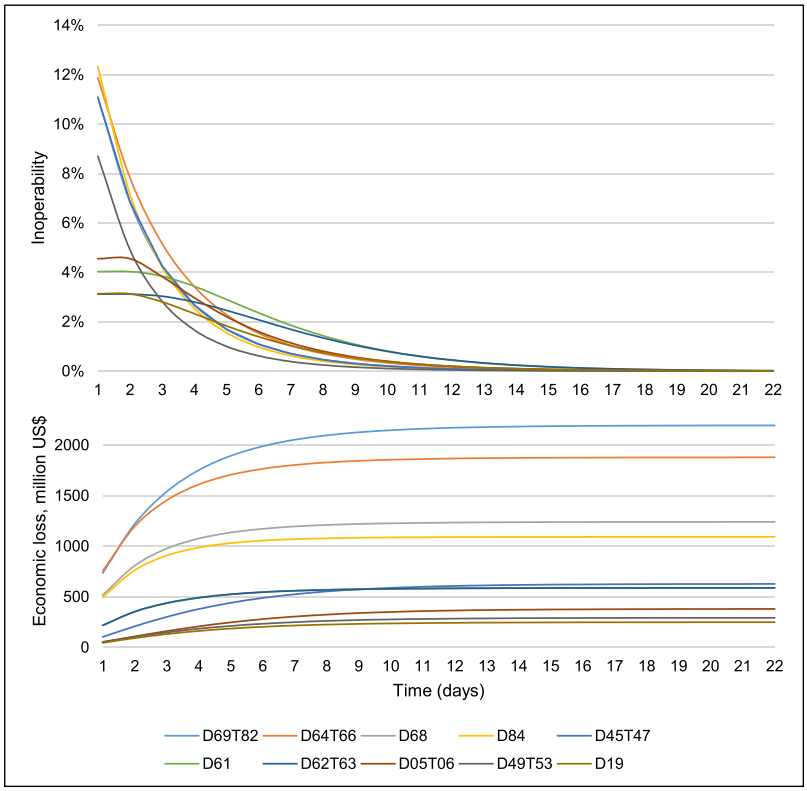

FIGURE 1. Inoperability Development of the Top 10 Inoperable Sectors (Top) and Cumulative Economic Losses for the Top 10 Affected Sectors (Bottom) for Scenario 1. *Note:* The figure illustrates how an initial disruption q(0) propagates through intersectoral dependencies represented by the Leontief matrix A and evolves over time into the sectoral inoperability vector q(t). The recovery time governs how quickly sectors return to normal functioning. The model iterates these interactions dynamically until a new equilibrium state is reached. D69T82: Professional, scientific, and technical services; D64T66: Financial and insurance activities; D68: Real estate activities; D84: Public administration and defense; compulsory social security; D45T47: Wholesale and retail trade, repair of motor vehicles; D61: Telecommunications; D62T63: IT and other information services; D05T06: Mining and extraction of energy producing products; D49T53: Transportation and storage; D19: Coke and refined petroleum products.

deliberately chose a simpler min/max setup. Given the limited empirical data on AI risks and the assumptions already required for the input–output model, the added complexity of a fuzzy model offers limited practical value in our context.

Data Sources for the Analysis of Economic Disruptions

Our model is based on the national input–output tables from the OECD (2018), which compile high-quality, transparent data from official sources. These tables show interindustry flows of goods and services (domestic and imported) for all OECD members and 28 nonmembers (including all G20 countries) from 2005 to 2015. Covered sectors are listed in Appendix B (available upon request). Table 1 provides a schematic overview of a national input–output table. Columns reflect production processes, while rows show output distribution.

AI RISK SCENARIOS

We have identified seven key scenarios that reflect the threats most frequently discussed in general media, industry studies, and academic publications. For the identification of these scenarios, we relied on a three-step approach: First, we conducted a structured review of academic and industry-oriented literature, including publications indexed in Web of Science and relevant gray literature. Second, we analyzed AI datasets and documentation platforms such as the AI Incidence Database and the AI Risk Repository, which compile known incidents and emerging risks; finally, we applied text mining to extract and rank the most relevant scenarios based on their frequency and prominence across sources. This combined methodology ensured a comprehensive and evidence-based selection of scenarios that are both plausible and impactful from an economic and risk management perspective (see Table 2).

TABLE 1
Schematic Representation of an Input–Output Transaction Table (Miller and Blair 2009)

		Producers as Consumers								Final Demand			
		Agriculture	Mining	Construction	Manufacturing.	Trade	Transportation	Services	Other Industry	Personal Consumption Expenditures	Gross Private Domestic Investment	Govt. Purchases of Goods & Services	Net Exports of Goods & Services
Producers	Agriculture												
	Mining												
	Construction												
	Manufacturing												
	Trade												
	Transportation												
	Services												
	Other Industry												
Value Added	Employees	Employee Compensation									Gross Domestic Product		
	Business Owners and Capital	Profit-Type Income and Capital Consumption Allowances											
	Government	Indirect Business Taxes											

TABLE 2
Summary of the Scenarios and References

Scenario	Narrative	References
1. Business Software Failure	Widespread failure of general-purpose AI systems embedded in office and enterprise software platforms (e.g., email, document management, financial reporting), disrupting administrative workflows.	Brundage et al. 2018; Dwivedi et al. 2023; Enderle 2025
2. Autonomous Vehicle Network Failure	AI-driven transport systems malfunction simultaneously across logistics hubs and urban areas, causing supply-chain breakdowns.	Litman 2024; Chafkin 2025
3. AI-Powered Misinformation Campaign	Large-scale release of targeted disinformation via AI-generated media disrupts political, media, and communication systems	Lee et al. 2023; Wack et al. 2025; Yan et al. 2025
4. Algorithmic Flash Crash in Financial Markets	Automated trading systems based on large language models (LLMs) or reinforcement learning agents trigger a cascading flash crash across asset classes.	Borch 2016; Makortoff 2025
5. LLM Misuse in Legal and Healthcare Settings	Incorrect or biased AI-generated decisions lead to legal, ethical, and operational failures in hospitals and law firms.	Binns et al. 2018; Hoffman and Podgurski 2021; Acheson 2024; Newman-Toker and Sharfstein 2024
6. AI-Enabled Cyberattack on Infrastructure	AI tools are used to execute a highly targeted cyberattack on critical infrastructure, including energy and communication networks.	Brundage et al. 2018; Guembe et al. 2022; ENISA 2024; Greenberg 2025; IBM 2025
7. AI Bias in Lending Algorithms	AI algorithms used for loan applications systematically discriminate against certain demographic groups, leading to financial losses for individuals and legal liabilities for financial institutions.	Ennis and Cook 2019; Garcia et al. 2024

There are multiple other scenarios discussed in the literature, including AI bias in hiring processes (e.g., Mujtaba and Mahapatra 2019), AI-augmented SCADA failure (e.g., Skrodelis et al. 2024), or systemic disruption resulting from misaligned AI behavior (e.g., Roose 2023). These highlight additional AI-related risk not covered in our core analysis but remain relevant for future modeling efforts. We exclude those in the main body of the article because of their partial overlap with other scenarios and their relative lower relevance, but for the sake of completeness we include them in the supplemental material (see Appendix C, available upon request, for a comprehensive overview).

All AI risk scenarios involve high potential for cumulative damage across sectors and borders. To capture this, we developed a standardized scenario classification combined with quantitative loss estimation using the dynamic inoperability input–output model. Table 3 outlines the input parameters used for the analysis. To define the corridor estimators—specifically, the ranges for initial inoperability and recovery times—we used again a three-stage approach based on (1) a structured review of academic and industry literature, (2) expert judgment from practitioners and researchers, especially in AI and risk management, and (3) structured input collected via the Prolific platform from 106 IT professionals (see Appendix C for details). This multisource strategy helps address the high uncertainty associated with emerging risks and provides a transparent foundation for the sensitivity analysis. We note that these key input assumptions remain subject to uncertainty, and therefore systematically vary the parameters in sensitivity analyses to better understand the potential range of economic impact. To enhance

TABLE 3
Scenarios and the Respective Input Parameters for the Input–Output Analysis

Scenario	Affected Sectors (OECD-Codes)	Initial Inoperability	Recovery Time (Days)
1. Business Software Failure	Financial and Insurance Activities (D64T66), Professional, Scientific and Technical Services (D69T82), Public Administration and Defense (D84), Telecommunication (D61), IT (D62T63), Real Estate Activities (D68)	0.05 – 0.10	4–15
2. Autonomous Vehicle Network Failure	Transportation and Storage (D49T53), Wholesale and Retail Trade (D45T47), Manufacturing (D20T33), Accommodation and Food Service Activities (D55T56), Telecommunication (D61), IT (D62T63)	0.10 – 0.30	5–21
3. AI-Powered Misinformation Campaign	Telecommunication (D61), IT (D62T63), Professional, Scientific, and Technical Services (D69T82), Financial and Insurance Activities (D64T66), Public Administration and Defense (D84), Arts, Entertainment, and Recreation (D90T96)	0.05 – 0.20	7–28
4. Algorithmic Flash Crash in Financial Markets	Financial and Insurance Activities (D64T66), Professional, Scientific, and Technical Services (D69T82), Telecommunication (D61), IT (D62T63)	0.20 – 0.40	3–10
5. LLM Misuse in Legal and Healthcare Settings	Human Health and Social Work Activities (D86T88), Professional, Scientific, and Technical Services (D69T82), Public Administration and Defense (D84)	0.10 – 0.40	7–21
6. AI-Enabled Cyberattack on Infrastructure	Electricity, Gas, Steam, and Air-Conditioning Supply (D35T39), Construction (D41T43), Public Administration and Defense (D84), IT (D62T63)	0.25 – 0.50	10–40
7. AI-Bias in Lending Algorithms	Telecommunication (D61), IT (D62T63), Financial and Insurance Activities (D64T66), Professional, Scientific, and Technical Services (D69T82), Public Administration and Defense (D84)	0.10 – 0.20	10–30

comparability, all scenarios here are simulated for the United States. However, analyses for other countries can be conducted using the OECD (2018) input–output tables.

EMPIRICAL RESULTS

Inoperability and Economic Loss Rankings for One Selected Scenario

While Table 3 shows the initial inoperability, that is, the immediate, sector-specific disruption assumed for each scenario, Table 4 presents the equilibrium after cascading effects propagate through the interindustry network captured by the DIIM. The large differences between sectors therefore reflect indirect, second-round, and feedback effects, which can substantially amplify or dampen the initial shock depending on the centrality and connectivity of each sector.

Demand-side inoperability and economic losses are the two resulting key outputs of the inoperability input–output model. Inoperability measures the percentage deviation from a sector's normal production, while economic loss captures the total monetary impact, including ripple effects. Both metrics should be considered in sector risk assessments, as they can lead to different rankings due to varying production volumes across sectors (Santos 2006). The 10 sectors with the highest cumulative economic losses (in million US$) and their respective average inoperability values of scenario 1 are summarized in Table 4. The total cumulative economic loss amounted to US$11.4 billion. Figure 1 shows the development of the inoperability and the cumulative economic loss of the top ten affected sectors, respectively.

The sectors with the highest inoperability are not necessarily those with the highest economic losses, and vice versa. To illustrate this, we present dynamic cross-prioritization plots (Resurreccion and Santos 2012), where each point reflects a

TABLE 4
Top 10 Affected Sectors Based on Average Inoperability for Scenario 1

Sector	Name	Economic Loss		Average Inoperability	
		Rank	Value (US$ million)	Rank	Value (%)[2]
D69T82	Professional, scientific, and technical services	1	2,172	2	0.35%
D64T66	Financial and insurance activities	2	1,863	3	0.30%
D68	Real estate activities	3	1,235	8	0.21%
D84	Public administration and defense; compulsory social security	4	1,090	10	0.17%
D45T47	Wholesale and retail trade; repair of motor vehicles	5	617	21	0.10%
D61	Telecommunications	6	584	4	0.29%
D62T63	Information technology (IT) and other information services	7	471	1	0.40%
D05T06	Mining and extraction of energy-producing products	8	377	5	0.27%
D49T53	Transportation and storage	9	289	18	0.13%
D19	Coke and refined petroleum products	10	248	19	0.12%

Note: The differences between sectors arise not only from the sector specific inoperability and recovery times (Table 3), but also from cumulative cascading and feedback mechanisms within the economic dependency structure. In Table 4, we use the average for inoperability and recovery times while further below (Table 5) we use their minimum and maximum values (0.05 to 0.1; 4 to 15 days) to show the variation of potential outcomes.

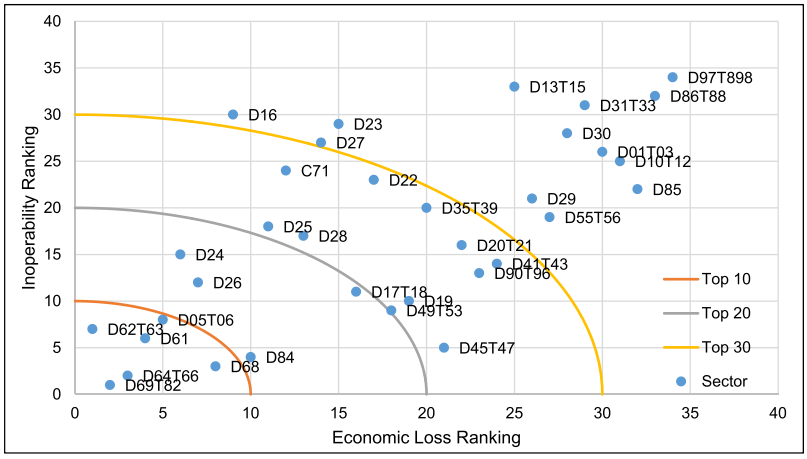

FIGURE 2. Dynamic Cross-Prioritization Plot.

sector's rank in terms of both inoperability and economic loss (see Figure 2). The three quarter circles in the plots represent top 10, top 20, and top 30 zones. A sector falls within a zone only if both its inoperability and economic loss ranks are below the respective threshold—thus, the top 10 zone may include fewer than 10 sectors. Additional plots for other scenarios are shown in Appendix D; Appendix E details all calculation steps and includes a link to the corresponding Excel tool (available upon request).

Aggregate Results across All Scenarios

Table 5 summarizes the total economic losses across seven AI risk scenarios, which differ in affected sectors, inoperability, and recovery times. Six of the seven scenarios show estimated losses between US$11 and 45 billion, while the most severe case—the AI-enabled cyberattack on infrastructure—reaches US$85 billion. Although significant, these figures remain in the corridor of the most catastrophic historical events, such as the 2011 Japan earthquake and tsunami (US$210 billion) or

TABLE 5
Summary of Total Economic Losses by Scenario

	Total economic damage (US$ million)								
		Variation inoperability only				Variation inoperability & recovery time			
Scenario	Mean	Min	Max	Range	Range/Mean	Min	Max	Range	Range/Mean
1. Business Software Failure	11,287	7,525	15,049	7,524	0.67	3,168	23,762	20,594	1.82
2. Autonomous Vehicle Network Failure	44,703	22,352	67,055	44,703	1.00	8,597	108,319	99,722	2.23
3. AI-Powered Misinformation Campaign	31,859	12,743	50,974	38,231	1.20	5,097	81,556	76,458	2.40
4. Algorithmic Flash Crash in Financial Markets	16,268	10,845	21,691	10,846	0.67	5,006	33,371	28,365	1.74
5. LLM Misuse in Legal and Healthcare Settings	37,472	14,989	59,956	44,967	1.20	7,494	56,208	48,714	1.30
6. AI-Enabled Cyberattack on Infrastructure	84,999	56,666	113,332	56,666	0.67	22,667	181,161	158,494	1.86
7. AI-Bias in Lending Algorithms	38,984	25,990	51,979	25,989	0.67	12,995	77,964	64,969	1.67

TABLE 6
Summary of Total Economic Losses by Scenario (with AI Dependency Level)

	Total economic damage (US$ million)						
	Mean	Variation of AI dependency level			Difference to Mean		
	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	none	low	medium	high	low	medium	high
Scenario	1/1/1	0.9/1/1.1	0.8/1/1.2	0.7/1/1.3	0.9/1/1.1	0.8/1/1.2	0.7/1/1.3
1. Business Software Failure	11,287	11,519	11,899	12,426	2.05%	5.42%	10.09%
2. Autonomous Vehicle Network Failure	44,703	45,219	46,106	47,372	1.16%	3.15%	5.97%
3. AI-Powered Misinformation Campaign	31,859	33,031	34,616	36,615	3.68%	8.65%	14.93%
4. Algorithmic Flash Crash in Financial Markets	16,268	19,154	22,268	25,611	17.74%	36.88%	57.43%
5. LLM Misuse in Legal and Healthcare Settings	37,472	36,933	36,725	36,849	−1.44%	−1.99%	−1.66%
6. AI-Enabled Cyberattack on Infrastructure	84,999	79,114	74,226	70,334	−6.92%	−12.67%	−17.25%
7. AI-Bias in Lending Algorithms	38,984	41,311	44,149	47,498	5.97%	13.25%	21.84%

Hurricane Katrina (US$125 billion) (Munich Re 2016). Overall, the loss estimates fall within the bounds of insurability and appear manageable for the insurance and reinsurance industry. For comparison, insured losses from Hurricane Katrina alone totaled US$60 billion. The only scenario that might require closer consideration in terms of insurability is the AI-enabled cyberattack on the critical infrastructure.

To assess the variability of loss estimates, we report minimum and maximum values based on (a) varying inoperability alone and (b) varying both inoperability and recovery time. These results reflect the uncertainty inherent in modeling AI risks, but also provide valuable insights into the potential economic scale of AI-related disruptions. Wide variations occur in scenario 2 and 3, with losses ranging from US$9 to 108 billion and US$5 to 82 billion. Some scenarios—such as LLM misuse in healthcare and legal settings—are relatively robust to uncertainty in recovery time, whereas others—like the AI-driven misinformation campaign—show highly volatile outcomes when both parameters are varied. From a risk governance and insurability perspective, the strong sensitivity of some scenarios to recovery assumptions suggests the need for tailored mitigation strategies, while the relative stability of others may indicate a more manageable risk profile for private insurers. For regulators, the findings point to the importance of scenario-specific preparedness: High-variance scenarios such as misinformation campaigns may require early-warning systems and contingency planning, while more stable risks could be addressed through conventional supervision and insurance market solutions.

The results indicate the potential severity of losses from AI-related events but do not assess their likelihood—an inherently difficult task. Some scenarios, like scenario 1, are based on real incidents and have already occurred, while others, such as a broad attack on infrastructure, remain hypothetical. This suggests that extreme scenarios may be rare but comparable in plausibility to other low-probability, high-impact events.

Integration of AI Dependency Level

To reflect that some sectors might experience more severe and less substitutable disruptions, we incorporate an AI dependency level into the DIIM parameterization. Initial inoperability values $\boldsymbol{q}$ were proportionally adjusted using sector-specific scaling coefficients (e.g., $0.9*\boldsymbol{q}$ for low, $1.0 * \boldsymbol{q}$ for medium, $1.1 * \boldsymbol{q}$ for high dependency). The sector-specific scaling coefficients are presented in Table 10 in Online Appendix B and were derived following Calvino et al. (2024), who present an AI intensity assessment by sector. Recovery times were also adjusted accordingly to reflect differences in substitutability using the same sector-specific scaling coefficients. This approach ensures that AI-intensive sectors such as finance or IT services exhibit greater operational fragility, also in line with other publications such as OECD et al. (2025), Singla et al. (2025), and Felten et al. (2021). Table 6 presents the baseline economic loss estimates from Table 5 (column 2), followed by the results under three different assumptions about AI dependency (columns 3 to 5). These dependency assumptions range from low adjustments (0.9/1/1.1) to more pronounced scaling (0.7/1/1.3). Columns 6 to 8 report the percentage deviations from the baseline in column 2.

All loss estimates remain within the corridor shown in Table 5, yet incorporating sector-level AI dependency introduces significant variations in losses. Scenarios that primarily affect highly AI-dependent sectors show upward adjustments. This is

TABLE 7
Estimated Economic Losses from Major Historical Catastrophes

Event	Year	Estimated Economic Loss (US$ million)	Key Affected Sectors	Reference
Japan Earthquake & Tsunami	2011	210,000	Manufacturing, energy, transport, construction, real estate, nuclear	Munich Re 2016
Hurricane Katrina	2005	125,000	Energy, construction, transport, real estate, public services	Munich Re 2016
Hurricane Sandy	2012	68,500	Utilities, transport, real estate, retail	Munich Re 2016
Deepwater Horizon Oil Spill	2010	65,000	Energy, environment, maritime, tourism, legal	Bousso 2018
9/11 Terror Attacks	2001	40,000	Air transport, finance, government	Carter 2021
NotPetya Cyberattack	2017	10,000	Logistics, IT, manufacturing, finance	Johansmeyer 2024

particularly visible in Scenario 4, where the affected industries—finance, IT, and professional services—are highly AI-intensive. Scenarios affecting a more heterogeneous set of sectors show mixed effects. Scenarios 5 and 6 exhibit lower losses under higher dependency levels. This occurs because these scenarios also impact sectors with low AI intensities, diluting the effect of dependency scaling. While higher dependency assumptions consistently lead to higher losses for most scenarios, the magnitude of the increase varies due to intersectoral spillover effects and the structure of the interdependency matrix. We also note that although the distribution of AI dependency across sectors is roughly balanced (15 sectors are designated as low, 11 as medium, 10 as high; see Online Appendix, Table 10), most modeled scenarios involve more AI-intensive industries, leading on average to higher losses when dependency is increased.

Benchmarking against Other Scenarios and Realized Losses

To evaluate the insurability and systemic relevance of AI risk scenarios, we benchmark their estimated economic losses against the results from Eling et al. (2023) and major historical catastrophic events. Table 7 provides a comparative overview, illustrating that the AI scenarios fall within or exceed the range of traditional large-scale disasters in terms of economic impact. We also note that the DIIM can be well applied also to the other scenarios presented in Table 7, given their regional but multisector impact. While the 9/11 terror attacks, for example, mainly affected aviation, finance, and government activities, Hurricane Katrina affected more the energy, construction, transport, real estate, and public sectors.

Compared with the extreme cyber risk scenarios analyzed by Eling et al. (2023), such as outage of a cloud service provider or SCADA system extortion, the current set of AI-related scenarios reflects a broader and more diversified systemic exposure. While both studies quantify total economic losses in the range of US$40 to 90 billion per event, the AI scenarios extend the scope beyond traditional cyber risk by integrating sociotechnical failures (e.g., LLM misuse in healthcare or AI-driven misinformation) and human–machine interaction risks (e.g., autonomous vehicle network failures). Furthermore, the AI cases demonstrate more cross-sectoral entanglement and feedback loops, highlighting that the insurability of such risks depends not only on technical vulnerabilities but also on algorithmic governance, data provenance, and societal trust. This broader framing suggests that future risk transfer mechanisms may require even more interdisciplinary modeling than that proposed in the cyber risk framework of the Eling et al. (2023) study.

CONCLUSIONS

This article presents a structured approach to estimating the economic impact of extreme AI risk scenarios using the dynamic inoperability input–output model. By combining qualitative scenario design with quantitative modeling, we address a critical gap in current AI risk analysis—namely, the lack of standardized, comparable, and empirically grounded loss estimates. Estimated losses across seven AI scenarios range from US$11 to 85 billion, with several scenarios falling within the range of private insurability, while others may require public–private risk-sharing mechanisms. In particular, the systemic nature of the AI-enabled cyberattack on critical infrastructure illustrates a scenario where the economic impact could exceed the risk-bearing

capacity of private insurers, potentially requiring government intervention or the establishment of public–private risk-sharing mechanisms.

Our findings suggest that while AI risks mirror cyber risks in their systemic potential and accumulation characteristics, they introduce new challenges tied to model monocultures, opacity, and rapid diffusion across critical sectors. This makes scenario-based stress testing not only useful but essential for insurers, regulators, and policymakers seeking to understand and manage AI-related systemic risks. Effective AI risk governance will require not only technical safeguards, but also cross-sectoral coordination, transparent reporting, and potentially new institutional frameworks to maintain economic and societal resilience.

This study has several limitations that must be acknowledged. First, the inoperability and recovery parameters are necessarily uncertain due to the near absence of historical data on AI-driven disruptions. The three-stage triangulation approach (literature review, expert elicitation, and survey evidence) can only provide corridors of plausible values rather than point estimates, and these corridors depend on the breadth and quality of available sources. Second, although the seven scenarios were designed to represent a balanced set of plausible extreme AI disruptions, they cannot cover the full spectrum of potential AI-related failures. Third, the model assumes that sectoral AI dependency translates proportionally into vulnerability, but empirical evidence on the substitutability of AI-driven tasks across industries is still lacking. Fourth, the DIIM framework captures economic propagation through intersectoral linkages but does not include behavioral adaptation, learning effects, substitution, or defensive investments. Finally, the lack of standardized, high-quality incident reporting for AI system failures limits the ability to calibrate or validate the model against real-world data. These limitations are not specific to this study but reflect the broader challenges inherent in emerging-risk quantification.

Future research could address these limitations in several ways. First, developing a standardized framework for documenting AI failures, similar to existing databases for cyber incidents or operational risk, would allow for empirical calibration and validation of disruption models; here from an actuarial point of view, not only the frequency but also the severity (that is estimating loss amounts) are critical. Second, microlevel studies of AI task substitutability and fallback procedures across industries would help refine sector-specific inoperability and recovery parameters. Third, future work should explore endogenous responses to AI failures, such as strategic substitution, manual overrides, demand shifts, or resilience investments, which are currently outside the DIIM framework. Fourth, alternative modeling approaches—such as agent-based models, network-based damage functions, or hybrid econometric–simulation architectures—could complement the input–output perspective and capture more complex propagation dynamics. Finally, comparative studies across countries and regulatory regimes could shed light on how institutional context shapes the economic consequences of AI disruptions. As AI adoption increases globally, the availability of empirical incident data and structured risk reporting is likely to grow, enabling more refined and empirically grounded analyses.

The article's standardized scenario taxonomy and sensitivity-based modeling framework offer a replicable foundation for future work. Although assumptions and uncertainties remain—particularly regarding expert-based parameterization and scenario frequency—our approach provides a starting point for better-informed decision-making. Future research should explore extensions to include reputational damage, positive demand shocks, and adaptive responses. As AI becomes foundational to our economies, developing robust tools to assess its downside risks is vital for safeguarding resilience.

DISCLOSURE STATEMENT

No potential conflict of interest was reported by the author.

REFERENCES

Acheson M. 2024. Texas Attorney General announces first-of-its-kind healthcare generative AI settlement. https://natlawreview.com/article/texas-attorney-general-announces-first-its-kind-healthcare-generative-ai-settlement

Ali J, Santos JR. 2015. Modeling the ripple effects of IT-based incidents on interdependent economic systems. Syst Eng. 18(2):146–161. https://doi.org/10.1002/sys.21293

Binns R, Veale M, Van Kleek M, Shadbolt N. 2018. "It's reducing a human being to a percentage": perceptions of justice in algorithmic decisions. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 377. https://doi.org/10.1145/3173574.3173951

Borch C. 2016. High-frequency trading, algorithmic finance, and the flash crash: reflections on eventalization. Econ Soc. 45(3-4):350–378. https://doi.org/10.1080/03085147.2016.1263034

Brundage M et al. 2018. The malicious use of artificial intelligence: forecasting, prevention, and mitigation. arXiv preprint. arXiv:1802.07228.

Bryson JJ, Diamantis ME, Grant TD. 2017. Of, for, and by the people: the legal lacuna of synthetic persons. Artif Intell Law. 25(3):273–291. https://doi.org/10.1007/s10506-017-9214-9

Bousso R. 2018. BP Deepwater Horizon costs balloon to $65 billion. Reuters. https://www.reuters.com/article/world/bp-deepwater-horizon-costs-balloon-to-65-billion-idUSKBN1F50O5

Calvino F, Dernis H, Samek L, Ughi A. 2024. A sectoral taxonomy of ai intensity (No. 30). OECD Publishing.
Carter RA. 2021. Promoting greater economic protection against man-made catastrophes: 20 years of lessons from 9/11. The Geneva Association. https://www.genevaassociation.org/publication/cyber/promoting-greater-economic-protection-against-man-made-catastrophes-20-years
Chafkin M. 2025. Why AI investors should worry about the self-driving car crash. Bloomberg. https://www.bloomberg.com/news/articles/2025-01-13/why-ai-investors-should-worry-about-the-self-driving-car-crash
Cimellaro GP, Reinhorn AM, Bruneau M. 2010. Framework for analytical quantification of disaster resilience. Eng Struct. 32(11):3639–3649. https://doi.org/10.1016/j.engstruct.2010.08.008
Dietzenbacher E, Miller RE. 2015. Reflections on the inoperability input–output model. Econ Syst Res. 27(4):478–486. https://doi.org/10.1080/09535314.2015.1063989
Dwivedi YK et al. 2023. "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges, and implications of generative conversational AI for research, practice and policy. Int J Inf Manage. 71:102642. https://doi.org/10.1016/j.ijinfomgt.2023.102642
Eling M, Elvedi M, Falco G. 2023. The economic impact of extreme cyber risk scenarios. North Am Actuar J. 27(3):429–443. https://doi.org/10.1080/10920277.2022.2034507
Enderle R. 2025 Jan 22. The coming catastrophic failure of AI in business. HPCwire. https://www.hpcwire.com/2025/01/22/the-coming-catastrophic-failure-of-ai-in-business/
ENISA. 2024. ENISA Threat Landscape 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
Ennis D, Cook T. 2019 Aug 16. Bias from AI lending models raises questions of culpability, regulation. Banking Dive. https://www.bankingdive.com/news/artificial-intelligence-lending-bias-model-regulation-liability/561085/
European Union. 2024. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations and Directives (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689.
Falco G et al. 2021. Governing AI safety through independent audits. Nat Mach Intell. 3(7):566–571. https://doi.org/10.1038/s42256-021-00309-0
Felten E, Raj M, Seamans R. 2021. Occupational, industry, and geographic exposure to artificial intelligence: a novel dataset and its potential uses. Strateg Manag J. 42(12):2195–2217. https://doi.org/10.1002/smj.3286
Garcia ACB, Garcia MGP, Rigobon R. 2024. Algorithmic discrimination in the credit domain: what do we know about it? AI Soc. 39(4):2059–2098. https://doi.org/10.1007/s00146-023-01676-3
Greenberg A. 2025 Apr 15. CyberAv3ngers: the Iranian saboteurs hacking water and gas systems worldwide. Wired. https://www.wired.com/story/cyber-av3ngers-iran-hacking-water-and-gas-industrial-systems
Guembe B et al. 2022. The emerging threat of AI-driven cyber attacks: a review. Appl Artif Intel. 36(1). https://doi.org/10.1080/08839514.2022.2037254
Haimes YY, Jiang P. 2001. Leontief-based model of risk in complex interconnected infrastructures. J Infrastruct Syst. 7(1):1–12. https://doi.org/10.1061/(ASCE)1076-0342(2001)7:1(1)
Haimes YY et al. 2005. Inoperability input-output model for interdependent infrastructure sectors. J Infrastruct Syst. 11(2):67–79. https://doi.org/10.1061/(ASCE)1076-0342(2005)11:2(67)
Heaven D. 2019. Why deep-learning AIs are so easy to fool. Nature. 574(7777):163–166. https://doi.org/10.1038/d41586-019-03013-5
Hendrycks D, Mazeika M, Woodside T. 2023. An overview of catastrophic AI risks. arXiv Preprint. arXiv:2306.12001.
Hoffman S, Podgurski A. 2021. Artificial intelligence and discrimination in health care. Case Western Reserve University School of Law. https://case.edu/law/sites/default/files/2021-01/Sharona%20CLE%202-2021_0.pdf
Holling CS. 1973. Resilience and stability of ecological systems. Annu Rev Ecol Syst. 4(1):1–23. https://doi.org/10.1146/annurev.es.04.110173.000245
IBM. 2025. 2025 IBM X-Force Threat Intelligence Index: large-scale credential theft escalates, threat actors pivot to stealthier tactics. https://newsroom.ibm.com/2025-04-17-2025-ibm-x-force-threat-index-large-scale-credential-theft-escalates,-threat-actors-pivot-to-stealthier-tactics
Johansmeyer T. 2024. Surprising stats: the worst economic losses from cyber catastrophes. The Loop. https://theloop.ecpr.eu/surprising-stats-the-worst-economic-losses-from-cyber-catastrophes
Jung J, Santos JR, Haimes YY. 2009. International trade inoperability input-output model (IT-IIM): theory and application. Risk Anal. 29(1):137–154. https://doi.org/10.1111/j.1539-6924.2008.01126.x
Lee NT, West DM, Tenpas D. 2023 Oct 10. How do artificial intelligence and disinformation impact elections? Brookings Institution. https://www.brookings.edu/articles/how-do-artificial-intelligence-and-disinformation-impact-elections/
Leontief WW. 1951. The structure of the American economy, 1919–1939: an empirical application of equilibrium analysis. Oxford University Press.
Leontief WW. 1966. Input-output economics. Oxford University Press.
Leontief WW. 1974. Structure of the world economy: outline of a simple input-output formulation. Am Econ Rev. 64(6):823–834.
Lian C, Haimes YY. 2006. Managing the risk of terrorism to interdependent infrastructure systems through the dynamic inoperability input-output model. Syst Eng. 9(3):241–258. https://doi.org/10.1002/sys.20051
Lian C, Santos JR, Haimes YY. 2007. Extreme risk analysis of interdependent economic and infrastructure sectors. Risk Anal. 27(4):1053–1064. https://doi.org/10.1111/j.1539-6924.2007.00943.x
Litman T. 2024. Autonomous vehicle implementation predictions: implications for transport planning. Victoria Transport Policy Institute. https://www.vtpi.org/avip.pdf
Mahmoud M et al. 2009. A formal framework for scenario development in support of environmental decision-making. Environ Modell Softw. 24(7):798–808. https://doi.org/10.1016/j.envsoft.2008.11.010
Makortoff K. 2025. Bank of England says AI software could create market crisis for profit. The Guardian. https://www.theguardian.com/business/2025/apr/09/bank-of-england-says-ai-software-could-create-market-crisis-profit
Miller RE, Blair PD. 2009. Input-output analysis: foundations and extensions. Cambridge University Press.
Mujtaba DF, Mahapatra NR. 2019. Ethical considerations in AI-based recruitment. 2019 IEEE International Symposium on Technology and Society (ISTAS). IEEE. p. 1–7. https://doi.org/10.1109/ISTAS48451.2019.8938018
Munich Re. 2016. Loss events worldwide 1980–2015. https://reliefweb.int/sites/reliefweb.int/files/resources/Loss_events_worldwide_1980-2015.pdf
Newman-Toker DE, Sharfstein JM. 2024. The role for policy in AI-assisted medical diagnosis. JAMA Health Forum. 5(4):E241339. https://doi.org/10.1001/jamahealthforum.2024.1339

Novelli C, Casolari F, Rotolo A, Taddeo M, Floridi L. 2024. AI risk assessment: a scenario-based, proportional methodology for the AI Act. DISO. 3(1):13. https://doi.org/10.1007/s44206-023-00056-5

OECD. 2018. Input-output tables 2018 edition. https://stats.oecd.org/Index.aspx?DataSetCode=IOTSI4_2018

OECD. 2021. State of implementation of the OECD AI principles: insights from national AI policies. https://oecd.ai

OECD, BCG, INSEAD. 2025. The adoption of artificial intelligence in firms: new evidence for policymaking. OECD Publishing. https://doi.org/10.1787/f9ef33c3-en

Panzieri S, Setola R. 2008. Failures propagation in critical interdependent infrastructures. IJMIC. 3(1):69–78. https://doi.org/10.1504/IJMIC.2008.018186

Rahwan I et al. 2019. Machine behaviour. Nature. 568(7753):477–486. https://doi.org/10.1038/s41586-019-1138-y

Resurreccion J, Santos JR. 2012. Multiobjective prioritization methodology and decision support system for evaluating inventory enhancement strategies for disrupted interdependent sectors. Risk Anal. 32(10):1673–1692. https://doi.org/10.1111/j.1539-6924.2011.01779.x

Roose K. 2023 May 30. A.I. poses "risk of extinction," industry leaders warn. The New York Times. https://www.nytimes.com/2023/05/30/technology/ai-threat-warning.html

Rose A, Sue Wing I, Wei D, Wein A. 2016. Economic impacts of a California tsu-nami. Natural Hazards Review. 17(2):04016002. https://doi.org/10.1061/(asce)nh.1527-6996.0000212

Santos JR. 2006. Inoperability input-output modeling of disruptions to interdependent economic systems. Syst Eng. 9(1):20–34. https://doi.org/10.1002/sys.20040

Singla A, Sukharevsky A, Yee L, Chui M, Hall B. 2025. The state of AI: how organizations are rewiring to capture value. McKinsey & Company.

Skrodelis H, Kelle R, Romanovs A. 2024. Cybersecurity in SCADA systems with advanced AI and ML techniques. Proceedings of the 2024 IEEE 65th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS). IEEE. p. 1–5. https://doi.org/10.1109/ITMS59813.2024.10778945

Uuk R et al. 2025. A taxonomy of systemic risks from general-purpose AI. arXiv. https://arxiv.org/abs/2412.07780

Wack M, Ehrett C, Linvill D, Warren P. 2025. Generative propaganda: evidence of AI's impact from a state-backed disinformation campaign. PNAS Nexus. 4(4):pgaf083. https://doi.org/10.1093/pnasnexus/pgaf083

Wei F, Koc E, Soibelman L, Li N. 2018. Disturbances to urban mobility and comprehensive estimation of economic losses. Polytechnica. 1(1–2):48–60. https://doi.org/10.1007/s41050-018-0005-1

World Economic Forum. 2025. AI in action: beyond experimentation to transform industry. https://reports.weforum.org/docs/WEF_AI_in_Action_Beyond_Experimentation_to_Transform_Industry_2025.pdf

Yan HY, Morrow G, Yang K-C, Wihbey J. 2025. The origin of public concerns over AI supercharging misinformation in the 2024 U.S. presidential election. HKS Misinformation Review. https://misinforeview.hks.harvard.edu/article/the-origin-of-public-concerns-over-ai-supercharging-misinformation-in-the-2024-u-s-presidential-election/