nature reviews physics

https://doi.org/10.1038/s42254-023-00676-y

Review article

Check for updates

Robustness and resilience of complex networks

Oriol Artime[1,2,3,15], Marco Grassia[4,15], Manlio De Domenico[5,6,7] ✉, James P. Gleeson[8], Hernán A. Makse[9], Giuseppe Mangioni[4] ✉, Matjaž Perc[10,11,12,13] & Filippo Radicchi[14]

Abstract

Complex networks are ubiquitous: a cell, the human brain, a group of people and the Internet are all examples of interconnected many-body systems characterized by macroscopic properties that cannot be trivially deduced from those of their microscopic constituents. Such systems are exposed to both internal, localized, failures and external disturbances or perturbations. Owing to their interconnected structure, complex systems might be severely degraded, to the point of disintegration or systemic dysfunction. Examples include cascading failures, triggered by an initially localized overload in power systems, and the critical slowing downs of ecosystems which can be driven towards extinction. In recent years, this general phenomenon has been investigated by framing localized and systemic failures in terms of perturbations that can alter the function of a system. We capitalize on this mathematical framework to review theoretical and computational approaches to characterize robustness and resilience of complex networks. We discuss recent approaches to mitigate the impact of perturbations in terms of designing robustness, identifying early-warning signals and adapting responses. In terms of applications, we compare the performance of the state-of-the-art dismantling techniques, highlighting their optimal range of applicability for practical problems, and provide a repository with ready-to-use scripts, a much-needed tool set.

Sections

A full list of affiliations appears at the end of the paper. ✉e-mail: manlio.dedomenico@unipd.it; giuseppe.mangioni@unict.it

Key points

- A variety of biological, social and engineering complex systems can be defined in terms of units that exchange information through interaction networks, exhibiting diverse structural patterns such as heterogeneity, modularity and hierarchy.
- Owing to their interconnected nature, complex networks can amplify minor disruptions to a system-wide level, making it essential to understand their robustness against both external perturbations and internal failures.
- The study of complex networks' robustness and resilience involves investigating phase transitions that usually depend on features such as degree connectivity, spatial embedding, interdependence and coupled dynamics.
- Network science offers a wide range of theoretical and computational methods for quantifying system robustness against perturbations, as well as grounded approaches to design robustness, identify early-warning signals and devise adaptive responses.
- These methods find application across a multitude of disciplines, including systems biology, systems neuroscience, engineering, and social and behavioural sciences.

Introduction

A broad spectrum of biological, social, socioecological and engineering systems is characterized by units — such as proteins, neurons, individuals or species — that exchange information by means of a complex network of interactions[1–3]. The resulting connectivity patterns are usually heterogeneous and fat-tailed, with a few units acting as hubs and several other units with a few connections[4–8], exhibiting a marked mesoscale organization into modules[9–13], hierarchies[14–16], networks of networks[17–22], high-order structures[23–25] and latent geometry[26–28].

Given the pervasive presence of complex networks in natural and artificial systems, it is important to understand under which conditions they can be fully functional and to what extent they are fragile to external perturbations and/or internal failures[29]. In fact, the interconnected nature of complex networks can be either beneficial or detrimental to disturbances. Networks exhibit a rich behaviour that ranges from absorbing — without relevant large-scale effects — specific types of perturbations to amplifying microscopic disruptions until they reach a system level. An emblematic example is the unfolding of a cascade of failures caused by perturbations localized on nodes that are central for information exchange (such as signalling, electricity redistribution and so on) between the units of a system[30,31]. Remarkably, the robustness and resilience of complex networks[32,33] are characterized by different types of phase transitions. The nature of these transitions depends on the structural features of a system (such as whether it is spatially embedded or not, interdependent with other systems or not, or multiplex[34–36]) and its dynamics (for instance, whether it has regimes in which collective behaviour emerges, such as in synchronization, epidemic spreading or coupled dynamics[37–40]).

The study of a system's response to perturbations in terms of structural and dynamical stability is crucial for applications because it can be used to anticipate critical transitions[41]. For instance, understanding cascading failure and robustness of a cell metabolic network[9,42] to activation or inhibition of specific enzymatic reactions can be used for developing specific therapies, drug repurposing and, more broadly, network and system's medicine[43]. Similarly, the robustness of protein–protein interaction networks to internal errors or external disruptions is strictly related to the function of a cell and its resilience across the tree of life[44]. In the human brain[45], localized disruptions can be related to strokes[46] and other pathological conditions. The stability[47–49] and restoration[50] of ecological and socioecological[51,52] systems depend on their robustness to disturbances. In social systems, the containment of epidemic outbreaks is intimately related to the percolation features of the underlying social network[38], and the propagation of systemic risks in financial and economic systems[53–56] depends on their resilience to cascading failures, similar to what happens in power grids which leads to generalized blackouts[57,58]. The efficiency[59,60] of traffic flows, from communication systems such as the Internet[61,62] to transportation networks such as the air routes[63], and their tolerance to errors and disruptions can be understood from percolation analysis.

The list of successful applications, stated above, is non-exhaustive. Nevertheless, despite their ubiquity and the importance of understanding the conditions leading to systemic breakdown, a systematic overview of the literature is still missing. We fill this gap by reviewing existing protocols for network dismantling and classify empirical case studies into three main phases: designing robustness, early-warning signals and adaptive responses. Specifically, we first introduce the theoretical framework to operationally define robustness and resilience. We then review the connection with percolation theory before describing theoretical and computational techniques adopted for optimal percolation and network dismantling. We next discuss cascading failures and the mechanisms leading to phase transitions that characterize the propagation of systemic risks. We describe the methods to prevent and react to systemic collapse and, finally, we conclude by identifying potential research directions for the near future. Node removal predominates in this Review, yet most of the concepts, metrics and techniques discussed throughout can be easily framed for link removal.

Background information

Throughout this Review, we consider systems characterized by a network structure. A network is a collection of units (nodes) non-trivially connected with each other by means of edges or links. In the physics literature, it is also common to describe them in terms of sites and bonds. A network can be mathematically represented by an adjacency matrix A, whose generic entry A_{ij} is positive if there is an interaction or relationship between the pair of nodes i and j, and zero otherwise. At the microscopic level, a widely used measure of connectivity is given by node's degree k_i, quantifying the number of links involving node i, whereas more sophisticated descriptors can be used to capture a variety of features, from the tendency to cluster in triangles to the centrality in information exchange between units[3].

Understanding how the structure and function of a network is affected by the failure of individual elements (nodes and/or edges) is a challenging task. In fact, microscopic failures do not sum linearly and, although most failures may not heavily affect the functionality of the underlying system, the removal of specific elements may cause its collapse. The more abrupt the transition to a dysfunctional state, the more challenging to capture early-warning signals to prevent it or to devise effective responses to mitigate it.

There are a variety of scenarios that should be considered, each with different implications. On the one hand, one can assume that

internal failures are randomly distributed, caused by a node (a router, for instance) or an edge (for example, a communication channel) breaking down. Yet, most real-world networks are robust against such random failures[29], owing to their highly heterogeneous connectivity[4]. On the other hand, network structure can be exploited by an agent to intentionally break the system via targeted attacks driven by some protocol. This is the case, for instance, of immunization policies[64], the crackdown of criminal, misinformation or malware networks[65,66], but also malicious attacks to power and natural gas distribution systems[67,68]. However, each attack has an intrinsic cost that depends on the specific system because removing a node or edge corresponds to an action, such as a vaccination, arrest, or shutdown of a server. An agent aims to minimize this cost by removing the minimum number of nodes and/or edges needed to reach a given target. In mathematical terms, this procedure is translated into the design of a removal protocol and a cost function to be optimized accordingly.

Unfortunately, finding the optimal set of sites or bonds to target is a challenging task even on small networks. An exhaustive search would need to explore all possible combinations of nodes and/or edges to remove. This operation scales exponentially with system size N because the number of units to remove to disrupt the system is not known a priori[69]. For instance, finding the optimal set of nodes on a small network with 50 nodes would require testing approximately $2^{50} \approx 10^{15}$ combinations.

The corresponding combinatorial optimization problem, called network dismantling, is thus NP-hard (that is, it cannot be solved optimally in polynomial time) and has usually been approached in rather different ways, including approximate theoretical models and computational heuristics.

Furthermore, there is no general agreement in the literature on how to measure the health of a system, or on what is the dismantling target, that is, the goal of the attack. In other words, how should one quantify the damage done so far to the system, with the aim of stopping the attack? And what function should one try to optimize during the dismantling process? Regarding measuring damage, the most common approach[70] involves percolation-related metrics, such as monitoring the size of the largest connected component (LCC) and stopping the attack once it has reached a given target size, although other network metrics such as efficiency[59,71] or nestedness[50,51,72] have been used. However, there is also no consensus on how small the connected components should be after the dismantling process. Rather, the size (either relative or absolute) that can be associated with the failure of the underlying system strongly depends on the system itself and on the application. For this purpose, some common values are 1%, 10%, 18% and 80% of the original size[4,66,68,69,73]. Regarding the optimization goal, some works aim at finding the smallest set of nodes possible[29,69], others aim at reducing the size of the LCC as much as possible after the beginning of the attack[68], whereas others aim to reduce the dismantling cost[66] as they assume that some nodes are more expensive than others to take down. Such goals are not necessarily compatible, and the choice of the goal depends again on the specific application and on the available resources (such as time or money) that can be used during the attack.

Another issue concerns the computational cost of the attacking algorithm itself, which can be measured in terms of runtime and memory usage. Computational complexity (or time complexity)[74] offers a way to measure the time spent by an algorithm to solve a problem and, thus, can be used to compare different algorithms rigorously. Specifically, the main assumption is that the runtime of the algorithm is proportional to the number of elementary operations it performs (expressed as a function of the input size) and that any kind of operation takes the same amount of time. Although this assumption is not exactly true, it is a good approximation that measures how the time spent scales with the input size and is not affected by the specific configuration of hardware, software or programming language because – at least theoretically – one could build an optimized configuration for each algorithm. In particular, the most used approximation, commonly used for comparisons, is the Big-O notation[74], representing the asymptotic number of operations performed as a function of the input size, and usually refers to the worst-case scenario, unless expressly specified otherwise. In fact, the best case is not relevant because it is usually associated with trivial instances, and the average case is generally hard to compute because it depends on the specific input and path in the algorithm. As an example, a time complexity of $O(N)$ indicates that, given the size of the input N, the algorithm performs N operations and $O(N^2)$ indicates that it performs N^2 operations. Similar considerations can be made for the spatial complexity, which measures how the memory usage scales with the size of the input. However, it is worth noting that spatial complexity is usually not considered in the literature because it is usually not a limiting factor for the algorithms.

In the next section, we discuss a direction connection between the aforementioned theoretical problems and percolation theory, a framework widely used in statistical physics to study the behaviour of a system and its critical response to perturbations.

Connection with percolation theory

Percolation is arguably the most direct and intuitive framework to approach network dismantling and, consequently, the most studied one. It is a famous model theoretically introduced in the study of gelation[75], later developed under the umbrella of statistical physics[32,76] and probability theory[77], and that has found many applications in different areas of science and engineering[78–80]. Percolation can be thought of as an experiment in which one removes nodes and/or links according to some predefined rules (also named attacking protocols) and then computes different statistical and geometrical properties of the residual network (Fig. 1a). This approach allows one to track the structural response of a system while its components are, for some reason (failures, maintenance, attacks and so on), out of action. The state of these components is considered binary: present (functional) or removed (failed), and one usually computes metrics related to the sizes of the remaining connected components formed by the non-failed nodes. The fruitful connection between percolation theory and network dismantling originates from the assumption that a bare-bones requirement for a system to function properly, whatever is its function, is to be globally connected. Hence, the loss of functionality owing to the network degradation maps to the phase transition of the percolation model. Operationally, this is conveniently characterized by quantities such as the critical point and the size of the LCC (also known as giant component in the thermodynamic limit), offering quantitative and qualitative insights of the dismantling process (Fig. 1b–d).

In complex networks, nodes are not structurally or functionally equivalent as they are in regular lattices. A plethora of methods and metrics to rank them according to different criteria exists, which are usually application-driven. This intrinsic heterogeneity offers a variety of attacking protocols, allowing one to assess network robustness under many physically relevant scenarios. For instance, a random selection of nodes is used to model failures and errors that occur in a system, whereas targeted attacks – driven by a more sophisticated

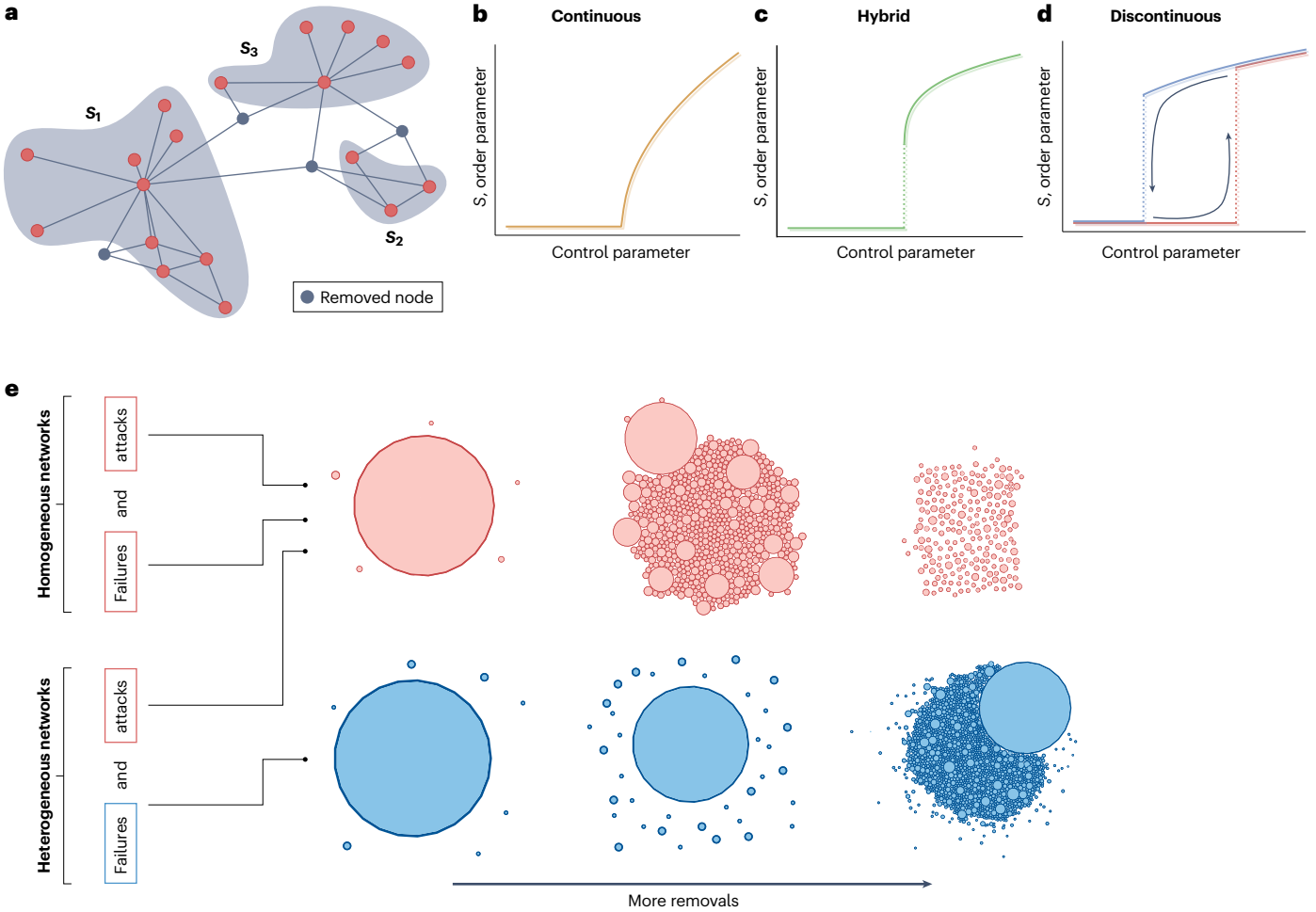


Fig. 1 | Percolation as static approach to network robustness. a, Network disintegration owing to the removal of some nodes (in grey), chosen according to a predefined removal protocol ϕ. As a results of the intervention, the network fragments in three connected components of sizes S_1, S_2 and S_3. These cluster sizes are a central quantity in the study of percolation. **b**–**d**, The nature of ϕ, related to the control parameter, heavily impacts on the response of the network, resulting in different sorts of phase transitions for the size of the giant (largest) component. **e**, How networks with homogeneous and heterogeneous connectivity patterns (roughly speaking, degree distributions with a second moment of similar order to the square of the mean or much larger than the mean, respectively) respond to failures and targeted attacks. Circles represent isolated components whose radius depend on their number of nodes. Each vertical column assumes the same number of nodes or links removed. Part **e** is adapted from ref. 225, CC BY 4.0.

protocol – can be implemented as informed interventions. Such interventions can be informed by topological information, such as those that remove nodes with the largest number of connections or with largest centrality[81,82], or by non-topological information, such as those informed by node or edge metadata[83].

There is a non-trivial interplay between the dismantling protocol and network topology. In both synthetic and empirical networks, homogeneous or heterogeneous connectivity patterns can induce radically different responses[29] (Fig. 1e). Homogeneous networks react to failures and attacks in a similar way because the largest possible degree is not far from the mean value, yielding always a finite dismantling point (Fig. 1e). However, for heterogeneous networks, such as scale-free networks, failures and attacks cause different responses because of the role the hubs have. Hubs are extremely good at holding together the network when malfunctions are placed uniformly at random, but if nodes are directly targeted, then the network breaks apart rapidly – the so-called robust-yet-fragile property of heterogeneous networks (Fig. 1e). This difference between homogeneous and heterogeneous networks agrees with the prediction of dismantling points in uncorrelated networks[84,85]; it was further formalized and quantified theoretically using an approach based on generating functions[86–89].

The advantage of the methods that rely on generating functions is their mathematical flexibility to encompass generalizations, while offering some predictive power about critical exponents[85,90,91], for example, or closed-form equations for the critical point and the size of the giant component[92]. Such methods assume that the underlying network is an annealed version of the configurational model; hence, they tackle robustness at an ensemble level and become useful to unravel the part played by the functional form of the degree distribution p_k or its parameters. For instance, given a degree-dependent protocol of

node removal ϕ_k, the size of the giant component S^{GF} is given by the solutions of

$$S^{GF} = G(1) - G(u) \quad (1)$$

$$u = 1 - H(1) + H(u), \quad (2)$$

where $G(z) \equiv \sum_k p_k \phi_k z^k$ and $H(z) \equiv \frac{1}{\langle k \rangle} \sum_k (k+1) p_{k+1} \phi_k z^k$ are the generating functions of the degree distribution and the excess degree distribution, respectively. (The excess degree is the number of connections minus one of a randomly chosen neighbour of a node). $\langle k \rangle$ denotes the mean degree. The dismantling point is given by $H'(1) = 1$. Similar equations can be written for the case of random link failures[93]. From these equations, one can easily check that the location of the dismantling point coincides in both site percolation (in which one removes nodes) and bond percolation (in which one removes links). Remarkably, the critical exponents characterizing the phase transition also coincide, and they are network-independent and equal to the mean-field predictions[76], as long as the connectivity patterns in the network are not too heterogeneous. However, these results do not hold for more heterogeneous networks: for instance, in scale-free networks, the universality equivalence breaks down[94], and the critical indices may depend on the exponent of the degree distribution[85].

The case of targeted attacks on links has been less explored in the literature. To encode the link information in the dismantling process, one would need to consider simultaneously the topological properties of the two nodes at the end of the link, requiring a more involved mathematical treatment than the one presented above[95]. Despite this fact, many empirical networks are weighted[96] or have features and/or metadata defined on the edges. Thus, formalizing the dismantling problem on these cases will no doubt be a fruitful future application of percolation theory.

Generating-function methods might not always be practical to accurately predict the robustness of empirical networks because one aims to know how a specific network topology, and not the underlying ensemble, reacts to malfunctions. In this case, message-passing methods, which take as input the actual connectivity of the networks instead of their degree distributions, might be more convenient to compute percolation quantities[97–100]. This approach leads to a more complicated mathematical and numerical treatment, but it often offers better estimates for the giant component and the critical point than the method based on generating functions[101,102].

As an example, if we denote by ϕ_i the probability that node i has not been removed, the size of the giant component S^{MP} of a network is given by

$$S^{MP} = \frac{1}{N} \sum_{i=1}^{N} s_i \quad (3)$$

$$s_i = \phi_i [1 - \prod_{j \in \mathcal{N}_i} (1 - t_{i \to j})] \quad (4)$$

$$t_{i \to j} = \phi_i [1 - \prod_{k \in \mathcal{Q}_{i \to j}} (1 - t_{j \to k})]. \quad (5)$$

Here, s_i represents the probability of node i to belong to the giant component, $\mathcal{N}_i$ denotes the neighbourhood of node i and $\mathcal{Q}_{i \to j}$ stands for the subset of nodes to whom j passes a (directed) message regarding the probability of belonging to the giant component through the edge that joins them. Typically, $\mathcal{Q}_{i \to j} = \mathcal{N}_j \backslash \{i\}$ to avoid backtracking messages, although other choices that take short-range loops into account are possible[102]. Close to the dismantling point, all the $t_{i \to j}$ tend to 0, so equation (5) can be expanded to obtain $\mathbf{t} = \boldsymbol{\phi} \circ (G\mathbf{t})$, where $\circ$ is the Hadamard product and $\boldsymbol{\phi} \equiv (\phi_1, \ldots \phi_2, \ldots, \phi_N \ldots \phi_N)$, with each ϕ_i appearing k_i times. G is a logical matrix of dimension $2|E| \times 2|E|$, where $|E|$ is the number of edges, and it depends on $\mathcal{Q}_{i \to j}$. The dismantling condition is given by the emergence of a non-trivial solution in the eigenvalue problem $G\mathbf{t} = \mathbf{t} \oslash \boldsymbol{\phi} \equiv \lambda \mathbf{t}$, where $\oslash$ is the Hadamard division and λ is the eigenvalue. The Perron–Frobenius theorem indicates that the non-trivial solution is related to the largest eigenvalue of the operator G. For a constant occupation probability $\phi_i = \phi$, one obtains $\phi_c = 1/\lambda_{max}$, where λ_{max} is the largest eigenvalue of G.

Message-passing methods can be developed for bond percolation, too. If a fraction $1 - \phi$ of links chosen uniformly at random is removed from the network, then the size of the giant component is given by S^{MP}/ϕ. Thus, message passing predicts the same percolation threshold for site and bond percolation, in agreement with the predictions based on generating functions[94]. Network dismantling based on link attacks can be readily implemented in this framework because the removal probability of each individual link can be encoded in a new vector of occupation probabilities ϕ' to be plugged in the message-passing equations for bond percolation.

Percolation theory also helps make predictions on the robustness of networks that display topological correlations, a feature that characterizes most empirical interconnected systems. One of these correlations is the so-called assortative mixing[103], that is, the tendency of nodes to be connected to peers of similar kind. Networks that are assortative in their degree tend to be more robust than those with disassortative patterns because hubs create a redundant core that hold the network together when faced with both random or hub attacks[104]. The presence of local clustering, that is, an overabundance of closed triangles with respect to a randomized network, has been also considered in different ways. Depending on how clustering is defined and on whether its value is high or low, the network might be considered more or less robust than its unclustered counterpart[105–108]. Going beyond local topological correlations, the robustness of networks that display mesoscale non-trivial structures is another phenomenon well-suited to being addressed under the percolation framework. One possible mesoscale structure is core–periphery network organization[109]. When these structures are attacked randomly, they can display two dismantling points: one owing to the nodes in the core and one for those in the periphery[110–112]. Another structure is k-cliques, whose percolation-based analysis has been useful to identify overlapping communities[113].

Dismantling can occur in an abrupt manner that is very difficult to anticipate, owing to the absence of apparent early-warning signals. Such sudden transitions can produce a huge socioeconomic impact. Some recent examples are the far-reaching consequences of the 2008 financial crisis[114] or the spread of COVID-19 (ref. 115) that led to a worldwide recession and a radical modification of living standards. Thus, identifying those scenarios in which a sudden transition might occur is valuable. Percolation theory offers a diversity of mechanisms that can induce such abrupt topological fragmentations. One is the so-called k-core percolation, in which all the nodes with degree less than k are removed, iteratively[116]. For $k = 2$, the transition is continuous, but for $k > 2$, it becomes hybrid. Bootstrap percolation, which allows removed nodes to recover if they have a number of neighbours above a certain threshold, can also present discontinuous and hybrid transitions[117].

Additionally, there is a family of models based on selection rules that might considerably accelerate or delay the critical point, at the expense, though, of drawing upon mesoscopic information[118–121]. Among these, the most famous is the product rule that leads to explosive percolation[122]. This product rule consists of picking uniformly at random two links and removing the one that maximizes the product of sizes of the components it joins: in this way, the onset of percolation becomes abrupt. Furthermore, the dismantling point occurs before that of the percolation case based on random link picking. Despite this abruptness, it was shown that the explosive transition of the product rule is actually continuous, but with a peculiar critical behaviour[123–125]. Further information about explosive percolation can be found in a recent review[126]. Finally, a last mechanism that might yield abrupt dismantling is associated with interdependencies when different networks are coupled. Interdependencies have a central role in the study of cascading failures, to be discussed in a next section, but they can be modelled with a static percolation framework and shed light on the conditions under which discontinuous transitions appear[127].

All in all, percolation is a central model in network robustness owing to its flexibility, its low computational cost and its analytical power[93]. It proposes protocols to dismantle interconnected systems according to some metric, thus unveiling the importance of these precise indicators of the vulnerability of a system. However, in other cases, the intervening protocols are metric-agnostic and goal-oriented. Following these lines, in the next section, we focus on algorithms that look for strategies to dismantle networks as efficiently as possible.

Optimal percolation and network dismantling

Searching for the optimal strategy, that is, finding the smallest set of nodes for the fastest network disintegration, is the optimal percolation problem[128], also known as network dismantling[69]. This is a combinatorial optimization problem that aims at finding the set of nodes (or edges) that disrupts a network the fastest when removed, breaking the LCC into isolated sub-components and, thus, efficiently degrading the functionality of a system. Such an optimization problem is computationally challenging even on small networks (that is, it is NP-hard), and in the literature, there is no agreement on how small the sub-components should be after the dismantling process, or even on the dismantling target.

Earlier work has aimed at finding the smallest set of nodes to break the network by characterizing their importance by a series of topological centralities. A simple strategy to break the network consists of attacking nodes in the order given by a centrality score. The most basic such score is the degree of the node, which privileges the hubs, following the intuition that the more connections, the better[29,73]. These strategies can also be divided in static and dynamic ones, the difference being that the former computes the removal order of nodes (or edges) at the beginning of the dismantling process, whereas the latter updates the order during it, thus accounting for the changing state of the network.

However, there are plausible circumstances in which the crucial nodes do not correspond to the most connected ones but to those nodes that have few connections, yet are strategically located within the core of the network. These topological bridges represent a fundamental notion in sociology known as "the strength of weak ties"[129]. Many heuristic centralities have been proposed to find these crucial nodes. They can be classified into broad classes as follows: degree-based (such as hubs and k-cores), shortest path-based (such as closeness and betweenness centralities), walks-based (such as eigenvector, eigenvalue and Katz centralities), random walk-based (such as PageRank), non-backtracking walk-based, and machine learning-based approaches. At a higher level of classification, one can distinguish between genuinely structural methods, based on topological descriptors, and genuinely dynamical methods, based on some kind of flow dynamics between nodes.

Optimal percolation systematizes the search for the optimal set of nodes to attack by attempting to find a configuration of nodes $\mathbf{n}^*$ corresponding to the minimal fraction of removals q_c^{opt} such that the LCC of the network G_∞ is disintegrated optimally[128]:

$$q_c^{\mathrm{opt}} = \min\{q \in [0,1] | G_\infty(q) = 0\}. \tag{6}$$

Optimal percolation is an NP-hard combinatorial problem[130], intractable because an explicit functional form of $G_\infty(\mathbf{n})$ is not feasible. However, an approximated solution for sparse networks[128] lead to the collective influence (CI) algorithm[131]. An approximate optimal set is obtained as an (infinite) sequence of optimized attacks expressed as successive approximations to the minimization of the largest eigenvalue of the non-backtracking matrix. It leads to the CI index of node i with degree k_i:

$$\mathrm{CI}_\ell(i) = (k_i - 1) \sum_{j \in \partial \mathrm{Ball}(i,\ell)} (k_j - 1), \tag{7}$$

where $\partial\mathrm{Ball}(i, \ell)$ is the surface of a ball of radius ℓ (estimated from shortest-path distances) around node i. This algorithm gives a good approximation to the optimal percolation set. Later, better algorithms based on message passing[132] and belief propagation[133] were proposed, including decycling and dismantling[69,134] and explosive percolation[64]. They have enriched our understanding by tackling the optimal percolation problem with rigorous theories, and they further generated a number of sophisticated and efficient algorithms that are applicable to large-scale complex systems.

A study[134] has shown that the optimal disintegration of the giant component is achieved by the disintegration of cycles (known as 'decycling') found by the minimum feedback vertex set. For sparse random networks, short loops rarely exist in small connected components. If the long loops in the giant component are cut, the network will break into small tree fragments. The optimal decycling threshold q_c^{dec} acts as an upper bound of the optimal percolation threshold q_c^{opt} (ref. 69). Optimal decycling is NP-hard and can be approximately solved via belief propagation algorithms. Two approaches were developed, the belief propagation-guided decimation algorithm[134] and the Min-Sum algorithm[69], that find smaller influencer sets than the CI algorithm, albeit at the expense of increasing complexity. In particular, both algorithms first decycle the network via message-passing algorithms then break the resulting forest (that is, a disjoint union of trees) using a tree-breaker algorithm. Whereas the computational complexity of each message-passing iteration is linear with the number of edges, the greedy tree-breaker algorithm proposed in ref. 69 scales as $O(N(\log(N+T))$, where T is the maximal diameter of the trees inside the forest and N is the number of nodes. Furthermore, the Min-Sum algorithm also includes a reinsertion phase at the end of the attack, consisting of a greedy process that reintroduces the nodes that are not actually needed to reach the desired target. The reinsertion phase is meant to reduce the number of nodes that are actually removed from the network — thus decreasing the cost of the attack — and should be used in heavy-tailed networks, in which the decycling and the dismantling problems are not equivalent. A sub-linear time complexity has been reported for this phase, but the exact complexity is not known[135].

Table 1 | Summary of the main algorithms for targeted attacks

Algorithm	Type	Dynamic[a]	Reinsertion[b]	Computational complexity[c]	Ref.
Collective influence (CI)	Influence maximization	Yes	Yes	$O(\|V\|\log\|V\|)$	131
Belief propagation-guided decimation (BPD)	Message passing-based decycling	Yes	No	$O(\|E\|T)$	134
Min-Sum	Message passing-based decycling	Yes	Yes	$O(\|E\|T) + O(\|V\|(\log(\|V\|) + T))$	69
Generalized network dismantling (GND)	Spectral partitioning	Yes	Optional	$O(\|V\|\log^{(2+\epsilon)}(\|V\|))$	66
Ensemble GND (EGND)	Spectral partitioning	Yes	Optional	$O(e)\cdot O(\text{GND})$	136
CoreHD	Degree-based decycling	Yes	Yes	$O(\|V\|)$ (on sparse networks)	135
Explosive immunization (EI)	Explosive percolation	Yes	No	$O(\|V\|\log(\|V\|))$	64
Graph dismantling with machine learning (GDM)	Machine learning	Static	Optional	$O(h(\|V\|+\|E\|))$	68
CoreGDM	Machine learning	Static	Yes	$O(h(\|V\|+\|E\|))$	138
FINDER	Machine learning	Yes	Optional	$O(\|E\| + \|V\|(1 + \log(\|V\|))$	137

$|V|$, number of nodes; $|E|$, number of edges; e, ensemble size; h, number of attention heads used. [a]Whether the algorithm is dynamic (or static). [b]Whether the algorithm includes a phase of reinserting nodes. [c]Reported for sparse networks.

Inspired by these decycling-based algorithms, other algorithms have been developed. CoreHD[135] is a simple and fast heuristic algorithm with complexity $O(N)$ (for sparse networks), the idea being to decycle the network by iteratively removing the nodes with the highest degree from the 2-core, then use the same tree-breaking and reinsertion algorithms used by Min-Sum. Explosive immunization[64] is based on the explosive percolation transition. Generalized network dismantling[66,136] aims to address the non-unit cost of removals and is based on iteratively removing those nodes that maximize an approximated spectral partitioning.

Other studies have also proposed machine learning-based attack strategies, such as graph dismantling with machine learning (GDM)[68] and FINDER[137]. Both use geometric deep learning, specifically graph neural networks, to learn an attack strategy on small synthetic networks. However, whereas GDM learns in a supervised manner on networks dismantled optimally via brute force, FINDER learns in a reinforcement fashion. Another algorithm is CoreGDM[138], which is inspired by CoreHD as it attacks the 2-core of the networks using GDM models. In addition, the performance of network embeddings in Euclidean and hyperbolic spaces has been investigated[139].

Optimal percolation was also studied on multiplex networks[140] and game theory[141].

In terms of dynamical information flow in the network, optimal percolation aims to find the minimal set of 'super-blockers' that could stop the spreading[142]. A dual problem is to find the super-spreaders of information that maximize the spreading if selected as seeds. In general, these two problems are not necessarily equivalent[143]. However, for a particular form of the linear threshold model of spreading with thresholds given by $k_i - 1$, optimal percolation is equivalent[128] to the influence maximization problem[130]. The goal of influence maximization problem is to find the optimal set of k-superspreaders (influencers) that would initiate the largest-scale process of information propagation in the network. For a given number of initial spreaders k, one wishes to find a k-node set S^* of maximum influence $\sigma(S^*)$:

$$S^* = \underset{|S|=k}{\operatorname{argmax}} \sigma(S) \tag{8}$$

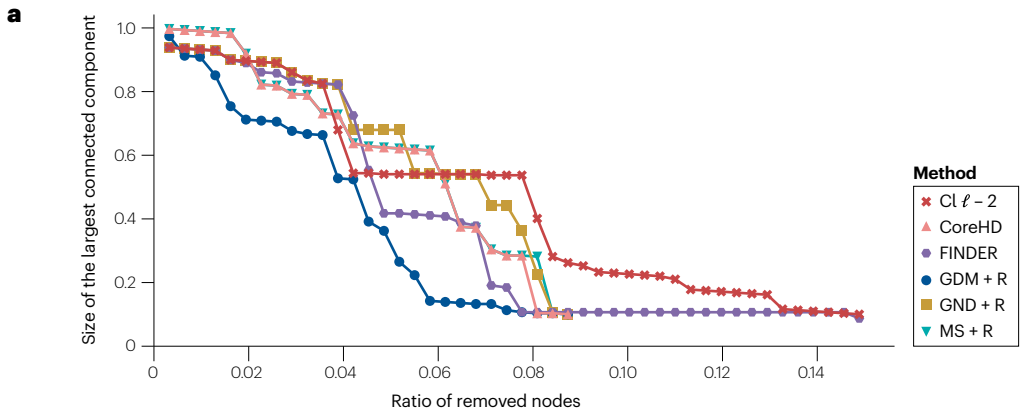
This approach opens the applicability of optimal percolation to a wide variety of societal problems and beyond[144]: theories of influencers encountering applications for identifying influential spreaders in social media, super-spreaders of disease in pandemics, essential gene mutations in genetic networks that could lead to disease, essential areas in the brain for integration, keystone species whose extinction could bring an ecosystem to the tipping point of collapse, and financial institutions that are 'too big to fail'.

To this aim, an approach based on network states encoded into suitably defined density matrices has been proposed[145]. In this approach, robustness is analysed at multiple scales corresponding to the timescales required for information to diffuse through the network[146]. Application to empirical social, biological and transportation systems has shown that nodes crucial for information dynamics are also responsible for keeping the network structurally integrated, but the opposite is not necessarily true and functional fragmentation happens before full structural disintegration[147].

A summary of the algorithms described above, along with their main features, can be found in Table 1. When performing robustness assessments, one needs to evaluate which is the most physically meaningful and computationally efficient approach for each particular network to be dismantled. For instance, if algorithms are applied to a corruption network (Fig. 2), the GDM algorithm with reinsertion is the one that dismantles it the fastest, in approximately 20 removals out of the 309 nodes. Yet, there is no one-size-fits-all algorithm, as we report in summary in Table 2 (full results in Supplementary Table 3). In it, we present a performance comparison on a large set of real-world networks from different application domains (biological, information, social and technological), finding that the best algorithm varies within and across domains. See Supplementary Tables 1 and 2 for further details on the chosen empirical networks and Supplementary Tables 4 and 5 for a comparison on synthetic networks and on the Lancichinetti–Fortunato–Radicchi[148] model.

Apart from the ad-hoc algorithms shown in Table 1, one could use direct optimization algorithms (such as simulated annealing, Tabu search or genetic algorithms) to find the optimal dismantling set q_c. However, owing to the large dimension of the search space, they do not scale well and, thus, are often unable to provide good solutions. As an example, the Min-Sum algorithm outperforms simulated annealing[135].

So far, we have approached robustness and resilience from the static viewpoint of percolation models. However, it is desirable to


a
Size of the largest connected component
1.0
0.8
0.6
0.4
0.2
0
0
0.02
0.04
0.06
0.08
0.10
0.12
0.14
Ratio of removed nodes
Method
Cl ℓ − 2
CoreHD
FINDER
GDM + R
GND + R
MS + R

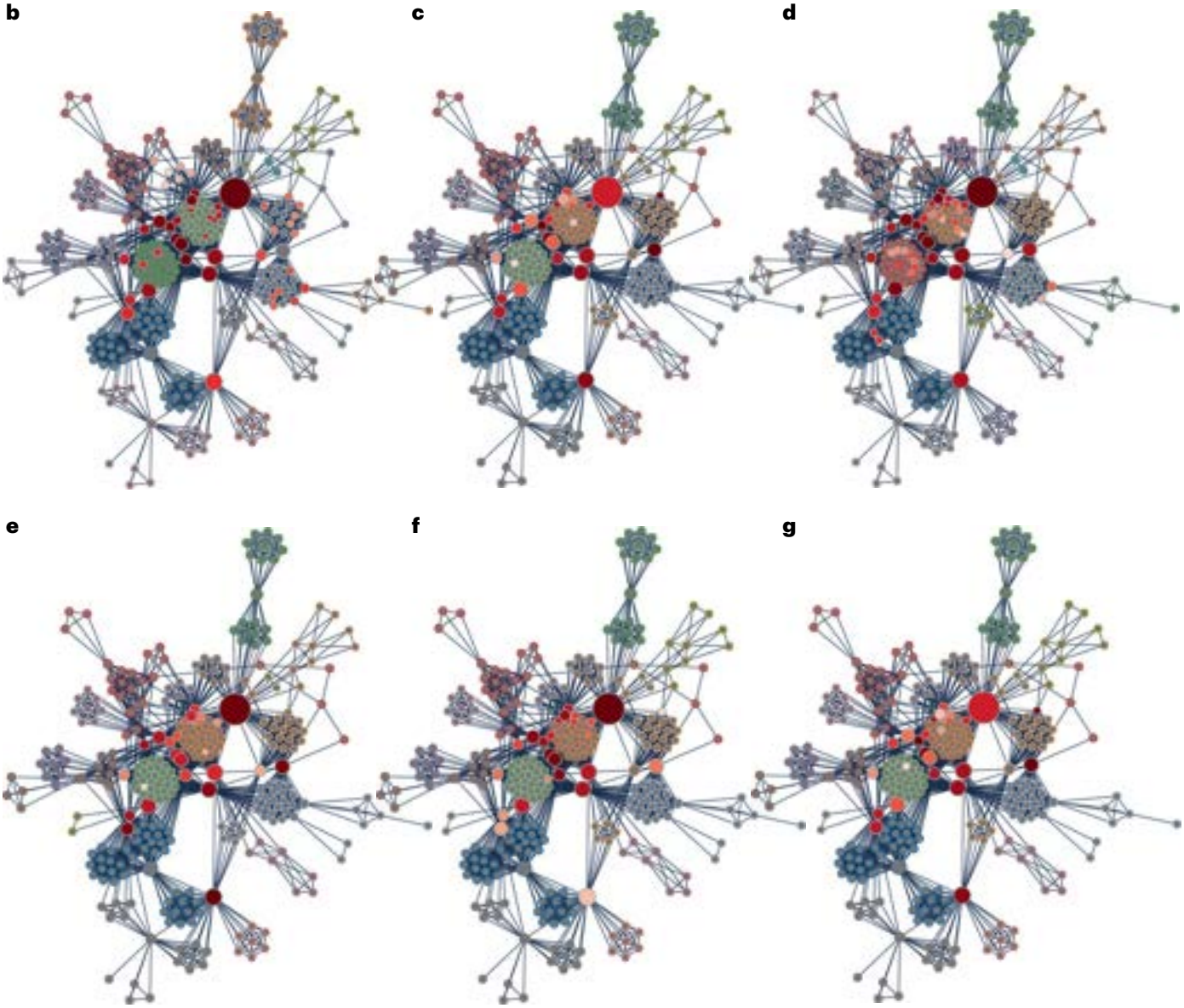

b
c
d
e
f
g

Fig. 2 | Comparison of state-of-the-art dismantling methods. a, Algorithms are compared in terms of their ability to drive the system — a Brazilian corruption network[65] with 309 nodes — towards disintegration, as measured by the relative size of the largest connected component. **b**–**g**, The disintegrating paths of the different curves shown in part **a**. The colour of the nodes represents (from dark red to white) the attack order (nodes in grey are not removed), and their size represents their betweenness value. The contour colour of remaining nodes represents the cluster they belong to after the attack. Part **a** is adapted from ref. 68, CC BY 4.0. MS+R, Min-Sum with reinsertion phase.

address the scenario in which small malfunctions, located in the network either randomly or in a targeted fashion, can spread and trigger global network-wide effects, known as cascades. We investigate them in the next section.

Cascading failures

One of the most damaging processes that can unfold in a network is a cascade of failures. The errors and attacks suffered by empirical systems usually are dynamical in nature and, even if they originate in a small, localized part of the system, they may spread further until the entire system catastrophically collapses. Examples include line outages in the power grid (Fig. 3a), mass extinctions in ecological areas and fake news or rumour spreading in online social platforms (Fig. 3b). It is crucial to understand the mechanisms under which such malfunctions are able to propagate and how the network is affected as they do so. In spite of the differences with the static percolation framework, some metrics borrowed from percolation are used to quantify the robustness and resilience to cascades, such as the size of the giant component of the non-failed network once the cascade stops, or the critical point at which the surviving giant component dismantles.

In this section, we review different approaches to cascading failures by using stylized models that seek to provide general insights into malfunction (or other) spreading. We do so from a statistical physics standpoint, namely, by disregarding the particular microscopic, domain-oriented aspects of particular systems that may go beyond this Review. Instead, we advocate for focusing attention on the large-scale patterns and the collective, emergent behaviours that are common to a variety of seemingly different networked systems.

One large family of models are those in which failures spread through interdependencies. This is a central concept in systems theory and refers to the dependency relations that exist between different microscopic and mesoscopic parts of a macroscopic system and that sustain the overall proper functionality. Examples pervade many branches of sciences across scales, from biochemistry to man-made planetary engineering systems[149]. Two equivalent theoretical frameworks, namely, multilayer networks[21,22,150–152] and networks of networks[153,154], have been successfully used to frame the modelling of such cascades. In them, each layer (or network) is associated with a subsystem and dependencies are encoded in the interlayer (or internetwork) links. At odds with static percolation, in this case, one deals with snapshots of a network that is progressively degraded, whose dismantling is dictated by dependency-related rules (Fig. 3c).

In 2003, the Italian power grid suffered an outage owing to a damaged power station that led to the failure of some Internet communication networks, which, in turn, created a feed-forward loop of failures among both systems. This situation inspired a theoretical model of cascading failures mediated by interdependencies in a bilayer network[17]. Percolation quantities, such as the size of the giant component, can be analytically tracked at each snapshot of a system evolving according to the model, yielding excellent agreement with simulations (Fig. 3d). The theory is flexible and admits generalizations to an arbitrary number of coupled subsystems[19,155], partial and asymmetric interdependency relations[156,157], and so on. For instance, if layer $i = 1, \ldots, n$ suffers a failure or an attack that leaves a fraction ϕ_i of functional nodes, and q_{ji} indicates the fraction of nodes in layer i that directly depend on nodes of layer j, then the stationary value of the giant component in layer i, S_i^{st}, can be obtained by solving the system of equations[19]

$$S_i^{\mathrm{st}} = x_i g_i(x_i), \tag{9}$$

$$x_i = \phi_i \prod_{j=1}^{K} [q_{ji} y_{ji} g_j(x_j) - q_{ji} + 1], \tag{10}$$

$$y_{ij} = \frac{x_i}{q_{ji} y_{ji} g_j(x_j) - q_{ji} + 1}, \tag{11}$$

where $g_i(z) \equiv 1 - G_i(z f_i(z) + 1 - z)$ and $f_i(z) = H_i(z f_i(z) + 1 - z)$. $G_i(x) \equiv \sum_k p_k^i x^k$ is the degree generating function and $H_i(x) = G_i'(x)/G_i'(1)$ is the excess degree generating function of a subsystem i, which has degree

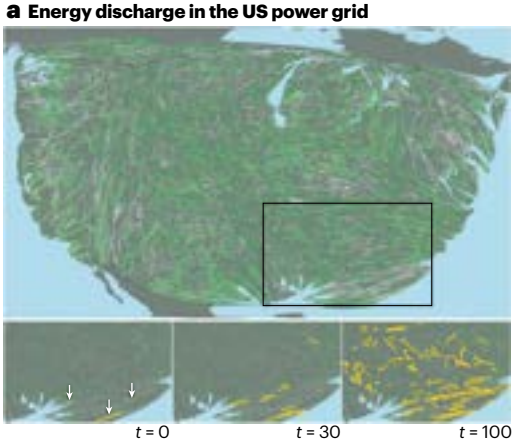
Table 2 | Average per-method area under the curve (AUC) of the dismantling of real-world networks, grouped per category

Network	AD	BC	EI σ_1	GDM	GND	FINDER	PR	MS	CI ℓ–2[a]	CoreHD	GDM +R	GND +R	MS +R
Biological result	114.3	143.0	125.6	109.3	123.1	110.8	129.8	133.9	101.0	116.7	103.8	113.7	117.3
Information result	162.9	255.4	150.2	127.2	147.3	193.7	173.1	647.8	262.7	121.0	110.7	116.8	126.8
Social result	123.2	150.6	141.8	112.0	117.4	120.1	131.5	221.1	111.4	128.7	106.5	114.3	128.2
Technological result	545.0	982.2	125.6	278.6	222.8	492.0	514.7	557.3	338.7	134.5	127.4	138.6	134.5
Grand average	240.5	390.0	137.6	158.3	153.0	233.2	240.4	399.7	207.2	126.6	112.6	121.2	127.9

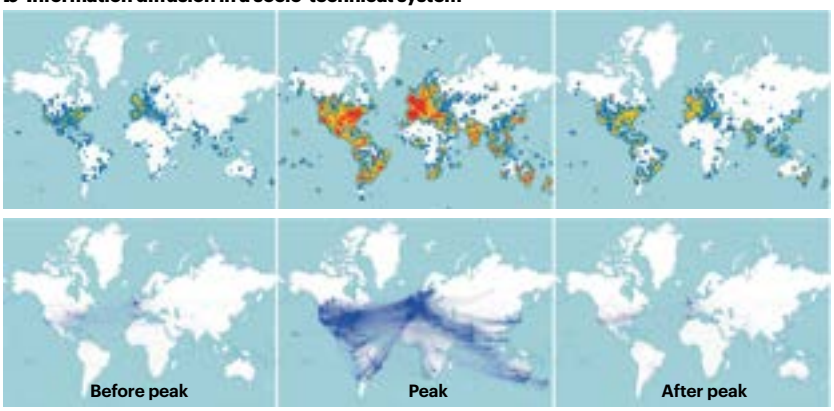
The dismantling target for each method is 10% of the network size. AUC is computed by integrating the $|\mathrm{LCC}(x)|/|V|$ (the size of the largest connected component (LCC) as a function of the removed nodes) values using Simpson's rule. For readability, AUC values of each network are expressed as the percentage of the value obtained by the best-performing method on that network, that is, the lower the AUC, the better. Full results are available in Supplementary Table 3. AD, adaptive degree; BC, betweenness centrality; CI, collective influence; EI, explosive immunization; GDM, graph dismantling with machine learning; GND, generalized network dismantling; MS, Min-Sum; PR, PageRank; +R, reinsertion phase is performed. [a]CI and CoreHD are compared with other +R algorithms as they include the reinsertion phase.

Empirical cascades

a Energy discharge in the US power grid



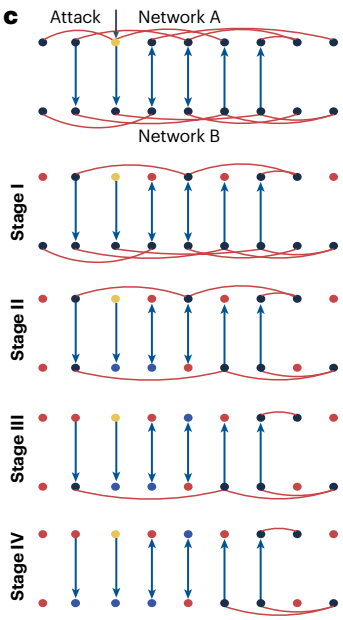
b Information diffusion in a socio-technical system



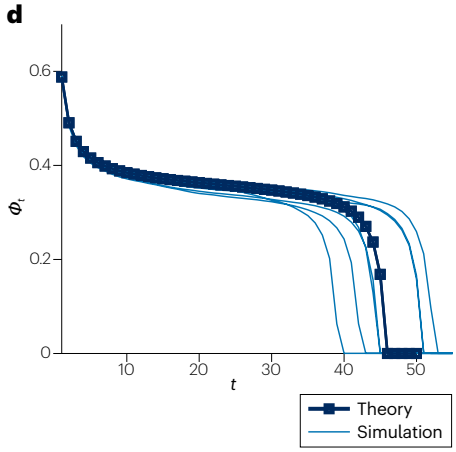
Modelling cascades

Triggered by structural interdependency

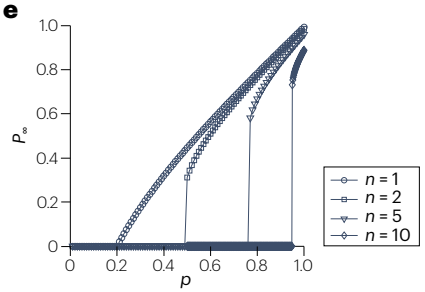
c



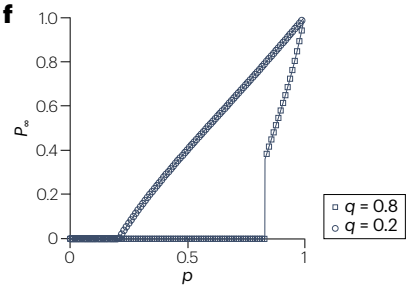
d



e

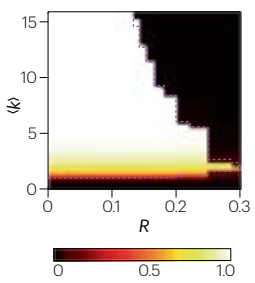


f

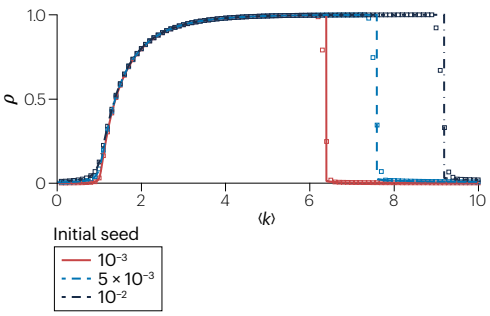


Triggered by thresholding processes

g



h



Triggered by overloading processes

i

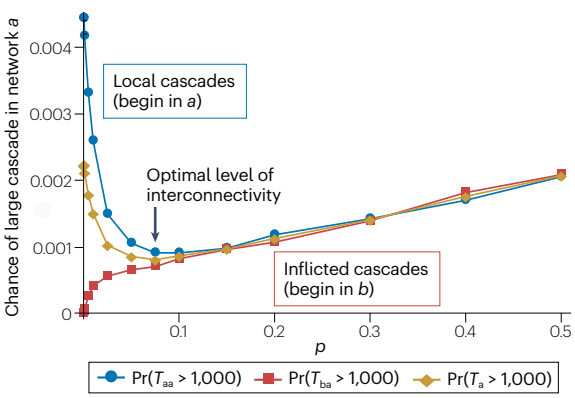


Fig. 3 | Evolving failures on networks. a, Cartogram with the state of power lines after the simulations of cascade spreading in the US–South Canada grid: lines that never underwent outage (green) and affected power lines (grey). Bottom row: snapshots of the evolution of the damaged lines (yellow) after a cascade triggered by three failures at a rescaled time $t = 0$. **b**, Information cascade on Twitter. Density of tweets (top row) about the discovery of the Higgs boson before, during and after the Nobel announcement and the corresponding network of re-shared messages (bottom row). **c**, Evolution of a failure sustained by dependency relations in a toy system with two coupled layers. Directed vertical arrows represent dependency relations. Node colours represent functional nodes (black), the node that initially fails (yellow), and units that are removed because either they do not belong to the largest cluster (red) or they depend on failed nodes in the other network (blue). **d**, Size of the giant component (ϕ_t) as a function of the cascade step (t). Light blue lines correspond to individual realizations of the dynamics, the markers indicate their average. The dark blue line is the theoretical prediction. **e**,**f**, Stationary size of the giant component (P_∞) as a function of the fraction of initially removed nodes (p). Solid lines show the theoretical predictions. n is the number of coupled layers; q is the fraction of interdependent nodes in a bilayer network. **g**, Size of the giant component at the cascade stop for the threshold model of ref. 170, as a function of the threshold R and the mean degree $\langle k \rangle$ of the underlying Erdős–Rényi network. The dashed line indicates the analytical prediction for the cascade emergence. **h**, Size of the giant component (ρ) at the cascade stop for fixed $R = 0.18$, as a function of the mean degree $\langle k \rangle$. **i**, Large load-shedding cascades can be mitigated at a non-trivial intermediate level of interconnectivity p between two networks (golden curve, diamond markers). However, too many or too few interconnections induce larger cascades and become detrimental for the robustness. T_{aa} (T_{ba}) is the cascade size unfolded on network a for cascades that started at network a (b). T_a is the size of cascades in network a without distinguishing where the cascade begins. Network a and b have 2,000 nodes. Part **a** reprinted with permission from ref. 58, AAAS. Part **b** adapted from ref. 226, Springer Nature Limited. Part **c** adapted from ref. 19, Springer Nature Limited. Parts **d**–**f** reprinted from ref. 19, Springer Nature Limited. Parts **g**,**h** adapted with permission from ref. 171, APS. Part **i** adapted with permission from ref. 190, PNAS.

distribution p_k^i. K is the number of layers connected to i by interdependence links. An analytical treatment of cascades driven by link failures is also possible[158], but this case has been scarcely studied in comparison with the node failure propagation mechanisms.

Equations (9)–(11) predict a rich variety of phenomena, which, however, have dramatic consequences for the robustness of interdependent systems. The most striking one is that the giant component at the end of the cascade suffers a discontinuous transition as the topological parameters of the network are varied. That transition translates into abrupt system collapses that are more difficult to anticipate as the number of fully coupled subsystems increases (Fig. 3e). This outcome can be attenuated by decreasing the level of interdependency among layers, recovering continuous dismantling if it is reduced enough (Fig. 3f). Most importantly, the analysis of equations (9)–(11) offers hints on how to improve the robustness of interdependent coupled systems. Three main methods have been identified: increasing the fraction of autonomous nodes[156], especially those with high degree[157]; designing dependency relations between nodes of similar degree[159,160]; and devoting special efforts to protect high-degree nodes against failures and attacks[157]. In the context of brain networks, robustness to interdependency-mediated cascades can be improved if topological correlations are taken into account[161]. We refer the reader to recent reviews[162,163] and references therein for a more in-depth discussion on this type of cascades.

Another family of models has its origin in theories of collective behaviour, the so-called threshold models. In these, we assume that the influence exerted by the neighbours of a node on its probability of changing state, that is, of going from functional to failed, is not linear in the number n of failed neighbours and, in fact, only takes effect above some threshold value of n[164–166]. This class of models has frequently been framed in the context of social psychology, to understand, for example, under what circumstances a social agent will decide to spread rumours, fads and fake news or to adopt behaviour. This problem is of course relevant to the context of network robustness and resilience at a societal level: it is well known that information spreading can represent a serious threat to public health systems, polarize debates and undermine public trust in democratic institutions[167,168], but spreading can also have positive impacts such as diffusing innovations[166,169]. In any case, these models can be readily framed as cascades occurring in other areas of interest.

The piece-wise, non-continuous influence of neighbours upon a node in a threshold model can be implemented in several ways. One option is to assume that a node will fail if a fraction, larger than a certain threshold, of its neighbours has also failed[170]. This simple model leads to a rich phenomenology, namely, the emergence of global cascades that are bounded in the parameter space by two transitions, one continuous and one discontinuous (Fig. 3g,h). Indeed, assuming that the initial number of failed nodes is small compared with the system size (see refs. 171,172 for the role the initial cascade seeding has) and that the threshold is the same for all nodes (the same phenomenology is observed for heterogeneous thresholds[170]), then global cascades are very rare when the threshold is large. When it is reduced, though, the network topology starts to have a role. If the mean degree is too small, there are very few nodes that can spread failures and they are isolated from each other; hence, global cascades cannot develop. However, if the mean degree is too large, the cascade cannot evolve because the large number of functional neighbours will stabilize the nodes to be always below the threshold. The lower critical mean degree is barely dependent on the threshold but the upper one strongly depends on it. It is between these two points that global cascades are easily triggered. The condition for the emergence of global cascades and estimates for their size have been successfully generalized to networks with topological correlations[173–177] and to temporal[178,179] and multiplex networks[180]. Similarly, more complex failing conditions have been used, such as combining relative and absolute thresholds[181], setting absolute thresholds only[182], or including a memory of past exposures to failures[183].

The final set of models we discuss in this section are overload models. In these, nodes (or links) sustain a load — electrical current in the power grid, network packets in the Internet, passengers in public transportation systems, or the amount of a certain product (such as wheat, rice and maize) in an international trade network, for example. The nodes remain functional as long as their load is kept below a threshold, the so-called capacity, which, a priori, can be modified, for instance, by human interventions. After a failure or an attack, load is redistributed according to some rules, which depend on the type of system one aims to model, causing a potential chain of overloads and new redistribution events across the network. The cascade finishes when all nodes restore their load below their capacity.

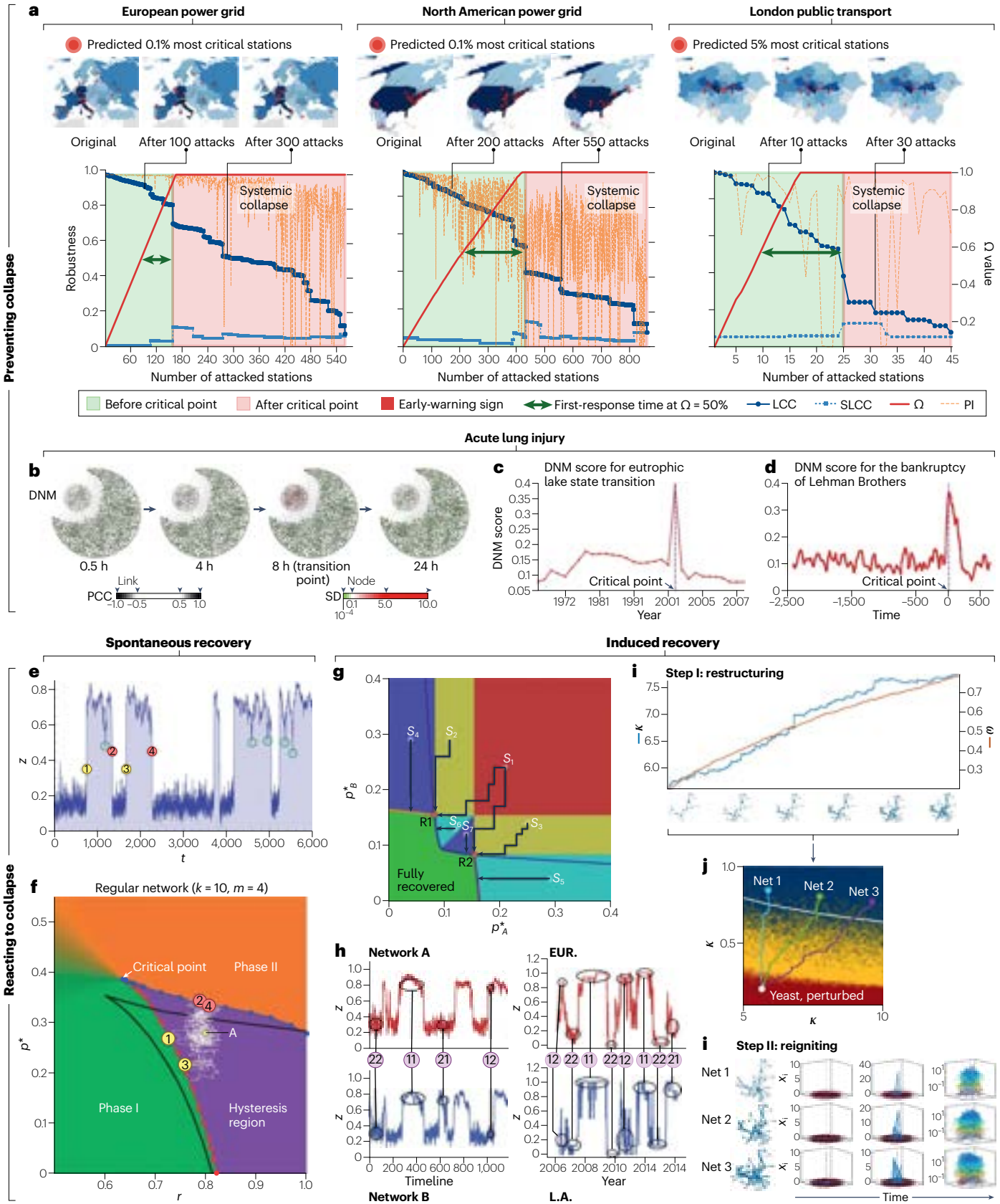

Preventing collapse
a
European power grid
North American power grid
London public transport
Predicted 0.1% most critical stations
Predicted 0.1% most critical stations
Predicted 5% most critical stations
Original
After 100 attacks
After 300 attacks
Original
After 200 attacks
After 550 attacks
Original
After 10 attacks
After 30 attacks
Robustness
Systemic collapse
Number of attacked stations
Ω value
Before critical point
After critical point
Early-warning sign
First-response time at Ω = 50%
LCC
SLCC
Ω
PI
Acute lung injury
b
DNM
0.5 h
4 h
8 h (transition point)
24 h
Link
PCC
Node
SD
c
DNM score for eutrophic lake state transition
DNM score
Critical point
Year
d
DNM score for the bankruptcy of Lehman Brothers
Critical point
Time
Spontaneous recovery
Induced recovery
Reacting to collapse
e
z
t
f
Regular network (k = 10, m = 4)
Critical point
Phase II
Phase I
Hysteresis region
A
p*
r
g
R1
R2
Fully recovered
p*B
p*A
i
Step I: restructuring
κ
e
j
Net 1
Net 2
Net 3
Yeast, perturbed
κ
i
Step II: reigniting
Net 1
Net 2
Net 3
Time
h
Network A
Network B
EUR.
L.A.
Timeline
Year

Fig. 4 | Preventing and reacting to network collapse. a, Early-warning signal measured by Ω for three distinct network infrastructures (top row) repeatedly attacked using a degree-based protocol, size of the largest connected component (LCC) and second-largest connected components (SLCC) (bottom row), and importance of the removal for the system integrity, as measured by the graph dismantling with machine learning (GDM) model (PI). **b**–**d**, A dynamical network marker (DNM)[227], which is correlated with the fluctuation strength in gene expressions (node colours) in a molecular network from lung tissue of mouse exhibiting a critical transition at 8 h (part **b**); DNM has been used for capturing early-warning signals in other systems, such as eutrophic lake states (part **c**) and daily prices of interest-rate swaps in the USD and EUR currency (part **d**). **e**,**f**, Regular network (degree connectivity $k = 10$, number of active sites $m = 4$, network size $N = 100$) with a fraction z of active nodes flipping between two collective modes over time (top) and trajectory of the system in the phase diagram, from $t = 0$ to the moment of the first transition (bottom), for the marked states. **g**,**h**, An optimal repair strategy for a system with two networks, characterized by a fraction $p_A^\star$ and $p_B^\star$ of internally failed nodes. Given the initial state S_i of a collapsed system, the repairing corresponds to minimize the distance between S_i and the nearest border of the green region, wherein the systems goes back to a fully functional state. Arrows indicate the followed trajectories, whereas R_1 and R_2 are triple points. Collective states, identified by marked numbers, for two synthetic (left) and empirical (right) coupled networks are shown, in the bottom. **i**–**k**, Restructuring and reigniting: a two-step procedure that drives a perturbed yeast protein interaction network from a collapsed phase (red) into the recoverable phase (blue). Part **a** reprinted from ref. 68, Springer Nature Limited. Parts **b**–**d** reprinted from ref. 227, Springer Nature Limited. Parts **e**,**f** reprinted from ref. 218, Springer Nature Limited. Parts **g**,**h** reprinted from ref. 215, Springer Nature Limited. Parts **i**–**k** reprinted from ref. 217, Springer Nature Limited. EUR, Europe; L.A., Los Angeles; PCC, Pearson Correlation Correlation; SD, standard deviation.

One of the most paradigmatic redistribution mechanisms is that of the sand-pile models of self-organized criticality[184,185]. These are characterized by a slow external driving (for instance, by introduction of load in the system) and very fast relaxations, wherein the cascade occurs (for instance, by overloaded nodes shedding load to their neighbours). The relaxation is considered to be so fast that no load is added during its evolution, which usually is a good approximation to empirical processes because the unfolding of a cascade is the fastest timescale. Because networks have nodes with a variable number of neighbours, a natural choice is to set the node capacity equal to the degree[186], although other choices are possible[187–189]. Moreover, to avoid a network becoming saturated with load, one needs to remove load with a certain probability when it is shed. Load shedding cascade models have been analysed in the context of interdependent power grids[190], in which an optimal level of coupling among networks to reduce the impact of the cascades has been found (Fig. 3i). Interesting phenomenology has been also reported, such as dragon king events (cascades of larger cascades) when the self-organized criticality rules are coupled to the Kuramoto model[191].

Other load redistribution mechanisms are also possible. One approach was proposed to further extend the interplay between structure and dynamics by associating load to betweenness[30] because there is a positive correlation between the shortest paths and traffic or route assignment. In that model, each node has a capacity proportional to its initial betweenness, and when a node fails, there is a global load redistribution, possibly causing the overload of new nodes that are not necessarily in the vicinity of the previous failure. This nonlocality can be readily visualized in spatially embedded networks[35]. A full, explicit characterization of nonlocality remains an analytical challenge, but some efforts have been made from different perspectives to better understand its complexities[192–195].

Networks with heterogeneous degree distributions, and thus with heterogeneous betweenness distribution[196], were found numerically to be incredibly weak to targeted attacks if the node capacity is not large enough[30]. In fact, the network could crash even if only one node, chosen among those with either the largest betweenness or degree, is taken down as initial stressor. Conversely, picking uniformly at random a single node as initial perturbation is not an efficient strategy to dismantle a network, even if the capacity of the nodes is low, independently of whether the network has homogeneous or heterogeneous connectivity. However, it has been analytically shown that for a large-enough set of randomly chosen nodes, the network can suffer a discontinuous dismantling transition[197]. Numerical evidence for a discontinuous transition has been further reported in both monoplex and multiplex networks[198]. Overload models have also been studied in the context of link failures and interventions[199–203].

So far, we have discussed the topological implications and the effectiveness of static interventions, as well as different mechanisms through which localized failures can spread across a macroscopic portion of a network. In the next section, we present the complementary point of view, namely, how to prevent and react to these phenomena in a proactive and premeditate manner.

Preventing and reacting to network collapse

A network collapse can be prevented by using design principles during the formative stages of a network that make it resilient to random failures and targeted attacks[204–208]. However, such design principles are not always used or, worse, can be outsmarted by advanced attack strategies that were not foreseeable during network formation. In such cases, early-warning indicators of an impending network collapse[68,209–214] and repairs and adaptive responses to an already evolving collapse[215–217] become the best line of defence. It may be possible to prevent systemic collapse either by favouring spontaneous recovery[218,219] or by inducing it through microscopic interventions[215–217,220], with cost-efficient network-based procedures[221,222].

Early attempts of network design can be traced back to augmentation problems in graphs, studied in the 1970s. A result from that time is the minimum number of edges necessary to make a directed graph strongly connected and to make an undirected graph bridge-connected or biconnected (a graph such that if any one vertex were to be removed, the graph would still remain connected). More recent network design strategies were proposed in the mid-2000s[204,205]. In particular, for scale-free networks and for networks with two-peak degree distributions, an optimal robustness is obtained if all but one of the nodes have the same degree, which should be close to the average number of links per node, while the one remaining node has a very large degree $k \propto N^{2/3}$, where N is the number of nodes that form the network[204]. Another approach is based on the relative drop in network performance and its minimization given a set of improvements consisting of either adding or removing specific links[205]. More precisely, if D denotes the set of possible damages that can be inflicted upon a network G, and if $\ell(G, d)$ is a map that yields the new network after the damage $d \in D$, then the importance of the damage d is given by the relative drop in the performance $\Delta\Phi^-/\Phi$, where $\Delta\Phi^- = \Phi(G) - \Phi[\ell(S, d)] \geq 0$. Moreover, the critical damage $d^* \in D$

is defined as the damage that minimizes $\Phi[\ell(G, d)]$. The vulnerability V of G owing to D can then bedefined as[205]

$$V(G,D) = \frac{\Phi(G) - W(G,D)}{\Phi(G)}, \tag{12}$$

where $W(G, D) = \Phi[\ell(G, d^*)]$ is the worst performance of G under the class of damages D. Analogously, one can define a set of improvements $i \in I$ to be made on the network G via the map $\aleph(G, i)$, such that the best improvability of the network subject to the critical improvement i^* is

$$M(G,I) = \frac{B(G,I) - \Phi(G)}{\Phi(G)}, \tag{13}$$

where $B(G, I) = \Phi[\aleph(G, i^*)]$ is the best performance of G under the class of improvements I. And as for the damages, the importance of i is given by the relative increase in the performance $\Delta\Phi^+/\Phi$, where $\Delta\Phi^+ = \Phi[\aleph(G, i)] - \Phi(G)$ (ref. 205). Nevertheless, there is a fundamental limit to what can be optimized: in fact, network robustness and its performance are competitive features hard to simultaneously maximize[223].

The concept of network design has been further extended[206] to interdependent networks[162,224]. The stability of a system of networks relies on the relation between the internal structure of a network and its pattern of connections to other networks[206]. More precisely, for an interdependent network to be considered robust by design, the interconnections should be provided by network hubs, whereas the connections between networks should be moderately convergent. If both these conditions hold, a system of networks can be considered stable and robust to failure. This result has also been proven correct experimentally using functional brain networks in task and resting states[206].

But despite best design practices, a network collapse oftentimes remains unavoidable. Early detection is in such cases crucial. An early attempt in this regard has shown that many topological properties of the Dutch interbank network displayed an abrupt change just prior to the 2008 global financial crisis[210]. For socioecological networks, the maximum element of the covariance matrix of the network serves as the basis for an early-warning indicator, which is an effective leading mark of network instability[211]. A similar concept has been outlined also for coupled human–environment systems[214], although not based on the network formalism but on the tipping point theory. Combining the theory on tipping points with patterns of network structure enables development of critical slowing-down indicators as early-warning signals for detecting the proximity to a potential tipping point in structurally complex ecological communities[212]. This approach successfully identified, based on 79 empirical mutualistic networks, specialist species that are probably the best indicator for monitoring the proximity of a community to collapse.

More recently, it was shown that a machine trained to dismantle relatively small systems is able to identify higher-order topological patterns and, thus, effectively disintegrate also large-scale social, infrastructural and technological networks[68], and do so more efficiently than human-based heuristics. Remarkably, it was also shown that the underlying procedure can be reversed engineered — as the machine could assesses the probability of future attacks to disintegrate the system — for developing early-warning signals of network collapse. More precisely, if S_o is the set of virtually removed nodes that cause the percolation of the network and

$$\Omega_m = \sum_{n \in S_o} p_n, \tag{14}$$

then the value of the early warning Ω for the network after the removal of a generic set S of nodes is given by

$$\Omega = \begin{cases} \Omega_s/\Omega_m & \text{if } \Omega_s \le \Omega_m \\ 1 & \text{otherwise} \end{cases} \tag{15}$$

where $\Omega_s = \sum_{n \in S} p_n$. The main idea here is that $0 \le \Omega_m \le 1$ quantifies the amount of damage the network will tolerate before it collapses, and $\Omega \to 1$ quickly when key nodes for the integrity of the network are removed[68] (Fig. 4).

Finally, if robust design and early-warning indicators fail and network collapse is already well underway, then adaptive responses and repair stand as the last two remaining options, as studied in ref. 215 for interacting financial networks. Optimal control theory and reinforcement learning have been used to determine optimal maintenance protocols to offset ageing in complex networks[216]. A two-step recovery scheme has also been developed, involving first a topological reconstruction and secondly dynamic interventions to revive a failed network by means of judiciously applied microscopic interventions[217] (Fig. 4).

Together, the protocols discussed in this section present the most commonly used means of preventing and reacting to network collapse, and they also probably form the most fertile grounds for future developments along these lines.

Outlook

As discussed in this Review, the problems connected to network dismantling are many, including theoretical challenges and problems concerning the development of algorithms able to dismantle large networks in a reasonable time. Although much work has been done so far, in each of the above points, open questions that require further research efforts remain.

One aspect that needs to be investigated is related to structure and function, and their interplay. Most of the dismantling methods present in the literature are based on attacks whose purpose is to strongly decrease the size of the LCCs. Although the size of the LCC is linked to the efficient functioning of a network in many cases, in general, this is not always true. For instance, on some networks, a task-dependent dismantling policy could produce more damage than one based only on topological criteria. As an example, the knowledge of the dynamics governing a power-grid network could suggest a more effective attack policy based on the removal of those nodes and/or arcs that are most critical for the network stability. In such a situation, many of the methods present in the literature are inapplicable and there is a strong need for new theoretical and computational techniques capable of functional dismantling networks, while accounting for the aspects connected with the dynamics on top of them[146,147].

To this aim, dismantling approaches based on the latent geometry of complex networks[28] also provide a promising research direction. Although methods based on machine learning already work in a latent space, there is still no in-depth investigation on how the geometry of a network is linked to its robustness. This knowledge could lead to the development of a completely new type of algorithms for both structural and functional network dismantling, but also for the improvement of the robustness and resilience of networks. In fact, although artificial intelligence-based techniques, such as machine learning, have had a large impact on many fields such as natural language, video and image processing, with popular applications such as chat bots and image generation, such impact has been, so far, more limited on networks. However, it is inevitable that such advancements — which have roots

in the understanding of the techniques, of the algorithms and of the hardware — will find their way to many network-related tasks.

Overall, understanding how systems react and adapt to external shocks is an overarching objective for the future. Research at the edge of statistical physics, network science and machine learning is expected to have a fundamental role for this purpose. Potential applications span from the cellular scale — in which molecular and systems biology need robust techniques to assess the potential impact of genetic or pharmaceutical interventions — to epidemiology and economics, in which shocks have the potential to become systemic and affect the structure and functioning of society.

Code availability

The code used for the performance comparisons can be found in the repository https://github.com/NetworkDismantling/review.

Published online: 8 January 2024

References

1. Albert, R. & Barabási, A.-L. Statistical mechanics of complex networks. *Rev. Mod. Phys.* **74**, 47 (2002).
2. Newman, M. E. The structure and function of complex networks. *SIAM Rev.* **45**, 167–256 (2003).
3. Boccaletti, S., Latora, V., Moreno, Y., Chavez, M. & Hwang, D.-U. Complex networks: structure and dynamics. *Phys. Rep.* **424**, 175–308 (2006).
4. Barabási, A.-L. & Albert, R. Emergence of scaling in random networks. *Science* **286**, 509–512 (1999).
5. Broido, A. D. & Clauset, A. Scale-free networks are rare. *Nat. Commun.* **10**, 1017 (2019).
6. Gerlach, M. & Altmann, E. G. Testing statistical laws in complex systems. *Phys. Rev. Lett.* **122**, 168301 (2019).
7. Voitalov, I., van der Hoorn, P., van der Hofstad, R. & Krioukov, D. Scale-free networks well done. *Phys. Rev. Res.* **1**, 033034 (2019).
8. Serafino, M. et al. True scale-free networks hidden by finite size effects. *Proc. Natl Acad. Sci. USA* **118**, e2013825118 (2021).
9. Guimera, R. & Nunes Amaral, L. A. Functional cartography of complex metabolic networks. *Nature* **433**, 895–900 (2005).
10. Newman, M. E. Communities, modules and large-scale structure in networks. *Nat. Phys.* **8**, 25–31 (2012).
11. Fortunato, S. & Hric, D. Community detection in networks: a user guide. *Phys. Rep.* **659**, 1–44 (2016).
12. Peixoto, T. P. & Rosvall, M. Modelling sequences and temporal networks with dynamic community structures. *Nat. Commun.* **8**, 582 (2017).
13. Fortunato, S. & Newman, M. E. 20 years of network community detection. *Nat. Phys.* **18**, 848–850 (2022).
14. Ravasz, E. & Barabási, A.-L. Hierarchical organization in complex networks. *Phys. Rev. E* **67**, 026112 (2003).
15. Clauset, A., Moore, C. & Newman, M. E. Hierarchical structure and the prediction of missing links in networks. *Nature* **453**, 98–101 (2008).
16. Peixoto, T. P. Hierarchical block structures and high-resolution model selection in large networks. *Phys. Rev. X* **4**, 011047 (2014).
17. Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E. & Havlin, S. Catastrophic cascade of failures in interdependent networks. *Nature* **464**, 1025–1028 (2010).
18. Mucha, P. J., Richardson, T., Macon, K., Porter, M. A. & Onnela, J.-P. Community structure in time-dependent, multiscale, and multiplex networks. *Science* **328**, 876–878 (2010).
19. Gao, J., Buldyrev, S. V., Stanley, H. E. & Havlin, S. Networks formed from interdependent networks. *Nat. Phys.* **8**, 40–48 (2012).
20. De Domenico, M. et al. Mathematical formulation of multilayer networks. *Phys. Rev. X* **3**, 041022 (2013).
21. Artime, O. et al. *Multilayer Network Science: From Cells to Societies. Elements in Structure and Dynamics of Complex Networks* (Cambridge Univ. Press, 2022).
22. Domenico, M. D. More is different in real-world multilayer networks. *Nat. Phys.* **19**, 1247–1262 (2023).
23. Lambiotte, R., Rosvall, M. & Scholtes, I. From networks to optimal higher-order models of complex systems. *Nat. Phys.* **15**, 313–320 (2019).
24. Battiston, F. et al. The physics of higher-order interactions in complex systems. *Nat. Phys.* **17**, 1093–1098 (2021).
25. Bianconi, G. *Higher Order Networks: an Introduction to Simplicial Complexes* (Cambridge Univ. Press, 2021).
26. De Domenico, M. Diffusion geometry unravels the emergence of functional clusters in collective phenomena. *Phys. Rev. Lett.* **118**, 168301 (2017).
27. García-Pérez, G., Boguñá, M. & Serrano, M. Multiscale unfolding of real networks by geometric renormalization. *Nat. Phys.* **14**, 583–589 (2018).
28. Boguna, M. et al. Network geometry. *Nat. Rev. Phys.* **3**, 114–135 (2021).
29. Albert, R., Jeong, H. & Barabási, A.-L. Error and attack tolerance of complex networks. *Nature* **406**, 378–382 (2000).
30. Motter, A. E. & Lai, Y.-C. Cascade-based attacks on complex networks. *Phys. Rev. E* **66**, 065102 (2002).
31. Motter, A. E. Cascade control and defense in complex networks. *Phys. Rev. Lett.* **93**, 098701 (2004).
32. Dorogovtsev, S. N., Goltsev, A. V. & Mendes, J. F. Critical phenomena in complex networks. *Rev. Mod. Phys.* **80**, 1275 (2008).
33. Liu, X. et al. Network resilience. *Phys. Rep.* **971**, 1–108 (2022).
34. Bashan, A., Berezin, Y., Buldyrev, S. V. & Havlin, S. The extreme vulnerability of interdependent spatially embedded networks. *Nat. Phys.* **9**, 667–672 (2013).
35. Zhao, J., Li, D., Sanhedrai, H., Cohen, R. & Havlin, S. Spatio-temporal propagation of cascading overload failures in spatially embedded networks. *Nat. Commun.* **7**, 10094 (2016).
36. Radicchi, F. & Bianconi, G. Redundant interdependencies boost the robustness of multiplex networks. *Phys. Rev. X* **7**, 011013 (2017).
37. Arenas, A., Díaz-Guilera, A., Kurths, J., Moreno, Y. & Zhou, C. Synchronization in complex networks. *Phys. Rep.* **469**, 93–153 (2008).
38. Pastor-Satorras, R., Castellano, C., Van Mieghem, P. & Vespignani, A. Epidemic processes in complex networks. *Rev. Mod. Phys.* **87**, 925 (2015).
39. De Domenico, M., Granell, C., Porter, M. A. & Arenas, A. The physics of spreading processes in multilayer networks. *Nat. Phys.* **12**, 901–906 (2016).
40. O'Keeffe, K. P., Hong, H. & Strogatz, S. H. Oscillators that sync and swarm. *Nat. Commun.* **8**, 1–13 (2017).
41. Scheffer, M. et al. Anticipating critical transitions. *Science* **338**, 344–348 (2012).
42. Smart, A. G., Amaral, L. A. & Ottino, J. M. Cascading failure and robustness in metabolic networks. *Proc. Natl Acad. Sci. USA* **105**, 13223–13228 (2008).
43. Barabási, A.-L., Gulbahce, N. & Loscalzo, J. Network medicine: a network-based approach to human disease. *Nat. Rev. Genet.* **12**, 56–68 (2011).
44. Zitnik, M., Sosič, R., Feldman, M. W. & Leskovec, J. Evolution of resilience in protein interactomes across the tree of life. *Proc. Natl Acad. Sci. USA* **116**, 4426–4433 (2019).
45. Bullmore, E. & Sporns, O. Complex brain networks: graph theoretical analysis of structural and functional systems. *Nat. Rev. Neurosci.* **10**, 186–198 (2009).
46. Siegel, J. S. et al. Disruptions of network connectivity predict impairment in multiple behavioral domains after stroke. *Proc. Natl Acad. Sci. USA* **113**, E4367–E4376 (2016).
47. May, R. M. Will a large complex system be stable? *Nature* **238**, 413–414 (1972).
48. Holling, C. S. Resilience and stability of ecological systems. *Ann. Rev. Ecol. Syst.* 1–23 (1973).
49. Pimm, S. L. The complexity and stability of ecosystems. *Nature* **307**, 321–326 (1984).
50. Pocock, M. J., Evans, D. M. & Memmott, J. The robustness and restoration of a network of ecological networks. *Science* **335**, 973–977 (2012).
51. Bascompte, J. & Stouffer, D. B. The assembly and disassembly of ecological networks. *Philos. Trans. R. Soc. Lond. B Biol. Sci.* **364**, 1781–1787 (2009).
52. Baggio, J. A. et al. Multiplex social ecological network analysis reveals how social changes affect community robustness more than resource depletion. *Proc. Natl Acad. Sci. USA* **113**, 13708–13713 (2016).
53. Gai, P. & Kapadia, S. Contagion in financial networks. *Proc. R. Soc. A Math. Phys. Eng. Sci.* **466**, 2401–2423 (2010).
54. Cimini, G., Squartini, T., Garlaschelli, D. & Gabrielli, A. Systemic risk analysis on reconstructed economic and financial networks. *Sci. Rep.* **5**, 15758 (2015).
55. Bardoscia, M. et al. The physics of financial networks. *Nat. Rev. Phys.* **3**, 490–507 (2021).
56. Grassia, M., Mangioni, G., Schiavo, S. & Traverso, S. Insights into countries' exposure and vulnerability to food trade shocks from network-based simulations. *Sci. Rep.* **12**, 4644 (2022).
57. Carreras, B. A., Lynch, V. E., Dobson, I. & Newman, D. E. Critical points and transitions in an electric power transmission model for cascading failure blackouts. *Chaos* **12**, 985–994 (2002).
58. Yang, Y., Nishikawa, T. & Motter, A. E. Small vulnerable sets determine large network cascades in power grids. *Science* **358**, eaan3184 (2017).
59. Crucitti, P., Latora, V., Marchiori, M. & Rapisarda, A. Efficiency of scale-free networks: error and attack tolerance. *Phys. A Stat. Mech. Appl.* **320**, 622–642 (2003).
60. Bertagnolli, G., Gallotti, R. & De Domenico, M. Quantifying efficient information exchange in real network flows. *Commun. Phys.* **4**, 125 (2021).
61. Doyle, J. C. et al. The "robust yet fragile" nature of the internet. *Proc. Natl Acad. Sci. USA* **102**, 14497–14502 (2005).
62. De Domenico, M. & Arenas, A. Modeling structure and resilience of the dark network. *Phys. Rev. E* **95**, 022313 (2017).
63. Scott, D. M., Novak, D. C., Aultman-Hall, L. & Guo, F. Network robustness index: a new method for identifying critical links and evaluating the performance of transportation networks. *J. Transp. Geogr.* **14**, 215–227 (2006).
64. Clusella, P., Grassberger, P., Pérez-Reche, F. J. & Politi, A. Immunization and targeted destruction of networks using explosive percolation. *Phys. Rev. Lett.* **117**, 208301 (2016).
65. Ribeiro, H. V., Alves, L. G. A., Martins, A. F., Lenzi, E. K. & Perc, M. The dynamical structure of political corruption networks. *J. Complex Netw.* **6**, 989–1003 (2018).
66. Ren, X.-L., Gleinig, N., Helbing, D. & Antulov-Fantulin, N. Generalized network dismantling. *Proc. Natl Acad. Sci. USA* **116**, 6554–6559 (2019).
67. Matke, C., Medjroubi, W. & Kleinhans, D. SciGRID — an open source reference model for the European Transmission Network (v0.2). http://www.scigrid.de (2016).

68. Grassia, M., De Domenico, M. & Mangioni, G. Machine learning dismantling and early-warning signals of disintegration in complex systems. *Nat. Commun.* **12**, 5190 (2021).
69. Braunstein, A., Dall'Asta, L., Semerjian, G. & Zdeborová, L. Network dismantling. *Proc. Natl Acad. Sci. USA* **113**, 12368–12373 (2016).
70. Schneider, C. M., Moreira, A. A., Andrade, J. S., Havlin, S. & Herrmann, H. J. Mitigation of malicious attacks on networks. *Proc. Natl Acad. Sci. USA* **108**, 3838–3841 (2011).
71. Kinney, R., Crucitti, P., Albert, R. & Latora, V. Modeling cascading failures in the North American power grid. *Eur. Phys. J. B* **46**, 101–107 (2005).
72. Alves, L. G. et al. The nested structural organization of the worldwide trade multi-layer network. *Sci. Rep.* **9**, 2866 (2019).
73. Cohen, R., Erez, K., Ben-Avraham, D. & Havlin, S. Breakdown of the internet under intentional attack. *Phys. Rev. Lett.* **86**, 3682 (2001).
74. Cormen, T., Leiserson, C., Rivest, R. & Stein, C. *Introduction to Algorithms* 4th edn (MIT Press, 2022).
75. Flory, P. J. Molecular size distribution in three dimensional polymers. I. Gelation. *J. Am. Chem. Soc.* **63**, 3083–3090 (1941).
76. Stauffer, D. & Aharony, A. *Introduction to Percolation Theory* (CRC, 2018).
77. Broadbent, S. R. & Hammersley, J. M. Percolation processes: I. crystals and mazes. *Math. Proc. Camb. Philos. Soc.* **53**, 629–641 (1957).
78. Isichenko, M. B. Percolation, statistical topography, and transport in random media. *Rev. Mod. Phys.* **64**, 961 (1992).
79. Sahimi, M. *Applications of Percolation Theory* (CRC, 1994).
80. Araújo, N., Grassberger, P., Kahng, B., Schrenk, K. & Ziff, R. M. Recent advances and open challenges in percolation. *Eur. Phys. J. Spec. Top.* **223**, 2307–2321 (2014).
81. Rodrigues, F. A. in *Network Centrality: an Introduction* 177–196 (Springer, 2019).
82. Holme, P., Kim, B. J., Yoon, C. N. & Han, S. K. Attack vulnerability of complex networks. *Phys. Rev. E* **65**, 056109 (2002).
83. Artime, O. & De Domenico, M. Percolation on feature-enriched interconnected systems. *Nat. Commun.* **12**, 2478 (2021).
84. Molloy, M. & Reed, B. A critical point for random graphs with a given degree sequence. *Random Struct. Algor.* **6**, 161–180 (1995).
85. Cohen, R., Ben-Avraham, D. & Havlin, S. Percolation critical exponents in scale-free networks. *Phys. Rev. E* **66**, 036113 (2002).
86. Gordon, M. Good's theory of cascade processes applied to the statistics of polymer distributions. *Proc. R. S. Lond. A Math. Phys. Sci.* **268**, 240–256 (1962).
87. Newman, M. E., Strogatz, S. H. & Watts, D. J. Random graphs with arbitrary degree distributions and their applications. *Phys. Rev. E* **64**, 026118 (2001).
88. Callaway, D. S., Newman, M. E., Strogatz, S. H. & Watts, D. J. Network robustness and fragility: percolation on random graphs. *Phys. Rev. Lett.* **85**, 5468 (2000).
89. Gross, T. & Barth, L. Network robustness revisited. *Front. Phys.* **10**, 823564 (2022).
90. Moore, C. & Newman, M. E. Exact solution of site and bond percolation on small-world networks. *Phys. Rev. E* **62**, 7059 (2000).
91. Goltsev, A. V., Dorogovtsev, S. N. & Mendes, J. F. Percolation on correlated networks. *Phys. Rev. E* **78**, 051105 (2008).
92. Newman, M. *Networks* (Oxford Univ. Press, 2018).
93. Li, M. et al. Percolation on complex networks: theory and application. *Phys. Rep.* **907**, 1–68 (2021).
94. Radicchi, F. & Castellano, C. Breaking of the site-bond percolation universality in networks. *Nat. Commun.* **6**, 10196 (2015).
95. Shiraki, Y. & Kabashima, Y. Cavity analysis on the robustness of random networks against targeted attacks: influences of degree-degree correlations. *Phys. Rev. E* **82**, 036101 (2010).
96. Barrat, A., Barthelemy, M., Pastor-Satorras, R. & Vespignani, A. The architecture of complex weighted networks. *Proc. Natl Acad. Sci. USA* **101**, 3747–3752 (2004).
97. Hamilton, K. E. & Pryadko, L. P. Tight lower bound for percolation threshold on an infinite graph. *Phys. Rev. Lett.* **113**, 208701 (2014).
98. Karrer, B., Newman, M. E. & Zdeborová, L. Percolation on sparse networks. *Phys. Rev. Lett.* **113**, 208702 (2014).
99. Radicchi, F. Percolation in real interdependent networks. *Nat. Phys.* **11**, 597–602 (2015).
100. Newman, M. Message passing methods on complex networks. *Proc. R. Soc. A* **479**, 20220774 (2023).
101. Radicchi, F. Predicting percolation thresholds in networks. *Phys. Rev. E* **91**, 010801 (2015).
102. Radicchi, F. & Castellano, C. Beyond the locally treelike approximation for percolation on real networks. *Phys. Rev. E* **93**, 030302 (2016).
103. Newman, M. E. Assortative mixing in networks. *Phys. Rev. Lett.* **89**, 208701 (2002).
104. Newman, M. E. Mixing patterns in networks. *Phys. Rev. E* **67**, 026126 (2003).
105. Serrano, M. Á. & Boguná, M. Percolation and epidemic thresholds in clustered networks. *Phys. Rev. Lett.* **97**, 088701 (2006).
106. Serrano, M. Á. & Boguná, M. Clustering in complex networks. II. Percolation properties. *Phys. Rev. E* **74**, 056115 (2006).
107. Berchenko, Y., Artzy-Randrup, Y., Teicher, M. & Stone, L. Emergence and size of the giant component in clustered random graphs with a given degree distribution. *Phys. Rev. Lett.* **102**, 138701 (2009).
108. Newman, M. E. Random graphs with clustering. *Phys. Rev. Lett.* **103**, 058701 (2009).
109. Rombach, M. P., Porter, M. A., Fowler, J. H. & Mucha, P. J. Core-periphery structure in networks. *SIAM J. Appl. Math.* **74**, 167–190 (2014).
110. Colomer-de Simón, P. & Boguñá, M. Double percolation phase transition in clustered complex networks. *Phys. Rev. X* **4**, 041020 (2014).
111. Allard, A., Althouse, B. M., Scarpino, S. V. & Hébert-Dufresne, L. Asymmetric percolation drives a double transition in sexual contact networks. *Proc. Natl Acad. Sci. USA* **114**, 8969–8973 (2017).
112. Hébert-Dufresne, L. & Allard, A. Smeared phase transitions in percolation on real complex networks. *Phys. Rev. Res.* **1**, 013009 (2019).
113. Derényi, I., Palla, G. & Vicsek, T. Clique percolation in random networks. *Phys. Rev. Lett.* **94**, 160202 (2005).
114. Claessens, S., Dell'Ariccia, G., Igan, D. & Laeven, L. Cross-country experiences and policy implications from the global financial crisis. *Econ. Policy* **25**, 267–293 (2010).
115. Fernandes, N. *Economic Effects of Coronavirus Outbreak (COVID-19) on the World Economy* IESE Business School Working Paper No. WP-1240-E (ECGI 2020).
116. Dorogovtsev, S. N., Goltsev, A. V. & Mendes, J. F. F. *k*-core organization of complex networks. *Phys. Rev. Lett.* **96**, 040601 (2006).
117. Baxter, G. J., Dorogovtsev, S. N., Goltsev, A. V. & Mendes, J. F. Bootstrap percolation on complex networks. *Phys. Rev. E* **82**, 011103 (2010).
118. Bohman, T. & Frieze, A. Avoiding a giant component. *Random Struct. Algor.* **19**, 75–85 (2001).
119. Spencer, J. & Wormald, N. Birth control for giants. *Combinatorica* **27**, 587–628 (2007).
120. Beveridge, A., Bohman, T., Frieze, A. & Pikhurko, O. Product rule wins a competitive game. *Proc. Am. Math. Soc.* **135**, 3061–3071 (2007).
121. Krivelevich, M., Lubetzky, E. & Sudakov, B. Hamiltonicity thresholds in Achlioptas processes. *Random Struct. Algor.* **37**, 1–24 (2010).
122. Achlioptas, D., D'Souza, R. M. & Spencer, J. Explosive percolation in random networks. *Science* **323**, 1453–1455 (2009).
123. Riordan, O. & Warnke, L. Explosive percolation is continuous. *Science* **333**, 322–324 (2011).
124. da Costa, R. A., Dorogovtsev, S. N., Goltsev, A. V. & Mendes, J. F. F. Explosive percolation transition is actually continuous. *Phys. Rev. Lett.* **105**, 255701 (2010).
125. Grassberger, P., Christensen, C., Bizhani, G., Son, S.-W. & Paczuski, M. Explosive percolation is continuous, but with unusual finite size behavior. *Phys. Rev. Lett.* **106**, 225701 (2011).
126. D'Souza, R. M., Gómez-Gardenes, J., Nagler, J. & Arenas, A. Explosive phenomena in complex networks. *Adv. Phys.* **68**, 123–223 (2019).
127. Son, S.-W., Bizhani, G., Christensen, C., Grassberger, P. & Paczuski, M. Percolation theory on interdependent networks based on epidemic spreading. *EPL (Europhys. Lett.)* **97**, 16006 (2012).
128. Morone, F. & Makse, H. A. Influence maximization in complex networks through optimal percolation. *Nature* **524**, 65–68 (2015).
129. Granovetter, M. S. The strength of weak ties. *Am. J. Sociol.* **78**, 1360–1380 (1973).
130. Kempe, D., Kleinberg, J. & Tardos, É. Maximizing the spread of influence through a social network. In *Proc. 9th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* 137–146 (ACM, 2003).
131. Morone, F., Min, B., Bo, L., Mari, R. & Makse, H. Collective influence algorithm to find influencers via optimal percolation in massively large social media. *Sci. Rep.* **6**, 30062 (2016).
132. Altarelli, F., Braunstein, A., Dall'Asta, L., Wakeling, J. R. & Zecchina, R. Containing epidemic outbreaks by message-passing techniques. *Phys. Rev. X* **4**, 021024 (2014).
133. Altarelli, F., Braunstein, A., Dall'Asta, L. & Zecchina, R. Optimizing spread dynamics on graphs by message passing. *J. Stat. Mech. Theory Exp.* **2013**, 09011 (2013).
134. Mugisha, S. & Zhou, H.-J. Identifying optimal targets of network attack by belief propagation. *Phys. Rev. E* **94**, 012305 (2016).
135. Zdeborová, L., Zhang, P. & Zhou, H.-J. Fast and simple decycling and dismantling of networks. *Sci. Rep.* https://doi.org/10.1038/srep37954 (2016).
136. Ren, X.-L. & Antulov-Fantulin, N. in *Complex Networks and Their Applications VIII* (eds Cherifi, H. et al.) 783–793 (Springer, 2020).
137. Fan, C., Zeng, L., Sun, Y. & Liu, Y.-Y. Finding key players in complex networks through deep reinforcement learning. *Nat. Mach. Intell.* **2**, 317–324 (2020).
138. Grassia, M. & Mangioni, G. in *Complex Networks XIV* (eds Teixeira, A. S. et al.) 86–94 (Springer Nature, 2023).
139. Osat, S., Papadopoulos, F., Teixeira, A. S. & Radicchi, F. Embedding-aided network dismantling. *Phys. Rev. Res.* **5**, 013076 (2023).
140. Osat, S., Faqeeh, A. & Radicchi, F. Optimal percolation on multiplex networks. *Nat. Commun.* **8**, 1540 (2017).
141. Szolnoki, A. & Perc, M. Collective influence in evolutionary social dilemmas. *EPL (Europhys. Lett.)* **113**, 58004 (2016).
142. Chen, B.-L. et al. Influence blocking maximization on networks: models, methods and applications. *Phys. Rep.* **976**, 1–54 (2022).
143. Radicchi, F. & Castellano, C. Fundamental difference between superblockers and superspreaders in networks. *Phys. Rev. E* **95**, 012318 (2017).
144. Makse, H. A. *The Science of Influencers and Superspreaders* (Springer Nature, 2023).
145. De Domenico, M. & Biamonte, J. Spectral entropies as information-theoretic tools for complex network comparison. *Phys. Rev. X* **6**, 041062 (2016).
146. Ghavasieh, A., Stella, M., Biamonte, J. & De Domenico, M. Unraveling the effects of multiscale network entanglement on empirical systems. *Commun. Phys.* **4**, 129 (2021).
147. Ghavasieh, A., Bertagnolli, G. & De Domenico, M. Dismantling the information flow in complex interconnected systems. *Phys. Rev. Res.* **5**, 013084 (2023).
148. Lancichinetti, A., Fortunato, S. & Radicchi, F. Benchmark graphs for testing community detection algorithms. *Phys. Rev. E* **78**, 046110 (2008).
149. Strogatz, S. et al. Fifty years of 'More is different'. *Nat. Rev. Phys.* **4**, 508–510 (2022).

150. Kivelä, M. et al. Multilayer networks. *J. Complex Netw.* **2**, 203–271 (2014).
151. Boccaletti, S. et al. The structure and dynamics of multilayer networks. *Phys. Rep.* **544**, 1–122 (2014).
152. Bianconi, G. *Multilayer Networks: Structure and Function* (Oxford Univ. Press, 2018).
153. Kenett, D. Y., Perc, M. & Boccaletti, S. Networks of networks — an introduction. *Chaos Solitons Fractals* **80**, 1–6 (2015).
154. Gao, J., Bashan, A., Shekhtman, L. & Havlin, S. *Introduction to Networks of Networks* (IOP, 2022).
155. Gao, J., Buldyrev, S. V., Havlin, S. & Stanley, H. E. Robustness of a network of networks. *Phys. Rev. Lett.* **107**, 195701 (2011).
156. Parshani, R., Buldyrev, S. V. & Havlin, S. Interdependent networks: reducing the coupling strength leads to a change from a first to second order percolation transition. *Phys. Rev. Lett.* **105**, 048701 (2010).
157. Schneider, C. M., Yazdani, N., Araújo, N. A., Havlin, S. & Herrmann, H. J. Towards designing robust coupled networks. *Sci. Rep.* **3**, 1–7 (2013).
158. Chen, S., Gao, Y., Liu, X., Gao, J. & Havlin, S. Robustness of interdependent networks based on bond percolation. *EPL (Europhys. Lett.)* **130**, 38003 (2020).
159. Parshani, R., Rozenblat, C., Ietri, D., Ducruet, C. & Havlin, S. Inter-similarity between coupled networks. *EPL (Europhys. Lett.)* **92**, 68002 (2011).
160. Buldyrev, S. V., Shere, N. W. & Cwilich, G. A. Interdependent networks with identical degrees of mutually dependent nodes. *Phys. Rev. E* **83**, 016112 (2011).
161. Reis, S. D. et al. Avoiding catastrophic failure in correlated networks of networks. *Nat. Phys.* **10**, 762–767 (2014).
162. Shekhtman, L. M., Danziger, M. M. & Havlin, S. Recent advances on failure and recovery in networks of networks. *Chaos Solitons Fractals* **90**, 28–36 (2016).
163. Valdez, L. D. et al. Cascading failures in complex networks. *J. Complex Netw.* **8**, cnaa013 (2020).
164. Schelling, T. C. Hockey helmets, concealed weapons, and daylight saving: a study of binary choices with externalities. *J. Confl. Resolut.* **17**, 381–428 (1973).
165. Granovetter, M. Threshold models of collective behavior. *Am. J. Sociol.* **83**, 1420–1443 (1978).
166. Easley, D. & Kleinberg, J. *Networks, Crowds, and Markets: Reasoning About a Highly Connected World* (Cambridge Univ. Press, 2010).
167. Gallotti, R., Valle, F., Castaldo, N., Sacco, P. & De Domenico, M. Assessing the risks of 'infodemics' in response to COVID-19 epidemics. *Nat. Hum. Behav.* **4**, 1285–1293 (2020).
168. Watts, D. J., Rothschild, D. M. & Mobius, M. Measuring the news and its impact on democracy. *Proc. Natl Acad. Sci. USA* **118**, e1912443118 (2021).
169. Valente, T. W. Network models and methods for studying the diffusion of innovations. *Model Methods Soc. Netw. Anal.* **28**, 98–116 (2005).
170. Watts, D. J. A simple model of global cascades on random networks. *Proc. Natl Acad. Sci. USA* **99**, 5766–5771 (2002).
171. Gleeson, J. P. & Cahalane, D. J. Seed size strongly affects cascades on random networks. *Phys. Rev. E* **75**, 056103 (2007).
172. Liu, R.-R., Wang, W.-X., Lai, Y.-C. & Wang, B.-H. Cascading dynamics on random networks: crossover in phase transition. *Phys. Rev. E* **85**, 026110 (2012).
173. Centola, D., Eguíluz, V. M. & Macy, M. W. Cascade dynamics of complex propagation. *Phys. A Stat. Mech. Appl.* **374**, 449–456 (2007).
174. Gleeson, J. P. Cascades on correlated and modular random networks. *Phys. Rev. E* **77**, 046117 (2008).
175. Dodds, P. S. & Payne, J. L. Analysis of a threshold model of social contagion on degree-correlated networks. *Phys. Rev. E* **79**, 066115 (2009).
176. Hackett, A., Melnik, S. & Gleeson, J. P. Cascades on a class of clustered random networks. *Phys. Rev. E* **83**, 056107 (2011).
177. Snyder, J., Cai, W. & D'Souza, R. M. Degree-targeted cascades in modular, degree-heterogeneous networks. *Phys. Rev. Res.* **4**, 013040 (2022).
178. Karimi, F. & Holme, P. Threshold model of cascades in empirical temporal networks. *Phys. A Stat. Mech. Appl.* **392**, 3476–3483 (2013).
179. Backlund, V.-P., Saramäki, J. & Pan, R. K. Effects of temporal correlations on cascades: threshold models on temporal networks. *Phys. Rev. E* **89**, 062815 (2014).
180. Brummitt, C. D., Lee, K.-M. & Goh, K.-I. Multiplexity-facilitated cascades in networks. *Phys. Rev. E* **85**, 045102 (2012).
181. Yu, Y. et al. System crash as dynamics of complex networks. *Proc. Natl Acad. Sci. USA* **113**, 11726–11731 (2016).
182. Galstyan, A. & Cohen, P. Cascading dynamics in modular networks. *Phys. Rev. E* **75**, 036109 (2007).
183. Dodds, P. S. & Watts, D. J. Universal behavior in a generalized model of contagion. *Phys. Rev. Lett.* **92**, 218701 (2004).
184. Bak, P., Tang, C. & Wiesenfeld, K. Self-organized criticality: an explanation of the 1/*f* noise. *Phys. Rev. Lett.* **59**, 381 (1987).
185. Bak, P., Tang, C. & Wiesenfeld, K. Self-organized criticality. *Phys. Rev. A* **38**, 364 (1988).
186. Bonabeau, E. Sandpile dynamics on random graphs. *J. Phys. Soc. Japan* **64**, 327–328 (1995).
187. Lise, S. & Paczuski, M. Nonconservative earthquake model of self-organized criticality on a random graph. *Phys. Rev. Lett.* **88**, 228301 (2002).
188. Goh, K.-I., Lee, D.-S., Kahng, B. & Kim, D. Sandpile on scale-free networks. *Phys. Rev. Lett.* **91**, 148701 (2003).
189. Lee, D.-S., Goh, K.-I., Kahng, B. & Kim, D. Sandpile avalanche dynamics on scale-free networks. *Phys. A Stat. Mech. Appl.* **338**, 84–91 (2004).
190. Brummitt, C. D., D'Souza, R. M. & Leicht, E. A. Suppressing cascades of load in interdependent networks. *Proc. Natl Acad. Sci. USA* **109**, E680–E689 (2012).
191. Mikaberidze, G. & D'Souza, R. M. Sandpile cascades on oscillator networks: the BTW model meets Kuramoto. *Chaos* **32**, 053121 (2022).
192. Daqing, L., Yinan, J., Rui, K. & Havlin, S. Spatial correlation analysis of cascading failures: congestions and blackouts. *Sci. Rep.* **4**, 5381 (2014).
193. Hines, P. D., Dobson, I. & Rezaei, P. Cascading power outages propagate locally in an influence graph that is not the actual grid topology. *IEEE Trans. Power Syst.* **32**, 958–967 (2016).
194. Schäfer, B., Witthaut, D., Timme, M. & Latora, V. Dynamically induced cascading failures in power grids. *Nat. Commun.* **9**, 1975 (2018).
195. Valente, A., De Domenico, M. & Artime, O. Non-Markovian random walks characterize network robustness to nonlocal cascades. *Phys. Rev. E* **105**, 044126 (2022).
196. Barthelemy, M. Betweenness centrality in large complex networks. *Eur. Phys. J. B* **38**, 163–168 (2004).
197. Kornbluth, Y. et al. Network overload due to massive attacks. *Phys. Rev. E* **97**, 052309 (2018).
198. Artime, O. & De Domenico, M. Abrupt transition due to non-local cascade propagation in multiplex systems. *New J. Phys.* **22**, 093035 (2020).
199. Moreno, Y., Pastor-Satorras, R., Vázquez, A. & Vespignani, A. Critical load and congestion instabilities in scale-free networks. *EPL (Europhys. Lett.)* **62**, 292 (2003).
200. Lai, Y.-C., Motter, A. E. & Nishikawa, T. Attacks and cascades in complex networks. *Complex Netw.* **650**, 299–310 (2004).
201. Wang, W.-X. & Chen, G. Universal robustness characteristic of weighted networks against cascading failure. *Phys. Rev. E* **77**, 026101 (2008).
202. Cao, X.-B., Hong, C., Du, W.-B. & Zhang, J. Improving the network robustness against cascading failures by adding links. *Chaos Solitons Fractals* **57**, 35–40 (2013).
203. Pahwa, S., Scoglio, C. & Scala, A. Abruptness of cascade failures in power grids. *Sci. Rep.* **4**, 3694 (2014).
204. Paul, G., Tanizawa, T., Havlin, S. & Stanley, H. E. Optimization of robustness of complex networks. *Eur. Phys. J. B* **38**, 187–191 (2004).
205. Latora, V. & Marchiori, M. Vulnerability and protection of infrastructure networks. *Phys. Rev. E* **71**, 015103 (2005).
206. Reis, S. D. S. et al. Avoiding catastrophic failure in correlated networks of networks. *Nat. Phys.* **10**, 762–767 (2014).
207. Carchiolo, V., Grassia, M., Longheu, A., Malgeri, M. & Mangioni, G. Network robustness improvement via long-range links. *Comput. Soc. Netw.* **6**, 12 (2019).
208. Carchiolo, V., Grassia, M., Longheu, A., Malgeri, M. & Mangioni, G. in *Internet and Distributed Computing Systems* (eds Xiang, Y. et al.) 270–277 (Springer, 2018).
209. Chen, L., Liu, R., Liu, Z.-P., Li, M. & Aihara, K. Detecting early-warning signals for sudden deterioration of complex diseases by dynamical network biomarkers. *Sci. Rep.* **2**, 342 (2012).
210. Squartini, T., Van Lelyveld, I. & Garlaschelli, D. Early-warning signals of topological collapse in interbank networks. *Sci. Rep.* **3**, 3357 (2013).
211. Suweis, S. & D'Odorico, P. Early warning signs in social-ecological networks. *PLoS ONE* **9**, e101851 (2014).
212. Dakos, V. & Bascompte, J. Critical slowing down as early warning for the onset of collapse in mutualistic communities. *Proc. Natl Acad. Sci. USA* **111**, 17546–17551 (2014).
213. Kuehn, C., Zschaler, G. & Gross, T. Early warning signs for saddle-escape transitions in complex networks. *Sci. Rep.* **5**, 13190 (2015).
214. Bauch, C. T., Sigdel, R., Pharaon, J. & Anand, M. Early warning signals of regime shifts in coupled human–environment systems. *Proc. Natl Acad. Sci. USA* **113**, 14560–14567 (2016).
215. Majdandzic, A. et al. Multiple tipping points and optimal repairing in interacting networks. *Nat. Commun.* **7**, 10850 (2016).
216. Sun, E. D., Michaels, T. C. T. & Mahadevan, L. Optimal control of aging in complex networks. *Proc. Natl Acad. Sci. USA* **117**, 20404–20410 (2020).
217. Sanhedrai, H. et al. Reviving a failed network through microscopic interventions. *Nat. Phys.* **18**, 338–349 (2022).
218. Majdandzic, A. et al. Spontaneous recovery in dynamical networks. *Nat. Phys.* **10**, 34–38 (2014).
219. Lin, Z.-H. et al. Non-Markovian recovery makes complex networks more resilient against large-scale failures. *Nat. Commun.* **11**, 2490 (2020).
220. Zhou, D. & Elmokashfi, A. Network recovery based on system crash early warning in a cascading failure model. *Sci. Rep.* **8**, 7443 (2018).
221. Pan, X. & Wang, H. Resilience of and recovery strategies for weighted networks. *PLoS ONE* **13**, e0203894 (2018).
222. Smith, A. M. et al. Competitive percolation strategies for network recovery. *Sci. Rep.* **9**, 11843 (2019).
223. Pasqualetti, F., Zhao, S., Favaretto, C. & Zampieri, S. Fragility limits performance in complex networks. *Sci. Rep.* **10**, 1774 (2020).
224. Di Muro, M. A., La Rocca, C. E., Stanley, H. E., Havlin, S. & Braunstein, L. A. Recovery of interdependent networks. *Sci. Rep.* **6**, 1–11 (2016).
225. Artime, O., d'Andrea, V., Gallotti, R., Sacco, P. L. & De Domenico, M. Effectiveness of dismantling strategies on moderated vs. unmoderated online social platforms. *Sci. Rep.* **10**, 14392 (2020).
226. De Domenico, M., Lima, A., Mougel, P. & Musolesi, M. The anatomy of a scientific rumor. *Sci. Rep.* **3**, 1–9 (2013).
227. Liu, R., Chen, P., Aihara, K. & Chen, L. Identifying early-warning signals of critical transitions with strong noise by dynamical network markers. *Sci. Rep.* **5**, 17501 (2015).

Acknowledgements
O.A. acknowledges financial support from the Spanish Ministry of Universities through the Recovery, Transformation and Resilience Plan funded by the European Union (Next Generation EU) and the University of the Balearic Island. M.D.D. acknowledges partial financial support from the University of Padua (PRD-BIRD 2022), from the INFN grant 'LINCOLN', from the EU funding within the MUR PNRR 'National Center for HPC, Big Data and Quantum Computing' (project number CN00000013 CN1) and from the University of Padua (PRD-BIRD 2022). J.P.G. is partly funded by Science Foundation Ireland grant numbers 16/IA/4470 and 12/RC/2289 P2. H.A.M. was supported by NSF-HNDS Award 2214217. G.M. acknowledges financial support from PNRR MUR project PE0000013-FAIR. M.P. was supported by the Slovenian Research and Innovation Agency (grant numbers P1-0403, J1-2457 and N1-0232). F.R. acknowledges support from the Army Research Office, award number W911NF-21-1-0194, and the Air Force Office of Scientific Research, award number FA9550-21-1-0446.

Author contributions
M.D.D. and G.M. decided the scope of the Review. M.G. performed benchmarking. All authors contributed to the writing of the manuscript.

Competing interests
The authors declare no competing interests.

Additional information
Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s42254-023-00676-y.

Peer review information *Nature Reviews Physics* thanks Xiao-Long Ren, Yi-Cheng Zhang and the other, anonymous, reviewer(s) for their contribution to the peer review of this work.

[1]Departament de Física de la Matèria Condensada, University of Barcelona, Barcelona, Spain. [2]Universitat de Barcelona Institute of Complex Systems (UBICS), University of Barcelona, Barcelona, Spain. [3]Universitat de les Illes Balears, Palma, Spain. [4]Department of Electric, Electronic and Computer Engineering, University of Catania, Catania, Italy. [5]Department of Physics and Astronomy, University of Padua, Padova, Italy. [6]Padua Center for Network Medicine, University of Padua, Padova, Italy. [7]Istituto Nazionale di Fisica Nucleare, Padova, Italy. [8]MACSI, Department of Mathematics & Statistics, University of Limerick, Limerick, Ireland. [9]Levich Institute and Physics Dept., City College of New York, New York, NY, USA. [10]Faculty of Natural Sciences and Mathematics, University of Maribor, Maribor, Slovenia. [11]Department of Physics, Kyung Hee University, Seoul, Republic of Korea. [12]Department of Medical Research, China Medical University Hospital, China Medical University, Taichung, Taiwan. [13]Complexity Science Hub Vienna, Vienna, Austria. [14]Center for Complex Networks and Systems Research, Luddy School of Informatics, Computing, and Engineering, Indiana University, Luddy Center for Artificial Intelligence, Bloomington, IN, USA. [15]These authors contributed equally: Oriol Artime and Marco Grassia.