INTERFACE

rsif.royalsocietypublishing.org

Research

Cite this article: Podobnik B, Horvatic D, Lipic T, Perc M, Buldú JM, Stanley HE. 2015 The cost of attack in competing networks. *J. R. Soc. Interface* **12**: 20150770.
http://dx.doi.org/10.1098/rsif.2015.0770

Received: 28 August 2015
Accepted: 30 September 2015

Subject Areas:
mathematical physics

Keywords:
complex networks, interactive networks, socioeconomic systems, network vulnerability, robustness, attacks

Author for correspondence:
D. Horvatic
e-mail: davorh@phy.hr

THE ROYAL SOCIETY
PUBLISHING

The cost of attack in competing networks

B. Podobnik[1,2,3], D. Horvatic[4], T. Lipic[1,5], M. Perc[6,7], J. M. Buldú[8,9] and H. E. Stanley[1]

[1]Center for Polymer Studies and Department of Physics, Boston University, Boston, MA 02215, USA
[2]Faculty of Civil Engineering, University of Rijeka, 51000 Rijeka, Croatia
[3]Zagreb School of Economics and Management, 10000 Zagreb, Croatia
[4]Faculty of Natural Sciences, University of Zagreb, 10000 Zagreb, Croatia
[5]Rudjer Boskovic Institute, Centre for Informatics and Computing, 10000 Zagreb, Croatia
[6]Faculty of Natural Sciences and Mathematics, University of Maribor, Koroška cesta 160, 2000 Maribor, Slovenia
[7]Department of Physics, Faculty of Sciences, King Abdulaziz University, Jeddah, Saudi Arabia
[8]Center for Biomedical Technology (UPM), 28223 Pozuelo de Alarcón, Madrid, Spain
[9]Complex Systems Group, Rey Juan Carlos University, 28933 Móstoles, Madrid, Spain

DH, 0000-0002-0411-8474; TL, 0000-0002-8037-8198; MP, 0000-0002-3087-541X; JMB, 0000-0002-9345-599X; HES, 0000-0003-2800-4495

Real-world attacks can be interpreted as the result of competitive interactions between networks, ranging from predator–prey networks to networks of countries under economic sanctions. Although the purpose of an attack is to damage a target network, it also curtails the ability of the attacker, which must choose the duration and magnitude of an attack to avoid negative impacts on its own functioning. Nevertheless, despite the large number of studies on interconnected networks, the consequences of initiating an attack have never been studied. Here, we address this issue by introducing a model of network competition where a resilient network is willing to partially weaken its own resilience in order to more severely damage a less resilient competitor. The attacking network can take over the competitor's nodes after their long inactivity. However, owing to a feedback mechanism the takeovers weaken the resilience of the attacking network. We define a conservation law that relates the feedback mechanism to the resilience dynamics for two competing networks. Within this formalism, we determine the cost and optimal duration of an attack, allowing a network to evaluate the risk of initiating hostilities.

1. Introduction

Recent research carried out on competing interacting networks [1–6] does not take into account the fact that real-world networks often compete not only to survive, but also to take over or even destroy their competitors [7]. For example, in international politics and economics, when one country imposes economic sanctions on another, feedback mechanisms can cause the country imposing the sanctions to also be adversely affected. The decision by a wealthier country to keep military spending at a high level long enough to exhaust its poorer competitor can also contribute to its own exhaustion [8]. Similarly, in warfare, any attack depletes the resources of the attacking force and can elicit a counter-attack from the competing force [9]. Also, in nature, an incursion between species can alter the dynamics of the predator–prey interaction [10].

Although, these competing interactions are a widespread real-world phenomenon, current studies analyse only the effects of an attack on attacked networks, but disregard its effect on the external attacking network. For example, for both single and interactive networks, existing studies on network robustness report that every network, regardless of the size and architecture, can eventually be destroyed [11–16]. But, what then prevents a network from attacking a weaker competitor or, what is the optimal moment for initiating or ending an attack? In order to identify the factors that inhibit a network from attacking and demolishing a weaker competitor and to determine the optimal moment and duration of an attack, we develop a theoretical framework that quantifies the cost of an

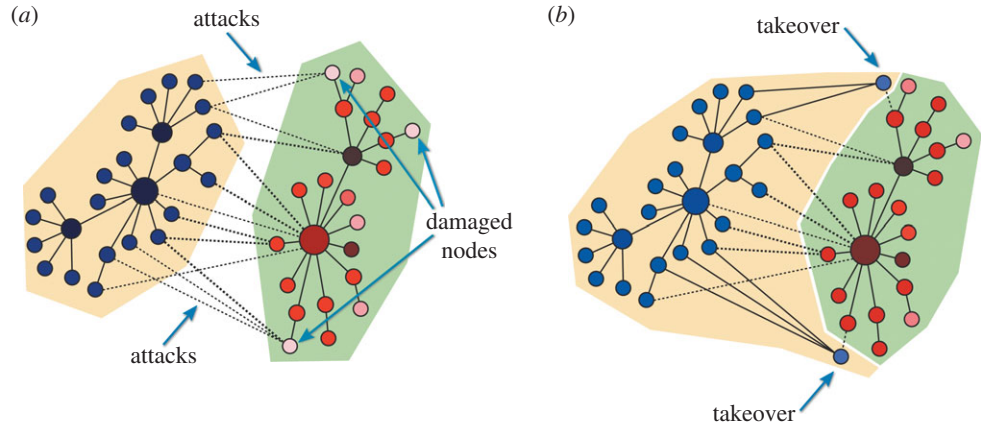

Figure 1. Attacks, failures, takeovers and their cost on the attacking network. In (*a*), we assume that each node in both the more resilient (stronger) network S and the less resilient (weaker) network W is described by the same failure probability. Different nodes spend different times during internal failure—the less opaque a node is, the more time it spends in internal failure. In (*b*), if a node in the weaker network W remains inactive more than some threshold time, it will be taken over by the stronger network S. However, network S pays for this takeover with a reduction in its resilience. (Online verison in colour.)

attack by connecting the feedback mechanisms and resilience dynamics between two competing dynamic networks with differing levels of resilience [17,18].

2. Theoretical framework

We introduce a general methodology that can be applied to networks of any size and structure. First, as an illustrative example, we describe two competing Barabási–Albert (BA) networks [19] that we designate network S and network W. This model differs from the single network BA model in that the two interconnected networks have both intranetwork and internetwork links [20]. One real-world example of this kind of network interaction is firms in an economic network that link with other firms both domestically and abroad.

Using the preferential attachment (PA) rule [19–21], we generate networks S and W starting with n_0 nodes in each network. At each time step, we add a new node that connects with m_S existing nodes in network S and with $m_{W,S}$ existing nodes in network W, where the probability of each connection depends on the total node degrees in networks S and W. Similarly, using the PA rule, we connect a new node in network W with m_W nodes in network W and with $m_{S,W} = m_{W,S}$ nodes in network S.

In a broad class of real-world networks, nodes can fail either owing to inherent reasons [22] or because their functionality depends on their neighbourhood [22,23]. Hence, any node in either of the two networks, e.g. a node n_i in network S with k_S neighbours in its own network and $k_{W,S}$ neighbours in network W, can fail at any moment, either internally—independent of other nodes—with a probability p_1 or externally with a probability p_2. Node n_i externally fails with a probability p_2 when, similar to the Watts model [23], the total fraction of its active neighbours is less than or equal to a fractional threshold T which is equal for all nodes in both networks. The larger the T-value, the less resilient the network. We assume that one of the two networks is more resilient than the other, distinguishing between strong network S and weak network W. We do so by assigning different fractional thresholds to the strong and weak networks, T_S and T_W, respectively, with $T_S < T_W$. As in reference [22], we assume that an internally failed node in network S or network W recovers from its last internal failure after a period τ. Consecutive failures of the same node stretch the effective failure times and introduce heterogeneity into the distribution of inactivity periods. Because, in real-world networks, it is dangerous for nodes to be inactive, we allow the strong network to take over nodes in the weak network when a node n_i spends more time in internal failure than $n\tau$, where n is a constant. Figure 1 qualitatively shows the interaction process.

3. Results

We quantify the current collective state of the strong and weak networks in terms of the fraction of active nodes, f_S and m_W, respectively [22,24,25]. We assume that initially both networks have internal and external failure probability values of $p_1 \equiv p_X$ and p_2, respectively. Figure 2*a* shows a two-parameter phase diagram for each network in which the hysteresis is composed of two spinodals separating two collective states, i.e. the primarily 'active' and the primarily 'inactive'. Figure 2*b* shows that increasing the value of p_1 leads to catastrophic first-order phase transitions in both networks. When each network recovers (i.e. when p_1 is decreased to previous values), the fraction of active nodes returns to an upper state. Nevertheless, the critical point in the recovery is well beyond the point at which the network collapses. Figure 2*b* also shows (solid line) that the initial choice of parameters makes network S more resilient to network fluctuations in the value of p_1 and that the fluctuation needed to initiate the collapse of network S ($p_1^S \equiv p_{1c}^S - p_X$) is much larger than the fluctuation needed to initiate the collapse of network W ($p_1^W \equiv p_{1c}^W - p_X$). Furthermore, network W is closer to a critical transition than network S.

Because network S has a higher resilience than network W and can more easily withstand fluctuations, S could induce the collapse of W by increasing p_1, but only if the fraction of its active links is not dramatically reduced. Figure 2*b* shows how when network S attacks network W by increasing p_1 to $\approx$0.002, the weak network becomes abruptly dysfunctional. Figure 2*b* also shows that when the values of p_1 are reset to their pre-attack levels the collapse of network W is permanent (red dashed line) and, if it ceases its attack, the

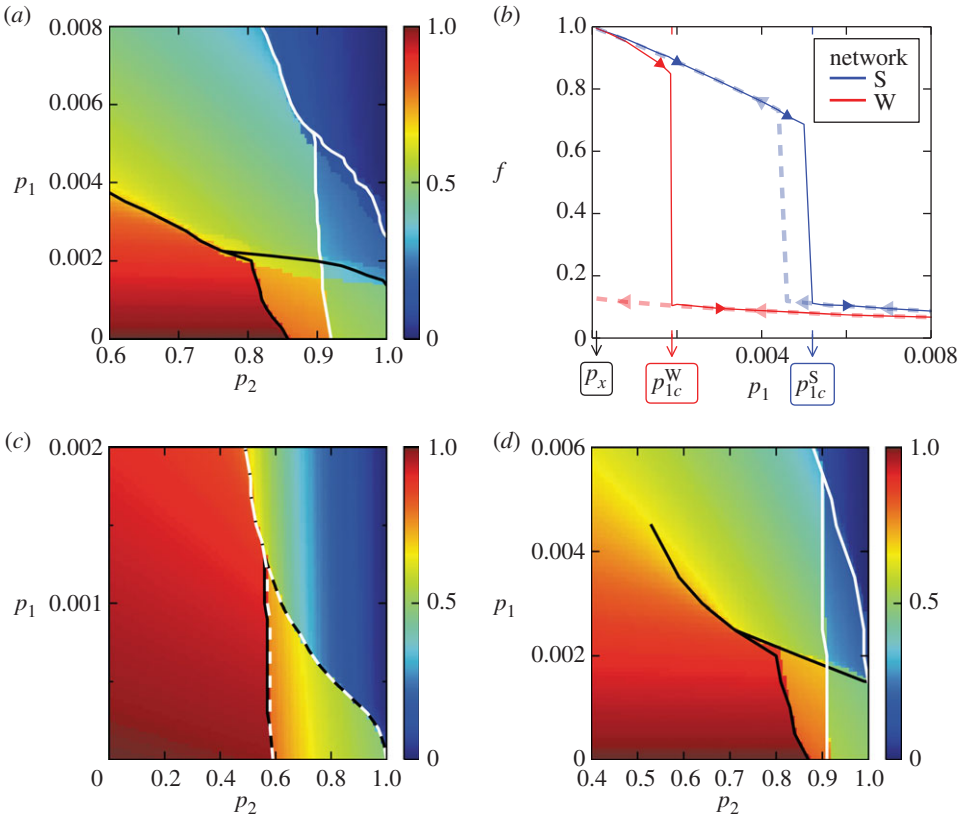

Figure 2. Attack strategy between two competing networks with different resilience levels and intra/interlink architecture. Shown are fractions of active nodes. The most resilient, strong network S (with $T_S = 0.3$) endangers and partially destroys its own nodes by increasing their internal failure probability p_1 in order to more severely damage the least resilient network W (with $T_W = 0.7$). Each of S and W has hysteresis composed of two spinodals, representing attacking and recovery phases. The recovery time is $\tau = 50$, and the takeover and cost mechanisms are disregarded. (*a*) Attacking strategy between two competing BA networks with parameters: $m_S = m_W = 3$ and $m_{S,W} = m_{W,S} = 2$. Strong network S wants to bring W in the parameter space between hystereses of W (black lines) and S (white lines), where S is predominantly active and W is predominantly inactive (see, *b*). Dark red (blue) is the parameter space where both S and W are active (inactive). (*b*) For $p_2 = 0.9$, fraction of active nodes in the strong f_S (blue lines) and weak f_W (red lines) networks as a function of the internal failure probability p_1. Hysteresis is a result of increasing p_1 from zero to one and then decreasing it back to zero. The increase in p_1 accounts for the attacks and the decrease for a repair of the network. (*c*) Same case as (*a*) but for two randomly connected competing Erdös–Renyi networks. (*d*) Same case as (*c*) but with an assortative mixing in the connection between networks: nodes with degree d_1 link, with probability $1/|d_1 - d_2 + 1|$, with nodes in the other network with degree d_2.

recovery of network S is complete and all of its inactive nodes are reactivated (see blue dashed line in figure 2*b*). Similarly, when economic sanctions in a financial system are lifted the weak economies are not restored, but the strong economics recover after suffering little damage.

Figure 2*c* shows a modified competing network structure in which there are two interconnected Erdös–Reny networks [26] with internetwork links chosen randomly. Although this structure differs quantitatively from the phase diagram of competing BA networks, the same kind of transition occurs in the random configuration. This indicates the generality of these critical transitions in competing networks. We obtain similar results when degree–degree correlations are introduced between the links connecting both networks. Figure 2*d* shows nodes in the strong network linking with nodes in the weak network only when they are of a similar degree (i.e. 'assortative mixing' [27]). As in the other configurations, the better position of the attacker enables the strong network to destroy the weak one and then return safely to its initial state.

3.1. Mean-field theory

Using mean-field theory, we analytically describe the attack and recovery process between two interconnected networks with random regular topologies where all nodes within the same network have the same degree. We assume that each node in network S is linked with k_S nodes in its own network and $k_{W,S}$ nodes in network W. Similarly, each node in network W is linked with k_W nodes in network W and $k_{S,W}$ nodes in network S. In both networks, the fraction of failed nodes is $a \equiv 1 - f$, where f is the fraction of functional nodes. We can approximate the values of a at each network by

$$a_S = p^*_{S,1} + p_{S,2}(1 - p^*_{S,1})E_S \tag{3.1}$$

and

$$a_W = p^*_{W,1} + p_{W,2}(1 - p^*_{W,1})E_W, \tag{3.2}$$

where $p^*_{S,1} \equiv 1 - \exp(-p_{S,1}\tau)$ [23] denotes the average fraction of internally failed nodes and $p_{S,2}E_S$ denotes the probability that a node in network S has externally failed

$$E_S = \sum_{j=0}^{t_S} \sum_{i=0}^{j} \binom{k_S}{k_S - i} a_S^{k_S - i}(1 - a_S)^i \binom{k_{W,S}}{k_{W,S} - (j - i)} a_W^{k_{W,S} - (j-i)}(1 - a_W)^{j-i}. \tag{3.3}$$

Here, t_S represents the absolute threshold of network S simply related to the fractional threshold T_S as $T_S = t_S/(k_S + k_{W,S})$: a node in network S can externally fail with a

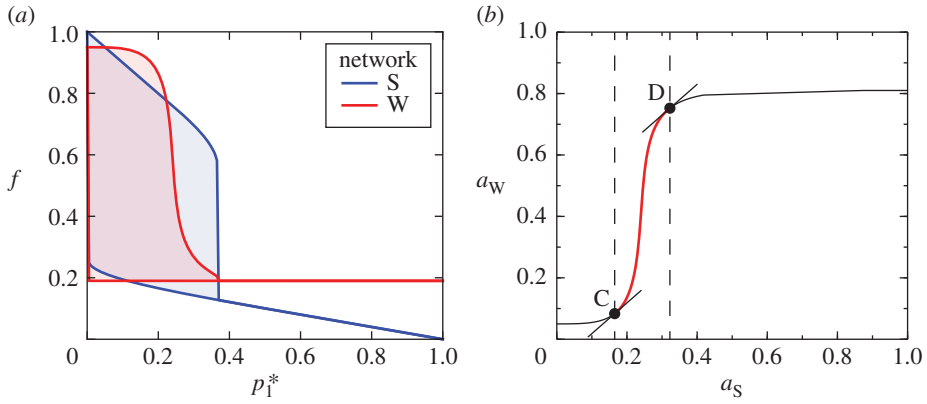

Figure 3. Identifying the optimal parameters for attacking a weak network. Analytical approach. Strong network S (less vulnerable) uses its own probability of internal failures $p^*_{S,1}$ to cause damage in weak network W and, unavoidably, induce partial self-destruction. Model parameters are $k_S = 20$, $k_{S,W} = k_{W,S} = 10$, $k_S = 5$, $t_S = 10$, $k_W = 10$, $p_{S,2} = p_{W,2} = 0.8$ and $p^*_{W,1} = 0.05$. In (*a*), fraction of active nodes in network S and W, $f_S = 1 - a_S$ and $f_W = 1 - a_W$, respectively. Strong network S (blue) deliberately initiates its own failures (increasing $p^*_{S,1}$) to create larger damage in a weak (more vulnerable) network W (red). Note that the fraction of active nodes exhibits a hysteresis behaviour for both networks, with a critical point at $p_C \approx 0.33$. In (*b*), we investigate when S should stop attacking W by increasing its probability of internal failure $p^*_{S,1}$. Shown are the fractions of failed nodes, $a_S = 1 - f_S$ and $a_W = 1 - f_W$. Between points C and D (dashed lines), an increase in $p^*_{S,1}$ induces more failures in the weaker network, leading to a comparative benefit. Beyond point D, the attack is not worthwhile for network S because it suffers the consequences more intensely than its competitor.

probability $p_{S,2}$ only when the number of active neighbours in both network S and network W is less than or equal to t_S. Similarly, we obtain E_W for network W by replacing S with W, and vice versa, in equation (3.3). Finally, we set network S to be more resilient than network W, by setting $t_S/(k_S + k_{W,S}) < t_W/(k_W + k_{S,W})$.

The analytical results of figure 3*a* indicate that when network S increases the internal failure probability $p_{S,1}$ and so $p^*_{S,1}$ in an effort to damage network W it also causes partial damage to itself. Although it first seems that increasing $p^*_{S,1}$ reduces more active nodes in network S than in network W, when $p^*_{S,1} > 0.18$, the fraction of active nodes in network W drops sharply and eventually $f_S > f_W$. This attack strategy by network S is thus effective. If $p^*_{S,1} > 0.33$, however, network S undergoes a first-order transition that leads to collapse, a situation that network S must clearly avoid.

Inspecting the recovery of the previous internal failure probability values after the attack, we find that the fraction of active nodes in both networks exhibit a hysteresis behaviour. Note that when the transition at $p^*_{S,1} \sim 0.33$ is surpassed neither network is able to restore its functioning to those levels attained prior to the attack.

The analytical results indicate that attacking network S is effective only for certain values of $p^*_{S,1}$. Thus, network S should increase $p^*_{S,1}$ only as long as the damage to network W continues to be greater than the damage to itself, i.e. only when $\Delta a_W > \Delta a_S$. Figure 3*b* shows the region in which attacks by network S are effective by showing the fraction of failed nodes in both networks in a two-dimensional phase space as the value of $p^*_{S,1}$ is increased. Two solid lines with a slope of one indicate the region in which an attack by network S is effective. When the slope of function $a_W = f(a_S)$ is greater than one (the region between the two shaded lines), increasing $p^*_{S,1}$ produces more damage in network W than in network S and is thus an effective attack strategy.

In order to measure the effect of capturing nodes from a competitor network and how takeovers can modify the resilience properties of a network, we design a model in which network S is again more resilient than network W ($T_S < T_W$) and where node n_i of network W is taken over by network S if its internal failure time exceeds $n\tau$, where τ is a certain failure time and n a constant. Note that the longer a node in network W remains inactive (i.e. the higher the value of n), the higher the probably that it will be acquired by network S. Real-world examples of this mechanism include sick or disabled prey in an ecological system [28,29] or countries whose economic systems remain in recession for too long.

3.2. Take over and conservation laws

To evaluate the acquisition costs in both networks, we define network wealth (capital) as proportional to two variables: the total number of links in the network—as defined in conservation biology [30,31]—and the resilience of the network. Note that if two networks have the same number of links but different resiliencies their wealth is not equal. Note also that when network S acquires a node of degree $k_{W,i}$ from network W the overall resilience of network S decreases because it has acquired a weaker node. Thus, network S pays an instantaneous, collective cost through a feedback mechanism that decreases its resilience from an initial threshold T_S to a new threshold T'_S.

One of the important issues in dynamic systems that has a critical point as an attractor is whether a conservation of energy is required in local dynamic interactions [32–34]. To quantify how threshold T'_s changes in competing networks, we define a conservation law that relates the feedback mechanism to the resilience dynamics as

$$N\langle k_S\rangle(T'_S - T_S) = k_{W,i}(T_W - T'_S). \tag{3.4}$$

Here, N is the size of the strong network, $\langle k_S\rangle$ its average degree, and $k_{W,i}$ the degree of the node that has been taken over. Thus, we assume that the more important the acquired node (i.e. the larger its degree $k_{W,i}$), the greater the cost to the resilience of network S, making it more vulnerable to future attacks. As a result, when a predator (strong) network S increases its size N and its degree $\langle k_s\rangle$, its acquisition cost, $T'_S - T_S$, will decrease.

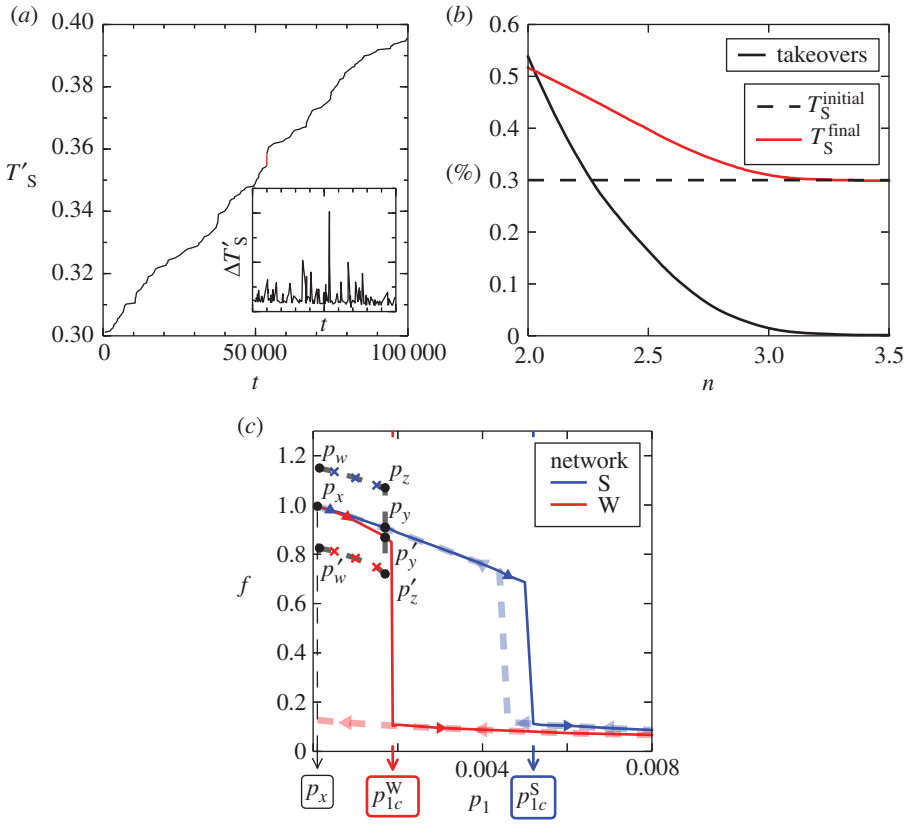

Figure 4. Cost and takeover mechanisms in two competing *BA* networks. (*a*) Threshold T'_S of network S as a function of time for two competing *BA* networks with $n = 2.5$ and $\tau = 50$. Fluctuations in the evolution of T'_S are a consequence of the degree of the acquired node: the higher the degree the higher the increase of T'_S. (*b*) Fraction of takeovers and final threshold as a function of the time $n\tau$ required to acquire a node from the weak network, with $\tau = 50$. As n increases, the number of takeovers decreases to zero. At the same time, the resilience of network S tends to the initial value $T_S = 0.3$. (*c*) Owing to takeovers the fraction of active nodes in the more resilient network, S can increase to values higher than one. In this example, network W is irreversibly damaged after p_1 is restored to its initial value. (Online verison in colour.)

Here, we quantify how threshold T'_S of the stronger network changes in competing networks where we assume that threshold T_W of the weaker network does not change, because every node has the same threshold. The stronger network S has the initial number of nodes N_S, the average degree $\langle k_S \rangle$. After multiple takeovers, where S took over nodes $n_{w,1}, n_{w,2}, \ldots, n_{w,n}$ with degrees $k_{w,1}, k_{w,2}, \ldots, k_{w,n}$, respectively, by using equation (3.4), we obtain

$$T'_S = \frac{(k_{w,1} + k_{w,1} + \cdots + k_{w,n})T_W + N_S\langle k_S \rangle T_S}{N_S\langle k_S \rangle + k_{w,1} + k_{w,1} + \cdots + k_{w,n}}. \tag{3.5}$$

Figure 4*a* shows that when network S acquires nodes in network W the threshold T'_S of network S is increasingly affected as time passes. In this example, a node in network W is taken over by network S when the node is in failure state longer than $n\tau$ time steps, where $n = 2.5$ and $\tau = 50$. Note that as network S acquires weak nodes, its threshold T'_S increases and it becomes more vulnerable. Figure 4*b* shows the interplay between the time required to acquire a node $n\tau$ and the threshold T'_S. Note that as $n\tau$ increases, takeovers become increasingly rare, and the final threshold of network S approaches its initial resilience, here $T_S = 0.3$.

Figure 4*c* shows that, if the example in figure 2*b* is extended to include a takeover mechanism, a fraction of active nodes f_S in network S—measured relative to the initial number of nodes in each network—reaches values higher than one, with a peak at $p_y \to p_z$. Note that when attacks cease (e.g. when, in an economic system, sanctions are lifted) decreasing the value of p_1, $p_z \to p_w$, the fraction of active nodes in network S increases, but network W is left irreversibly damaged (see the closed hysteresis $p'_y \to p'_z \to p'_w$).

3.3. Threshold diversity in competing networks

Thus far, we have studied competing interconnected networks in which there is only one threshold characterizing each network. However, in real-world interconnected networks, commonly, the functionality of a node in a given network is not equally sensitive to its own neighbours and those of the other network. To this end, we assume that node n_i in network S can externally fail with probability p_2 if the fraction of the active neighbours of node n_i in network S is equal to or lower than some threshold T_S, or if the fraction of the active neighbours of node n_i in network W is equal to or lower than some threshold $T_{W,S}$. We similarly define external failure in the less resilient network W by replacing threshold T_S with T_W. The functioning of each node is thus dependent on its neighbours in network S and network W, but with different sensitivities—different resilience to external fluctuations.

Figure 5*a* shows, for a given set of parameters, a two-parameter phase diagram of competing networks, a model that incorporates the threshold separation for external failure but excludes takeover and feedback mechanisms. This model resembles that in figure 2, but uses different configurations. Suppose network S spontaneously activates at time t_0 but, owing to differences in the variables characterizing network

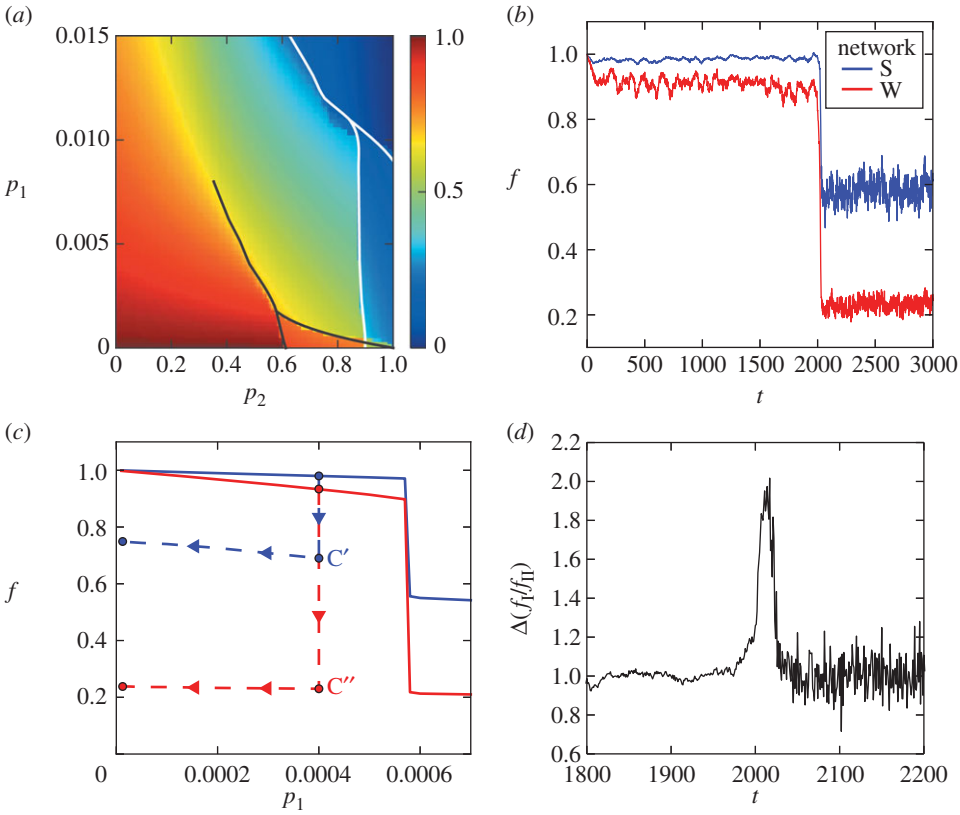

Figure 5. Quantification of the optimal attack duration. Model parameters are: $m_S = 6$, $m_W = 3$, $m_{S,W} = m_{W,S} = 2$. Similar to figure 4 but now with two thresholds used for defining resilience of each network. External failure thresholds are $T_W = 0.7$, $T_S = 0.3$ and $T_{S,W} = 0.4$. In (*a*), we find the phase diagram in model parameters (p_1, p_2) where each network has its own hysteresis. The takeover mechanism is disregarded and recovery time is $\tau = 50$. In (*b*), for each network, we show the time evolution of the fractions of active nodes with the takeover mechanism included where we use a takeover period of 1.5τ, $p_1 = 0.0004$ and $p_2 = 0.6$. At some point, S creates larger damage in a weak (less resilient) network W than to itself. (*c*) Related to (*b*), as a result of the attack, both networks are damaged, but W is damaged more. We also show how the fractions change with decreasing p_1 during the recovery phase. (*d*) Early-warning signal for determining when the attack should be stopped, defined as the change in the ratio between two fractions, $f_I(t + \Delta t)/f_{II}(t + \Delta t) - f_I(t)/f_{II}(t)$, where $\Delta t = 20$. The attack should be stopped when the indicator reaches the maximum.

S and network W, initiates a substitution mechanism, not a takeover. Thus, each time node n_i in network W spends a time period in an inactive mode that exceeds the substitution time—e.g. in ecology, a period of time without food—n_i is replaced by a new node from network S. Figure 5*b* shows the fraction of active nodes in each network calculated relative to the initial number of nodes at time t_0. Fractions of active nodes of both networks exhibit a catastrophic discontinuity (a phase flip) at $t \approx 2000$, which is characteristic of a first-order transition. Because both networks are interdependent, substituting nodes from the less resilient network W affects the functionality of network S even more dramatically than that shown in figure 2. Thus, beyond some threshold, we expect that additional weakening of network W will also permanently damage network S. This demonstrates how dangerous an attacking strategy can be for an attacker in a system of interdependent networks, e.g. between countries that are at the same time competitors and economics partners.

Figure 5*c* shows that when the attacks and substitutions cease, the fractions of active nodes in network S and network W reach points C' and C'', respectively. If the probability of internal failure p_1 spontaneously decreases during the recovery period because of network interdependence the functionality of network S is not substantially improved. The triumph of network S over network W has its price. In ecology, for example, although the population of each species tends to increase, a dominance strategy is risky, e.g. the extinction of a key species can trigger, through a cascade mechanism [15,35], the extinction of many other species [36].

Figure 5*d* shows the change in the ratio between the fraction of active nodes in network S and network W as a function of time. This ratio can serve as an early-warning mechanism [37] that indicates when attacks should be stopped. Optimally, the stopping time for attacks will be when the ratio reaches its maximum.

Finally, figure 6*a* shows that when the feedback mechanism (the cost of taking over) defined in equation (3.4) is included, the fraction of active nodes in each network exhibits an even richer discontinuous behaviour than in figure 5*c*, where the cost was excluded. After 50 000 steps, because of the decrease in network S's resilience after each substitute, the final fraction of active nodes in network S is substantially smaller than the corresponding fraction in figure 5*c* (i.e. when the cost is excluded). At the same time, figure 6*b* shows that an increase in the takeover time $n\tau$ decreases the fraction of substitutes.

4. Summary

In conclusion, we have presented a theoretical framework based on resilience, competition and phase transitions to introduce a cost-of-attack concept that relates feedback

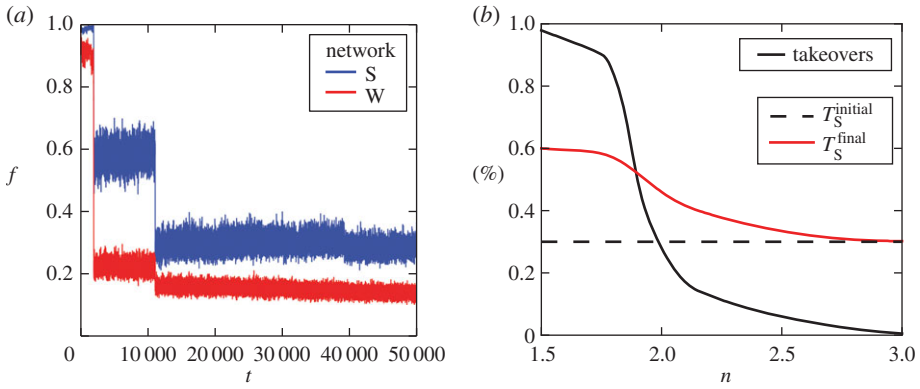

Figure 6. Evaluating the effect of the cost mechanism. Model parameters are $m_S = m_W = 3$, $m_{S,W} = m_{W,S} = 2$, $p_1 = 0.0004$, $p_2 = 0.6$. (*a*) The cost of the attacking strategy with takeover mechanism additionally decreases network resilience. The fraction of active nodes exhibits more discontinuities than in the case where the cost of an attack was excluded (figure 5). This is a consequence of the larger change in the resilience of S owing to inclusion of the cost mechanism. (*b*) The fraction of takeovers and threshold T_S' of the stronger network S as a function of takeover time $n\tau$, with $\tau = 50$. (Online verison in colour.)

mechanisms to resilience dynamics defined using a linear conservation law. Our model for competing networks can be applied across a wide range of human activities, from medicine and finance to international relations, intelligence services and military operations.

We focus on a specific context where a more resilient network attacks a less resilient competitor network. The model assumptions about the structure and dynamics for two interactive networks with competing interactions and different resilience levels have to be adjusted in regard to different real-world scenarios (see the electronic supplementary material, S4).

The ability to measure attacker network resilience and its attack cost is crucial, because every weakening of the resilience reduces the probability of the survival of the network under future attacks. For example, in political socio-economic systems, a network-based approach for overcoming competing countries could be more effective by applying economical sanctions than by carrying out military actions. Interdependent links established between countries during prosperous times can facilitate sanctions (intentional fluctuations) that are used as a weapon when more resilient countries try to overcome less resilient countries. They can also facilitate the global propagation of economic recessions (spontaneous fluctuations). During long economic crises, these interdependent links can become fatal for less resilient countries, whose weakness is enhanced by being underdogs in a global network-of-networks and, at the same time, whose resources can be captured by more powerful countries.

Although our proposed framework is suited for representing the simplest case of bilateral economic interdependence between just two countries (networks), it provides the basis for more general scenarios of alliances of more countries (networks). The concept of alliance where some countries unite in order to attack some other alliance is especially interesting when there is heterogeneity in resilience of allied attacker countries. For example, the most dominant countries economically can increase their dominance at the expense of their partners in the alliance or they can, on the other hand, depend on the alliance's weakest country (see the electronic supplementary material, S4A).

In addition to the intentional fluctuations characteristic of human societies, our methodology can also be applied to a broad class of complex systems in which spontaneous fluctuations occur, from brain functioning to ecological habitats and climate fluctuations [30,36,38–43]. The methodology is based on specific structure, dynamics and mechanisms of the model of networks with competing interactions and different resilience levels, which have to be adjusted for different systems and contexts of application (see the electronic supplementary material, S4).

Authors' contributions. B.P., D.H., T.L., M.P., J.M.B. and H.E.S. conceived and designed the research. B.P., D.H., T.L. carried out the numerical simulations, analysed the results and developed the theory. All authors discussed the results and contributed to the text of the manuscript.

Competing interests. We declare we have no competing interests.

Funding. B.P. was partially supported by the University of Rijeka. M.P. acknowledges support from the Slovenian Research Agency (grant no. P5-0027), and from the Deanship of Scientific Research, King Abdulaziz University (grant no. 76-130-35-HiCi). J.M.B. acknowledges financial support from MINECO (project FIS2013-41057-P). The Boston University work was supported by ONR grant no. N00014-14-1-0738, DTRA grant no. HDTRA1-14-1-0017 and NSF grant no. CMMI 1125290. The authors declare no competing financial interests.

Acknowledgements. We thank Jacobo Aguirre and David Papo for discussions.

References

1. Bastolla U, Fortuna MA, Pascual-García A, Ferrera A, Luque B, Bascompte J. 2009 The architecture of mutualistic networks minimizes competition and increases biodiversity. *Nature* **458**, 1018–1020. (doi:10.1038/nature07950)
2. Rohr RP, Saavedra S, Bascompte J. 2014 On the structural stability of mutualistic systems. *Science* **345**, 416.
3. Aguirre J, Papo D, Buldú JM. 2013 Successful strategies for competing networks. *Nat. Phys.* **9**, 230–234. (doi:10.1038/nphys2556)
4. D'Souza RM. 2013 Complex network: a winning strategy. *Nat. Phys.* **9**, 212–213. (doi:10.1038/nphys2571)
5. Kivela M, Arenas A, Barthelemy M, Gleeson JP, Moreno Y, Porter M. 2014 Multilayer networks. *J. Complex Netw.* **2**, 203–271. (doi:10.1093/comnet/cnu016)

6. Scholtes I, Wider N, Pfitzner R, Garas A, Tessone CJ, Schweitzer F. 2014 Causality-driven slow-down and speed-up of diffusion in non-Markovian temporal networks. *Nat. Commun.* **5**, 5024. (doi:10.1038/ncomms6024)
7. Thebault E, Fontaine C. 2010 Stability of ecological communities and the architecture of mutualistic and trophic networks. *Science* **329**, 853–856. (doi:10.1126/science.1188321)
8. Richardson LF. 1935 The mathematical psychology of war. *Nature* **135**, 830–831. (doi:10.1038/135830c0)
9. Shakarian P, Lei H, Lindelauf R. 2014 Power grid defense against malicious cascading failure. (http://arxiv.org/abs/1401.1086)
10. Scheffer M, Carpenter S, Foley JA, Folke C, Walker B. 2001 Catastrophic shifts in ecosystems. *Nature* **413**, 591–596. (doi:10.1038/35098000)
11. Podobnik B, Lipic T, Horvatic D, Majdandzic A, Bishop SR, Eugene Stanley H. 2015 Predicting the lifetime of dynamic networks experiencing persistent random attacks. *Sci. Rep.* **5**, 14286. (doi:10.1038/srep14286)
12. Albert R, Jeong H, Barabási AL. 2000 Error and attack tolerance of complex networks. *Nature* **406**, 378–382. (doi:10.1038/35019019)
13. Cohen R, Erez K, ben-Avraham D, Havlin S. 2000 Resilience of the internet to random breakdowns. *Phys. Rev. Lett.* **85**, 4626–4628.
14. Reis SDS, Hu Y, Babino A, Andrade Jr JS, Canals S, Sigman M, Makse HA. 2014 Avoiding catastrophic failure in correlated networks of networks. *Nat. Phys.* **10**, 762–767. (doi:10.1038/nphys3081)
15. Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S. 2010 Catastrophic cascade of failures in interdependent networks. *Nature* **464**, 1025–1028. (doi:10.1038/nature08932)
16. Dorogovtsev SN, Goltsev AV. 2008 Critical phenomena in complex networks. *Rev. Mod. Phys.* **80**, 1275–1335. (doi:10.1103/RevModPhys.80.1275)
17. May R. 2013 Networks and webs in ecosystems and financial systems. *Phil. Trans. Soc. A* **371**, 20120376. (doi:10.1098/rsta.2012.0376)
18. Downing AS, van Nes EH, Mooij WM, Scheffer M. 2012 The resilience and resistence of an ecosystem to a collapse of diversity. *PLoS ONE* **7**, e46135. (doi:10.1371/journal.pone.0046135)
19. Barabási A, Albert R. 1999 Emergence of scaling in random networks. *Science* **286**, 509–512. (doi:10.1126/science.286.5439.509)
20. Podobnik B, Horvatic D, Dickison M, Stanley HE. 2012 Preferential attachment in the interaction between dynamicly generated interdependent networks. *EPL* **100**, 50004. (doi:10.1209/0295-5075/100/50004)
21. Perc M. 2014 The Matthew effect in empirical data. *J. R. Soc. Interface* **11**, 20140378. (doi:10.1098/rsif.2014.0378)
22. Majdandzic A, Podobnik B, Buldyrev SV, Kenett DY, Havlin S, Eugene Stanley H. 2014 Spontaneous recovery in dynamical networks. *Nat. Phys.* **10**, 34–38. (doi:10.1038/nphys2819)
23. Watts DJ. 2002 A simple model of global cascades on random networks. *Proc. Natl Acad. Sci. USA* **99**, 5766–5771. (doi:10.1073/pnas.082090499)
24. Podobnik B, Majdandzic A, Curme C, Qiao Z, Zhou W-X, Stanley HE, Li B. 2014 Network risk and forecasting power in phase-flipping dynamic networks. *Phys. Rev. E* **89**, 042807. (doi:10.1103/PhysRevE.89.042807)
25. Podobnik, Horvatic D, Bertella MA, Feng L, Huang X, Li B. 2014 Systemic risk in dynamical networks with stochastic failure criterion. *EPL* **106**, 68003. (doi:10.1209/0295-5075/106/68003)
26. Erdös P, Rényi A. 1959 On random graphs. *I. Publ. Math.* **6**, 290–297.
27. Newman MEJ. 2002 Assortative mixing in networks. *Phys. Rev. Lett.* **89**, 208701. (doi:10.1103/PhysRevLett.89.208701)
28. Errington PL. 1946 Predation and vertebrate populations. *Q. Rev. Biol.* **21**, 144–177. (doi:10.1086/395220)
29. Genovart M, Negre N, Tavecchia G, Bistuer A, Parpal L, Oro D. 2010 The young, the weak and the sick: evidence of natural selection by predation. *PLoS ONE* **5**, e9774. (doi:10.1371/journal.pone.0009774)
30. Hunter ML. 1996 *Fundamentals of conservation biology*. Oxford, UK: Blackwell Science.
31. Costanza R *et al.* 1997 The value of the world's ecosystem services and natural capital. *Nature* **387**, 253–260. (doi:10.1038/387253a0)
32. Bak P, Tang C, Wiesenfeld K. 1987 Self-organized criticality: an explanation of 1/f noise. *Phys. Rev. Lett.* **59**, 381–384. (doi:10.1103/PhysRevLett.59.381)
33. Noel PA, Brummitt CD, D'Souza RM. 2013 Controlling self-organizing dynamics on networks using models that self-organize. *Phys. Rev. Lett.* **111**, 078701. (doi:10.1103/PhysRevLett.111.078701)
34. Markovic D, Gros C. 2014 Power laws and self-organized criticality in theory and nature. *Phys. Rep.* **536**, 41–74. (doi:10.1016/j.physrep.2013.11.002)
35. Mold JW, Stein HF. 1986 The cascade effect in the clinical care of patients. *New Engl. J. Med.* **314**, 512–514. (doi:10.1056/NEJM198602203140809)
36. Estes JA, Duggins DO, Rathbun GB. 1989 The ecology of extinctions in kelp forest communities. *Conserv. Biol.* **3**, 252–264. (doi:10.1111/j.1523-1739.1989.tb00085.x)
37. Dakos V, Scheffer M, van Nes EH, Brovkin V, Petoukhov V, Held H. 2008 Slowing down as an early warning signal for abrupt climate change. *Proc. Natl Acad. Sci. USA* **105**, 14 308–14 312. (doi:10.1073/pnas.0802430105)
38. Adger WN, Hughes TP, Folke C, Carpenter SR, Rockström J. 2005 Social–ecological resilience to coastal disasters. *Science* **309**, 1036–1039. (doi:10.1126/science.1112122)
39. Thompson JN. 2005 *The geographic mosaic of coevolution*. Chicago, IL: University of Chicago Press.
40. De Lange HJ, Sala S, Vighi M, Faber HJ. 2010 Ecological vulnerability in risk assessment. A review and perspectives. *Sci. Total Environ.* **408**, 3871–3879. (doi:10.1016/j.scitotenv.2009.11.009)
41. Nowak MA, Highfield R. 2011 *Supercooperators: altruism, evolution, and why we need each other to succeed*. New York, NY: Simon and Schuster.
42. Vespignani A. 2012 Modelling dynamical processes in complex socio-technical systems. *Nat. Phys.* **8**, 32–39. (doi:10.1038/nphys2160)
43. Battiston S, Caldarelli G, Georg C, May R, Stiglitz J. 2013 Complex derivatives. *Nat. Phys.* **9**, 123–125. (doi:10.1038/nphys2575)