The cost of attack in competing networks

B. Podobnik1,2,3, D. Horvatic4, T. Lipic1,5, M. Perc6,7, J. M. Buldú8,9 and H. E. Stanley1

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

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
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 $m_{WS}$ 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 $m_{WS} = m_{WS}$ 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 $k_{WS}$ neighbours in network W, can fail at any moment, either internally—dependent 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 $\tau$. 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 $p_1 = p_X$ and $p_2$, respectively. Figure 2a 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 2b 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 2b 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 ($p_1^S = p_{X1} - p_X$) is much larger than the fluctuation needed to initiate the collapse of network W ($p_1^W = p_{X2} - p_X$). 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 2b shows how when network S attacks network W by increasing $p_1$ to $\approx 0.002$, the weak network becomes abruptly dysfunctional. Figure 2b 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
recovery of network S is complete and all of its inactive nodes are reactivated (see blue dashed line in figure 2b). Similarly, when economic sanctions in a financial system are lifted the weak economies are not restored, but the strong economies recover after suffering little damage.

Figure 2c shows a modified competing network structure in which there are two interconnected Erdős–Rényi 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 2d 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 \( a = 1 - f \), 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 \( p_{S,1} = 1 - \exp(-p_S) \) [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

\[
E_S = \sum_{i=0}^{k_S} \sum_{i=0}^{k_S} \left( \frac{k_S}{k_S - i} \right) k_S^{k_S - i} (1 - a_S)^i \left( k_{W,S} \right)^{k_{W,S} - (j - i)} (1 - a_W)^{i - j} \tag{3.3}
\]

Here, \( t_S \) represents the absolute threshold of network S simply related to the fractional threshold \( T_S = t_S/ (k_S + k_{W,S}) \); a node in network S can externally fail with a
probability $p_{S,2}$ only when the number of active neighbours in both network $S$ and network $W$ is less than or equal to $t_f$. Similarly, we obtain $t_f(N)$ 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 $t_f(N) = t_f(N_S) < t_f(N_W)$. 

The analytical results of figure 3a indicate that when network $S$ increases its 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 the fraction of 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 $p_{S,1}^* < 0.33$, 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 $\Delta t_{W} > \Delta t_{S}$. Figure 3b 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 $\tau$ 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 probability 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 resilientities 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

$$N(k_S)(T_S' - T_S) = k_{W,i}(T_W - T_S').$$

Here, $N$ is the size of the strong network, $(k_S)$ 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 $(k_S)$, 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 \( T_i = 0.3 \). (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 \( p_i \) is restored to its initial value. (Online version 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 \( n_{ac1}, n_{ac2}, \ldots, n_{acn} \) with degrees \( k_{ac1}, k_{ac2}, \ldots, k_{acn} \), respectively, by using equation (3.4), we obtain

\[
T'_S = \frac{\langle k_{ac1} + k_{ac2} + \cdots + k_{acn} \rangle T_W + N_S \langle k_S \rangle T_S}{N_S \langle k_S \rangle + k_{ac1} + k_{ac2} + \cdots + k_{acn}}.
\] (3.5)

Figure 4a 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 4b 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 4c shows that, if the example in figure 2b 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 \( p_S \). Note that when attacks cease (e.g. when, in an economic system, sanctions are lifted) decreasing the value of \( p_1, p_2 \) the fraction of active nodes in network S increases, but network W is left irreversibly damaged (see the closed hysteresis \( p'_S \rightarrow p'_1 \rightarrow p'_S \)).

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 \( T_{WS} \), or if the fraction of the active neighbours of node \( n_i \) in network W is equal to or lower than some threshold \( T_{WS} \). 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 5a 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
At some point, S creates larger damage in a weak (less resilient) network W than to itself. (we show the time evolution of the fractions of active nodes with the takeover mechanism included where we use a takeover period of 1.5 should be stopped, defined as the change in the ratio between two fractions, thresholds used for defining resilience of each network. External failure thresholds are is damaged more. We also show how the fractions change with decreasing (a phase flip) at order transition. Because both networks are interdependent, substituting nodes from the less resilient network W affects (the cost of taking over) defined in equation (3.4) is included, the (a) Quantification of the optimal attack duration. Model parameters are: $m_S = 6, m_W = 3, m_{SW} = m_{WS} = 2$. Similar to figure 4 but now with two thresholds used for defining resilience of each network. External failure thresholds are $T_W = 0.7, \gamma_s = 0.8$ and $T_{SW} = 0.4$. 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 permanently damage network S. This demonstrates how expect that additional weakening of network W will also discontinuous behaviour than in figure 5 \[ \Delta f(t) = f(t) - f_0(t) \text{ where } \Delta t = 20. \] 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 5b 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 5c 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 5d 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 6a 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 5c, 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 5c (i.e. when the cost is excluded). At the same time, figure 6b shows that an increase in the takeover time $\tau_T$ 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
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-HIC). 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. Kivelä 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)
