

STRATEGIC NETWORK DISRUPTION AND DEFENSE

BRITTA HOYER

Paderborn University

KRIS DE JAEGER

Utrecht University

Abstract

We study a game between a network designer, who uses costly links to connect nodes in a network, and a network disruptor who tries to disrupt the resulting network as much as possible by deleting either nodes or links. For low linking costs networks with all nodes in symmetric positions are a best response of the designer under both link deletion and node deletion. For high linking costs the designer builds a star network under link deletion, but for node deletion excludes some nodes from the network to build a smaller but stronger network. For intermediate linking costs the designer again builds a symmetric network under node deletion but a star-like network with weak spots under link deletion.

1. Introduction

A large part of the recent economic literature regarding networks (for an overview, see Goyal 2007; Jackson 2008) has focused on strategic network formation and games being played on networks. Consequently, one of the principal concerns of this literature is the cooperative side of networks.¹ What has been generally ignored so far (at least in economics research) is that networks, once they are formed, may be attacked from the outside. If the network itself is a commodity, such as is the case for military communications networks or terrorist networks, the network or the players within the network might become targets of an outside force. Consequently, not only are the individuals in the network threatened by an attack but also the network as a whole is threatened.

¹ Note that cooperation within networks may be modeled by means of noncooperative game theory, e.g., Bala and Goyal (2000).

Britta Hoyer, Paderborn University, Warburger Str. 100, 33098 Paderborn, Germany (britta.hoyer@wiwi.upb.de). Kris De Jaegher, Utrecht School of Economics, Utrecht University, Kriekenpitplein 21-22, 3584 EC, Utrecht, the Netherlands (K.Dejaegher@uu.nl).

We would like to thank Sanjeev Goyal, Henk Meijer, Stephanie Rosenkranz, Bastian Westbrock, Vincent Buskens and Kirby Fears as well as participants at the EEA (2011), the ICS-USE Workshop (2010), the Second Brazilian Workshop of the Game Theory Society (2010), the NAKE Research Day (2010) and the 21st Game Theory Festival at Stony Brook (2010) for useful comments and suggestions. Any remaining errors, however, remain our own.

Received April 28, 2015; Accepted June 5, 2015.

© 2016 Wiley Periodicals, Inc.

Journal of Public Economic Theory, 18 (5), 2016, pp. 802–830.

Arguilla and Ronfeldt (2000) refer to this concept of fighting against networked adversaries as “netwars.” Dekker and Colbert (2004) find that two trends have recently emerged in military as well as civilian communications. The first is that the communications sector has become increasingly centered around networks and the second is that there is an “increasing threat to communications infrastructure. In the civilian sphere, the threat is from terrorist attacks, while in the military sphere this comes from the increasing tendency to view communications networks as high-value targets” (Dekker and Colbert 2004, p. 359). What we look at in this paper is the addition of links to the network to keep the players within the network safe, where in the absence of a network adversary these links would be redundant. The following example illustrates the type of games we are looking at.

- Military units and the communication links between them can together be considered as military networks.² Particularly, if communication has to be achieved over larger distances these communications links are subject to interruptions that can be caused, for example, by the deliberate jamming of frequencies³ (link deletion) or by the deliberate elimination of units that enable communication (node deletion). Designers of such communications networks must therefore take such deliberate attacks into account and build networks that will still be functional in the event of such an attack. Thus, in the absence of a threat, sending the same signal via multiple routes to communicate between two units is redundant and causes the network designer to incur unnecessary costs. If there is a threat, however, they can be used to make the network safe against the disruption of links.

While it is important to understand how these networks are created, how they work together, and what technologies they use, Arguilla and Ronfeldt (2000, p. xi) state that “the defining level of a netwar actor is its organizational design. ... To cope with a network, analysts must first learn what *kind* of network it is and then draw on the best methods for analysis.” Therefore, in this paper, we focus purely on the structure of the network and how to best defend it given a certain type of attack strategy. What are the implications for the design and defense strategy of network designers when taking the possibility of disruption into account? Given the fact that additional links are used to keep the network safe, how does the cost of adding links affect network structure? Does it matter if the attack is targeted at nodes or links in the network? And are there certain network structures that are inherently “safe” against the disruption of a number of links or nodes? These are the questions addressed in this paper.

To capture the influence of the threat of an attack on the structure of the network, our paper models a sequential game between a network designer and a network disruptor. We model network structure as being determined by a network designer, because in the first instance we want to gain insight into what is an efficient defense strategy for the network as a whole. Therefore, we can simply model the game as being played between a network designer and a network disruptor. We begin by looking at the benchmark case in which there is no threat of a disruption. We then proceed to look at cases where the network designer faces a network disruptor, where we consecutively look at low, high,

² Lipsey (2006) contains an overview of military and security networks with references outside the field of game theory.

³ That such a threat actually exists can be seen from the efforts taken by government agencies to find a disruption-tolerant network. Raytheon BBN Technologies reportedly “was awarded a \$81 million contract to create a collaborative technology alliance in network science” (Baburajan 2010) and in 2010 demonstrated a field experiment of a disruption-tolerant military network (Baburajan 2010).

and intermediate linking costs. In the extensions, we additionally look at the case of asymmetric information.

The rest of the paper is organized as follows. After a literature review in Section 2, Section 3 presents our model of design, defense, and disruption of the network. Section 4, 5, and 6 consecutively deal with low, high, and intermediate linking costs. In Section 7, we add some extensions to the model by looking at the case of imperfect information. Section 8 concludes. In the Appendix, we give some graph-theoretic background.

2. Literature Review

While some aspects of network disruption have received attention in economics, we found that there is no parsimonious model that focuses on the structural implications of adding a network disruptor to a simple network formation model with homogeneous players.⁴ To give an overview, the existing work in the economics literature can broadly be grouped into two different categories according to the focus of the network disruptor.

In the first group of papers it is the network disruptor's purpose to learn as much as possible of the information that is generated within a network, whereas the network aims to keep this information secret. This group of papers includes the work by Enders and Su (2007), Enders and Jindapon (2010), and Baccara and Bar-Isaac (2008), who take a game-theoretic approach similar to ours. In these models more links within a network allow more information to be produced. These papers then deal with the dual nature of links, which on the one hand enable information sharing but on the other hand allow the effect of an attack to spread through the network. Larson (2013) also deals with the problem of the dual nature of links in a network. In his model good items (e.g., news, stock tips) as well as bad items (e.g., viruses, biological as well as technological) can spread throughout a network. Players consequently want to be as connected as possible to receive all the benefits. However, at the same time, in order not to receive the bad items, they want to limit the extent to which they are connected. To protect themselves, players are then allowed to put effort into security, which is modeled as a screening device that will save them from receiving the bad items. A similar approach is found in Goyal and Vigier (2014), who focus on the protection of certain key nodes within the network. Here the device to protect these key nodes is modeled as a "firewall" which will keep the attack from spreading through them. A very recent paper focusing on a game between a network designer and a network disruptor is Dziubiński and Goyal (2013), where the network designer may protect certain nodes. Unlike in the paper by Goyal and Vigier (2014), here an attack cannot spread through the network. Additionally the designer also has the possibility to use additional links to protect the network instead of building a firewall around certain nodes. Another paper that uses a similar approach is Hong (2008),⁵ who also uses a "firewall" as protection in an information security network setting. He then focuses on the stability of such networks and on the extent to

⁴ For a justification in terms of applications, see Arguilla and Ronfeldt (2000), who find that many networked groups are actually without leaders. Whereas this does not mean that all members of such a group are actually equal, it goes a long way in justifying the assumption of homogeneity of the nodes we use here.

⁵ Kovenock and Roberson (2010) recently looked in a similar way at network defense, yet their paper is less relevant to our model, because network structure is not taken into account. Instead, in their paper network vulnerability arises because of the production function generated by the nodes in the network, where in one extreme one node suffices to obtain full production, and in the other case all nodes are necessary for full production.

which they are “hacking-proof.” However, a network disruptor may instead want to try and stop covert information from being produced. In our model, we focus on this type of preventive disruption.

The second group of papers centers around the topic of protecting certain key nodes on the side of the network designer, and on the network disruptor’s efforts to find such key players or key links to attack. In Bier, Oliveros, and Samuelson (2007) for example, the focus lies on defending certain nodes. In their model, a defender needs to decide on how to allocate defensive efforts over two targets for attack. Just as is the case in our model, it may be optimal to defend the locations in an asymmetric way, leaving weak spots. Yet, whereas in their approach this is due to the fact that nodes have asymmetric values, in our model weak spots are simply a consequence of the network designer’s decisions as all nodes have equal values. In Ballester, Calvo-Armengol, and Zenou (2006), the focus lies instead on the disruption of the network. The “key player” in the network is defined as the node with the highest degree of Bonacich centrality (a centrality measure used in social network analysis). It is the disruptor’s goal, then, to find this key player and attack it. An example of the game played is the coordination of criminal activity. As opposed to this in our model, the centrality of any one player is not as important, because the network designer can fight against disruption by reorganizing the network. The focus in Hong (2009) lies on certain key links. In his model, terrorists try to carry an explosive through an exogenously given transport network, modeled as a directed flow network. By shutting down a minimal number of links, security services try to stop the explosive from reaching its destination. In contrast to this, our model focuses on undirected networks and network defense consists of adding links, not deleting them. McBride and Hewitt (2013) add imperfect information on the side of the network disruptor to such a model, and consider targeted as well as random attacks on the structure of the network. We instead want to look at a more parsimonious model where all nodes are homogeneous, and where any asymmetry in the network is a consequence of the network defense strategy.

Recently some work has been done on network disruption models, in which the nodes are themselves decision makers. In Hoyer (2012), the focus lies on targeted attacks on the links of the model. Billand *et al.* (2011) look at a network formation model where players initiate links forming an information network. Whereas Hoyer (2012) is looking at the implications of a targeted attack on the links of the network, they analyze the implications of random node failure.

In non-game-theoretic/noneconomic literature related to our paper, the following papers providing related insights are worth mentioning. An influential paper is Albert, Jeong, and Barabasi (2000), which treats a stochastic network generation process that yields networks with properties that are often observed in real-world networks (e.g., preferential attachment). It is shown that these networks are robust against random attacks, but vulnerable to targeted attacks.⁶ Similarly, star architectures do badly in our analysis under node deletion. In the context of vulnerability of road networks, Taylo, Sekhar, and D’Este (2006) treat the adding of links as a mechanism of network protection. They are interested, however, in the effect that this has on several vulnerability measures, whereas our focus is on network structure. Schwartz *et al.* (2011) also model a game between a network designer and disruptor. However, they focus on the connection between network reliability and security using a model of an undirected graph in which links may be unreliable. The non-game-theoretic paper most related to our

⁶ For a more strictly mathematical treatment of such models, see Bollobás and Riordan (2003).

work is Dekker and Colbert (2004), who study the node (link) connectivity of networks, which is the smallest number of nodes (links) which upon deletion results in a disconnected graph. Using certain graph-theoretic properties that we also look at, they state that a graph is optimally connected if its node respectively link connectivity is equal to the minimal degree in the network. Finally, they show that networks that have certain symmetry properties are optimally connected. However, as is usually the case in graph-theoretic literature, the authors do not consider linking to be costly and do not model strategic disruption.

3. The Model

Consider a finite set of nodes $N = \{0, 1, \dots, n-1\}$, where $n > 1$.⁷ We say that there is a link (there is no link) between node i and node j when $g_{ij} = 1$ ($g_{ij} = 0$). Links are assumed to be undirected, so that it is always the case that $g_{ij} = g_{ji}$. A network in our model is a pair (N, g) , consisting of the set of nodes N , and the set g of all links g_{ij} such that $g_{ij} = 1$. We only look at simple networks, thus every pair of nodes can only be directly linked via one link. The term *order* refers to the number of nodes n in the network. Denote by G the set of all possible networks on N . A subnetwork (N^2, g^2) of (N^1, g^1) is a network such that $N^2 \subseteq N^1$, and $g^2 \subseteq g^1$, where g^2 is defined on the set N^2 . $l(g)$ denotes the set of links in the network, and $|l(g)|$ the cardinality of this set, or link cardinality of the network. We say that two nodes are connected to one another if a path exists between them in g . We say that a path exists between nodes i and j if a set of nodes $\{i_1, \dots, i_k\}$ exists such that $g_{ii_1} = g_{i_1 i_2} = \dots = g_{i_{k-1} i_k} = g_{i_k j} = 1$. We denote the set of nodes with whom node i is connected as $N_i(g)$. Given a network g , a pair (C, g^C) , with $C \subseteq N$, $g^C \subseteq g$ is called a component of g if for every distinct pair of nodes i and j in C we have $j \in N_i(g)$, and if there is no strict superset C' of C for which this is true. Before describing the model we will still define some key network architectures. A *star* has a central node i such that for all $j \in N \setminus i$ it is the case that $g_{ij} = 1$, and there are no other links in the network. A *line* is an alternating sequence of nodes and links, which begins and ends with a node, and where each link connects exactly two nodes. A *circle* is an alternating sequence of nodes and links, in which each node receives exactly two links.

We consider the following Stackelberg game. At Stage 1, the designer constructs a network (N, g^1) , with $g^1 \in G$, referred to as the predisruption network, where in short-hand we use g^1 to denote this network, suppressing the set of nodes. At Stage 2, in two variants of our game, the network disruptor after observing g^1 either has a budget D_l available reflecting the number of links he can remove from g^1 (link deletion), or has a budget D_v available reflecting the number of nodes he can remove from g^1 (node deletion). The assumption that the disruptor has a disruption budget reflects, in a simplified way, that disruption is costly, where different disruption budgets can be interpreted as corresponding to different levels of disruption costs the disruptor may be facing. In the case of link deletion, given the available disruption budget D_l , the disruptor removes a set l of links from g^1 , with $l \subseteq g^1$ and $|l| \leq D_l$, resulting in a postdisruption network (N, g^2) , or g^2 in short-hand notation, where $g^2 = g^1 \setminus l$. In the case of node deletion, given budget D_v he removes a set v of nodes, with $v \subseteq N$ and $|v| \leq D_v$, resulting in a post-disruption network (N^2, g^2) , where $N^2 = N^1 \setminus v$, and where g^2 consists of all the links in g^1 for which both $g^1_{ij} = 1$, and $i, j \in N^2$. In short-hand notation, we again denote such a postdisruption network as $g^2 = g^1 \setminus v$, and denote the disruptor as removing $v \subseteq g^1$.

⁷ The usual labeling of nodes in the networks literature is $1, \dots, n$. We diverge from this, as we later introduce a class of networks (circulants), where the labeling needs to start from 0.

The designer obtains the payoff $u(g^2) - c[|l(g^1)|]$, where $u(\cdot)$, with $u' > 0$, is the value of g^2 to the designer, and $c[\cdot]$, with $c' > 0$, is the cost function for the designer over the number of links in g^1 . The disruptor obtains the payoff $-u(g^2)$. The Stackelberg equilibrium can be found by backward induction. For any given g^1 , the disruptor chooses $h(g^1) \in \operatorname{argmin}_{h \subseteq g^1, |h| \leq D_h} u(g^1 \setminus h)$, where $h = l, v$ under respectively link deletion and node deletion. Given this fact, the designer chooses $g^{1*} \in \operatorname{argmax}_{g^1 \in G} u(g^1 \setminus h(g^1)) - c[|l(g^1)|]$, again for $h = l, v$. It should be stressed that, while upon disruption it is network g^2 that is obtained, we are interested in the structure of the predisruption network g^{1*} in a Stackelberg equilibrium, or in short the Stackelberg g^{1*} .

Conceptually, one can find the Stackelberg g^{1*} by using either of two alternative approaches. In a first approach, the first step is to determine the set $G(\bar{u})$ such that $\forall g^1 \in G(\bar{u}) : u(g^1 \setminus h(g^1)) = \bar{u}$, and to find $g_{\min}^1(\bar{u}) \in \operatorname{argmin}_{g^1 \in G(\bar{u})} |l(g^1)|$, i.e., to find the g^1 which achieves a target postdisruption value \bar{u} with a minimal number of links. The focus in the first step therefore lies on the optimal structure of g^1 . The second step is to determine a g^{1*} such that $u(g^{1*} \setminus h(g^{1*})) = \max_{\bar{u}} \bar{u} - c[|l[g_{\min}^1(\bar{u})|]|]$, where this step focuses on the cost-benefit analysis to the designer among optimally structured g^1 of different values. In what we call Approach 1, we limit ourselves to the “structural” Step 1 to find g^1 that achieve a given value \bar{u} with a minimal number of links. As long as, with this minimal number of links, it is not possible to achieve a higher \bar{u} , each $g_{\min}^1(\bar{u})$ characterized by Step 1 is a Stackelberg g^{1*} for some cost function $c[\cdot]$. This is because $c[\cdot]$ can always be such that $\partial c[|l[g_{\min}^1(\bar{u})|]|]/\partial \bar{u}$ is everywhere higher (lower) than one (i.e., the marginal benefit to the designer of u) for $u > \bar{u}$ ($u < \bar{u}$).

In the second approach to find the Stackelberg equilibrium, the first step is to define the set $G(B)$ such that $\forall g^1 \in G(B) : |l(g^1)| = B$, i.e., all predisruption networks with exactly B links, and of finding $g_{\max}^1(B) \in \operatorname{argmax}_{g^1 \in G(B)} u(g^1 \setminus h(g^1))$. The focus in this step lies again on the optimal structure of g^1 . The second step consists of finding $g^{1*} = g_{\max}^1(B^*)$ such that $B^* \in \operatorname{argmax}_B u(g_{\max}^1(B) \setminus h(g_{\max}^1(B))) - c[B]$, and focuses again on the cost-benefit analysis of the designer among optimally-structured networks. In what we refer to as Approach 2, we focus on the problem of finding the highest values the designer can achieve with a given linking budget B . As long as this value cannot be achieved with a budget lower than B , each $g_{\max}^1(B)$ is a Stackelberg g^{1*} for some cost function $c[\cdot]$. This is because $c[\cdot]$ can always be such that $c'[B]$ is everywhere higher (lower) than $\partial u(g_{\max}^1(B) \setminus h(g_{\max}^1(B)))/\partial B$ for $B' > B$ ($B' < B$).

We now continue to take more specific assumptions on the form of $u(\cdot)$. Intuitively, $u(g^2)$ should be larger the more connected g^2 is. We first assume that nodes are completely symmetric, and second, that there is no information decay, so that it does not matter how two nodes are connected, as long as they are connected. It follows then that the value of g^2 is only a function of the orders of the components of which it consists. We assume in particular that $u(g^2) = \max(C_1, C_2, \dots)$, or in other words: the value of network g^2 is equal to the order of its largest component. This means that the designer in our model seeks to maximize the order of the largest component in g^2 , while the disruptor seeks to minimize the order of the largest component in g^2 . Intuitively, a single extra node attached to an existing component benefits all nodes already in the component, so that $u(\cdot)$ is a convex function of the connectedness of g . Our assumption that $u(\cdot)$ equals the order of the largest component approximates a convex $u(\cdot)$, while maintaining tractability.⁸

⁸ We are indebted to an anonymous referee for pointing out that this is not always a good approximation. For instance, with 100 nodes, the approximation predicts that a network consisting of 51

Looking at the side of the network disruptor, it is clear that in any equilibrium, the disruptor decides on a certain number of links or nodes to be deleted. Given such a number of nodes or links, it must be the case that the disruptor chooses a best response, previously defined as $h(g^1)$, in the form of an optimal network disruption strategy. This strategy of the network disruptor can be described by an algorithm, which can be found in the Appendix. Alternatively, one could consider more standard concepts used in social network analysis, such as betweenness centrality, Bonacich centrality, degree centrality, or closeness centrality, to define which links (nodes) the disruptor will target. While such concepts are relevant for the disruption of random networks, in our model the designer responds to a threat of disruption. He will therefore avoid central nodes or bridging links as much as possible, as they will be automatic targets of the disruptor. This in turn then makes an analysis of the disruptor's strategy in terms of centrality futile.

In our further analysis, in Section 4 we will focus on the case where linking costs are so low that the designer constructs a network g^1 with the highest possible postdisruption value, or in short a *max-proof network*. For link deletion it is possible for the designer to keep every node connected after disruption as long as using a sufficient number of links. For node deletion, on the contrary, the disruptor is always able to delete at least D_v nodes, so that a max-proof network g^1 retains a single component connecting $(n - D_v)$ nodes post disruption. We here adopt Approach 1, and look for the minimal number of links with which the designer achieves a max-proof network, meaning that we look for a *minimal max-proof network*.

In Section 5, we focus on the case where linking costs are so high that the designer does not want to use links on top of the minimal number of links, $(n - 1)$, needed to construct a component with order n in the absence of a disruptor.⁹ We here adopt Approach 2, and look for the maximum value that the designer can achieve with a linking budget $B = (n - 1)$, under both link deletion and node deletion. In Section 6, we explore the case of intermediate linking costs, by looking at the structure of *minimal (max - 1)-proof networks*. These are networks g^1 such that post disruption one node fewer is connected in the unique component than the maximal achievable, so that the order of this component is $(n - 1)$ in the case of link deletion, and $(n - D_v - 1)$ in the case of node deletion, where this order is achieved with a minimal number of links. We here again apply Approach 1.

4. Low Linking Costs

We start with the case where linking costs are so low that the designer constructs a max-proof network, though the designer will still make sure that such a network is constructed with a minimal number of links, as links are assumed to be costly (Approach 1).¹⁰ To describe minimal max-proof networks, we can make use of existing graph-theoretic results on connectivity (see Boesch 1986). The *degree* of a node is

connected nodes and 49 isolates is better than a network consisting of two components of 50 nodes. Yet, the difference in the number of links used in these two examples is so large that the designer never faces such extreme trade-offs. For short explanations of the expected differences if one would change the modeling decisions, please see footnotes 10 and 26.

⁹ The distinction in terms of linking costs only makes sense if we assume that the cost of disruption is relatively high. For low costs of disruption the network disruptor would simply attack all links/nodes, rendering the level of linking costs irrelevant.

¹⁰ Note that for the case of low linking costs it does not matter if the designer maximizes the order of the largest remaining component or any other function, because he aims for full protection of the network.

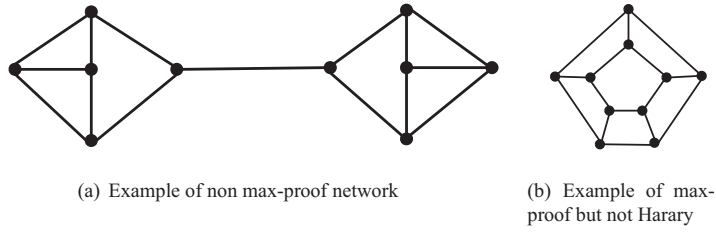
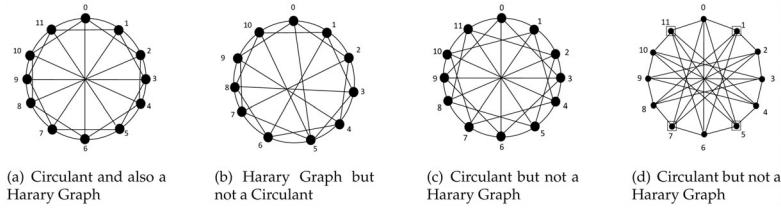
Figure 1: 3-regular networks for $n = 10$.

Figure 2: (Almost) 5-regular networks.

the number of links of this node. An r -regular network is a network in which each node has the same degree r . As follows from Harary (1962, Theorems 1 and 2), if $n(D_h + 1)$ is even (for $h = l, v$), the lowest number of links with which minimal max-proofness can potentially be achieved is in connected $(D_h + 1)$ -regular networks; if $n(D_h + 1)$ is odd, this is the case for almost regular connected networks where $(n - 1)$ nodes have degree $(D_h + 1)$, and one node has degree $(D_h + 2)$.

Although not all (almost) regular graphs are minimal max-proof, Harary's results can be applied to show that regular or (almost) regular networks which are minimal max-proof always exist, by constructing so-called *Harary graphs*. The simplest case is obtained when $D_h = 1$, as the only 2-regular connected network is the circle, which is then the only minimal max-proof network architecture under both link and node deletion. Intuitively, minimal max-proof networks for $D_h > 1$ can now be constructed by adding links to the circle in a symmetric manner until an (almost) regular network is obtained. Links should be added avoiding clusters of linked nodes, with few links between the clusters, as such networks are easily disconnected. For an example of a network that is 3-regular, but is not max-proof for either $D_l = 2$ or $D_v = 2$, see Figure 1(a) (due to Boesch 1986, p. 242).

Harary graphs are defined as follows. Denote by $\lfloor x \rfloor$ the largest integer not larger than x . Then in a Harary graph, each node i has a link to the nodes $i \pm 1, i \pm 2, \dots, i \pm \lfloor (D_h + 1)/2 \rfloor \pmod{n}$ (meaning that each node is linked to each node one label away, two labels away, and so on); additionally if $(D_h + 1)$ is odd, each node $i = 1, 2, \dots, \lfloor (n - 1)/2 \rfloor$ has a link to node $i + \lfloor n/2 \rfloor$ (meaning that "diagonals" are added to the network). Examples are the regular graph in Figure 2(a), with $n = 12$ and $(D_h + 1) = 5$, and the almost regular graph in Figure 2(b) with $n = 11$ and $(D_h + 1) = 5$ (where in the latter figure, node 5 has degree 6, and all other nodes have degree 5). Harary graphs with $(D_h + 1) = 4$ are obtained when removing the diagonals from Figures 2(a) and 2(b). Theorems 1 and 2 of Harary (1962) directly imply that all Harary graphs are minimal max-proof under both link deletion and node deletion.

It should be stressed that Harary graphs are only a subset of the set of minimal max-proof networks under link deletion and node deletion. For instance, for $n = 10$

the network in Figure 1(b) is minimal max-proof for $D_l = 2$ or $D_v = 2$, but is not a Harary graph. As pointed out by Boesch (1986, p. 234), general graph-theoretic results that can be applied to characterize the complete set of minimal max-proof networks are unlikely to emerge, and the best approach is then to define a set of networks that is as comprehensive as possible. This is the case for a subset of the so-called *circulant graphs*. While the disadvantage of these networks is that they are only defined for $n(D_h + 1)$ even, in this case they define a much larger class of minimal max-proof networks than Harary graphs, which are then a strict subset of the set of appropriate circulants. Moreover, they illustrate the fact that the set of minimal max-proof networks for node deletion with disruption budget D_v is a subset of the set of minimal max-proof networks for link deletion with disruption budget $D_l = D_v$. This follows from a standard result in graph theory that every network that is max-proof under node deletion with disruption budget D_v is also max-proof under link deletion with disruption budget $D_l = D_v$ (see Theorem 5.1 in Harary 1969).

In a circulant graph $C_n(a_1, a_2, \dots, a_k)$, where $0 < a_1 < a_2 < \dots < a_k < \frac{n+1}{2}$, each node i has a link to the nodes $i \pm a_1, i \pm a_2, \dots, i \pm a_k \pmod{n}$. The sequence (a_i) is called the *jump sequence* and a_i is called a jump.¹¹ Examples of circulants are Figures 2(a), 2(c), and 2(d). Figure 2(a) is both a Harary graph and a circulant; Figure 2(b) is a Harary graph, but not a circulant; Figures 2(c) and 2(d) are circulants, but not Harary graphs. We now formulate Proposition 1 about circulants,¹² showing that under link deletion all circulants are minimal max-proof for an appropriate disruption budget, whereas under node deletion all circulants with convex jumps are minimal max proof for an appropriate disruption budget. The circulants in Figures 2(a) and 2(c) are minimal max-proof under both link deletion and node deletion for appropriate disruption budgets. The circulant in Figure 2(d), however, has nonconvex jumps, and is only minimal max-proof under link deletion. Under node deletion, by removing nodes 1, 5, 7, and 11, the disruptor splits up the network in a component of six nodes, and one of two nodes. The circulants described in Proposition 1 are Stackelberg networks for some cost function, as with a linking budget that just allows the designer to construct circulants he cannot do better, simply because max-proofness is the best that can be achieved.

PROPOSITION 1:

- (i) Any connected circulant graph with link cardinality $n(D_l + 1)/2$ is minimal max-proof under link deletion with a disruption budget D_l .
- (ii) Any connected circulant graph with link cardinality $n(D_v + 1)/2$ is minimal max-proof under node deletion with a disruption budget D_v , if $a_1 = 1$ and the jumps are convex, i.e., $a_{i+1} - a_i \leq a_{i+2} - a_{i+1}$ for $1 < i < (D_v + 1)$.

Proof:

- (i) As follows from Mader (1971), every connected r -regular node-symmetric graph¹³ is max-proof under link deletion. As every circulant is node-symmetric,

¹¹ The definition and notation given below follows the one given by Boesch and Tindell (1984).

¹² Because the circulant graphs we are looking at here all have a first jump of size 1, all have the circle as a basis, and they coincide with the *overlapping neighborhood networks* in Bramoullé and Kranton (2007). However, the structure of the circulant networks we look at here is more restrictive than in Bramoullé and Kranton.

¹³ For a definition of node symmetry, see Chiang and Chen (1995).

it follows that every circulant with link cardinality $n(D_l + 1)/2$ is minimal max-proof under link deletion with a disruption budget of D_l .

- (ii) It follows that every circulant with convex jumps that has link cardinality $n(D_v + 1)/2$ is minimal max-proof under node deletion with a disruption budget D_v .

The minimality claim in the statements results, as with the minimal number of links needed to construct max-proof networks it is not possible to do better. ■

In terms of the military communications application introduced earlier, we conclude that for low linking costs a designer need not construct a different network architecture depending on whether the attack is directed at the physical parts of the network (thus the nodes) or at the frequencies (the links)—though a wider set of networks work for attacks aimed at the frequencies. If additional links are used as a defense mechanism and are relatively cheap to introduce, then constructing a symmetric network, such that the network does not consist of local clusters with few links between them, is a best response under both link deletion and under node deletion. Yet, as we will now go on to show, as soon as we move away from low linking costs, it stops being the case that the same architectures can be used for link deletion and for node deletion.

5. High Linking Costs

We now look at prohibitively high linking costs, and using *Approach 2* implement this by assuming that the designer has a budget of only $B = (n - 1)$ links. In the absence of a disruptor, this budget is just sufficient to connect all nodes, which the designer can do by means of any network connecting n nodes using exactly $(n - 1)$ links; thus any *minimally connected network*. When a disruptor is present, however, the structure of the minimally connected network matters. Moreover, the designer's best response structure now depends on whether link deletion (Section 5.1) is faced, or node deletion (Section 5.2).

5.1. Link Deletion—High Linking Costs

We show that the star is the strict best response of a designer with linking budget $B = (n - 1)$, who faces a disruptor with any disruption budget $D_l > 0$. It is easy to see that the maximal damage which the disruptor can do to a star is to disconnect exactly D_l nodes. To show that the star is the designer's strict best response, we show in Proposition 2 that the designer cannot do better by constructing nonstars. First, we show that the disruptor can remove strictly more nodes in any nonstar minimally connected network than in the star network. Second, we show that the designer ends up with fewer than $(n - D_l)$ nodes in the largest remaining component, after having constructed a g^1 that consists of a component that does not connect all n nodes. Before showing Proposition 2, we first show a general result about nonstar minimally connected networks (Lemma 1), and then treat the special case where $D_l = 1$ (Lemma 2).

LEMMA 1: *For $n \geq 4$, under link deletion, a disruptor with a disruption budget of D_l can disconnect at least $(D_l + 1)$ nodes in every nonstar minimally connected network.*

Proof: For $n < 4$ the line is the only minimally connected network architecture, which makes the analysis trivial. We therefore assume $n \geq 4$. There need to be at least two end-nodes in any minimally connected network, since by definition any minimally connected

network does not contain a circle.¹⁴ Take any minimally connected network and let node k be an end-node (hence connected of degree 1). By definition, node k must have a link to a node i in the network (otherwise the network would not be connected). Since the network is not a star, node i cannot receive another $(n - 2)$ link, next to link g_{ki} . Therefore there needs to be at least one more node h , which is only linked to i indirectly through node j . Consequently, it follows that if we delete link g_{ij} , at least two nodes are separated from the largest remaining component. This is because either nodes i and k are separated from the largest remaining component, or nodes j and h (possibly along with further nodes to which they are connected). The $(D_l - 1)$ remaining links that are deleted each time result in the separation of at least one node, as every link in a minimally connected network is a link cut.¹⁵ ■

The designer could also decide to leave some nodes isolated, and to use the links saved to construct a smaller but stronger component. To compare this to the star, we start with the special case where $D_l = 1$. Clearly, leaving one node isolated then suffices to fully protect the remaining nodes, as the designer can use $B = (n - 1)$ to construct a circle connecting $(n - 1)$ nodes. The designer can never do better by leaving more nodes isolated, whereas connecting the $(n - 1)$ nodes in another manner than in a circle means leaving end nodes, so that the disruptor can still remove nodes from the connected component. Therefore, we can directly state that in the special case $D_l = 1$, both the star connecting n nodes and the circle connecting $(n - 1)$ nodes are best responses to the designer.

LEMMA 2: *The best response strategy for a designer with a linking budget of $B = (n - 1)$ when facing a disruptor with a disruption budget of $D_l = 1$ is to build a star network including n nodes or a circle network including $(n - 1)$ nodes. In both cases g^2 is of order $(n - 1)$.*

Yet, if a circle connecting $(n - 1)$ nodes is constructed given a disruption budget of $D_l > 1$, the disruptor can cut the circle into several pieces of order $\lceil (\frac{n}{D_l}) \rceil$, where by $\lceil x \rceil$ we denote the smallest natural number larger than a number x .¹⁶ This leaves the designer worse off than with the largest remaining component if he builds the star connecting n nodes. An alternative for the designer is to leave more than one node isolated, where it is easy to see that the number of nodes that are left isolated, equals the number of links that can be added on top of the minimal number of links necessary to construct a minimally connected component. Proposition 2 builds on Lemma 1 to show that as long as n is not very small and D_l is not very large, leaving more nodes isolated is never a better option than constructing a star.

PROPOSITION 2: *When facing a disruptor with a disruption budget of $1 < D_l < (n - 2)$ the strict best response of the designer with a linking budget of $B = (n - 1)$ with $n > 5$ is to build a star network.*

¹⁴ For proof see, e.g., Bondy and Murty (2008), Proposition 4.2.

¹⁵ See Bondy and Murty (2008), Proposition 4.1, which states that in a minimally connected network each two nodes are connected by exactly one path. Therefore, it holds that in a minimally connected network each link is a link cut. For the definition of a link cut, see the Appendix.

¹⁶ Here this notation is introduced to avoid problems with divisibility.

Proof: We prove this proposition in three parts. Part 1 shows that nonstar minimally connected networks always do worse than the star. Parts 2 and 3 show that the same holds for a smaller connected component.

- *Part 1.* By Lemma 1, in every nonstar minimally connected graph, at least $(D_l + 1)$ nodes can be removed. Further, the maximal damage caused to a star network is to disconnect D_l nodes. Consequently, the largest remaining component in the star network is strictly larger than that in any other minimally connected network.
- *Part 2.* We show that any connected component that is not max-proof can never be a best response of the designer. Leaving x nodes unconnected allows the designer to build a minimally connected component with x added links. Since any nonminimally connected component is a minimally connected component with added links (for a proof, see Theorem 1.3.3. in Cohn 2003, p. 19), we can analyze this by comparing the size of the disruption budget with the amount of nodes x that the designer chooses to leave unconnected.
 - Leaving x nodes unconnected:
 1. Suppose $D_l < x$. In the star network only D_l nodes can be disconnected. So g^2 given that g^1 is a star is always of a larger order.
 2. Suppose $D_l > x$. The x added links can be disrupted by the disruptor, leaving at best a minimally connected network. Here we need to distinguish between two cases:
 - * Suppose that the connected component *cannot* be represented as a star with added links. Then by taking out the x added links, the disruptor leaves a nonstar minimally connected component. By Lemma 1, the disruptor can thus additionally disconnect at least $(D_l + 1 - x)$ nodes from the component. Therefore the postdisruption network in the star is strictly larger.
 - * Suppose that the connected component *can* be represented as a star with added links and that $n > 5$. Because we only analyze simple networks, these links will be used to link the end-nodes of the star with one another. Let the disruptor delete $(x - 2)$ ¹⁷ of these added links in such a way that there is no end-node in the network that is adjacent to both of the remaining two added links.¹⁸ The remaining network will thus be a star with two links added such that $g_{jk} = 1$ and $g_{ab} = 1$ with $j \neq k \neq a \neq b$. By deleting the links that nodes a and b have to the center, the disruptor can thus disconnect 2 additional nodes from the network, next to the $(D_l - x)$ nodes he can disconnect due to the size of his disruption budget. The largest remaining component is then of order $(n - x - 2 - (D_l - x)) = n - 2 - D_l$, which is strictly smaller than the largest remaining component in a star network.
 3. Suppose $D_l = x$. Unless the designer builds a max-proof component, at least one more node can be disconnected.
 - We thus need to solely look at max-proof component where $D_l = x$.

¹⁷ For the case of $x = 1$ this is impossible. However, for $n > 4$, thus in all interesting cases, it then holds that there are at least two end-nodes that are not linked to one another, so the analysis still holds.

¹⁸ For $x = 2$ this condition may not be fulfilled. However, in such a case there are at least two end-nodes that are not linked to one another and could be removed for any relevant case ($n > 5$).

- *Part 3.* Looking at building a max-proof component, given his linking budget of $B = (n - 1)$, the designer can connect exactly $m = \frac{2(n-1)}{D_l+1}$ nodes in such a component. He therefore needs to leave $(n - m)$ nodes unconnected. Since no additional node can be disconnected, after the disruption $(n - m)$ nodes remain unconnected. By comparison, in the star network D_l nodes are unconnected after disruption. Consequently, if $D_l < (n - m)$ holds, the star network is a strict best response. This holds if $1 < D_l < (n - 2)$, so that the star is a strict best response in all interesting cases, as for $D_l = (n - 1)$ and $D_l = (n - 2)$ the results do not depend on the structure of the network. ■

It can be easily verified that this same analysis also holds, generally, for any case where $B = (n - x)$, with $x > 1$, i.e., for any case in which the linking budget is smaller than the number of nodes that can be used to build the network. The reasoning for the case of $B = (n - x)$ runs completely parallel to that for the case of $B = (n - 1)$: the fact that there are only $(n - x)$ links can be treated as if there are only $(n - x + 1)$ nodes, as at least $(x - 1)$ nodes cannot be connected. These results suggest that even without the influence of information decay in the network, there are incentives to build networks with a limited diameter, such as the star network.

However, since the star network seems a very specific result, as a further sensitivity check we also look at the case of $B = n$. Here the case of $D_l = 1$ is a limit case, where one extra link in the budget makes one jump from what we have called high linking costs (with the star as an optimal network) to low linking costs (with the circle as an optimal network). For $D_l = 1$, the designer is thus able to build a max-proof network (the circle). For disruption budgets larger than 1, however, we can show that the star network remains the best response architecture for the designer. This of course means that we deviate from Approach 2 and do not force the designer to use up all his n links. Instead, although he could use n links, he will continue to use $(n - 1)$ links and build a star network, as this is his best response.¹⁹ To see this, we again need to compare the star network with all other minimally connected networks and networks consisting of a smaller but stronger connected component. Lemma 3 runs completely parallel to Proposition 2 for the case of $B = (n - 1)$. Therefore we relegate the proof to the working paper version of this paper (cf. Hoyer and De Jaegher 2010, p. 15).

LEMMA 3: *With a linking budget of $B = n$ it is a weak best response of the designer to build a star network, when facing a disruptor with a disruption budget of $D_l > 1$ and when it holds that $n > 5$.*

Therefore, while all minimally connected networks are equally good responses if there is no threat of an attack, the star is the only best-response minimally connected network in case of an impending attack for a linking budget of $B = (n - 1)$. Additionally, we showed that the case of the star network as a best response is not a highly special case. In fact, it holds in its strict version for $B = (n - x)$ and it is a weak best response for the case of $B = n$ and $D_l > 1$.

¹⁹ While this at first does not seem to fit with Approach 2, it does if you consider that links are costly and the designer is of course not forced to use up his budget.

5.2. Node Deletion—High Linking Costs

For node deletion we can immediately show that for the case of $D_v = 1$, the best the designer with a linking budget of $B = (n - 1)$ can do is to build a circle containing $(n - 1)$ nodes. This suggests that in general, the designer should build a smaller, stronger component, an intuition that we will indeed confirm in this section. In order to show that it is not a best response for the designer to construct a minimally connected predisruption network, we must first know the order of the largest remaining postdisruption component given a minimally connected predisruption network.

LEMMA 4: *In any minimally connected network, the largest remaining component after an attack by a disruptor on the nodes of the network with a disruption budget D_v , will be maximally of order $\lceil (n - D_v) / (D_v + 1) \rceil$.*

Proof: Consider a minimally connected network of order n . Consider in this network a link g_{ij} with the following properties. If node j is targeted by the disruptor, among the components in $g^2 = g^1 \setminus j$ that do not include i , the largest component has order of at most $\lceil \frac{n-D_v}{D_v+1} \rceil$ and if he targets node i instead, among the components in $g^2 = g^1 \setminus i$ that include j the largest component has order larger than $\lceil \frac{n-D_v}{D_v+1} \rceil$. So the disruptor will disrupt node j and the largest remaining component in $g^2 = g^1 \setminus j$ that includes i is maximally of order $n - \lceil \frac{n-D_v}{D_v+1} \rceil - 1$. Every minimally connected network of order n contains at least one such link g_{ij} . This is because in a minimally connected network, every node is a node cut lying on a path between two end nodes.²⁰ Therefore, every deleted node cuts the network into at least two components. As one deletes consecutive nodes along the path between two end nodes, the order of one component becomes smaller, while the order of the other component gets larger. By continuity, one must meet a link g_{ij} with the properties specified above.

Applying the same reasoning to one more node removed in $g^2 = g^1 \setminus j$ connected to i , and so on until D_v nodes have been disrupted, a component remains that has order at most equal to $n - D_v \lceil \frac{n-D_v}{D_v+1} \rceil - D_v$. But $n - D_v \frac{n-D_v}{D_v+1} - D_v = \frac{n(D_v+1)}{D_v+1} - \frac{D_v(n-D_v)}{D_v+1} - \frac{D_v(D_v+1)}{D_v+1} = \frac{n}{D_v+1} - \frac{D_v}{D_v+1}$.²¹ ■

For the case $D_v = 1$ this means that the largest remaining component will maximally be of order $\lceil \frac{n-1}{2} \rceil$. Comparing this with the largest remaining component in a circle network, we can see that the circle is indeed a strict best response architecture of the designer for the case $D_v = 1$.

PROPOSITION 3: *For $D_v = 1$, and a linking budget of $B = (n - 1)$ nodes, the designer's strict best-response architecture is the circle containing $(n - 1)$ nodes.*

Proof: *Step 1.* Every component that links $(n - 1)$ nodes using $(n - 1)$ links and is not a circle of order $(n - 1)$ has at least one end node. It follows that in this component, the disruptor can delete at least one extra node on top of the deleted node. Together with the node that was not connected in the predisruption network, this means that a largest postdisruption component of, at most, $(n - 3)$ nodes remains. *Step 2.* Every

²⁰ For the definition of a node cut, see the Appendix.

²¹ We are omitting the $\lceil \cdot \rceil$ notation here. This is just for simplicity reasons in the following calculation. However, by omitting it, we are simply putting an upper bound on the order of the last component of higher order and therefore are not making any mistake.

network that links fewer than $(n - 1)$ nodes has a largest postdisruption component that is smaller than $(n - 2)$ because by definition at least one node can be taken out. *Step 3.* In the circle that links $(n - 1)$ nodes using $(n - 1)$ links, if one node is deleted, a postdisruption component connecting $(n - 2)$ nodes remains. ■

For $D_v > 1$, we cannot give a full characterization of the designer's best response g^1 . However, we can show that any best-response g^1 has isolates. We first note that the line connecting n nodes achieves the maximal order for the largest remaining component as set out in Lemma 4. Second, we derive in Lemma 5 the order of the largest remaining component in the circle connecting $(n - 1)$ nodes. Finally, in Proposition 4 we show that this order is larger than the order of the largest remaining component in the line connecting n nodes.

LEMMA 5: *In a circle network of order $(n - 1)$, the disruptor with a disruption budget of D_v will cause maximal damage by cutting the network into D_v separate components, each maximally of order $\lceil \frac{(n-1-D_v)}{D_v} \rceil$.*

Proof: As the circle is completely symmetric, any disruption strategy by the disruptor can be seen as the deletion of one random node in the circle and $(D_v - 1)$ further nodes. After the deletion of this random node, the remaining network takes the form of a line, i.e., a minimally connected component of order $(n - 1)$, in which the disruptor can delete $(D_v - 1)$ nodes. It follows directly from Lemma 4 that the largest remaining postdisruption component has an order of $\lceil \frac{(n-2)-(D_v-1)}{(D_v-1)+1} \rceil = \lceil \frac{(n-1-D_v)}{D_v} \rceil$. ■

PROPOSITION 4: *When facing a disruptor with a node disruption budget D_v the circle architecture of order $(n - 1)$ is a weakly better response than the line architecture with order n . For $(n - 1) \geq D_v(D_v + 3)$ the circle of order $(n - 1)$ is a strictly better response. For $D_v > \lceil \frac{n-1}{2} \rceil$ the circle of order $(n - 1)$ and the line of order n are equally good responses.²²*

Proof: We prove each part of the statement in a separate step.

- From Lemma 4 we know that the largest remaining postdisruption component with a predisruption line of n nodes has order $\lceil \frac{(n-D_v)}{(D_v+1)} \rceil$. By Lemma 5 we know that the largest remaining postdisruption component in a circle of order $(n - 1)$ has order $\lceil \frac{(n-D_v-1)}{D_v} \rceil$. Ignoring the fact that both terms should be natural numbers, it is straightforward to calculate that $\frac{(n-D_v)}{(D_v+1)} < \frac{(n-D_v-1)}{D_v} \Leftrightarrow D_v < \frac{(n-1)}{2}$. Hence if $D_v < \frac{(n-1)}{2}$ the circle is strictly better than the line. However, taking the need for the terms to be natural numbers back into account, this inequality does not always hold. What does hold however, is that if $D_v < \frac{(n-1)}{2}$ then $\lceil \frac{(n-D_v)}{(D_v+1)} \rceil \leq \lceil \frac{(n-D_v-1)}{D_v} \rceil$, since it holds that if $x < y$, then $\lceil x \rceil \leq \lceil y \rceil$. Thus the circle is a weakly better response than the line.
- Note that if $x + 1 \leq y$ then $\lceil x \rceil < \lceil y \rceil$ is always satisfied.²³ Thus, if $\frac{n-D_v}{D_v+1} + 1 \leq \frac{n-D_v-1}{D_v}$, then the circle of order $(n - 1)$ is a strictly better response than the line of order n . This is the case if $(n - 1) \geq D_v(D_v + 3)$.

²² These two conditions are stated in different terms for convenience. Comparing them shows that they are mutually exclusive for the range of disruption budgets we are looking at here.

²³ This is because if $x + 1 < y$ then $\lceil x \rceil < x + 1 \leq y \leq \lceil y \rceil$.

- For $D_v \geq \lceil \frac{(n-1)}{2} \rceil$, in both the mentioned circle and line, the disruptor can reduce the postdisruption network to a set of isolated components, so that both architectures are equivalent in this extreme case. ■

With Proposition 4 we do not imply that the circle network is the best possible network for a designer to build in the case of node deletion under high linking costs. We merely use Proposition 4 to show that it is never a strict best response to build a network including all nodes for the case of high linking costs. In fact, in Lemma 6 we show that for $B = (n - 1)$ and $D_v > 2$, a network in which the designer builds a max-proof component and leaves some nodes isolated strictly dominates the circle network under certain conditions.

LEMMA 6: *For any linking budget $B = (n - 1)$ links, and any disruption budget $D_v > 2$, a max-proof network strictly dominates the circle network of order $(n - 1)$ for all $(n - 1) \geq D_v(D_v + 3)$.*

Proof: We know by Lemma 5 that the largest remaining component in a circle network after an attack by a disruptor with a disruption budget of D_v is $\lceil [(n - 1) - D_v]/D_v \rceil$. The largest remaining component in a max-proof network after disruption with a disruption budget of D_v is $\lceil 2 * (n - 1)/(D_v + 1) - D_v \rceil$. The lemma now follows by the fact that if $x \geq (y + 1)$ then $\lceil x \rceil > \lceil y \rceil$.²⁴ Using this fact,

$$\frac{2 * (n - 1)}{(D_v + 1)} - D_v \geq \frac{(n - D_v - 1)}{D_v} + 1 \Leftrightarrow (n - 1) \geq \frac{D_v^2(D_v + 1)}{D_v - 1}.$$

Note that for $D_v > 2$, $D_v(D_v + 3) > \frac{D_v^2(D_v + 1)}{D_v - 1}$. Consequently, if $(n - 1) \geq D_v(D_v + 3)$, then the max-proof component is a strictly better response than the circle network of order $(n - 1)$, which in turn, by Proposition 4, is for the same range a strictly better response than the line network of order n . ■

This suggests that, instead of building a large connected predisruption component, a designer should rather build a smaller but more highly connected predisruption component, even though this means that he will have to leave a number of nodes unconnected. Due to the limited number of available links, building large connected predisruption components always implies that they are very vulnerable to disruption. There may be better architectures where nodes are left unconnected, enabling the designer to construct a stronger component. For these more general cases, the main insight, namely that the designer will leave nodes unconnected to build a smaller but stronger connected component remains the same. We will also show that the designer should not build the strongest component possible, as he would have to leave too many nodes unconnected. However, since these cases are hard to characterize, we will show what such networks can possibly look like only by means of an example.

Take a disruptor with a disruption budget of $D_v = 2$. Given a linking budget of $B = (n - 1)$ a max-proof component needs to be 3-regular and can be built using $\frac{2}{3} * (n - 1)$ nodes and thus leaving $\frac{1}{3} * (n - 1) + 1$ nodes unconnected.²⁵ For a linking budget of $B = 24$ links and $n = 25$, the network that results can be depicted as in Figure 3(a).²⁶ The circle in Figure 3(c) includes 24 nodes in the connected

²⁴ For more extensive reasoning, see the previous footnote.

²⁵ Assuming that $(n - 1)$ is divisible by 3 and a 3-regular network exists.

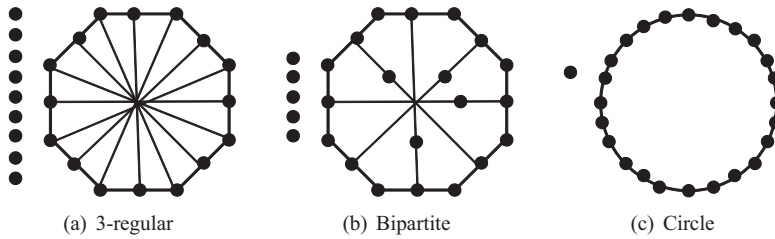


Figure 3: Different 25-node networks.

predisruption component. Figures 3(a) and 3(c) therefore represent, respectively, the smallest and largest candidate connected predisruption components that might be best responses by the designer.²⁷ The bipartite network in Figure 3(b) represents an intermediate solution, because here there are 20 nodes in the connected predisruption component. A graph G is called *bipartite* if it is possible to divide the node set into two sets, n_1 and n_2 , where each link connects a node of subset n_1 with a node of subset n_2 and no two nodes of the same set are directly linked.

However, the order of the largest connected component in g^2 is not only determined by the order of the connected component in g^1 , but also by the damage which the disruptor can cause given $D_v = 2$. In Figure 3(a), the connected component is max-proof and the largest remaining connected component in g^2 is therefore of order 14. In Figure 3(c), removing two nodes leaves a largest remaining connected component in g^2 of order 11. In the bipartite network in Figure 3(b), the maximum damage the disruptor can cause is to disconnect one additional node from the connected component leaving a largest connected component in g^2 of order 17. Thus, the best option of the designer in this case is to build the bipartite network.

Even in this short example with a limited number of nodes, we can see that there is a definite trade-off between building a larger but weaker network and building a smaller but stronger network. While building a network with a max-proof component dominates the option of building a cycle network, as has been seen in the example above (and is proven for a general case in Lemma 6), we have also seen in the example above that both extreme cases (the cycle and the max-proof component) are dominated by a middle option.²⁸

²⁶ The example in Figure 3 illustrates that deviating from the simplifying assumption that the designer only cares about the order of the largest component does not lead to different results. If the designer values the sum of the information levels obtained by all the nodes, then the value of g^2 equals the sum of the squared orders of all components in g^2 . Let the designer now consider a wider class of g^1 similar to Figure 3(a), all consisting of multiple 3-regular components. The designer can then with 24 links construct two 3-regular eight-player components, or four 3-regular 4-player components. In these networks, while the disruptor can still not remove more than two nodes, the number of isolates is the same as in Figure 3(a), and because of the multiple components the designer is worse off. In the same manner, as alternatives to Figure 3(b), the designer may consider two 10-player pair 3-regular components, or four 5-player pair 3-regular components, and as alternatives to Figure 3(c) he may consider any g^1 where 24 nodes are connected in one or more circles. Each time, these networks use 24 links and leave the same number of isolates as in Figure 3, but make the designer worse off than with the single component in Figure 3.

²⁷ We don't need to consider the case of minimally connected networks here, as we have already shown in Lemma 5 and Proposition 4 that the circle leads to a weakly larger connected postdisruption component than any minimally connected network.

²⁸ A proof that the circle and the max-proof network are not best responses of the designer can be found in Lemmata A.12 and A.13 in Hoyer and De Jaegher (2010, p. 35). There it is shown that networks that

It is conceivable that the designer can achieve the same utility with a lower budget, in which case the networks we have derived given a budget $B = (n - 1)$ are not Stackelberg networks. Yet, with a smaller budget, the designer is certainly not able to construct a connected g^1 . It follows that high linking costs exist such that the designer constructs a g^1 that is not connected. We have thus seen in this section that, unlike the case of low linking costs, the most robust network topology is quite different for the cases of node deletion and link deletion. In the link deletion case, it is always optimal to include all nodes in the predisruption component, whereas in the node deletion case, the designer is better off leaving out a number of nodes to build a smaller but stronger predisruption network. In general it seems that nodes are harder to protect in a network than links, not only because in the node deletion case nodes will be disrupted by definition, but also because all links attached to a node may be removed from the network once the node has been deleted. Therefore, it is much harder to keep nodes safe from disruption than to keep links safe.

In terms of our military communications network application, this means that first of all, for high linking costs, it is important to know whether the attack will be directed at the links or the nodes of the network. If the links are being targeted, building a star network, taking into account that in case of an attack some communication facilities will be lost, is the best option. Should, on the other hand, the nodes be under attack, then the only viable option is to build a smaller component that is more highly connected. Otherwise, even when taking out just a couple of nodes, the network as a whole can be disconnected into a number of small, scattered groups.

6. Intermediate Linking Costs

We have so far treated the extreme cases where either links are cheap enough for the designer to build a completely proof network, or where links are so expensive that the designer does not want to add any links above the minimum needed to connect all nodes. In this section, we explore one particular in-between case, where linking costs are intermediate, so that the designer will not protect the network to the maximal extent, but at the same time will use a number of links higher than the minimal number of links necessary to connect the nodes. We here initially take Approach 1, and investigate minimal $(\max - 1)$ -proof networks, that is g^1 such that, upon best response disruption, g^2 consists of a component with order $(n - 1)$ and one isolated node for link deletion (respectively of a component with order $(n - D_v - 1)$ and one isolated node for node deletion). As we will show, typically many more links are needed to construct minimal max-proof networks rather than minimal $(\max - 1)$ -proof networks, such that aspects of intermediate linking costs are already caught by marginally deviating from the goal of max-proofness. For example, a network consisting of $n = 12$ nodes needs exactly 24 links to achieve max-proofness against a disruption budget of $D_v = 3$ or $D_l = 3$. As opposed to this, to achieve $(\max - 1)$ -proofness when facing a disruptor with a disruption budget of $D_v = 3$ or $D_l = 3$ only 18 links are needed for node deletion and only 16 links are needed for link deletion. Thus even in this small example already the designer needs one fourth fewer links to achieve $(\max - 1)$ -proofness as compared to max-proofness.

By analogy of a subset of the regular networks being minimal max-proof, good candidates for minimal $(\max - 1)$ -proof networks are those where every directly linked pair

are neither fully robust against disruption and do not include all nodes in the predisruption component will be the best response of the designer.

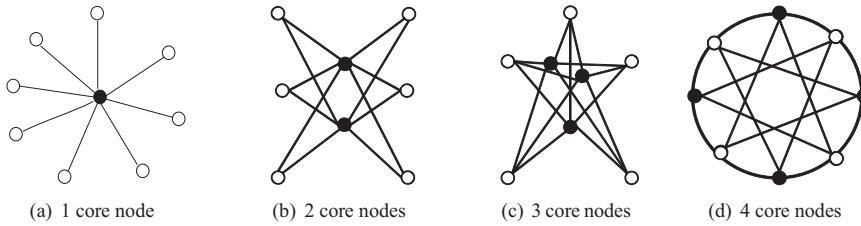


Figure 4: Pair 6-regular networks.

of nodes jointly has exactly $(D_l + 1)$ links to the remaining nodes (link deletion) and respectively has exactly $(D_v + 1)$ neighbors connecting them to the remaining nodes (node deletion),²⁹ because every link in these networks is critical in ensuring that the disruptor is just not able to remove two links/nodes. We term such graphs *pair r -regular networks*. The reason for focusing on such networks is that they are easy to construct: start from a single directly linked pair, and give it a number of r links/neighbors. Each of the resulting new pairs of directly linked nodes in turn need r links/neighbors, and so on.

Our analysis of pair r -regular networks proceeds as follows. In Lemma 7, we first derive some characteristics of pair r -regular networks, and show how these characteristics relate to the order of these networks. In Lemma 8, by imposing that it should not be possible to disconnect nondirectly linked pairs of nodes, we show that max-proofness imposes restrictions on the order of pair r -regular networks in a different manner under node deletion and under link deletion. In Lemma 9, we show that pair r -regular networks are candidate Stackelberg networks, because with the number of links used to construct such networks, it is not possible to construct max-proof networks. Finally, we illustrate how pair r -regular networks can be constructed such that it is not possible to remove sets of nodes of order larger than 2. We summarize our results on intermediate linking costs in Proposition 5.

As will be shown in Lemma 7, in any pair r -regular network each node has one of two degrees, namely either a high degree, or a weakly lower degree, where high-degree nodes are only linked to low-degree nodes, and vice versa. Contrary to what is the case for regular networks, for given r , we show that not all pair r -regular networks have the same link cardinality; in particular, for given r , the link cardinality of pair r -regular networks is lower the larger the difference between the degree of the low-degree and the high-degree nodes. As an example, Figure 4 presents four pair 6-regular networks for $n = 8$, where filled nodes have high degree, and empty nodes have low degree. As can be seen, the link cardinality of the network is larger the larger the number of high-degree nodes.

LEMMA 7: *All pair r -regular networks, where r_1 denotes the degree of nodes in the set n_1 (high degree nodes) and r_2 the degree of nodes in the set n_2 (low degree nodes), fulfill the following basic characteristics:*

- *In any connected pair r -regular network, we have $n_1 = n * [r_2 / (r_1 + r_2)] = n * [r_2 / (r + 2)]$ and $n_2 = n * [r_1 / (r_1 + r_2)] = n * [r_1 / (r + 2)]$, and the network has exactly $n * [r_1 r_2 / (r_1 + r_2)] = n * [r_1 (r + 2 - r_1) / (r + 2)]$ links.*

²⁹ Note that again here the requirement for node deletion is more restrictive than that for link deletion.

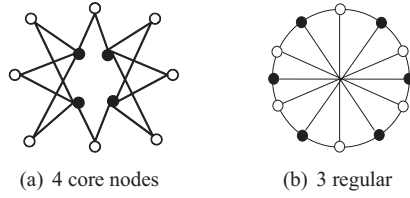


Figure 5: Pair 4-regular networks.

- *Pair r -regular networks have fewer links the smaller their r_2 , and the pair r -regular networks with $r_2 = 1$ have the smallest number of links in this set.*

Proof: We prove each of these statements independently:

- Any pair r -regular network has nodes with only two different degrees. It follows that for link cardinality B , the number of links used in the network, it is the case that $B = n_1 r_1 = n_2 r_2$. Combining this with the fact that $(n_1 + n_2) = n$, and using the fact that $(r_1 + r_2 - 2) = r$, the given expressions for n_1 and n_2 are obtained. These expressions, and the fact that $B = n_1 r_1 = n_2 r_2$, again allow us to calculate that $B = n * [r_1 r_2 / (r_1 + r_2)] = n * [r_2 (r + 2 - r_2) / (r + 2)]$.
- A pair r -regular network with $r_2 = 1, r_1 = (r + 1)$ is only possible with the star architecture, and is pair $(n - 2)$ -regular. The smallest possible r_2 is then $r_2 = 1$. In the expression $B = n * [r_2 (r + 2 - r_2) / (r + 2)]$ derived in the proof of the previous statement, the number of links used is smaller the smaller r_2 . The result follows. ■

Lemma 7 suggests that in order to minimize the link cardinality of the network, the designer should maximize the difference between the degree of high- and low-degree nodes. Yet, in order for pair r -regular networks to be $(\max - 1)$ -proof for disruption budget $r = (D_h + 1) (h = l, v)$, the disruptor should not be able to remove nondirectly linked pairs of nodes either. We show in Lemma 8 that, for r even and at least 4, this restricts the candidate $(\max - 1)$ -proof networks in the set of pair r -regular networks, to regular networks in the case of node deletion, and to networks where high-degree nodes have degrees at most two units larger than low-degree nodes in the case of link deletion. In the latter case, a designer wanting to use a minimal number of links, will then attempt to give the high-degree nodes a degree exactly two units higher than the low-degree nodes.

For instance, for $n = 8$ and $D_l = 5$, the disruptor can separate five nodes in Figure 4(a), two nodes in Figure 4(b), and only one node in Figures 4(c) and 4(d). However, Figure 4(c) has smaller link cardinality. Intuitively, just as for high linking costs, the designer builds a star-like network involving several spokes and a few central nodes. In order to ensure that only one spoke can be removed, spokes should have a sufficient number of links. However, for node deletion, just as is the case for high linking costs, building star-like networks is not a good idea, as the disruptor can then cause great damage by removing central nodes. For instance, for $n = 12$ and $D_v = 3$, the disruptor can reduce the largest component to order 4 in the pair 4-regular Figure 5(a) by removing three central nodes, but in the pair-4 regular and 3-regular Figure 5(b), can only separate one node from the rest by deleting three nodes.

LEMMA 8: *Let $(D_h + 1)$ be even and ≥ 4 . Then:*

- (i) *for $h = l$, if a pair $(D_l + 1)$ -regular network exists with $r_1 = (D_l + 1)/2 + 2$, $r_2 = (D_l + 1)/2$, then this is the pair $(D_l + 1)$ -regular network with the smallest link cardinality, such that no more than one low-degree node can be separated;*
- (ii) *for $h = v$, the pair $(D_v + 1)$ -regular network with $r_1 = r_2 = (D_v + 3)/2$ is the pair $(D_v + 1)$ -regular network with the smallest link cardinality, such that no more than one low-degree node can be separated on top of the nodes which are deleted.*

Proof:

- (1) If $r_2 \leq (r - 1)/2$, the disruptor is able to delete several nodes with degree r_2 , by either deleting all their links in the case of link deletion, or all their neighbors in case of node deletion.
- (2) Consider two neighbors of a type 1 node x_1 . By definition, these two neighbors are type 2 nodes. Each of them has $(r_2 - 1)$ type 1 neighbors other than x_1 . If $[2 * (r_2 - 1) + 1] \leq D_v = (r - 1)$, then by taking all the $[2(r_2 - 1) + 1]$ type 1 neighbors of the two mentioned type 2 nodes out, the disruptor can take out two extra nodes.

The results now follow from Lemma 7. ■

Next, in order to check that the subset of pair r -regular network characterized in Lemma 8 are candidate Stackelberg networks, following Approach 2 we show in Lemma 9 that with a budget exactly sufficient to construct the pair r -regular networks as characterized in Lemma 8, it is not possible to achieve a max-proof network.

LEMMA 9: *Let $r \geq 2$ and let it not be the case that both $r_1 = 2$ and $r_2 = 2$. Then, with any number of links $B = n[r_1 r_2 / (r_1 + r_2)]$ that just allows the designer to build a pair r -regular network, he cannot build an r -regular network.*

Proof: The r -regular connected network uses more links than the pair r -regular network iff $n * r/2 > n * [r_1 r_2 / (r_1 + r_2)] \Leftrightarrow (r_1 + r_2 - 2)(r_1 + r_2) > 2 * r_1 r_2 \Leftrightarrow r_1^2 + r_2^2 > 2(r_1 + r_2)$.

The results of Lemmata 7 to 9 are summarized in Proposition 5. ■

PROPOSITION 5:

- (i) *Link deletion. Let $B = n[r_1 r_2 / (r_1 + r_2)]$, with $r_1 = (D_l + 1)/2 + 2$, $r_2 = (D_l + 1)/2$. Then a pair $(D_l + 1)$ -regular network, where high degree nodes have degree r_1 and low degree nodes have degree r_2 , is the pair r -regular network with the lowest link cardinality, such that no pair of nodes can be separated, and with this budget the designer cannot construct a max-proof network.*
- (ii) *Node deletion. Let $B = n[r_1 r_2 / (r_1 + r_2)]$, with $r_1 = r_2 = (D_v + 3)/2$. Then a $(D_v + 3)/2$ -regular network is the pair r -regular network with the lowest link cardinality, such that no pair of nodes can be separated, and with this budget the designer cannot construct a max-proof network.*

Missing from Proposition 5 are conditions on the specified pair r -regular networks such that it is also not the case that larger subsets of nodes than pairs can be separated. A

systematic analysis of such conditions is outside of the scope of this paper. We only point out that examples suggest that this can be achieved by appropriately connecting the network. In case of node deletion, appropriate circulants can be constructed, where we point out that, if $a_1 = 1$, it needs to be the case that $a_2 = 3$, because otherwise connected pairs share too many neighbors. In case of link deletion, we point out that pair r -regular networks, where every low-degree node is directly linked to every high-degree node and vice versa, will necessarily be $(\max - 1)$ -proof.

In terms of the military application introduced earlier, our analysis suggests that for intermediate linking costs, when facing a possible attack on the links of the network the designer should construct a star-like architecture, consisting of one or more central nodes, and a number of spokes, such that the disruptor can only take out a few spokes. In case the disruptor targets the actual communication bases, the designer should not distinguish between central and noncentral nodes, as otherwise the central nodes would be a good target. The disruptor then again needs to construct networks with a sufficient degree of symmetry.

7. Extensions

Finally, we look at some extensions to the model we have analyzed so far. Here we will look at both link deletion and node deletion. In most applications of a network disruption model, there will be information asymmetries, as either designer or disruptor lack information. Therefore, we will investigate the robustness of our results in the case of asymmetric information. In the first instance in Section 7.1, we look at the case of a lack of information on the side of the designer by keeping the information on what type of disruption budget the disruptor has private. Thus, while the designer knows the size of the network disruption budget, he does not know whether the disruptor will attack links or nodes within the network. In a second extension in Section 7.2, we consider lack of information on the side of the disruptor. Here we assume that the disruptor does not know the structure of the network, but only knows the number of nodes within the network for the case of node deletion or the number of links for the case of link deletion. He thus randomly attacks the network.

7.1. Asymmetric Information: Network Designer

For low linking costs, we have seen in Section 4 that the same structure can be used as a best response for link deletion and node deletion. Therefore, adding uncertainty about the type of attack does not matter for the analysis. The best response is to build a network that is max-proof under node deletion as well as link deletion. Contrary to that, we have seen in Sections 5.1 and 5.2 that for high linking costs the most robust network structures for link deletion and node deletion differ greatly. Whereas for link deletion the most robust network structure for any disruption budget is the star network, for node deletion the optimal network structure highly depends on the number of nodes and the size of the disruption budget. We have shown that leaving some nodes unconnected and building a max-proof component is in any case a better response for the designer than the minimally connected network including all nodes or a cycle network leaving one node unconnected. Since the max-proof component has clear properties, we can compare it to the star network. In this way we can find a lower boundary on the probability that the form of the attack will indeed be link deletion, for the designer to find the star network a best reply. We cannot exclude that there are better replies than

the star network, even for this lower bound. What we do provide is a necessary condition for the star network to be a best response.

Since we are comparing node deletion and link deletion when the disruption budget is of the same size, we denote $D_v = D_l = D$. We have shown that under link deletion the largest remaining component in a star network will be of order $(n - D)$. Under node deletion, it is straightforward to see that the largest remaining component will be of order 1 as the disruptor can simply disrupt the central node. For the network using fewer than n nodes in the connected component, we have shown that given a linking budget of $B = (n - 1)$ exactly $m = \frac{2(n-1)}{D+1}$ nodes can be used to build a max-proof component. The order of the largest remaining component for link deletion will then be $\frac{2(n-1)}{D+1}$ and for node deletion it will be $\frac{2(n-1)}{D+1} - D_v$. Comparing these two payoffs we find that the lower boundary on the probability that the attack will be directed toward the links of the networks has to be at least 0.75 for the star network to be a better response than the max-proof network for $D > 1$.³⁰ The 0.75 is chosen purely for convenience. As it is only a necessary condition for a lower bound we did not calculate a sharp bound. Given that the max-proof network is not necessarily the best response of the designer, this is thereby a necessary but not sufficient condition that therefore works as a lower boundary on the probability of link deletion.

PROPOSITION 6: *For the case of high linking costs, where the designer has a linking budget of $B = (n - 1)$, a necessary condition for the star network to be a best-response structure for $D > 1$, if the designer does not know the type of the disruptor's budget, is that the probability of an attack on the links of the network exceeds 0.75.*

Proof: Assume α is the probability that the designer faces link deletion and $(1 - \alpha)$ is the probability that he faces node deletion.

$$\alpha * (n - D) + (1 - \alpha) * 1 > \alpha * m + (1 - \alpha) * (m - D) \Leftrightarrow \frac{\alpha}{(1 - \alpha)} > \frac{2n - 3 - D^2 - 2D}{nD - n - D^2 - D + 2}. \quad (1)$$

Given the claim that the probability of link deletion, α , has to be at least 0.75, this needs to hold as long as $\frac{\alpha}{(1 - \alpha)} > 3$. Thus:

$$\frac{2n - 3 - D^2 - 2D}{nD - n - D^2 - D + 2} > 3 \Leftrightarrow n > \frac{9 - 2D^2 - D}{5 - 3D}. \quad (2)$$

The right-hand side of this inequality is decreasing in D , and holds for any $n > 3$ if $D > 1$. Consequently, for all $n > 3$, the star may only be a best response network structure if the designer believes that the probability that the attack will indeed be directed toward the links of the network exceeds 0.75. ■

7.2. Asymmetric Information: Network Disruptor

We now turn to the case of asymmetric information on the side of the disruptor only. Thus, while the designer knows whether he is facing link deletion or node deletion, the

³⁰ For $D = 1$ we have seen that the circle network and the star network lead to a largest remaining component of the same order under link deletion, whereas the circle is always preferred under node deletion. Therefore the star will never be preferred under information asymmetry.

disruptor does not know the network structure. In this case asymmetric information is modeled as the disruptor having no or only limited information on the structure the designer chooses. In particular, we assume that the disruptor can observe which of the nodes are situated in the same component, and can observe the set of links formed by the designer. However, for any individual link, he cannot observe which two nodes in particular it connects. Intuitively, the disruptor may be able to observe the level of activity in the network, and infer who is (directly or indirectly) able to receive information from whom, but he is not able to observe the actual network structure.³¹ Looking first at the case of low linking costs, it is straightforward to see that a range of linking costs exists for which the designer will still build a max-proof network in the case of link deletion as well as node deletion. For both types of disruption, irrespective of the disruptor's knowledge of the network structure he will not be able to disconnect any additional node from the connected component. Thus, the max-proof network remains a best response.

To analyze the case of high linking costs, we look at link and node deletion separately. In both cases we will first look at the intuition, before formally proving our results in Proposition 7. For link deletion, it is easy to see that nothing changes concerning the best response structure of the designer. Building a star network is a best reply in the case of perfect information and it also holds for imperfect information, as it does not matter which links the disruptor targets.

For node deletion we have shown above that for the case of high linking costs we cannot strictly define the best response architecture of the designer. Consequently, for the same reasons as in the previous section we use the max-proof component here as a benchmark case. For $B = (n - 1)$, the designer can then use $m = \frac{2(n-1)}{D_v+1}$ nodes in the connected component, leaving $n - m$ nodes unconnected. Consider the case of $D_v = 1$. The max-proof component is then the circle of order $(n - 1)$ and the largest remaining component will be given by $(n - 2)$. Comparing this with the largest remaining component in a star network which is given by $\frac{1}{n} * 1 + (1 - \frac{1}{n}) * (n - 1)$, we find that even for this case where only one node needs to be left out to build a max-proof component, it holds that the largest remaining component in the star network is expected to be larger than that in the circle network for any n . Since for an increase in the disruption budget, even more nodes need to be left out of the predisruption connected component to make it max-proof, it is clear that the star will then also be a better reply strategy than the max-proof component. As this is in essence a simultaneous move game, it directly follows that the designer needs to randomize about which node to put into the center position for the star to be an equilibrium network, as then the disruptor would still be uninformed about exactly which star the designer builds, in the sense that he does not know which one of the nodes will be the central player. Therefore, it follows that for node deletion for the case of high linking costs with imperfect information on the side of the disruptor the star network is a better response than the max-proof network for any n , if the designer randomizes about which node is in the center.

³¹ Here it is important to note that there are two major differences between what we are modeling in Section 7.2 and the analysis of random attacks by nature. Whereas we assume that the disruptor does know which nodes are in the connected component and which are not, in a game against nature this would not be known. For the case of node deletion, this would lead to the max-proof component being a more attractive option for the designer, whereas for link deletion this would not hold. Additionally, one cannot assume that nature would follow a best reply strategy, which means that in the star network the designer would not have to randomize about which node is in the center of the star.

PROPOSITION 7: *If there is imperfect information on the side of the disruptor about the structure of the network, the best reply structure for low linking costs is the max-proof network for both link deletion and node deletion. For high linking cost the best reply structure for link deletion is the star network, and for node deletion the star network is a better reply than the max-proof component using fewer nodes, assuming that the disruptor knows which nodes are in the connected component.*

Proof: The results for low linking costs as well as for high linking costs and link deletion follow directly from the discussion above. For the case of high linking costs and node deletion, comparing the expected payoff of the star network with that of the max-proof component for the case of $D_v \geq 1$, the expected order of the largest remaining component when building a star network is $\frac{D_v}{n} * 1 + (1 - \frac{D_v}{n})(n - D_v)$, because the network will be completely disconnected if the disruptor deletes the central node, while the chances of deleting the central node are low. This can be rewritten as $\frac{D_v - nD_v + D_v^2}{n} + n - D_v$. The order of the largest remaining component if the designer builds a max-proof component will be $\frac{2(n-1)}{D_v+1} - D_v$, if the disruptor only targets within the connected component. By definition then irrespective of which nodes he targets, no additional nodes can be disconnected. Thus, comparing the two payoffs, the following needs to hold for the star network to be a better response:

$$\frac{D_v - nD_v + D_v^2}{n} + n > \frac{2(n-1)}{D_v+1}. \quad (3)$$

It is straightforward to see that the right-hand side of the equation is strictly decreasing in D_v . Taking the partial derivative of the left-hand side with respect to D_v , we find that the function has a minimum at $D_v = \frac{n-1}{2}$ and is decreasing in D_v for $D_v < \frac{n-1}{2}$ and increasing in D_v for $D_v > \frac{n-1}{2}$. Given that the function is continuous and for all $n > 1$ the inequality in (3) holds for $D_v = 1$ as well as at the minimum, which is reached at $D_v = \frac{n-1}{2}$, we can conclude that the inequality is always fulfilled. ■

We have, thus, seen in these robustness checks that for the case of low linking costs our model is robust to introducing asymmetric information on the side of the designer as well as on the side of the disruptor. However, for the case of node deletion the star network becomes a better response structure than the max-proof component using fewer than n nodes in the case of asymmetric information on the side of the network disruptor, whereas the max-proof component was a better response in our original model.

8. Discussion

In this paper, we looked at the purely structural implications of network design. Abstracting from asymmetric values of nodes and asymmetric values of links, we looked at what happens when a network is under attack by a disruptor either attacking the links or the nodes of the network. We analyzed the implications of different linking cost levels on such a network structure and which network structures are safe against attacks.

Summarizing our results, when linking costs are low the designer protects his network by constructing a regular network where all nodes are equally well protected. When linking costs are high, contrary to what is the case for low linking costs the best-response architectures under link and node deletion look fundamentally different. Under link deletion, it is a best response to connect all nodes in a star network. Under node deletion, it is a best response to leave some nodes out of the network, and build a smaller and stronger component. For intermediate linking costs, our analysis suggests

that, under link deletion, star-like networks should be constructed, while under node deletion, whenever possible, all nodes get the same degree.

Thus comparing link deletion and node deletion, it can be said that while the optimal network structures start off completely differently for high linking costs, they move in the same direction if linking costs are sufficiently low. Additionally, for the case of intermediate linking costs, it can be seen that, although the optimal structures are more similar than for high linking costs, there are still decisive differences between best-response structures for node deletion and link deletion. In cases where linking is extremely expensive, the knowledge about whether nodes or links are a potential target for disruption is vitally important when forming a network that is to be as proof as possible against disruption. Thus our analysis suggests that by increasing linking costs, the knowledge about which part of the network is being targeted becomes more vital for the designer.

We end by exploring possibilities for future research, where the key question is to extend our present approach of a designer to a multi-player game, where the nodes in the network are actual players. Let us start by looking at agents' incentives to form links, independently from the presence of a disruptor. In a more realistic model, there may be information decay, where information is worth less the larger the distance it traveled in the network (Jackson and Wolinsky 1996; Bala and Goyal 2000). From the perspective of information sharing, it is efficient for nodes to be as close to one another as possible, as is the case in the star; in equilibrium, players also have the tendency to connect to a central node, such that the star is likely to arise. As our analysis shows, at least for high linking costs the star is also efficient under link deletion. However, it is a bad network under node deletion. Further, players' incentives to link to certain nodes may not only depend on the information obtained from those nodes, but may also depend on players' preferences. A well-known phenomenon in sociology is homophily, where in networks birds of a feather flock together (McPherson, Smith-Lovin, and Cook 2001). This should lead to clustering, with only few links between the clusters. As shown in our analysis, such preferences are in direct conflict with efficient defense against network disruption, as a deletion of a few links or nodes may then cause great damage to the network.

Further, players may also directly take into account network defense and network disruption when deciding on which links to form. In one type of network formation extension of our model, we could assume that players dislike being removed from a network. An example would be a member of an illegal network who does not want to be arrested. In some of our results, it is efficient to leave weak spots in the network, which are then more likely to be removed from the network. But individual players may not want to be at such weak spots then. In another type of network extension of our model, players may on the contrary like to be at vulnerable positions in a network. If a firm defects to a competing alliance, then this need not make the firm worse off. In its present network, each firm may try to maneuver itself in a crucial position, in order to have larger bargaining power in its network. This follows Burt (1992)'s argument that an individual may gain advantage by bridging structural holes in networks, thus assuring that information exchange takes place between different groups (for recent game-theoretic translations of this argument, see Goyal and Vega-Redondo 2007; Kleinberg *et al.* 2008). In our argument, this strong position as such does not relate to the bridging function, but to the fact that a disruptor is willing to give such a bridge player a large payment for defecting, creating a very viable outside option for the player, and increasing his bargaining power in his present network. This does not mean, however, that in equilibrium such bridging positions may ever arise, as every player seeks to obtain them.

Appendix

The Network Disruptor's Algorithm

Before we define the algorithm to find the disruptor's best response, we need to introduce some graph-theoretic concepts of connectivity that will be used in the algorithm.

DEFINITION 1: A link (or set of links) (ij) in a connected graph g , is called a link cut L , if g_{-L} is disconnected.

DEFINITION 2: A node (or set of nodes) i in a connected graph g , is called a node cut V , if g_{-V} is disconnected.

The connectivity of a graph can be considered in terms of nodes and links. The node connectivity κ of a graph is defined as the smallest number of nodes whose removal from the graph will lead to a disconnected graph or a single node. The link connectivity λ of a graph is defined as the smallest number of links whose removal from the graph will lead to a disconnected graph or a single node. From these definitions follow the definitions of node (link) cuts. A node (link) cut V (L) is a set of nodes (links) whose removal will lead to a disconnected graph. Thus for any given graph a node (link) cut has to be of at least cardinality κ (λ).³²

The Algorithm:

- (1) Consider the cardinality of all link cuts L (node cuts V) such that g_{-L} (g_{-V}) is the empty graph. If $L \leq D_l$ ($V \leq D_v$), it is a best response for the disruptor to delete this link cut (node cut). Stop. Otherwise move on to the next step.
- (2) Consider the cardinality of all link cuts L (node cuts V) such that the smallest connected component in g_{-L} (g_{-V}) is of order 2. If $L \leq D_l$ ($V \leq D_v$), it is a best response for the disruptor to delete this link cut (node cut). Stop. Otherwise move on to the next step.
(...)
- (3) Consider the cardinality of all link cuts L (node cuts V) such that the smallest component in g_{-L} (g_{-V}) is of order x . If $L \leq D_l$ ($V \leq D_v$), it is a best response for the disruptor to delete this link cut (node cut). Stop. Otherwise move on to the next step.
(...)
- (4) Consider the degree of connectivity. If $D_l < \lambda$ ($D_v < \kappa$), no link cut L (node cut V) exists that has a cardinality below D_l (D_v), thus no node can be disconnected. Stop.

References

- ALBERT, R., H. JEONG, and A.-L. BARABASI (2000) Error and attack tolerance of complex networks, *Nature* **406**(6794), 378–382.
- ARGUILLA, J., and D. RONFELDT (eds.) (2000) *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica. CA: RAND Corporation.

³² A well-known theorem in graph theory (Whitney's Theorem) then states that $\kappa \leq \lambda \leq \eta_i$, where η_i denotes the degree of node i . For a proof of this, see, for example, Diestel (2005, p. 12).

- BABURAJAN, R. (2010) Raytheon BBN Technologies Demos Disruption-Tolerant Network, *TM-Cnet.com* June 4, 2010.
- BACCARA, M., and H. BAR-ISAAC (2008) How to organize crime, *The Review of Economic Studies* **75**, 1039–1067.
- BALA, V., and S. GOYAL (2000) A noncooperative model of network formation, *Econometrica* **68**, 1181–1229.
- BALLESTER, C., A. CALVO-ARMENGOL, and Y. ZENOU (2006) Who's who in networks. Wanted: The key player, *Econometrica* **74**, 1403–1417.
- BIER, V. M., S. OLIVEROS, and L. SAMUELSON (2007) Choosing what to protect: Strategic defensive allocation against an unknown attacker, *Journal of Public Economic Theory* **9**, 563–587.
- BILLAND, P., C. BRAVARD, S. S. IYENGAR, R. KUMAR, and S. SARANGI (2011) Network stability in the context of information games under node failure, Working Paper, Florida International University.
- BOESCH, F. (1986) Synthesis of reliable networks: A survey, *IEEE Transactions on Reliability* **35**, 240–246.
- BOESCH, F., and R. TINDELL (1984) Circulants and their connectivities, *Journal of Graph Theory* **8**, 487–499.
- BOLLOBÁS, B., and O. RIORDAN (2003) Robustness and vulnerability of scale-free random graphs, *Internet Mathematics* **1**(1), 1–35.
- BONDY, J. A., and U. S. R. MURTY (2008) *Graph Theory*, 2nd ed. London: Springer.
- BRAMOULLÉ, Y., and R. KRANTON (2007) Public goods in networks, *Journal of Economic Theory* **135**, 478–494.
- BURT, R. S. (1992) *Structural Holes*. Cambridge, MA: Harvard University Press.
- CHIANG, W., and R. CHEN (1995) The (n, k) -star graph: A generalized star graph, *Information Processing Letters* **56**(5), 259–264.
- COHN, P. (2003) *Basic Algebra: Groups, Rings, and Fields*. London: Springer.
- DEKKER, A., and B. COLBERT (2004) Network robustness and graph topology. In *27th Australasian Computer Science Conference*, edited by V. Estivill-Castro, Volume 26, 359–368.
- DIESTEL, R. (2005) *Graph Theory*. Heidelberg, Germany: Springer Verlag.
- DZIUBIŃSKI, M., and S. GOYAL (2013) Network design and defence, *Games and Economic Behavior* **79**, 30–43.
- ENDERS, W., and P. JINDAPON (2010) Network externalities and the structure of terror networks, *Journal of Conflict Resolution* **54**, 262–280.
- ENDERS, W., and X. SU (2007) Rational terrorists and optimal network structure, *Journal of Conflict Resolution* **51**, 33–57.
- GOYAL, S. (2007) *Connections: An Introduction to the Economics of Networks*. Princeton, NJ: Princeton University Press.
- GOYAL, S., and F. VEGA-REDONDO (2007) Structural holes in social networks, *Journal of Economic Theory* **137**, 460–492.
- GOYAL, S., and A. VIGIER (2014) Attack, defence and contagion in networks, *Review of Economic Studies* **81**, 1518–1542.
- HARARY, F. (1962) The maximum connectivity of a graph, *Proceedings of the National Academy of Sciences of the United States of America* **48**(7), 1142–1146.
- HARARY, F. (1969) *Graph Theory*. Reading, MA: Addison-Wesley.
- HONG, S. (2008) Hacking-proofness and stability in a model of information security networks, Working Paper, Vanderbilt University.
- HONG, S. (2009) Enhancing transportation security against terrorist attacks, Working Paper, Vanderbilt University.
- HOYER, B. (2012) Network disruption and the common enemy effect, TKI Discussion Paper Series (12-06).
- HOYER, B., and K. DE JAEGER (2010) Strategic network disruption and defense, TKI Discussion Paper Series (10-13).
- JACKSON, M. O. (2008) *Social and Economic Networks*. Princeton, NJ: Princeton University Press.

- JACKSON, M. O., and A. WOLINSKY (1996) A strategic model of social and economic networks, *Journal of Economic Theory* **71**, 44–74.
- KLEINBERG, J., S. SURI, E. TARDOS, and T. WEXLER (2008) Strategic network formation with structural holes. In *Proceedings of the 9th ACM Conference on Electronic Commerce*, 284–293.
- KOVENOCK, D., and B. ROBERSON (2010) The optimal defense of networks of targets, Working Paper, Purdue University.
- LARSON, N. (2013) Network security, Working Paper, American University.
- LIPSEY, R. A. (2006) Network warfare operations: Unleashing the potential. Mimeo, Center for Strategy and Technology, Air War College, Air University.
- MADER, W. (1971) Minimalen-fach kantenzusammenhängende Graphen, *Mathematische Annalen* **191**(1), 21–28.
- MCBRIDE, M., and D. HEWITT (2013) The enemy you can't see: An investigation of the disruption of dark networks, *Journal of Economic Behavior and Organization* **93**, 32–50.
- MCPHERSON, M., L. SMITH-LOVIN, and J. M. COOK (2001) Birds of a feather: Homophily in social networks, *Annual Review of Sociology* **27**, 415–444.
- SCHWARTZ, G., S. AMIN, A. GUEYE, and J. WALRAND (2011) Network design game with both reliability and security failures. In *49th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, IEEE, 675–681.
- TAYLOR, M., S. SEKHAR, and G. D'ESTE (2006) Application of accessibility based methods for vulnerability analysis of strategic road networks, *Networks and Spatial Economics* **6**, 267–291.