Network Vulnerability: A Designer-Disruptor Game*

Hans Haller†

February 2016

Abstract

We focus on the crucial role of network architecture in the defence against targeted attacks. A two-stage strategic game between a network designer and a network disruptor is analyzed. Given a set of nodes, the designer builds a network by investing in costly links. In the second stage, the disruptor deletes (possibly in a costly way) some of the links or nodes to reduce the designer's benefit from the network. General results deal with existence, uniqueness and comparative statics of Stackelberg (i.e., subgame perfect) equilibria. More specific issues are addressed under the assumption of a fixed budget for one or both players.

JEL Classification: C72, D85

Key Words: strategic network disruption,
strategic network design,
strategic network games

*I would like to thank Christophe Bravard for insightful comments.

†Department of Economics, Virginia Polytechnic Institute and State University, Blacksburg, VA 24061-0316, USA. *email: haller@vt.edu.*

1 Introduction

Networks are ubiquitous in contemporary economies and societies: distribution and transportation networks, financial, communication, information and social networks, among others. With the growing importance of networks, various academic disciplines have become increasingly involved in the study of network formation and utilization.[1] The growing importance of networks has also aggravated the consequences of network failure and misuse. Like every infrastructure, physical networks are exposed to damage caused by faulty design and materials, decay, natural disaster, and human error. However, networks, especially financial, communication and information networks can also be the outright target of adversarial attacks. One possibility is the infiltration of the network for the purpose of military, political or industrial espionage or identity theft. Another possibility are attempts to disrupt or modify the operations of the network, be it by jamming the network, planting viruses and misinformation, or destroying parts of the network.

There already exists a large literature dealing with network vulnerability and security, primarily on the software side. A game-theoretical approach lends itself to analyze the interaction between attackers and defenders of networked systems. Frequently, a natural modeling choice is a strategic game à la Stackelberg where the defender takes precautionary measures against an attack, anticipating how the attacker will respond.

We are going to disregard specific hardware or software solutions that the defender might employ. Rather, we address the question how the choice of network architecture facilitates or prevents and impedes attacks.[2]

[1] Myerson (1977, 1991), Jackson and Wolinsky (1996), and Bala and Goyal (2000) have pioneered the analysis of strategic network formation games. See also the monographs by Goyal (2007), Vega-Redondo (2007) and Jackson (2008). Since the early 90s, a sizeable literature on pairwise interactions between neighbors on a graph has emerged, with important contributions by Anderlini and Ianni (1996), Berninghaus and Schwalbe (1996a,b), Blume (1993, 1995), Ellison (1993), Goyal and Janssen (1997), among others. In recent years, the study of cooperative games played on graphs has become an active research area. After the pioneering work of Erdös and Rényi (1960) and others, numerous articles have been devoted to the study of exogenously formed random graphs. For an example of an endogenously created random graph, see Ioannides (1990).

[2] It is well recognized in the literature that the vulnerability of a network depends on

We develop a Stackelberg game between a network designer DES and a disruptor DIS. DES moves first and creates links between a given set of nodes.[3] DIS moves second and deletes (destroys, disables) some or all of the existing links and nodes. The model builds upon and is motivated by the work of Hoyer and De Jaegher (2015) who characterize the designer's best network architecture(s) — given certain modes of attack by the disruptor. Such a network would constitute the Stackelberg equilibrium choice of DES if specific assumptions on the costs of link formation, the costs of link and node deletion, and the protagonists' benefits from the post-attack network were made. In contrast to Hoyer and De Jaeger (abbreviated HDJ in the sequel), the emphasis of the current contribution lies on full-fledged Stackelberg equilibria: their existence, uniqueness, and comparative statics. These issues are addressed in Section 3.

In Section 4, we address or at least touch upon further pertinent issues, some old, some novel: We demonstrate the sensitivity of equilibrium outcomes to the choice of value function. Following up and drawing on the results of Hoyer and De Jaegher, we elaborate on the sensitivity of equilibrium outcomes to the mode and size of an attack. In addition to the previous result that an effective network architecture against link attacks (e.g., a star) can differ drastically from an effective network architecture vis-à-vis node attacks (e.g., a circle and an isolated node), we find that the nature and number of equilibrium networks changes in a non-monotonic way as the size of the attack varies. The usefulness of multi-graphs as a defense against link attacks is illustrated. Finally, we exemplify the differences in vulnerability against random failure and targeted attacks.

Dziubiński and Goyal (2013) consider a model where the disruptor attacks (deletes) nodes. The designer forms costly links, but can also immunize a set of nodes against attacks at a cost. Their model further differs from ours and the model of Hoyer and De Jaegher in the choice of value and cost

its topology or architecture, among other factors. See, e.g., Albert et al. (2000), Eusgeld et al. (2009), Liu and Başar (2014).

[3]Design and create tend to have a positive connotation. Yet DES is not necessarily the "good guy". The formal model encompasses the design and defence of criminal or terrorist networks as well.

functions. They find that "if defence is affordable and reliable, then the network is sparse and heterogeneous, and either centrally or fully protected. On the other hand, if defence is relatively costly compared to linking, then dense and homogeneous networks arise in equilibrium." Remarks 1 and 2 refer to some of the differences between their and our model. In our model as well as those of Dziubiński and Goyal (2013) and Hoyer and De Jaegher (2015), a successful attack on a node may affect other nodes in that paths to, from or through the deleted node are destroyed. But the other nodes remain intact (persist) unless they are also targets of successful attacks by the disruptor. Goyal and Vigier (2014) consider a very different scenario, where a successfully attacked node serves as the basis for attacks from inside the network, aimed at neighboring nodes — a contagion effect.

Bravard and Charroin (2015) study a model with link attacks. The designer achieves a positive payoff only if the residual network is connected, using in fact one of value functions adopted by Dziubiński and Goyal (2013). She forms links, having a choice between destructible and indestructible links, with the restriction that the designed graph (network) has a minimally connected subgraph whose links consist of the indestructible links in the entire network. If indestructible links are relatively cheap, then in subgame perfect equilibrium, the designer will form a minimally connected network all of whose links are indestructible. In such a network, all nodes are "protected", in contrast to the findings of Dziubiński and Goyal (2013). This conforms with the prior finding of Hoyer and De Jaegher (2015) that the mode of attack matters, with the added insight that the mode of defence may matter as well. Landwehr (2015) considers modifications of the model of Dziubiński and Goyal (2013) and Bravard and Charroin (2015), respectively, replacing protected nodes by imperfectly protected nodes in the case of node attacks and indestructible links by imperfectly protected links in the case of link attacks, respectively.

The next section introduces the formal model and concepts. Section 5 contains concluding remarks. Section 3 addresses existence, uniqueness and comparative statics of equilibria while Section 4 addresses further pertinent issues.

2 The Designer-Disruptor Game

There are numerous ways to model

- the vulnerability of networks to attacks and
- defensive measures against attacks.

We consider a situation without ex ante distinguished nodes or links. Any asymmetry concerns the network architecture and is endogenous. There are two agents in the model, a *network designer* DES and a *network disruptor* DIS. One can think of a sequential game à la Stackelberg where the designer moves first and the disruptor moves second.

2.1 Networks (Graphs)

There is a finite set of nodes $V = \{1, \ldots, N\}$ with $N > 2$. A **network** is an undirected graph (V, g) with node set (vertex set) V and link set (edge set) g. Since V is given, g identifies the network, "is" the network. The cardinality $|g|$ denotes the number of links in g, also known as size of g. The link set g can be identified with the adjacency matrix (g_{ij}), a symmetric $N \times N$ matrix such that for $1 \leq i < j \leq N$, $g_{ij} = g_{ji} = 1$ if there is a direct link between i and j and $g_{ij} = g_{ji} = 0$ otherwise. For our purposes, it proves useful to set $g_{ii} = 0$ for all i, since we exclude loops.

An undirected graph (V', g') is a subgraph of (V, g) if $V' \subseteq V$ and $g' \subseteq g$. We then write $(V'g') \trianglelefteq (V, g)$. For $V' \subseteq V$, the induced subgraph (V', g') is given by $g'_{ij} = g_{ij}$ for $i, j \in V'$. At times, we will use the notation $g'(V', g)$ for the sake of clarity.

Multigraphs. Hoyer and De Jaegher (2015) allude to military units and the communication links between them, which together can be considered as military networks. Interruptions caused by the deliberate jamming of frequencies constitutes an instance of link deletion or "link attack". Additional frequencies to communicate between two units can be used to make the network safer against the disruption of links. Such a network constitutes

a multigraph — which has not been considered by Hoyer and De Jaegher. A multigraph is a graph which is permitted to have multiple or parallel edges that is, different edges that have the same end nodes. Thus two vertices may be directly connected by more than one edge. There are two distinct notions of multiple edges:

Edges without own identity: The identity of an edge is defined solely by the two nodes it connects. In this case, the term "multiple edges" means that the same edge can occur several times between these two nodes. Formally, this can be described by a multiset of edges.

Edges with own identity: Edges are primitive entities just like nodes. When multiple edges connect two nodes, these are different edges.

We are going to identify a multigraph by means of a generalized adjacency matrix: $g_{ij} = k$ means that there are k edges or links that directly connect the distinct nodes i and j. In principle, this representation allows both interpretations, edges without own identity and edges with own identity. In view of the motivating example of military networks, we prefer the second interpretation. If $i \neq j$ and $g_{ij} = k$, then k links have to be destroyed in order to sever all direct links between i and j. Let M denote the set of $N \times N$-matrices representing multigraphs on a given set of nodes $\{1, \ldots, N\}$.

2.2 Parameters of the Game

Hereafter let $V^1 = \{1, \ldots, N\}$ with $N > 2$ be a given set of nodes. A designer-disruptor game $\mathcal{G}$ is given by the two players DES and DIS and V^1, $\mathfrak{c}(\cdot)$, $\mathfrak{C}(\cdot)$, and v where

- $\mathfrak{c}(\cdot)$ is a cost function for DES;
- $\mathfrak{C}(\cdot)$ is a cost function for DIS;
- v is the benefit or value function for DES (and $-v$ is the benefit for DIS).

Further details of the game are furnished in Subsection 2.3.

2.3 Sequencing and Payoffs

One can distinguish between the pre-disruption network $G^1 = (V^1, g^1)$ and the post-disruption network $G^2 = (V^2, g^2)$. It is assumed that the designer DES moves first and forms a network $G^1 = (V^1, g^1)$ with given node set V^1, i.e., DES chooses g^1. The disruptor DIS moves second and attacks and destroys (deletes, renders dysfunctional) a number D of links or nodes, depending on the mode of attack, and a residual network results, a subnetwork $G^2 = (V^2, g^2)$ of (V^1, g^1). The payoffs are

$\mathfrak{U}_{DES} = v(G^2) - \mathfrak{c}(|g^1|)$,

$\mathfrak{U}_{DIS} = -v(G^2) - \mathfrak{C}(D)$

where $v(G^2) \geq 0$, $\mathfrak{c}(x)$ is increasing in $x \geq 0$ and unbounded from above with $\mathfrak{c}(0) = 0$, $\mathfrak{C}(x)$ is increasing in $x \geq 0$ and unbounded from above, with $\mathfrak{C}(0) = 0$, and D is the "size of the attack".[4]

Let us define for $x = 0, 1, \ldots$ the right-hand discrete derivative or marginal cost $\mathfrak{mc}_+(x) = \mathfrak{c}(x+1) - \mathfrak{c}(x)$ and for $x = 1, 2, \ldots$ the left-hand marginal cost $\mathfrak{mc}_-(x) = \mathfrak{c}(x) - \mathfrak{c}(x-1)$. Then $\mathfrak{mc}_-(x) = \mathfrak{mc}_+(x-1)$. Further

$$\begin{aligned}
\mathfrak{c} \text{ is convex} &\iff \mathfrak{mc}_+ \text{ is non-decreasing} \\
&\iff \mathfrak{mc}_- \text{ is non-decreasing} \\
&\iff \mathfrak{mc}_+(x) \geq \mathfrak{mc}_-(x) \text{ for } x = 1, 2, \ldots \ . \\
\mathfrak{c} \text{ is strictly convex} &\impliedby \mathfrak{mc}_+ \text{ is increasing} \\
&\iff \mathfrak{mc}_- \text{ is increasing} \\
&\iff \mathfrak{mc}_+(x) > \mathfrak{mc}_-(x) \text{ for } x = 1, 2, \ldots \ .
\end{aligned}$$

We assume that the value function $v(\cdot)$ is weakly increasing in the sense that

1.) $(V', g') \trianglelefteq (V, g)$ implies $v(V', g') \leq v(V, g)$.

We further assume that multiple links do not affect the efficacy of the network per se while possibly contributing to the protection of the network, that is,

2.) $g_{ij} > 0 \Leftrightarrow g'_{ij} > 0$ for all ij implies $v(V, g) = v(V, g')$.

Let $g^o = \emptyset$ denote the empty edge set, $G^o = (\emptyset, \emptyset)$ denote the empty network

[4] If $\mathfrak{c}(0) = 0$, $\mathfrak{c}(x)$ is increasing in $x \geq 0$ and convex, then $\mathfrak{c}(x) \geq x \cdot \mathfrak{c}(1)$ for $x \geq 1$ and, thus, $\mathfrak{c}(\cdot)$ is unbounded from above. The analogous observation holds for $\mathfrak{C}(\cdot)$.

and $G^c = (V^1, g^c)$ denote the complete network on V^1, i.e., $g^c_{ij} = 1$ for all $i, j \in V^1, i \neq j$. Let $\bar{v} = v(G^c) - v(G^o)$, the maximum value differential, $\overline{\overline{B}}$ be the smallest $x \in \mathbb{N}$ with $\bar{v} \leq \mathfrak{c}(x)$ and $\overline{\overline{D}}$ be the smallest $x \in \mathbb{N}$ with $\bar{v} \leq \mathfrak{C}(x)$.

2.4 Specific Value Functions

Some of our results do not impose any assumptions in addition to 1.) and 2.) on the value function v. However, the analysis in Section 4 relies on specific value functions. Let $G^2 = (V^2, g^2)$ be a graph with node set V^2 and edge set g^2. Denote by $C_1(G^2), C_2(G^2), \ldots, C_m(G^2)$ the connected components of G^2. The value function v^* assigns to G^2 the size of the largest connected component(s) of G^2: $v^*(G^2) = \max\{|C_1(G^2)|, \ldots, |C_m(G^2)|\}$. $v = v^*$ underlies the work of Hoyer and De Jaegher (2015) and the results reported in Section 4.[5]

The value function $v^\square$ assigns to G^2 the sum of the squared sizes of all connected components: $v^\square(G^2) = \sum_k |C_k(G^2)|^2$.[6] $v^\square$ belongs to the family of component-additive value functions $v^f(G^2) = \sum_k f(|C_k(G^2)|)$ considered by Dziubiński and Goyal (2013).

Both v^* and $v^\square$ are used in Example 2 to show that the choice of value function affects Stackelberg equilibrium outcomes. Both satisfy 1.) and 2.). As a rule, $1 \leq v^*(G^2) \leq N$ and $1 \leq v^\square(G^2) \leq N^2$. However, $v^*(G^2) = v^\square(G^2) = 0$ if and only if all nodes are deleted.

Dziubiński and Goyal (2013) study a benchmark model based on the "connectivity problem" where the designer gets a positive benefit only if the

[5] If G^1 is an initial graph and G^2 is the residual graph after a number of nodes or links are deleted, then $\Delta = v^*(G^1) - v^*(G^2)$ is a conceivable measure of the damage inflicted on the graph that will be used in Subsection 4.5. If G^1 is the "giant component" of the realization of a random graph, then $v^*(G^2)/v^*(G^1)$ constitutes the fraction of the giant component that is still intact after the deletion of nodes or links. $1 - v^*(G^2)/v^*(G^1) = (v^*(G^1) - v^*(G^2))/v^*(G^1)$ is the relative damage inflicted. The latter two measures lend themselves for diagrammatical representations and are adopted by Albert et al. (2000) and Barrat et al. (2008).

[6] Suppose that similar to the connections model without decay of Jackson and Wolinsky (1996), a node receives one unit of benefit from each node to which it is connected (including itself). Then the total value accruing to the members of the k^{th} component $C_k(G^2)$ is $|C_k(G^2)|^2$. The total value for the entire node set V^2 is $v^\square(G^2)$.

residual network is connected. More specifically, the corresponding value function is given as

$$v^{\bullet}(G^2) = \begin{cases} 1 \text{ if } G^2 \text{ is connected;} \\ 0 \text{ otherwise.} \end{cases}$$

2.5 Stackelberg Equilibrium

In the sequential game, the network designer DES moves first, choosing g^1 so that the network (graph or multi-graph) $G^1 = (V^1, g^1)$ results. At the second stage, the network disruptor DIS deletes a number of nodes or links of G^1 so that a subnetwork (subgraph) $G^2 = (V^2, g^2)$ of G^1 results. More precisely, if DIS first deletes a subset H of V^1, then $V^{1\prime} = V^1 \setminus H$ obtains, with induced subgraph $G^{1\prime} = (V^{1\prime}, g^{1\prime})$ where $g^{1\prime} = g'(V^{1\prime}, g^1)$. Next, DIS deletes a subset h of $g^{1\prime}$, resulting in $g^2 = g^{1\prime} \setminus h$. The final outcome of DIS's deletions is the network $G^2 = (V^2, g^2)$ where $V^2 = V^{1\prime}$.

Let $D_n = |H|$, $D_l = |h|$, $D = D_n + D_l$. DIS aims to maximize $\mathfrak{U}_{DIS} = -v(G^2) - \mathfrak{C}(D)$ given g^1. At equilibrium, for every g^1, DIS chooses a set of nodes $H(g^1)$ and a set of links $h(g^1)$ resulting in a subgraph $G^2(g^1)$ such that $\mathfrak{U}_{DIS}$ is maximized. Given the best response outcome $G^2(g^1)$, DES achieves payoff $\mathfrak{U}_{DES} = v(G^2(g^1)) - \mathfrak{c}(|g^1|)$ when choosing g^1. At the specific equilibrium, DES chooses a g^1 that maximizes that payoff.

More formally, a Stackelberg equilibrium is a list $(g^{1*}, (H(g^1), h(g^1))$ that prescribes the following strategic choices. For each g^1, DIS plans to attack a subset $H(g^1)$ of V^1 and a subset $h(g^1)$ of $g'(V^1 \setminus H(g^1), g^1)$ so that with $V^2(g^1) = V^1 \setminus H(g^1)$, $g^2(g^1) = g'(V^1 \setminus H(g^1), g^1) \setminus h(g^1)$ and $G^2(g^1) = (V^2(g^1), g^2(g^1))$:

$$(H(g^1), h(g^1)) \in \underset{\substack{H \subseteq V^1 \\ h \subseteq g'(V^1 \setminus H,\, g^1)}}{\arg\max} \{-v(V^1 \setminus H, g'(V^1 \setminus H,\, g^1) \setminus h) - \mathfrak{C}(|H| + |h|)\}.$$

If link attacks are ruled out, then for each g^1: $h(g^1) = \emptyset$ and

$$H(g^1) \in \underset{H \subseteq V^1}{\arg\max} \{-v(V^1 \setminus H, g'(V^1 \setminus H,\, g^1)) - \mathfrak{C}(|H|)\}.$$

If node attacks are ruled out, then for each g^1: $H(g^1) = \emptyset$ and

$$h(g^1) \in \arg\max_{h \subseteq g^1} \{-v(V^1, g^1 \setminus h) - \mathfrak{C}(|h|)\}.$$

DES chooses

$$g^{1*} \in \arg\max_{g^1} \{v(G^2(g^1)) - \mathfrak{c}(|g^1|)\}. \tag{1}$$

Stackelberg equilibrium is of course just another term for a subgame perfect equilibrium of the two-stage game — and in principle, all Stackelberg equilibria can be obtained via backward induction.

3 Equilibrium Analysis: Existence, Uniqueness, Comparative Statics

If we allow for multiple links between two nodes, then there is no a priori bound on the number of links. However, because of the unboundedness of $\mathfrak{c}$ and $\mathfrak{C}$, the following holds:

Lemma 1. *In a Stackelberg equilibrium,* $|g^{1*}| \leq \overline{\overline{B}}$ *and* $|H(g^1)|+|h(g^1)| \leq \overline{\overline{D}}$ *for all* g^1*.*

PROOF. Suppose $|g^{1*}| > \overline{\overline{B}}$. Then

$$\begin{aligned} & v(G^2(g^{1*})) - \mathfrak{c}(|g^{1*}|) - [v(G^o) - \mathfrak{c}(0)] \\ = \;& [v(G^2(g^{1*})) - v(G^o)] - \mathfrak{c}(|g^{1*}|) \\ \leq \;& \bar{v} - \mathfrak{c}(|g^{1*}|) \;<\; \bar{v} - \mathfrak{c}(\overline{\overline{B}}) \;\leq\; \bar{v} - \bar{v} \;=\; 0, \end{aligned}$$

which means that g^o is a better choice than g^{1*} for DES as Stackelberg leader. Similarly, the cost of destroying more than $\overline{\overline{D}}$ links or nodes exceeds DIS's benefit from destroying more than $\overline{\overline{D}}$ links or nodes. ■■

3.1 Existence

On the basis of Lemma 1 and its proof, each player will choose from a finite set of alternatives when acting in his or her interest. Therefore, the game is essentially finite. A finite game, however, need not have a Nash equilibrium in pure strategies. In contrast, a finite Stackelberg game with a leader and a follower does have a Stackelberg equilibrium.[7]

Proposition 1. *There exists a Stackelberg equilibrium.*

PROOF. For each $g^1 \in M$, the set

$$S(g^1) = \{(H,h) : H \subseteq V^1, h \subseteq g'(V^1 \setminus H,\, g^1), |H| + |h| \leq \overline{\overline{D}}\}$$

[7]The situation might be different with several leaders or several followers.

is finite and non-empty. Hence the set

$$S^*(g^1) = \underset{\substack{H \subseteq V^1 \\ h \subseteq g'(V^1 \setminus H,\, g^1)}}{\arg\max} \{-v(V^1 \setminus H, g'(V^1 \setminus H,\, g^1) \setminus h) - \mathfrak{C}(|H| + |h|)\}$$

is non-empty. Choose $(H(g^1), h(g^1)) \in S^*(g^1)$, with resulting residual network $G^2(g^1) = (V^2(g^1), g^2(g^1)) = (V^1 \setminus H(g^1), g'(V^1 \setminus H(g^1), g^1) \setminus h(g^1)$.

The set $T = \{g^1 : |g^1| \leq \overline{\overline{B}}\}$ is finite and non-empty. Hence the set

$$T^* = \underset{g^1 \in T}{\arg\max} \{v(G^2(g^1)) - \mathfrak{c}(|g^1|)\}$$

is non-empty. Choose $g^{1*} \in T^*$.

Then the family $\{g^{1*}, ((H(g^1), h(g^1))_{g^1 \in M}\}$ constitutes a Stackelberg equilibrium. ■ ■

3.2 Uniqueness

Equilibrium outcomes need not be unique. The best one can hope for is equality of DES's payoffs across equilibria. However, that need not be the case either as the following example shows.

Example 1. Let $N = 4$, $v = v^*$, $\mathfrak{c}(x) = 0.3x$ for $x = 0, 1, 2$, $\mathfrak{c}(3) = 1.15$, $\mathfrak{c}(4) = 1.75$, $\mathfrak{c}(5) = 2.4$, $\mathfrak{c}(6) = 3.6$, and $\mathfrak{C}(0) = 0$, $\mathfrak{C}(1) = 0.95$, $\mathfrak{C}(x) = 1.2x$ for $x = 2, \ldots, 6$. Let us rule out multi-graphs, which will be justified later. Let $B = |g^1|$.

- If $B = 0$, then $\mathfrak{U}_{DES} = 1$.
- If $B = 1$, DIS will attack one of the endpoints of the single link, resulting in $\mathfrak{U}_{DES} = 1 - 0.3 = 0.7$.
- If $B = 2$ and, for instance g^1 has links 12 and 34, then to reduce $v(G^1) = 2$ by 1, DIS would have to attack at least two nodes or links — which costs more than 1. Hence $\mathfrak{U}_{DES} = 2 - 0.6 = 1.4$.

- If $B = 3, 4, 5$, then g^1 is connected and missing at least one link, say 12. All nodes will be isolated if DIS attacks nodes 3 and 4. Then DIS has a gain of benefit 3 at a cost of 2.4. If g^1 is a star, attacking merely the center of the star will do. If g^1 is a line, DIS's best choice is reducing v by 2 by attacking one node. In any case, $\mathfrak{U}_{DES} \leq 2 - 1.15 = 0.85$.
- If $B = 6$, then DIS will attack one node, yielding $\mathfrak{U}_{DES} = 3 - 3.6 = -0.6$.

In some instances, the disruptor is indifferent between deleting links or nodes. But in all cases, the disruptor can inflict maximal damage by attacking only nodes. Since duplicating links does not provide added protection against node attacks, the network designer would incur unnecessary costs when resorting to multi-graphs. Hence we can disregard the possibility of multi-graphs. It follows that there is one type of Stackelberg equilibria. DES chooses the network g^{1*} with the two links 12 and 34 (or a network with the same architecture) and DIS plays a best response against any choice of g^1. DES obtains equilibrium utility $\mathfrak{U}_{DES} = 1.4$.

Notice that if *ceteris paribus* $\mathfrak{C}(1) = 1.2$, then DIS does not attack a network with $B = 1$, resulting in $\mathfrak{U}_{DES} = 1.7$. Hence such networks become the only equilibrium choice of DES.

Finally, let us consider another variant of the example where *ceteris paribus* $\mathfrak{C}(1) = 1$. Then in case $B = 1$, DIS is indifferent between not attacking and attacking the single link or one of the endpoints of the link. This implies that there are two types of Stackelberg equilibria, the type of equilibria from above with the stipulation that DIS attacks when $B = 1$ and a second type where DES chooses $B = 1$ and DIS does not attack given that choice. Now the payoff for DES is no longer equalized across equilibria: DES prefers the second type, which yields payoff 1.7. □□

In the version of the example where $\mathfrak{C}(1) = 1$, the reason for multiple equilibrium payoffs for DES is the fact that the Stackelberg follower DIS has two best responses against $B = 1$, associated with different payoffs for DES. The following condition rules out that possibility:

(C) Best Response Independence of Leader Payoffs:
For each g^1, if both $G^2 = (V^2, g^2)$ and $\widehat{G}^2 = (\widehat{V}^2, \widehat{g}^2)$ result from a best response of DIS against g^1, then $v(G^2) = v(\widehat{G}^2)$.

In case (C) holds, we can assign to every g^1 an "indirect utility" $u(g^1) = v(G^2)$ where G^2 results from some best response against g^1.

Proposition 2. *If (C) is satisfied, then DES obtains the same payoff in all Stackelberg equilibria.*

PROOF. (C) implies that we can assign a net utility $U(g^1) = u(g^1) - \mathfrak{c}(|g^1|)$ to every g^1. In equilibrium, DES chooses a g^1 that maximizes U. Hence the assertion. ■■

Corollary 1. *Suppose v assumes values in $\mathbb{Q}$, the set of rational numbers; $\mathfrak{c}(x) = c \cdot x$ and $\mathfrak{C}(x) = C \cdot x$ for $x = 0, 1, \ldots$, with $c > 0$ and $C > 0$ irrational numbers. Then (C) holds and DES obtains the same payoff in all Stackelberg equilibria. Moreover, if g^{1*} and $\overline{g}^{1*}$ are both Stackelberg equilibrium choices by DES, then $u(g^{1^*}) = u(\overline{g}^{1*})$ and $|g^{1*}| = |\overline{g}^{1*}|$.*

PROOF. First, take any choice g^1 of DES and let G^2 and $\widehat{G}^2$ be the results of two best responses against g^1 where DIS deletes D and $\widehat{D}$ lines or nodes, respectively. Then the two best responses yield identical payoffs to DIS, that is, $-v(G^2) - C \cdot D = -v(\widehat{G}^2) - C \cdot \widehat{D}$. Hence $v(\widehat{G}^2) - v(G^2) = C \cdot (D - \widehat{D})$. Now the left-hand side of this equation is a rational number whereas the right-hand side is irrational unless $D = \widehat{D}$. Hence $D = \widehat{D}$ and, consequently, $v(G^2) = v(\widehat{G}^2)$. We have shown (C): For each g^1, if both G^2 and $\widehat{G}^2$ result from a best response of DIS against g^1, then $v(g^2) = v(\widehat{g}^2)$.

Second, the validity of (C) implies that DES obtains the same payoff in all Stackelberg equilibria (by Proposition 2).

Third, let g^{1*} and $\overline{g}^{1*}$ be both Stackelberg equilibrium choices by DES. The respective payoffs are $U(g^{1*}) = u(g^{1^*}) - c \cdot |g^{1*}|$ and $U(\overline{g}^{1*}) = u(\overline{g}^{1*}) - c \cdot |\overline{g}^{1*}|$, which both maximize $U(g^1) = u(g^1) - c \cdot |g^1|$. Hence $u(g^{1^*}) - c \cdot |g^{1*}| = u(\overline{g}^{1*}) - c \cdot |\overline{g}^{1*}|$. By the same argument as in the first part, $u(g^{1^*}) = u(\overline{g}^{1*})$

and $|g^{1*}| = |\overline{g}^{1*}|$ as asserted. ■■

3.3 Comparative Statics

One might expect that if link formation becomes more costly for the network designer, then DES creates fewer links in equilibrium. If (C) holds, then it turns out that after an increase in marginal costs, DES will not create more links than in the equilibrium with the least number of links prior to the cost increase.

Proposition 3. *Let*
$\mathcal{G}$ *be a game given by* $V^1, \mathfrak{c}(\cdot), \mathfrak{C}(\cdot)$, *and* v *and*
$\widetilde{\mathcal{G}}$ *be a game given by* $V^1, \widetilde{\mathfrak{c}}(\cdot), \mathfrak{C}(\cdot)$, *and* v.
Suppose (C), that is "Best Response Independence of Leader Payoffs" and

(i) $\widetilde{\mathfrak{mc}}_+(x) > \mathfrak{mc}_+(x)$ *for* $x = 0, 1, \ldots$.

If $\{g^{1*}, \ldots\}$ *is a Stackelberg equilibrium of* $\mathcal{G}$ *and* $\{\widetilde{g}^{1*}, \ldots\}$ *is a Stackelberg equilibrium of* $\widetilde{\mathcal{G}}$, *then* $|g^{1*}| \geq |\widetilde{g}^{1*}|$.

PROOF. Because of (C), DES's decision problem amounts to maximization of $U(g^1) = u(g^1) - \mathfrak{c}(|g^1|)$ in $\mathcal{G}$ and to maximization of $\widetilde{U}(g^1) = u(g^1) - \widetilde{\mathfrak{c}}(|g^1|)$ in $\widetilde{\mathcal{G}}$. Consider a Stackelberg equilibrium $\{g^{1*}, \ldots\}$ of $\mathcal{G}$ and a Stackelberg equilibrium $\{\widetilde{g}^{1*}, \ldots\}$ of $\widetilde{\mathcal{G}}$. Then

(ii) $u(g^{1*}) - \mathfrak{c}(|g^{1*}|) \geq u(\widetilde{g}^{1*}) - \mathfrak{c}(|\widetilde{g}^{1*}|)$;

(iii) $u(\widetilde{g}^{1*}) - \widetilde{\mathfrak{c}}(|\widetilde{g}^{1*}|) \geq u(g^{1*}) - \widetilde{\mathfrak{c}}(|g^{1*}|)$.

Suppose $|g^{1*}| < |\widetilde{g}^{1*}|$. This together with (i) and (ii) implies
$\widetilde{\mathfrak{c}}(|\widetilde{g}^{1*}|) - \widetilde{\mathfrak{c}}(|g^{1*}|) > \mathfrak{c}(|\widetilde{g}^{1*}|) - \mathfrak{c}(|g^{1*}|) \geq u(\widetilde{g}^{1*}) - u(g^{1*})$ and, consequently, $u(g^{1*}) - \widetilde{\mathfrak{c}}(|g^{1*}|) > u(\widetilde{g}^{1*}) - \widetilde{\mathfrak{c}}(|\widetilde{g}^{1*}|)$. But the latter contradicts (iii). Hence to the contrary, $|g^{1*}| \geq |\widetilde{g}^{1*}|$ has to hold. ■■

If (C) or (i) fails to hold, merely increasing the costs for DES need not yield the conclusion $|g^{1*}| \geq |\widetilde{g}^{1*}|$. In case the costs for DIS are increased,

the comparative statics can go either way. On the one hand, since DIS is less likely to attack a given network (or carries out a more moderate attack), DES may achieve a certain outcome G^2 with less investment in links. On the other hand, the more restrained response of DIS may induce DES to aim for a more valuable outcome than the original G^2 and invest more.

3.4 Sensitivity with Respect to the Value Function

Hoyer and De Jaegher (2015) work with the specific value function v^*, which facilitates their analysis. They suggest that v^* is an approximation for other convex v. They also provide two instances, in their footnotes 10 and 26, where it serves that purpose well. In general, however, equilibrium outcomes can be very sensitive to the choice of value function as the following example illustrates.

Example 2. Let $N = 7$, $\mathfrak{c}(x) = \epsilon \cdot x$ for $x = 0, 1, \ldots, 7$, with $\epsilon \approx 0$, $\mathfrak{c}(x) > 49$ for $x > 7$, $\mathfrak{C}(1) = 1.2$, $\mathfrak{C}(2) = 2.5$, and $\mathfrak{C}(x) > 49$ for $x > 2$. We assume until further notice that DIS is restricted to node attacks. We distinguish candidates for g^{1*} by the size of the largest component, i.e., by $\|g^1\| = v^*(V^1, g^1)$.

PART I: $v = v^*$. In case $\|g^1\| = 7$, there are three possibilities. (a) g^1 is minimally connected. By Proposition 5, after an optimal attack by DIS, the remaining largest component will have at most size $\lceil 5/3 \rceil = 2$. (b) There are seven links and the largest component contains a node j with degree 1. Then DIS will delete the neighbor of j and a second node different from j so that $v(G^2) \leq 4$ and DES obtains at most payoff $4 - 7\epsilon$. (c) If g^1 is a circle, DIS will delete two nodes so that a component of size 2 and a component of size 3 are left.

$\|g^1\| = 6$. If the largest component contains a node j with degree 1, then DIS will delete the neighbor of j and a second node different from j so that $v(G^2) \leq 3$. If each node in the component has degree 2, then the component is a circle and DIS will delete two nodes so that two components of size 2 are left. If each node in the component has degree at least 2, there remain two possibilities. Either there are two nodes with degree 3 or there is one node

of degree 4. In both cases, if a node i with degree greater than 2 is deleted, then there is a node j with a single neighbor k in the reduced component. Hence deletion of i and k yields $v(G^2) \leq 3$ and is in DIS's interest.

$\|g^1\| = 5$. If the largest component contains a node j with degree 1, then DIS will delete the neighbor of j and a second node different from j so that $v(G^2) \leq 2$. If each node in the component has degree 2, then the component is a circle and DIS will delete two nodes so that a components of size 2 and a component of size 1 are left. If each node in the component has degree at least 2, then there can be at most four nodes with degree greater than 2. Let i be a node with degree 2. Deletion of its two neighbors yields $v(G^2) \leq 3$ and is in DIS's interest.

$\|g^1\| = 4$. If the largest component constitutes a complete subgraph, then deletion of one node leaves a component of size 3 and deletion of two nodes leaves a component of size 2. Hence DIS abstains from attacking and $v(G^2) = 4$. If a pair of nodes i and j in the largest component is not directly linked, then DIS will delete the other two nodes of the component so that i and j become isolated.

It follows that in each Stackelberg equilibrium of the game $\mathcal{G}^*$ given by V^1, $\mathfrak{c}(\cdot)$, $\mathfrak{C}(\cdot)$, and v^*, DES chooses a g^{1*} consisting of a completely connected component of size 4 plus 3 isolated nodes, using only 6 links — and DIS refrains from attacking when g^{1*} is chosen. Then DES obtains payoff $4 - 6\epsilon$.

PART II: $v = v^{\square}$. First, consider g^{1*} consisting of a completely connected component of size 4 plus 3 isolated nodes — which would be a Stackelberg equilibrium outcome when $v = v^*$. Now with value function $v^{\square}$, DIS deletes two nodes regardless of the choice of g^1. In particular, given g^{1*}, DIS deletes two nodes of the largest component so that the residual graph $G^2 = (V^2, g^2)$ consists of three isolated points and a component of size 2. Consequently, DES achieves payoff $3 \cdot 1^2 + 2^2 - 6\epsilon = 7 - 6\epsilon$. In all other cases with $\|g^1\| = 4$, at best DES is left with a component of size 3 and two isolated points, hence a payoff less than 11.

Alternatively, consider the circle with seven nodes. The best attack for DIS leaves a component of three nodes and a component of two nodes, yielding payoff $3^2 + 2^2 - 7\epsilon = 13 - 7\epsilon$ to DES. It follows that DES does not choose any g^1 with $\|g^1\| = 4$ in a Stackelberg equilibrium of the game $\mathcal{G}^{\square}$ given by V^1, $\mathfrak{c}(\cdot)$, $\mathfrak{C}(\cdot)$, and $v^{\square}$.

Comparison of PARTS I and II shows that different value functions can lead to completely different equilibrium network architectures.

FLEXIBLE MODE OF ATTACK. Our conclusion persists when DIS can delete a total of two nodes or links. First, since a completely connected component with four nodes is a 3-regular graph, it remains connected after the removal of two links. Second, removal of one link and one node leaves a connected component with two nodes. In both cases, DIS does not want to attack. It follows that DES chooses g^{1*} consisting of a completely connected component of size 4 plus 3 isolated nodes in each Stackelberg equilibrium of the game $\mathcal{G}^*$ given by V^1, $\mathfrak{c}(\cdot)$, $\mathfrak{C}(\cdot)$, and v^*.

If DIS deletes two links from the circle with seven nodes, he minimizes $v^{\square}$ by leaving a component of size 4 and a component of size 3. If DIS deletes a node and a link from the circle, his best choice is to leave two components of size 3. Hence in both cases, the outcome for DES is better than under a pure node attack. Hence it is still the case that DES does not choose any g^1 with $\|g^1\| = 4$ in a Stackelberg equilibrium of the game $\mathcal{G}^{\square}$ given by V^1, $\mathfrak{c}(\cdot)$, $\mathfrak{C}(\cdot)$, and $v^{\square}$. $\square\square$

Remark 1 is going to present further evidence for the sensitivity of equilibrium outcomes to the choice of value function.

4 Fixed Budgets and Fixed Type of Attack

The argument of Lemma 1 shows that DES will never choose a g^1 with $|g^1| > \overline{\overline{B}}$ and that DIS will never delete nodes and links whose total number exceeds $\overline{\overline{D}}$. But it is conceivable that DES and DIS adhere to smaller bounds $\overline{B} < \overline{\overline{B}}$ and $\overline{D} < \overline{\overline{D}}$, respectively. Prior budgetary commitments can impose such bounds. One can also view the restrictions as capacity constraints. Moreover, DIS may only attack in a particular way. One reason can be the prior adoption of a particular technology. Another reason could be that a different type of attack proves prohibitively costly. It is also conceivable that $\overline{D} > \overline{\overline{D}}$ if DIS is committed to do a certain amount of damage regardless of costs. Following Hoyer and De Jaegher (2015), we are going to explore the consequences of restrictions on budgets or types of attack. Like Hoyer and De Jaegher, we assume $v = v^*$ throughout this section unless stated otherwise.

4.1 Sensitivity to the Mode and Potential Size of an Attack: An Example

Let us begin with an example that demonstrates how some restrictions impact equilibrium outcomes.

Example 3. Let $N = 7$, $\overline{B} = 6$, $\overline{D} = 3$, and $v = v^*$. Suppose that DIS is committed or restricted to attacking only links. Then by Proposition 4, star networks are the only equilibrium choice of the network designer, leading to G^2 with $v(G^2) = 4$.

Alternatively, suppose that DIS is committed or restricted to attacking only nodes. Then deletion of the center of a star leads to G^2 with $v(G^2) = 1$. In fact, by Proposition 5, any minimally connected g^1 leads to a G^2 with $v(G^2) = 1$ when the disruptor causes maximal damage. Checking all possible g^1 shows that there are three network architectures that give rise to a residual network G^2 with $v(G^2) > 1$ when the disruptor causes maximal damage. One consists of two triangles and an isolated node. The second consists of a line with four nodes and a triangle. The third consists of a circle with

five nodes and a pair of nodes. All three result in G^2 with $v(G^2) = 2$. In every Stackelberg equilibrium, the network designer chooses one of the three architectures. Notice, that in some equilibria, neither DES nor DIS uses its full capacity.

If ceteris paribus $\overline{D} = 2$, then three more network architectures can occur as equilibrium choice of g^1:

- A square together with a pair of nodes and an isolated node.
- A circle of six nodes plus an isolated node.
- A line containing all seven nodes.

If ceteris paribus $\overline{D} = 1$, then by Proposition 7, a circle of six nodes plus an isolated node constitutes the unique network architecture that qualifies as equilibrium choice of g^1. □□

The example shows that both the type and the potential size of an attack affect equilibrium play. Both the number and the architecture of DES's equilibrium choices vary with the type and the potential size $\overline{D}$ of an attack. Notice that there is no monotonic relationship between $\overline{D}$ and the number of various network architectures that may occur in equilibrium.

Remark 1. Observe that in the example, sometimes the equilibrium choice of g^1 has nontrivial components together with an isolated node. This would never happen with the value function $v^\bullet$ used by Dziubiński and Goyal (2013). In that case, either g^1 is empty or (V^1, g^1) is connected in equilibrium.

4.2 Some General Results

Here we report some general results of Hoyer and De Jaegher (2015) that are of interest in our context. Several of their findings have been referred to in the last two examples.

Proposition 4 (HDJ, Proposition 2)**.** *Suppose the disruptor attacks only links,* $N > 5, \overline{B} = N - 1, 1 < \overline{D} < N - 1$*. Then the designer's best choice is a star network.*

Proposition 5 (HDJ, Lemma 4)**.** *Given any minimally connected network g^1, a disruptor who only attacks nodes can assure that the remaining network G^2 satisfies $v(G^2) \leq \lceil (N - \overline{D})/(\overline{D} + 1) \rceil$.*[8]

Proposition 6 (HDJ, Lemma 5)**.** *If the disruptor only attacks nodes and g^1 is a circle with $N - 1$ nodes, then the disruptor inflicts maximal damage by cutting the network into $\overline{D}$ separate components, each maximally of order $\lceil (N - 1 - \overline{D})/\overline{D} \rceil$.*

Proposition 7 (HDJ, Proposition 3)**.** *If the disruptor only attacks nodes, $\overline{B} = N - 1$, $\overline{D} = 1$, then the designer's unique equilibrium network architecture consists of a circle of $N - 1$ nodes and an isolated node, resulting in G^2 with $v(G^2) = N - 2$ under a most damaging attack.*

Remark 2. Suppose that under the hypothesis of Proposition 7, a link can be traded for immunizing a node against attacks. Then the network consisting of a star of $N-1$ nodes with an immunized center plus an isolated node constitutes a second equilibrium network architecture, even though stars without an immunized center are very vulnerable to node attacks. Hence the possibility to immunize nodes against attacks makes a difference. Stars with an immunized center do also arise as equilibrium network architectures in some instances of the model of Dziubiński and Goyal (2013).

4.3 Preference for Mode of Attack

Suppose a network contains a link from node i to node j. We assume throughout that deletion of one of the two nodes, say i, has potentially several effects, as is typically the case in communication networks.[9] First, it renders the link at hand dysfunctional which can also be achieved by deleting the link. In addition, it eliminates the node i and, thus, reduces the cardinality of the component containing i and j, even if the rest of the component remains

[8] For $r \in \mathbb{R}$, $\lceil r \rceil$ denotes the smallest integer greater than or equal to r.

[9] As an exception, deletion of a node may not have any further effect in a road network: The roads originating from a location may remain intact when the location becomes inoperative.

connected, an effect that does not occur under link deletion. Also, deletion of i renders all the direct links of i, not just the one to j dysfunctional, in case i has more than one direct link. Hence deletion of a node is at least as effective as deletion of one of its direct links — and often more effective. This observation has immediate consequences:

Proposition 8. *Let V^1, $\mathfrak{c}(\cdot)$, $\mathfrak{C}(\cdot)$, $\overline{B}$, $\overline{D}$, and an arbitrary v be given.*

(a) *Consider the game $\mathcal{G}$ where DIS can attack combinations of nodes and links and the game $\mathcal{G}'$ where DIS can only attack nodes. Then g^{1*} is the action of DES in some Stackelberg equilibrium of $\mathcal{G}$ if and only if it is the action of DES in some Stackelberg equilibrium of $\mathcal{G}'$.*

(b) *Consider further the game $\mathcal{G}''$ where DIS can only attack links. Then DES does not fare worse (and sometimes fares better) in a Stackelberg equilibrium of $\mathcal{G}''$ than in a Stackelberg equilibrium of $\mathcal{G}'$.*

PROOF. (a) Suppose DIS can choose combinations of nodes and links to delete. For any best response against a choice g^1 of DES, there exists an equally good response where DIS only deletes nodes. Hence if DIS plays best responses in $\mathcal{G}$ that yield residual networks $G^2(g^1)$, then there exist best responses in $\mathcal{G}'$ that render residual networks $G^{2\prime}(g^1)$ such $v(G^{2\prime}(g^1)) = v(G^2(g^1))$. Hence if g^{1*} maximizes $v(G^2(g^1)) - \mathfrak{c}(|g^1|)$, then it maximizes $v(G^{2\prime}(g^1)) - \mathfrak{c}(|g^1|)$. This shows the "only if" part.

Conversely, if DIS plays specific best responses in $\mathcal{G}'$ that yield residual networks $G^{2\prime}(g^1)$, then these are also best responses in $\mathcal{G}$, yielding the same residual networks. Hence a Stackelberg equilibrium of $\mathcal{G}'$ is also a Stackelberg equilibrium of $\mathcal{G}$. This shows the "if" part.

(b) Let $G^{2\prime\prime}(g^1)$ be the outcomes of best responses of DIS in some Stackelberg equilibrium of $\mathcal{G}''$ and $G^{2\prime}(g^1)$ be the outcomes of best responses of DIS in some Stackelberg equilibrium of $\mathcal{G}'$. Since node attacks are at least as effective as link attacks, it follows that $v(G^{2\prime\prime}(g^1)) \geq v(G^{2\prime}(g^1))$ for all g^1. It follows that

$$\max_{g^1} [v(G^{2\prime\prime}(g^1)) - \mathfrak{c}(|g^1|)] \geq \max_{g^1} [v(G^{2\prime}(g^1)) - \mathfrak{c}(|g^1|)]$$

where the first maximum is DES's payoff in the first equilibrium and the second maximum is DES's payoff in the second equilibrium. In Example 3, DES fares better under link attacks. ■■

There is one instance where node attacks are always better for DIS and worse for DES than link attacks. Suppose the disruptor has a fixed budget $\overline{D} \in \{1, \ldots, N-2\}$ that allows him to attack a total of $\overline{D}$ links or nodes. Suppose further that DES is willing to invest in a network g^1 that offers maximal protection against a node attack of size $\overline{D}$, that is, after deletion of any $\overline{D}$ nodes of V^1, a connected network G^2 with $N-\overline{D}$ nodes remains. Then if instead $\overline{D}$ links in (V^1, g^1) were deleted, a connected network $(V^1, g^{1\prime})$ with N nodes would result, clearly a worse outcome for DIS and a better outcome for DES.

This conclusion follows from a graph-theoretic inequality due to Hassler Whitney.[10] For a graph G, define its connectivity $\kappa(G)$ as the minimum number of nodes whose removal results in a disconnected graph (or a trivial graph with a single node) and its link-connectivity $\lambda(G)$ as the minimum number of links whose removal results in a disconnected or trivial graph. Whitney's theorem asserts $\lambda(G) \geq \kappa(G)$. In the case at hand, $\kappa(V^1, g^1) > \overline{D}$. Hence $\lambda(V^1, g^1) > \overline{D}$. One can show by means of an induction argument: Suppose g^1 offers maximal protection against a node attack of size $\overline{D}$. If DIS launches a combined attack, deleting D_n nodes and D_l links so that $D_n + D_l = \overline{D}$, then the maximal damage inflicted is increasing in D_n.

Remark 3. The fact that DIS never strictly prefers link attacks hinges on the assumption that the cost of an attack depends on the total size of the attack, $D = D_l + D_n$. Suppose that in Example 1, node attacks are slightly more expensive than link attacks, say by 0.01 per attacked node. Then in case $B = 1$, DIS prefers attacking the single link to attacking one of the endpoints of the links whereas in case $B = 6$, DIS will attack one node. Hence rather small cost differences between link and node attacks can make a significant difference.

[10] See Whitney (1932, Theorem 5), Harary (1969, Theorem 5.1).

4.4 Duplicate Links (Multigraphs) and Redundancies

Duplicate links do not provide added protection against node attacks. But they can be effective against link attacks as the following example shows.

Example 4. Suppose that DIS is restricted to link attacks. Let $N = 4$, $\mathfrak{c}(x) = 0.49x$ for $x = 0, 1, \ldots$ and $\mathfrak{C}(x) = 0.51x$ for $x = 0, 1, \ldots$. Then DIS will not attack the complete network, but will delete all links of all other non-empty graphs g^1. Hence in the Stackelberg equilibrium, DES chooses $g^{1*} = g^c$, DIS does not attack g^{1*} and deletes all links of non-empty $g^1 \neq g^c$.

Next consider $\mathfrak{c}(\cdot)$ as before and $\mathfrak{C}(x) = 0.49x$ for $x = 0, 1, \ldots$. Then DIS will delete every link in any network with simple links and DES chooses $g^{1*} = \emptyset$ in equilibrium.

Finally, suppose that $\mathfrak{c}(x) = 0.29x$ for $x = 0, 1, \ldots$ and $\mathfrak{C}(x) = 0.49x$ for $x = 0, 1, \ldots$. Then DIS does not attack the network of Figure 2 consisting of a 4-node circle with double links plus two diagonal links and DES prefers forming that multi-graph to $g^1 = \emptyset$. This shows that DES might form a multi-graph if it is the only way to guarantee a non-trivial network and its formation is not too costly.

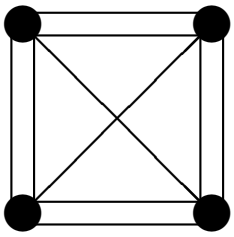

Figure 2

One obtains an equilibrium network architecture by removing one vertical and one horizontal link. □□

Remark 4. If the sole objective is to protect the network against targeted attacks or random failure, then redundant links can be desirable. Indeed, redundant links may occur in equilibrium when the costs of links formation are

sufficiently low like in Example 4. However, if the costs of link formation are high as in Example 1, then equilibrium networks tend to lack redundancies. Cost considerations are also the main reason in practice why redundancies are not implemented in communication networks. In their study of the long-haul fiber-optic infrastructure of the US, Durairajan et al. (2015) observe a significant amount of infrastructure sharing for economic reasons, which reduces the resilience of the network. A few new fiber routes would reduce risk and delays.

4.5 Random Failure versus Targeted Attack

The findings of Albert et al. (2000) and Barrat et al. (2008, Ch. 6) suggest that heterogeneous networks suffer less from wide-spread random failure of nodes than homogeneous networks. The reason is that crucial nodes are deleted with fairly small probability. In contrast, a targeted attack of comparable size would delete first the nodes most crucial for the connectivity of the network, then the second most crucial nodes, and so on. This renders heterogeneous networks more vulnerable than homogeneous networks that do not have any distinguished nodes. Albert et al. (2000) take the "giant components" of realizations of random graphs as ex ante networks; an exponential network as proxy for a homogeneous network and a scale-free network as an instance of an inhomogeneous network. The basic arguments also apply in our context. Let us consider an example with $N = 4n$ where n is a large natural number. We consider a star with center 1 as an instance of a heterogeneous network and the circle as an instance of a homogeneous network and assume that half of the nodes are removed. We measure the damage by $\Delta = v^*(V^1, g^1) - v^*(V^2, g^2)$ where (V^1, g^1) is the ex ante network and (V^2, g^2) is the ex post network. The expected damage in case of random failure is denoted $E\Delta$. In either case, $v^*(V^1, g^1) = N = 4n$.

Targeted Attack
In the case of the star, it suffices to delete the center to obtain $v^*(V^2, g^2) = 1$. In the case of the circle, going around the circle and deleting every second

node results in $v^*(V^2, g^2) = 1$. In both cases, $\Delta = 4n - 1$.

Random Failure on the Star
The number of subsets of nodes of size $2n$ is

$$\begin{aligned}\binom{4n}{2n} &= \frac{(4n)!}{(2n)!(2n)!} \\ &= \frac{4n(4n-1)!}{n(2n-1)!(2n)!} \\ &= 4 \cdot \frac{(4n-1)!}{(2n-1)!(2n)!}.\end{aligned}$$

The number of subsets of nodes of size $2n$ that contain node 1, the center of the star is

$$\binom{4n-1}{2n-1} = \frac{(4n-1)!}{(2n-1)!(2n)!}.$$

Hence the probability that a random sample of size $2n$ contains the center of the star is $1/4$. It follows that the expected damage caused by the random failure of $2n$ nodes is

$$E\Delta = \frac{1}{4} \cdot (4n-1) + \frac{3}{4} \cdot 2n = \frac{5}{2}n - \frac{1}{4}.$$

Random Failure on the Circle
Let C be a subset of nodes of size n that constitutes a path of length $n - 1$. The number of subsets of nodes of size $2n$ that contain C is

$$\binom{3n}{n} = \frac{(3n)!}{n!(2n)!}.$$

Hence the probability that a random sample of size $2n$ contains C is

$$\begin{aligned} & \frac{(3n)!}{n!(2n)!} \Big/ \frac{(4n)!}{(2n)!(2n)!} \\ = & \frac{(3n)!(2n)!}{(4n)!n!} \\ = & \frac{2n \cdot \ldots \cdot (n+1)}{4n \cdot \ldots \cdot (3n+1)} \\ = & \prod_{k=0}^{n-1} \frac{2n-k}{4n-k} < \left(\frac{1}{2}\right)^n . \end{aligned}$$

Therefore,

$\mathsf{Prob}(v^*(V^2, g^2) \geq n) < 4n \cdot (\frac{1}{2})^n$ and

$\mathsf{Prob}(\Delta > 3n) = \mathsf{Prob}(v^*(V^2, g^2) < n) > 1 - 4n \cdot (\frac{1}{2})^n$, which implies

$E\Delta > \mathsf{Prob}(\Delta > 3n) \cdot 3n > (1 - 4n \cdot (\frac{1}{2})^n) \cdot 3n$.
It follows that $E\Delta > 3n - \frac{1}{4}$ for sufficiently large n.

Comparison
The comparison shows that the circle incurs more damage under random failure than the star. If $\overline{D}$, the number of failing nodes increases from 1 to $4n$, $E\Delta$ increases in both cases, with maximum value $4n$ at $\overline{D} = 4n$. Typically, the star incurs less damage than the circle.

Under a targeted attack of size $2n$, the damage is $4n-1$ for both the star and the circle. However, as we vary the size of the attack from $\overline{D} = 1$ to $\overline{D} = 4n$, a drastic difference between the two network architectures appears. In the case of the star, $\Delta = 4n - 1$ for $\overline{D} = 1, \ldots, 4n - 1$ while $\Delta = 4n$ for $\overline{D} = 4n$. In contrast, Proposition 6 yields for the circle that $v^*(V^2, g^2) = \lceil (4n - \overline{D})/\overline{D} \rceil = \lceil 4n/\overline{D} \rceil - 1$ as a function of $\overline{D}$ that first strictly decreases and then weakly decreases. Hence Δ first strictly increases and eventually weakly increases in $\overline{D}$, beginning with 1, 301, 401, 451, 481, 501, 515, 526, 534, 541, 546, 551, 558, 561, 563, 565, 567, 569, 571, 572, 573, 574, 576, 577,

577, 578, 579, 580, 581, 581, etc.

To conclude, the qualitative conclusions in the context of large random graphs are by and large confirmed in our example.

Link Deletion
One can alternatively consider the deletion of $2n$ links from the star or the circle. In the case of the star, random failure and targeted attack have the same effect. There always remains a connected component of size $2n$ so that $\Delta = 2n$ and $E\Delta = 2n$. Due to the special features of the circle, the analysis of random failure and of targeted attacks is essentially the same as for node deletion: A targeted attack results in $\Delta = 4n - 1$. Random failure yields $E\Delta > 3n - 1/4$ for sufficiently large n.

Remark 5. Christophe Bravard has pointed out that the consequences of targeted attacks correspond to the worst outcomes under random failure. In other words, one may attempt to minimize either the average damage or the greatest possible damage under random failure. A similar distinction plays a role in studies of computational complexity: For example, Klee and Minty (1972) show for the classical simplex algorithm of linear programming that "the number of pivots or iterations that may be required is not majorized by any polynomial function of the two parameters that specify the size of the program." In contrast, Borgwardt (1982) finds for a variant of the simplex algorithm an explicit upper bound for the expected number of pivot steps, which is polynomial in the size parameters. Both results have been extended to various versions of the simplex algorithm. Notice, however, that average running times depend on the assumed distribution of the parameters.

5 Concluding Remarks

We have analyzed the Stackelberg equilibria of a designer-disruptor game where the designer creates the links of a network and subsequently the disruptor deletes some links or nodes. Our investigations confirm the view that network topology or architecture matters, both for performance and for

vulnerability. We have not attempted to provide a comprehensive characterization of equilibrium network architectures. Such a characterization seems a formidable task. Indeed, the most closely related literature, Hoyer and De Jaegher (2015) and Dziubiński and Goyal (2013), falls short of a full characterization.

Variable Strength of Links and Nodes. Dziubiński and Goyal (2013) allow the designer to form links, but also to render some or all of the nodes immune against attacks. Bravard and Charroin (2015) allow the designer to choose between destructible and indestructible links. In contrast, we consider the possibility of multiple links and, hence, multigraphs.[11] Multiple direct links between two nodes make it more costly for the disruptor to interrupt the direct connection between the two nodes. A conceivable extension of our model would allow the designer to choose variable strengths for links and nodes. A network might be described by a generalized adjacency matrix (g_{ij}) where for $i \neq j$, g_{ij} indicates how much it would cost the disruptor to delete the link between i and j whereas g_{ii} stands for the cost of deleting node i. Then $g_{ii} = \infty$ would represent the extreme case where i is immune against deletion.

Other Scenarios. Future research could examine cyber warfare where both sides are designer of a network as well as disruptor of each other's network. A player has to decide how much of the available resources to each task, network design and network disruption. A different extension could look at situations where a designer creates links, but also some of the nodes of the network.

Common Enemy Effects. Changes of behavior, like the frequently observed common enemy effect, can often be explained by a change of preferences. The typical common enemy effect consists in a group of people showing more cohesion when confronted with an outside threat. Hoyer and

[11] Multigraphs appear also in Bravard and Charroin's (2015) condensation networks, an auxiliary construction.

De Jaegher (2012) present a designer-disruptor game of network formation with a group of designers as Stackelberg leaders and a single disruptor as follower. The designers play a specific network formation game known as the two-way information flow model without decay. The disruptor subsequently deletes some of the links. Presence of the disruptor does not alter the designers' preferences, but nonetheless can effect their equilibrium behavior. A more connected network would indicate a positive common enemy effect. On the one hand, additional links may be created if they protect against disruption. On the other hand, some link may no longer be formed because it is bound to be deleted or is worth less when disruption occurs. Hoyer and De Jaegher (2012) find that for low linkage costs, there is a negative common enemy effect in that the pairwise stable networks are less connected than they would be otherwise and aggregate welfare declines even if one disregards the destruction of some of the formed links. For high linkage costs, a positive common enemy effect is found. Hence strategic interaction with stable preferences can generate positive or negative common enemy effects.

Hoyer and De Jaegher (2012) employ pairwise stability as the solution concept for the designer game at the first stage. In contrast, Haller and Hoyer (2015) resort to Nash equilibrium in the first-stage game. This constitutes more strategic behavior on the part of the designers and partially reverses the prior findings: For sufficiently low linkage costs, the external threat can lead to a more connected network. For very high but not prohibitively high linkage costs, the equilibrium network can be minimally connected and efficient in the absence of the external threat whereas it is always empty and inefficient in the presence of the external threat. These results confirm the previous insight of Hoyer and De Jaegher that strategic interaction alone can generate positive or negative common enemy effects, without reliance on psychological or other explanations. They provide the novel insight that the sign of the common enemy effect also depends on the intensity of strategic behavior.

References

Albert, R., Jeong, H., Barabási, A.-L., 2000: "Error and Attack Tolerance of Complex Networks", *Nature*, 406, 378-382.

Anderlini, L., Ianni, A., 1996: "Path Dependence and Learning from Neighbours," *Games and Economic Behavior*, 13, 141-177.

Bala, V., Goyal, S., 2000: "A Non-Cooperative Model of Network Formation", *Econometrica,* 68, 1181-1229.

Barrat, A., Barthélemy, M., Vespignani, A., 2008: *Dynamic Processes on Complex Networks*. Cambridge University Press: Cambridge, New York.

Berninghaus, S.K., Schwalbe, U., 1996a: "Evolution, Interaction, and Nash Equilibria," *Journal of Economic Behavior and Organization*, 29, 57-85.

Berninghaus, S.K., Schwalbe, U., 1996b: "Conventions, Local Interaction, and Automata Networks," *Journal of Evolutionary Economics*, 6, 297-312.

Blume, L.E., 1993: "The Statistical Mechanics of Strategic Interaction," *Games and Economic Behavior*, 5, 387-424.

Blume, L.E., 1995: "The Statistical Mechanics of Best-Response Strategy Revisions," *Games and Economic Behavior*, 11, 111-145.

Borgwardt, K.-H., 1982: "The Average Number of Pivot Steps Required by the Simplex-Method is Polynomial," *Zeitschrift für Operations Research*, 26, 157-177.

Bravard, C., Charroin, L., 2015: "Optimal Design and Defense of Networks under Link Attacks," WP 1519, GATE Lyon Saint-Étienne.

Durairajan, R., Paul Barford, P., Sommers, J., Willinger, W., 2015: "InterTubes: A Study of the US Long-haul Fiber-optic Infrastructure," *SIGCOMM '15*, 565-578.

Dziubiński, M., Goyal, S., 2013: "Network Defence and Design," *Games and Economic Behavior*, 79, 30-43.

Ellison, G., 1993: "Learning, Local Interaction, and Coordination," *Econometrica*, 61, 1047-1071.

Erdös, P., Rényi, A., 1960: "On the Evolution of Random Graphs," *Publications of the Mathematical Institute of the Hungarian Academy of Sciences*, 5, 17-61.

Eusgeld, I., Kröger, W., Sansavini, G., Schläpfer, M., Zio, E., 2009: "The Role of Network Theory and Object-oriented Modeling within a Framework for the Vulnerability Analysis of Critical Infrastructures," *Reliability Engineering and System Safety*, 94, 954-963.

Goyal, S., 2007: *Connections: An Introduction to the Economics of Networks.* Princeton: Princeton University Press.

Goyal, S., Vigier, A., 2014: "Attack, Defense and Contagion in Networks," *Review of Economic Studies*, 81, 1518-1542.

Haller, H., Hoyer, B., 2015: "Note on the Common Enemy Effect under Strategic Network Formation and Disruption," mimeo.

Harary, F., 1969: *Graph Theory.* Perseus Books: Reading, MA.

Hoyer, B., De Jaegher, K., 2012: "Network Disruption and the Common Enemy Effect," *TKI Discussion Paper Series*, 12-06, Utrecht University.

Hoyer, B., De Jaegher, K., 2015: "Strategic Network Disruption and Defense," forthcoming in *Journal of Public Economic Theory*.

Ioannides, Y.M., 1990: "Trading Uncertainty and Market Form," *International Economic Review*, 31, 619-638.

Jackson, M.O., 2008: *Social and Economic Networks.* Princeton: Princeton University Press.

Jackson, M.O., Wolinsky, A., 1996: "A Strategic Model of Economic and Social Networks," *Journal of Economic Theory*, 71, 44-74.

Klee, V., Minty, G.J., 1972: "How Good is the Simplex Algorithm?" pp. 159-175 in Shisha, O. (Ed.): *Inequalities - III*, Academic Press: New York and London.

Landwehr, J., 2015: "Network Design and Imperfect Defense," Working Paper 537, Center for Mathematical Economics, Bielefeld.

Liu, J., Başar, T., 2014: "Toward Optimal Network Topology Design for Fast and Secure Distributed Computation," pp. 234-245 in R. Poovendran, W. Saad (Eds.): *Decision and Game Theory for Security*, Lecture Notes in Computer Science 8840, Proceedings of GameSec 2014, Springer: Cham, Heidelberg et al.

Myerson, R.B., 1977: "Graphs and Cooperation in Games," *Mathematics of Operations Research*, 2, 225-229.

Myerson, R.B., 1991: *Game Theory: Analysis of Conflict*. Harvard University Press: Cambridge, MA.

Vega-Redondo, F., 2007: *Complex Social Networks*. Cambridge University Press: Cambridge, UK.

Whitney, H., 1932: "Graphs and the Connectivity of Graphs", *American Journal of Mathematics*, 54, 150-168.