UNIVERSITY OF CAMBRIDGE
Faculty of Economics

Institute for New Economic Thinking

Cambridge-INET Institute

Cambridge-INET Working Paper Series No: 2015/22

Cambridge Working Paper in Economics: 1565

CONFLICT AND NETWORKS

Marcin Dziubiński (University of Warsaw)
Sanjeev Goyal (University of Cambridge)
Adrien Vigier (University of Oslo)

Conflict remains a central element in human interaction. Networks - social, economic and infrastructure - are a defining feature of society. The two intersect in a wide range of empirical contexts. This motivates the recent interest in conflict and networks. The aim of the survey is to present the general themes, provide a survey of the nascent research and point to a number of interesting open questions.

Conflict and Networks

Marcin Dziubiński* Sanjeev Goyal † Adrien Vigier‡

March 15, 2015

Abstract

Conflict remains a central element in human interaction. Networks – social, economic and infrastructure – are a defining feature of society. The two intersect in a wide range of empirical contexts. This motivates the recent interest in conflict and networks.

The aim of the survey is to present the general themes, provide a survey of the nascent research and point to a number of interesting open questions.

*Institute of Informatics, Faculty of Mathematics, Informatics and Mechanics, University of Warsaw, Email: m.dziubinski@mimuw.edu.pl

†Faculty of Economics and Christ's College, University of Cambridge. Email: sg472@cam.ac.uk

‡Department of Economics, University of Oslo. Email: a.h.vigier@econ.uio.no

This paper has been prepared for the Oxford Handbook on Economics of Networks, edited by Yann Bramoulle, Andrea Galeotti and Brian Rogers.

We thank the editors for very helpful comments on an earlier draft. We also thank Vessela Daskalova, Julien Gagnon, Michiel de Jong, and Anja Prummer for helpful discussions. Marcin Dziubiński acknowledges support from Homing Plus programme of the Foundation for Polish Science, via the project 'Strategic Resilience of Networks'. Sanjeev Goyal acknowledges support from a Keynes Fellowship, The Cambridge-INET Institute and the European Research Area Complexity-Net under grant 'Resilience and interaction of networks in ecology and economics'.

1 Introduction

Conflict remains a central element in human interaction. Networks – social, economic and infrastructure – are a defining feature of society. So it is natural that the two should intersect in a wide range of empirical contexts. This motivates the recent interest on conflict and networks. The aim of the paper is to provide a survey of this research.

We find it useful to start with specific empirical phenomena involving conflict and networks.

1. Robustness of Infrastructure Networks: Highways, aviation, shipping, pipelines, train systems, and telecommunication networks are central to a modern economy. These networks face a variety of threats ranging from natural disasters to human attacks. The latter may take a violent form (guerrilla attacks, attacks by an enemy country, and terrorism) or a non-violent form (as in political protest that blocks transport services).[1] A network can be made robust to such threats through additional investments in equipment and in personnel. As networks are pervasive, the investments needed could be very large; this motivates the study of targeted defence. What are the 'key' parts of the network that should be protected to ensure maximal functionality? Moreover, taking a longer term view, how should networks be designed to enhance their robustness to threats?

2. Cybersecurity: As energy, communication, travel, consumer interaction increasingly adopt digital networks, cybersecurity has emerged as a major priority. In the United States, this is a responsibility of the Department of Homeland Security (DHS). Its mission statement reads,"Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace. We rely on this vast array of networks to communicate and travel, power our homes, run our economy, and provide government services."[2] At the heart of these developments is the question of how to design networks

[1]The US Office of Infrastructure Protection says, "Our nation's critical infrastructure is crucial to the functioning of the American economy... (It) is increasingly connected and interdependent and protecting it and enhancing its resilience is an economic and national security imperative Department of Homeland Security (2012). For an introduction to network based conflict, see Arquilla and Ronfeldt (2001) and Zhu and Levinson (2011); for news coverage of the effects of natural disasters and human attacks on infrastructure networks, see Eun (2010), Kliesen (1995), India Today (2011) and Luft (2005).

[2]In 2009, roughly 10 million computers were infected with malware designed to steal online credentials. The annual damages caused by malware is of the order of 9.3 billion Euros in Europe, while in the US the annual costs of identity theft are estimated at 2.8 billion USD (Moore, Clayton and Anderson (2009)). One indicator of the economic magnitude of the problem is the valuation of security firms: Intel bought McAfee in 2010, for 7.68 billion USD (bbc.co.uk; 19 August 2010).

so that they are robust to attacks.

3. Criminal networks: Criminal activity, being illegal, it is especially difficult for participants to enforce formal contracts. Trust and networks of favor exchange are especially important in crime. This suggests that personal connections may be important for crime; however, the investigation and capture of one agent by police can expose connected others. What is the best way to organize criminal network?

4. Civil wars and armed conflict: Conflict takes place between countries or communities that are geographically contiguous (Caselli et al. (2014)). Conflict between two entities however typically has spillovers on neighboring third parties, which is turn may travel through the network of relations. We wish to understand how the network structure shapes conflict and determines the winners and losers.

5. Strategic alliances: A common feature of civil unrest and international conflict is the salience of networks of alliances. For example, through the 19th century and the early part of the 20th century, shifting strategic alliances were a salient feature of European politics.[3] Empirical research shows that violent international conflict was more common in the hundred years prior to 1950 as compared to the years after that. The stability of alliances exhibits a corresponding time line: alliances were much less stable in the period prior to 1950 than in the period since. Finally, we know that international trade has grown steadily since the 1950's (Jackson et al., 2014). Is there a systematic relation between these stylized facts?

Inspired by applications 1, 2 and 3, we start with a discussion of the design and defence of networks that face threats. As networks carry out a variety of functions, different aspects of networks generate value depending on the context. Similarly, threats come in different forms: in some cases, the threat is posed by an intelligent adversary (such as the police or investigating agency, terrorists or political protestors), while in others it comes from nature (in the form of floods and earthquakes). Similarly, the dynamics of the threat also vary. Viruses and worms spread through computer connections; contagion is an important aspect of these threats. On the other hand, an earthquake or a storm damages a specific port or an airport or a railway station. By varying these different dimensions of the problem we generate an ensemble of different scenarios. The key question here is: how should networks be designed

[3]The Triple Alliance between Germany, Austria-Hungary and Italy and the Triple Entente involving Britain, France and Russia played a key role in shaping World War 1.

and defended in the face of threats? Section 2 provides a survey of the existing research and concludes with the discussion of a number of open questions.[4]

Motivated by application 4, we then turn to the study of conflict between nodes located in a network. Section 3 takes up the case of conflict in fixed networks. Connections between nodes determine who is in conflict with whom. The nodes choose how much to invest in conflict and the conflicts yield prizes to winners. We study both static models and also the dynamics of resource accumulation through war and conquest. The section ends with a discussion of open problems.

The study of war naturally leads us to the study of alliances in conflict: in application 5, a salient feature of civil and international conflict is the existence of alliances among warring parties. As the example of World War 1 illustrates, these alliances can have a decisive influence on the shape of conflict. Section 4 starts with the study the nature of conflict under given alliance structures and then moves on to the formation and stability of alliances.

Section 5 contains concluding remarks.

2 Network Design and Defence

The examples in the introduction illustrate a range of empirical contexts where networks face threats. The key question in this field is how to design and defend networks against these threats. The research on this question is at an early stage. We provide a survey of this work and point to a number of interesting open problems.

While there are different aspects of networks that create value, in the literature to date much attention has centered on the setting where network connectivity is central to value. Thus network value is increasing and convex in its size (i.e., the number of nodes). The threat to the network is modeled as a game of conflict between a Designer (and the nodes in the network) and an Adversary. The Designer chooses a network. The Designer (or the nodes) and the adversary then allocate their resources across the network. There is conflict between the attack and defence resources. In the infrastructure example, attack or damage of a specific part of the network (a node or a link) compromises the network by disrupting flows along paths. We study this disruption in terms of break down in connectivity of the network. In

[4]The problem of network design and defence has been extensively studied in electrical engineering and computer science; for an overview of this work, see Alpcan and Başar (2011), Anderson (2001) and Roy et al. (2010). The economics literature surveyed below contributes to this field by developing a general framework that combines strategic interaction with a rich formulation of network value.

the cybersecurity example, the spread of worms and viruses through the network connections is central to the damage. We develop a model of contagion through networks. The literature has focused on zero-sum games. We shall follow the literature in this regard.

We start with the problem of contagion in networks. We first set up and solve the first best solution. There are two players, a Designer and an Adversary. The Designer chooses both the design of the network and the allocation of defence resources. The Adversary observes these choices and then attacks particular nodes of the network. We then move to a discussion of the game where the Designer creates the network, but the nodes in the network choose defence allocations. This is motivated by applications in cybersecurity where individual computer users generally choose their own security.

We then turns to infrastructure robustness. We will first discuss optimal design and defence. Finally, motivated by the interest in the robustness of infrastructure networks, we will study optimal defence of a given network. As networks are pervasive, the investments needed to protect them can be very large; this motivates the study of targeted defence. What are the 'key' nodes to defend to maximize functionality of the network? We also study how networks affect the intensity of conflict, a question that will reappear in the subsequent sections, when we study conflict among nodes located in networks.

2.1 Connectivity and Network Value

We now introduce some terminology and notation. There is a set of nodes $N = \{1, \ldots, n\}$, $n \geq 2$. A link between two nodes i and j is represented by $g_{ij} \in \{0, 1\}$: we set $g_{ij} = 1$ if there is a link between i and j, and $g_{ij} = 0$ otherwise. Links are undirected, i.e. $g_{ij} = g_{ji}$. The nodes and the links together define a network g.

A path between two nodes i and j in network g is a sequence of nodes $i_1, \ldots, i_k$ such that $g_{ii_1} = g_{i_1i_2} = ... = g_{i_{k-1}i_k} = g_{i_kj} = 1$. Two nodes are said to be connected if there exists a path between them. A component of the network g is a maximal set of nodes such that any two elements in it are connected. $\mathcal{C}(g)$ is the set of components of g and $C_i(g)$ is the component containing node i. We let $|C|$ indicate the cardinality (or size) of the component C. A maximum component of g is a component with maximal cardinality in $\mathcal{C}(g)$. A network with a single component is said to be connected.[5] A network g' on N' is a sub-network of g

[5]The complete network, or a clique, g^c, has $g_{ij} = 1$, for all pairs (i, j). The empty network, g^e, has $g_{ij} = 0$ for all pairs (i, j). A core-periphery network has two types of nodes, N_1 and N_2. Nodes in N_1 constitute the periphery and have a single link each and this link is with a node in N_2; nodes in N_2 constitute the core and are fully linked with each other and with a subset of nodes in N_1. When the core contains a single node, we

if and only if $N' \subseteq N$, and $g'_{ij} = 1 \Rightarrow g_{ij} = 1$ and $i, j \in N'$. We let $\mathcal{G}(g)$ denote the set of all sub-networks of g.

Following Myerson (1977), we assume that the value of a network is the sum of the value of the different components and that the value of any component is a function of its size only. Let the function $f : \mathbb{N} \to \mathbb{R}_+$ specify a value to component size. Our interest is in network generated value and so we assume increasing and convex returns to size of component.

Assumption A.1: *The value of network g is given by*

$$\Pi(g) = \sum_{C \in \mathcal{C}(g)} f(|C|). \tag{1}$$

where f is (strictly) increasing, (strictly) convex and $f(0) = 0$.

Increasing and convex network value functions arise naturally in the large literature on network externalities (see e.g. Katz and Shapiro (1985) and Farrell and Saloner (1986)). In that literature, the value to a consumer from buying a product is related to the number of other consumers who buy the same product, i.e., belong to the same network. In its simplest form this gives rise to the quadratic form $f(n) = n^2$. This functional form also arises in the communications model in the literature on network economics (see e.g. Goyal (1993) and Bala and Goyal (2000)) and is consistent with Metcalfe's Law, concerning the nature of value in telecommunication networks.

On the other hand, suppose that subsets of nodes perform various tasks, each task being of equal value normalized to 1. A task is carried out if and only if the subset of nodes performing that task is connected. The value of the network is the total value of tasks performed. A component with m nodes thus generates value $2^m - 1$ (as there are exactly $2^m - 1$ tasks which m nodes can perform). This yields a network value that is exponential in the size of components; it is consistent with Reed's law (Reed, 2001) on value of networked systems.

Conflict and contagion: In this section we will study the optimal defence and design of networks that face contagious attacks. In their influential paper on computer security, Staniford et al. (2002) identify stealth worms and viruses as the main threats to security in computer networks. Using data from actual attacks, they argue that adversaries scan the network to explore its topology and the vulnerabilities of nodes, prior to attack. In the first instance,

have a star network. For a general introduction to networks concepts and terminology, see Goyal (2007).

the objective is to deploy a worm on selected nodes in the network. Deployed worms then exploit communication between nodes to progressively take control of neighboring nodes in the network. The likelihood of capture of a node and the spread of the worm in a network depends on the strength of the worm, the topology of connections and on vulnerabilities of individual nodes. These considerations motivate the following theoretical model, due to Goyal and Vigier (2014).

They consider a setting with two players: a Designer and an Adversary. The Designer moves first and chooses a network and an allocation of defense resources. The Adversary then allocates attack resources on nodes; if an attack succeeds then the Adversary decides on how successful resources should navigate the network. The model has three important ingredients: the value of the network (summarized in assumption (A.1) above), the technology of conflict between defense and attack resources, and the spread of successful attack resources through the network.

They assume that the value of a network is increasing and convex in the number of interconnected nodes (Assumption A.1 above). They model the conflict between defense and attack resources on a network node as a *Tullock contest*.[6] The contest defines the probability of a win for Designer and Adversary, as a function of their respective resources. The resources of the loser of the contest are eliminated, the winner retains his resources. In case the Adversary wins a contest on a node, the winning attack resources can move and attack neighboring nodes. The dynamics of conflict continue as long as both defense and attack resources coexist. The initial network design and the conflict dynamics yield a probability distribution on surviving nodes, i.e., nodes that have not been captured by the Adversary. The Designer and Adversary are engaged in a zero sum game; so, given a defended network, we consider the minimum payoff of the Designer given all possible attacks. An *optimal defended network* maximizes this (minimum) payoff.

We let $d \in \mathbb{N}$ (resp. $a \in \mathbb{N}$) denote the total resources of the Designer (resp. Adversary). A strategy for the Designer is a pair $(g, \mathbf{d})$, where g is a network defined on nodes in N and $\mathbf{d}$ is a vector specifying the defense resources allocated at each node such that $\sum d_i = n$. A strategy for the Adversary is a pair $(\mathbf{a}, \Delta)$. The vector $\mathbf{a}$ specifies the attack resources initially allocated at each node. The matrix $\delta = (\delta_{ij})_{i,j \in N}$, on the other hand, describes the spread of attack resources during the course of time.

Given a defended network $(g, \mathbf{d})$, let K denote the subset of protected nodes and O the

[6]Here we build on the rich literature on rent seeking and conflict, see Garfinkel and Skaperdas (2012), Tullock (1980) and Hirshleifer (1995).

subset of unprotected nodes. Further, for $i \in N$ let $O_i \subseteq O$ denote the subset of unprotected nodes which can be reached from i through some path such that each node on that path lies in O. The set O_i will sometimes be called the unprotected neighbourhood of i. Similarly, let $K_i \subseteq K$ denote the subset of protected nodes which can be reached from i through some path such that each node on that path lies in O.

Attack resources a_i and defense resources d_i located on a node i engage in a *contest* for control of the node. If $a_i + d_i > 0$ then, following Tullock (1980):

$$\text{probability of successful attack} = \frac{a_i^\gamma}{a_i^\gamma + d_i^\gamma}, \tag{2}$$

where $\gamma > 0$. If a_i is 0 then the probability of successful attack is 0, irrespective of the value of d_i: a node is safe if it is not under attack.

We will provide an informal sketch of the dynamics; for details refer to Goyal and Vigier (2014). At the start, the Adversary captures all nodes that are attacked and unprotected. After that the Adversary captures O_i. He then reallocates a_i attack resources to an uncaptured and protected node. The result below holds for a range of spread matrices. A defended network will be called optimal if it maximizes the minimum expected network value from all attacks possible.

The key to the analysis is whether or not a few nodes are 'essential' to the network value given by assumption A.1. In the case where $f(x) = x^2$, as n grows, the impact of eliminating a few nodes vanishes. On the other hand, if $f(x) = 2^x - 1$, the impact does not vanish: $\lim_{n\to\infty}(n-a)^2/n^2 = 1$, whereas $\lim_{n\to\infty}(2^{n-a}-1)/(2^n-1) = 1/2^a < 1$. The methods of analysis for the two cases involve different arguments.

We will henceforth assume that the following limit exists, and define:

$$\ell = \lim_{n\to\infty} \frac{f(n-1)}{f(n)}.$$

A defended network $(g, \underline{d})$ is optimal if $\overline{\Pi}^e(g, \underline{d}) \geq \overline{\Pi}^e(g', \underline{d}')$ for all defended networks $(g', \underline{d}')$.

Given $\epsilon > 0$, a defended network $(g, \underline{d})$ is ϵ-optimal if $\overline{\Pi}^e(g, \underline{d}) \geq (1-\epsilon)\overline{\Pi}^e(g', \underline{d}')$ for all defended networks $(g', \underline{d}')$. A star network in which all defence resources are allocated to the central node is referred to as a Center-Protected (CP) Star.

We are now ready to state the main result from Goyal and Vigier (2014).

Theorem 1 *Assume that (A.1) holds, $a/d \in \mathbb{N}$ and $n > a + 1$. Let $\epsilon > 0$ and consider the class of connected networks. There exists n_0 such that, for all $n > n_0$:*

1. *If $\ell < 1$ the CP-star is uniquely optimal.*

2. *If $\ell = 1$ the CP-star is ϵ-optimal.*

We illustrate the general line of argument with an example, by comparing the expected network value achieved with a CP-star to the value achieved with a symmetric 2-hubs network as illustrated in Figure 2.1. The defended network has $|K| = 2$ protected nodes, with one link between them, and each protected node has $n - 2/2$ nodes in its unprotected neighbourhood. We assume that d is even and each protected node has $d/2$ defence units allocated to it. To simplify the exposition, we also assume $a = d$. The aim is again to find a way to attack this network and leave the Designer with expected network value less than $\frac{d}{d+a} f(n - a)$; this will show that the CP-star performs best in this case too.

Consider the following attack strategy, where the Adversary allocates 1 unit of resource to exactly $a/2$ nodes of the periphery of each protected node. There are four possible outcomes of the two contests on the hubs: either both hubs survive, both hubs are captured or one hub survives and the other is captured. Given the equal resources engaged in contests, it follows that the first two outcomes each arise with probability 1/4. The two outcomes define terminal states of the dynamics, represented at the top and the bottom end of Figure 2.1. There is a probability 1/2 that one of the hubs survives and the other is captured. This is represented in the middle of the Figure 2.1. Capture of a hub triggers the capture of its respective peripheral nodes. All attack resources then target the surviving hub, inducing a second round of contests. With probability 1/2 the hub survives the attack, and with probability 1/2 it is captured. If the hub is captured then this triggers the capture of the remaining peripheral nodes. This brings to an end the dynamics of conflict.

The probability density P on surviving nodes is: with probability 1/2 all nodes are captured, with probability 1/4 half the nodes survive and with probability 1/4 all nodes survive. Observe that this distribution is first order stochastically dominated by the distribution P' such that with probability 1/4 all nodes are captured, with probability 1/2 half the nodes survive and with probability 1/4 all nodes survive. But P' is in turn second order stochastically dominated by the distribution P'' in which all nodes are captured with probability 1/2, and all nodes survive with probability 1/2. Noting that P'' is the distribution facing the Designer

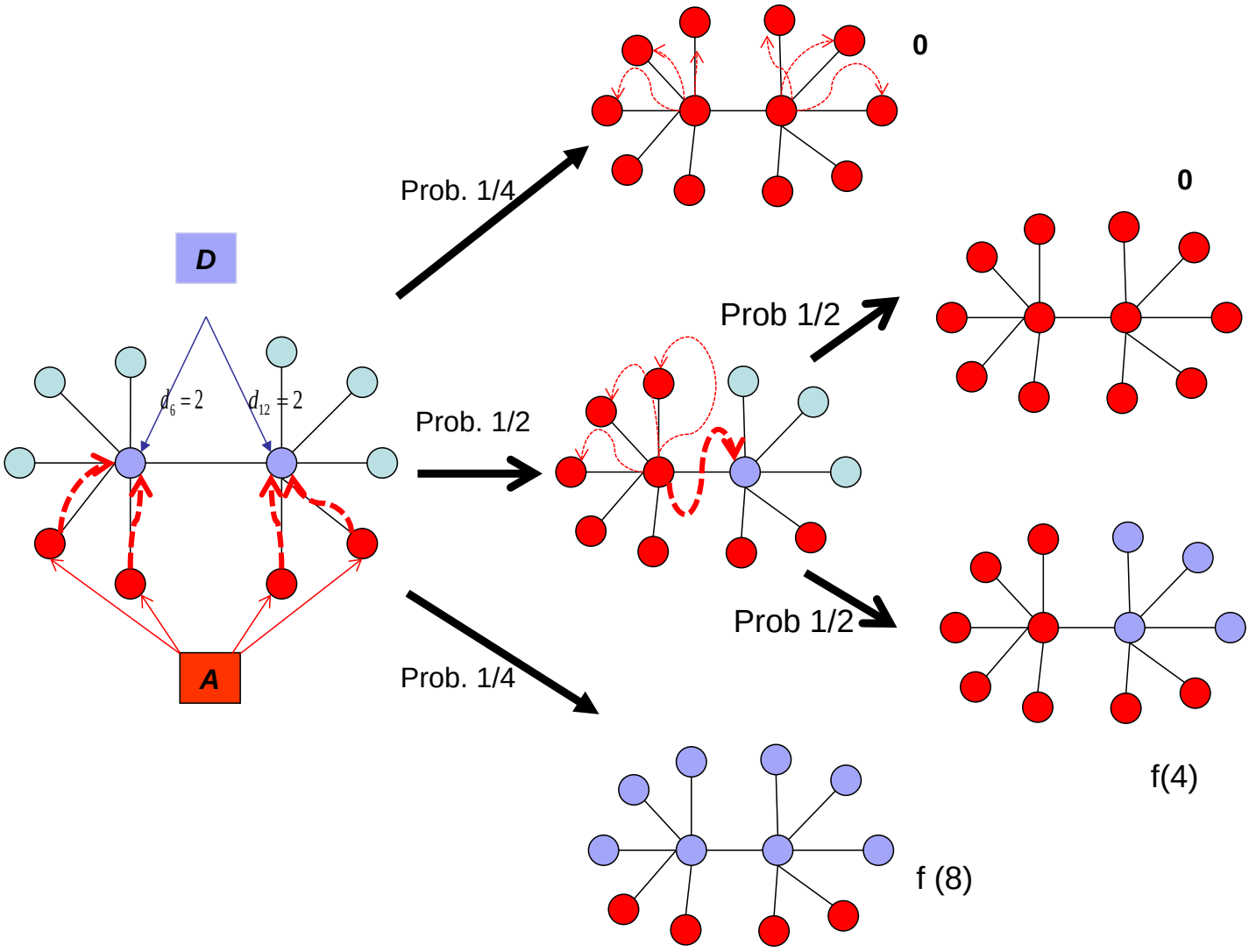

Figure 1: Mimic attack on two-hub network: $n = 12$, $a = d = 4$.

if he chooses a CP-star finishes to show that the CP-star dominates the 2-hubs network examined here, given that f is increasing and convex. Goyal and Vigier (2014) generalize these ideas to cover all connected networks and establish:

Theorem 1 is a powerful result. It holds for all payoff functions which satisfy (A.1): so the result does not depend on the curvature (i.e. the extent of convexity) of f. The result holds for all γ in the Tullock contest function: so the conclusion is robust with respect to the technology of conflict. The result holds for all resource configurations between the Designer and the Adversary such that $a/d \in \mathbb{N}$.

Empirical work on networks draws attention to the prominence of the hub-spoke network architecture (see e.g., Goyal (2007); Newman (2010)). In an influential paper, Albert et al. (2000) argue that these architectures are vulnerable to strategic attacks since potential adversaries can significantly reduce their functionality by removing only a few hub nodes. By contrast, the above analysis highlights the attractiveness of these architectures in a setting where defence resources are scarce and network value is convex.

Decentralized defence: Theorem 1 provides us a result on the optimal defence and design of a network facing an intelligent adversary threat. In the context of cybersecurity, investments in protection are typically made by individual nodes. Heterogeneities in the network structure create corresponding differences in individual incentives and in externalities. Thus Theorem 1 provides us a benchmark. We now turn to the question of how network design should address the variety of network externalities? In this context, the standard understanding of externalities is that individual returns to security may be lower than collective returns, due to the risks of contagion. However, in a setting where the Adversary chooses targets, there is an additional and novel consideration: investing in security diverts the attack to other nodes. This potentially negative externality brings a new set of considerations into play. We follow Cerdeiro et al. (2015) in this discussion.[7]

The Designer first chooses the network over the n nodes. Given this network, each of the n nodes (simultaneously) chooses whether to protect or not; protection carries a fixed cost. Finally, the Adversary chooses a node to attack. If the attacked node is protected, then all nodes survive the attack. If the attacked node is not protected, then this node and all nodes with a path to the attacked node through unprotected nodes are eliminated. Nodes are assumed to derive benefits from their connectivity: the payoff of a node is increasing in the

[7]For a general survey of games played on networks, see chapter XX by Bramoulle and Kranton (2015).

size of its surviving component. A node's net payoffs are equal to its connectivity payoffs less the amount spent on protection. The Designer is utilitarian: he seeks to maximize the sum of nodes' payoffs. The Adversary is intelligent, purposefully choosing the attacked node so as to minimize connectivity-related payoffs.

We start with a study of the first best design and defence profile. We show that for low protection costs, all nodes should be protected and any connected network is optimal. For intermediate costs of protection, the Designer chooses a star network and protects its center only. The Adversary then eliminates a single spoke of the star. If protection costs are high, the Designer splits the network into equal size components and leaves all nodes unprotected. The Adversary eliminates one of these components.

This sets the stage for the decentralized problem. Observe that if defence is sufficiently expensive (so that no protection is first best), no protection is the unique equilibrium defence of any first best network. At the other extreme, if protection is sufficiently cheap (so that full protection is first best), there exist networks that implement the first best in every equilibrium. Departures from first best welfare will therefore arise only for intermediate costs of protection; that is, when a center protected star is optimal. The Designer cannot attain first best payoffs in equilibrium, as the only equilibria on star networks are those where either all or no node protects.

We now examine the optimal design problem in greater detail. When a center protected star is first best but all nodes protect in equilibrium, protection decisions involve negative externalities and exhibit strategic complementarities. Nodes have incentives to protect and divert the Adversary's attack to other parts of the network. How can the Designer induce some nodes to be eliminated in equilibrium? Connected networks are not the best way to address the over-protection problem. When a connected network has an equilibrium achieving higher welfare than full protection, there always exists a disconnected network that welfare-dominates it. Thus, if the Designer is to avoid the over-protection problem, he must disconnect the network and sacrifice some nodes.

The analysis summarized so far assumes that individual coordinate on equilibria that achieve maximum equilibrium welfare. In general, however, some of these networks may feature multiple equilibria that achieve vastly different welfare levels. How can the Designer tackle potential coordination problems? To illustrate the issue, suppose that the costs of protection are such that maximum equilibrium welfare is achieved via full protection on a connected network. The network where nodes are arranged on a cycle has a full protection equilibrium. However, if the cost of protection outweighs the benefits of surviving in isolation,

there is another equilibrium on this network where no node protects and the Adversary brings down the entire network. Cerdeiro et al. (2015) provide a necessary and a sufficient condition for a network to induce full protection in any equilibrium. Such networks are *sparse* in the following sense: they must feature a node that can block the Adversary's attack, thus saving a large part of the network.

The contribution of the paper lies at the intersection of economics and computer science literature. For an early contribution in the study of decentralized defence, see Kunreuther and Heal (2004). Aspnes et al. (2006) studies security choices by nodes in a fixed network when nodes only care about their own survival, attack is random, and both protection as well as contagion are perfect. The focus is on computing the Nash equilibria of the game. They provide approximation algorithms for finding the equilibria. In a recent paper, Acemoglu et al. (2013) study the incentives for protection in a setting when both defence and contagion are imperfect.[8]

The relationship with Goyal and Vigier (2014) is worth discussing as they highlight the large effects of decentralized defence for optimal network design. In Goyal and Vigier (2014) the optimal design is a star network and optimal allocation of resources is exclusively on the central node. By contrast, when individual nodes choose security, the optimal design has to address problems of too much as well as too little protection. This best way to tackle over-protection is by disconnecting the network and sacrificing some nodes. Potential under-protection problems are addressed by creating equal components. Finally, coordination problems in security are mitigated through the creation of 'sparse' networks that contain critical nodes.

2.1.1 Non-contagious threats

In its strategy statement, the US Office of Infrastructure Protection says, "Our nation's critical infrastructure is crucial to the functioning of the American economy... (It) is increasingly connected and interdependent and protecting it and enhancing its resilience is an economic and national security imperative Department of Homeland Security (2012)." In these contexts the primary cost of an attack is in terms of nodes (and links) that are eliminated and the consequent loss in the connectivity of the network. This motivates the study of networks in a setting with non-contagious attacks. In parallel with our discussion of contagious risk we

[8]There is also a very active research programme in financial contagion, see e.g., Blume et al. (2011), Acemoglu et al. (2015) Cabrales et al. (2010), and Elliot et al. (2014)). For a survey of this issues see Chapter XX by Cabrales et al. (2015).

start with a study of optimal defence and design.

The presentation here draws on Dziubiński and Goyal (2013). There is a Designer and an Adversary. The Designer moves first and chooses a network and defence allocation. The Adversary moves next. Costs of attack are sunk; the Adversary can choose up to $k \leq n-2$ nodes to eiminate/remove. The costs of the Designer are linear: there is a cost $c_{\rm l} > 0$ for every link, and a cost $c_{\rm d} > 0$, for defending a node. Defence is perfectly reliable. Given network g, the set of defended nodes, Δ, the set of attacked nodes, $X \subseteq N$, the payoff to the defender and Adversary, are respectively:

$$\begin{aligned}\Pi^{\rm D}(g,\Delta,X;c_{\rm d},c_{\rm l}) =& \Phi(g-(X\setminus\Delta)) - c_{\rm d}|\Delta| - c_{\rm l}|g| \\ \Pi^{\rm A}(g,\Delta,X) =& -\Phi(g-(X\setminus\Delta)).\end{aligned}$$

It is useful to consider the connectivity based value function; for the analysis of general value functions that satisfy assumption A.1 see Dziubiński and Goyal (2013). In this case the residual network has value 1 if it is connected and 0 otherwise. Now the equilibrium has a simple structure. One of the following three possible outcomes arises: one, the network is empty and there is no defence; two, there is no defence, the network involves redundant links, and three, the star network with protected center.

The exact levels of costs for each of the above outcomes can be derived by applying a result due to Harary (1962). Harary (1962) showed that a network that cannot be disconnected by removal of k nodes requires exactly $\lceil \frac{n(k+1)}{2} \rceil$ links. Moreover any such network is regular of degree $(k+1)$, or almost regular, having one node of degree $(k+2)$ (if both n and k are odd). The set of these graphs is denoted by $\mathcal{M}(n,k)$.[9] Dziubiński and Goyal (2013) establish the following result.

Proposition 1 *Consider the Designer-Adversary game under connectivity based value function and suppose that $k \leq n-2$. In equilibrium*

1. *The Designer chooses network g and defence Δ:*
   - *If $c_{\rm l} < 1/\left\lceil \frac{n(k+1)}{2} \right\rceil$ and $c_{\rm d} > c_{\rm l}\left(\left\lceil \frac{n(k-1)}{2} \right\rceil + 1\right)$, then $g \in \mathcal{M}(k,n)$ and $\Delta = \varnothing$.*
   - *If $c_{\rm l}(n-1) + c_{\rm d} < 1$ and $c_{\rm d} < c_{\rm l}\left(\left\lceil \frac{n(k-1)}{2} \right\rceil + 1\right)$, then g is a star and the central node is defended.*

[9] The set $\mathcal{M}(n,k)$ is not empty, as it includes *Harary graphs* defined by Harary to obtain the upper bound on the number of links.

- *Otherwise g is empty and $\Delta = \varnothing$.*

2. *The Adversary chooses: a separating cut for g and Δ, if it exists; if it does not exist then all cuts yield the same payoff.*

The proposition above illustrates the trade off faced by the Designer. If costs of defence are high relative to the costs of linking the Designer chooses a regular and dense network. On the other hand, when costs of defence are relatively low the Designer chooses the star network and defends the hub node.

A comparison between Goyal and Vigier (2014) and Dziubiński and Goyal (2013) helps us to understand the role of contagion in the optimal defence and design. In the latter paper, when defence units are 0, the Designer defends the network by adding more links and so the optimal network is $(k+1)$-connected. By contrast, in Goyal and Vigier (2014), when there is no defence, the Designer defends the network by separating it into distinct components. This is due to the implicit cost to linking introduced by the possibility of contagion.

Finally, in Dziubiński and Goyal (2014), the equilibrium will typically involve protection of multiple nodes. By contrast, Goyal and Vigier (2014) show that under a wide variety of circumstances, the Designer will assign all resources to the central node of a star.

The defence of a network: In some contexts – such as trains or roads or telecommunications – the network involves very large and time consuming investments. So it is important to study the problem of defending a given network. The focus is on where to allocate resources to maintain the network in the face of threats that potentially damage or knock out nodes. The presentation draws on Dziubiński and Goyal (2014).

They consider a two-player sequential move game with a Defender and an Adversary. In the first stage, the Defender chooses an allocation of defence resources. In the second stage, given a defended network, the Adversary chooses the nodes to attack. Successfully attacked nodes (and their links) are removed from the network, yielding a residual network. The goal of the Defender is to maximize the value of the residual network, while the goal of the Adversary is to minimize this value.

Fix a network g on a set of nodes $N = \{1, \ldots, n\}$, where $n \geq 3$. A *defence* is a set of nodes $\Delta \subseteq N$. The set of attacked nodes $X \in\subseteq N$ chosen by the Adversary is called a *cut*. Removing a set of nodes $X \subseteq N$ from the network creates *residual network* $g - X$. It is assumed that that the defence is perfect: a protected node cannot be removed by an attack,

while any attacked unprotected node is removed with certainty. Given a defence Δ and a cut X, a set $Y = X \setminus \Delta$ will be removed from the network.

Defence resources are costly: the cost of defending a node is $c_{\mathrm{d}} > 0$. Given network g, defender's payoff from strategy $\Delta \subseteq N$, when faced with opponent strategy $X \subseteq N$, is

$$\Pi^{\mathrm{D}}(\Delta, X; g, c_{\mathrm{d}}) = \Phi(g - (X \setminus \Delta)) - c_{\mathrm{d}}|\Delta|. \tag{3}$$

where $\Phi(\cdot)$ satisfies assumption (A.1).

Attack resources are costly: the cost of attacking a node is given by $c_{\mathrm{a}} > 0$. Given defended network (g, Δ), payoff to the Adversary from strategy $X \subseteq N$ is

$$\Pi^{\mathrm{A}}(\Delta, X; g, c_{\mathrm{a}}) = -\Phi(g - (X \setminus \Delta)) - c_{\mathrm{a}}|X|. \tag{4}$$

They study the (sub-game perfect) equilibrium of this game.

Dziubiński and Goyal (2014) show that the Adversary should target nodes that separate the network, while the defender must protect nodes that block these separators, i.e., their *transversal*. They then study the relation between network architecture and the intensity of conflict (the sum of resources allocated to attack and defence) and the prospects of active conflict (when some nodes are defended while some are attacked). To get a sense of the issues, it is useful to begin with a simple example.

Example 1 *Defending a star network*

Consider the star network with $n = 4$ and $\{a\}$ as central node (as in Figure 1). The value function is $f(x) = x^2$. As is standard, we solve the game by working backward. For every defended network (g, Δ) we characterize the optimal response of the Adversary. We then compare the payoffs to the defender from different (g, δ) profiles and compute the optimal defence strategy. Equilibrium outcomes are summarized in Figure 2.

A number of points are worth noting.

1. Observe that removing node a disconnects the network; this node is a *separator*. Moreover, there is a threshold level of cost of attack (7) such that the Adversary either attacks a or does not attack at all when $c_{\mathrm{a}} > 7$. Protecting this node is also central to network defence.

2. The intensity of conflict exhibits rich patterns: when costs of attack are very large there is no threat to the network and no need for defence. If the costs of attack are small,

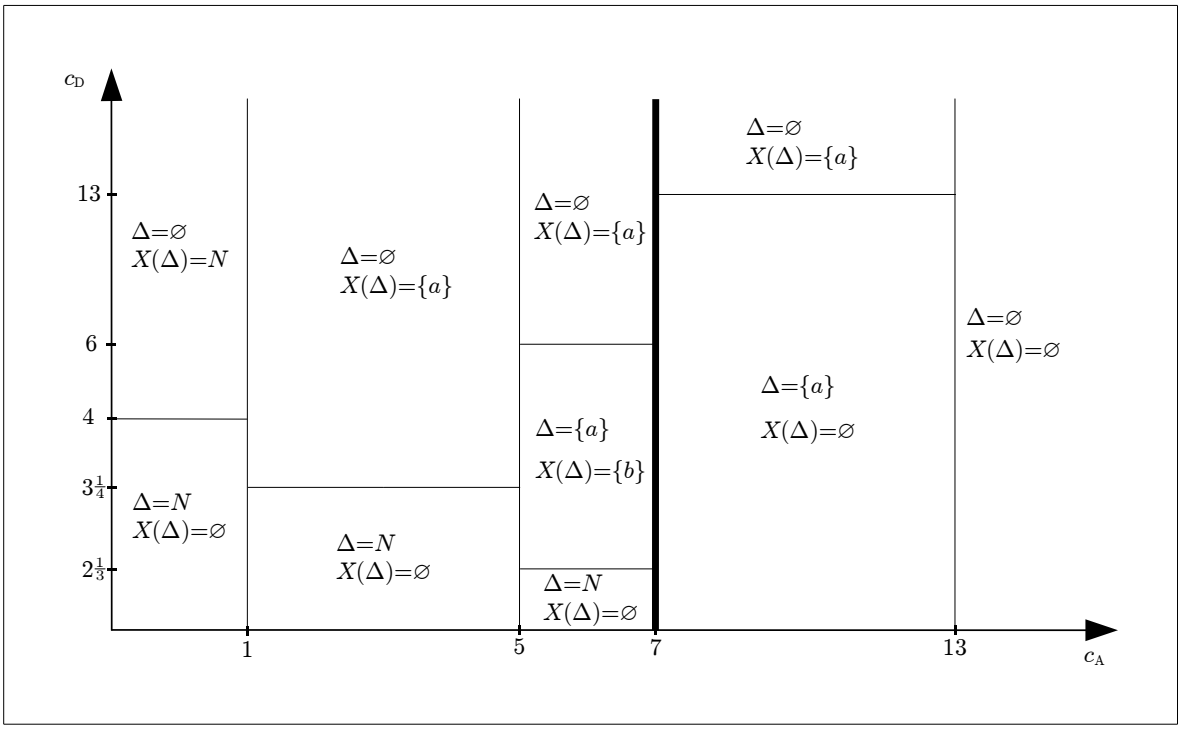

Figure 2: Equilibrium outcomes: star network ($n = 4$) and $f(x) = x^2$.

intensity of conflict hinges on the level of defence costs. When they are low all nodes are protected and there is no attack (the costs of conflict are nc_{d}), if they are high then there is no defence but all nodes are eliminated (the costs of conflict are nc_{a}). For intermediate costs of attack and defence, both defence and attack are seen in equilibrium.

3. The size of the defence may be non-monotonic in the cost of attack. Fix the cost of defence at $c_{\mathrm{d}} = 3.5$. At a low cost of attack ($c_{\mathrm{a}} < 1$) the defender protects all nodes, in the range $c_{\mathrm{a}} \in (1, 5)$ he protects 0 nodes, in the range $c_{\mathrm{a}} \in (5, 13)$ he protects $\{a\}$, and then in the range $c_{\mathrm{a}} > 13$, he stops all protection activity. Similarly, the size of the attack strategy may be non-monotonic in the cost of attack.

△

Turning now to the analysis for general networks, we note first that given the convexity in the value function of networks, disconnecting a network is especially damaging. A cut $X \subseteq N$ is a *separator* if $|\mathcal{C}(g)| < |\mathcal{C}(g - X)|$. However, a network will normally possess multiple separators and the Adversary should target the most effective ones. A separator $S \subseteq N$ is *essential* for network $g \in \mathcal{G}(N)$, if for every separator $S' \subsetneq S$, $|\mathcal{C}(g-S)| > |\mathcal{C}(g-S')|$. The set

of all essential separators of a network g is denoted by $\mathcal{E}(g)$. Figures 3-4 illustrates essential separators in some well known networks.

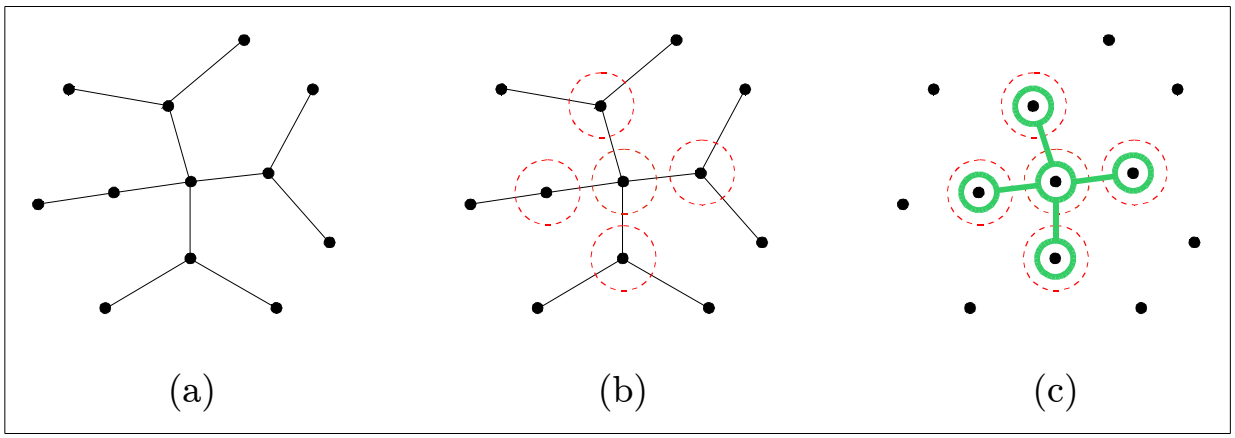

Figure 3: (a) Tree network, (b) essential separators, (c) minimum transversal.

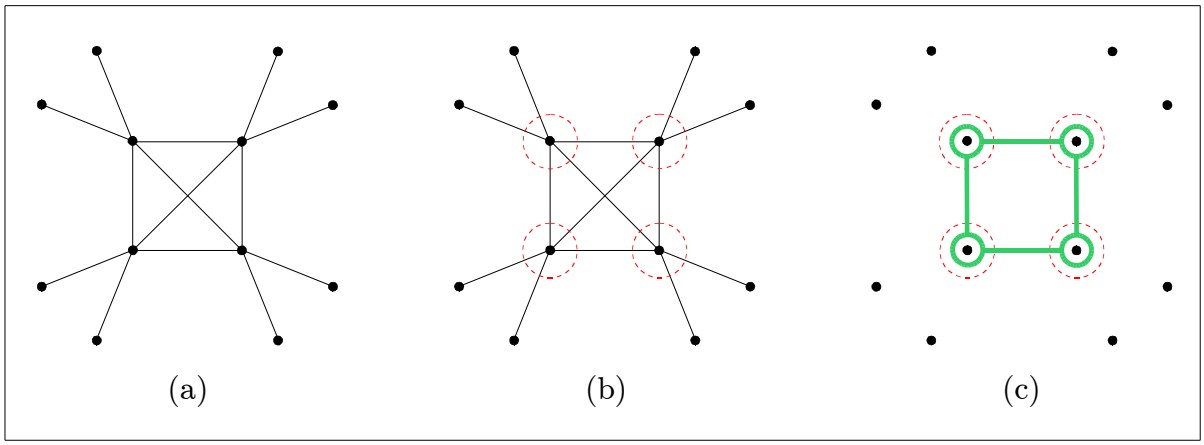

Figure 4: (a) Core-periphery network, (b) essential separators, (c) minimum transversal

The second element is the level of costs. As illustrated by Example 1, the network defence problem can be divided into two parts, depending on the cost of attack. Given $x \in \mathbb{N}$, $\Delta f(x) = f(x+1) - f(x)$ is the marginal gain to a node in the value of a component of size x. Under Assumption A.1, $\Delta f(x)$ is strictly increasing. It is useful to separate two levels of costs: one, high costs with $c_{\mathrm{a}} > \Delta f(n-1)$, and two, low costs with $c_{\mathrm{a}} < \Delta f(n-1)$.

We present the case of high cost as it brings out some of the main insights in a straightforward way. Facing a high cost, the Adversary must disconnect the network, i.e., choose a separator or not attack the network at all. Clearly, the Adversary would never use an essential

separator that yields a lower payoff than the empty cut. Given cost of attack c_a and network g, the set of individually rational separators is $\mathcal{E}(g, c_a) = \{X \in \mathcal{E}(g) : \Phi(g) - \Phi(g - X) \geq c_a|X|\}$.

We now turn to equilibrium strategies of the Designer. Again, it is instructive to start with the setting where cost of attack is high. An optimal strategy of the defender should block a subset of individually rational essential separators in the most economical way. Given a family of sets of nodes, $\mathcal{F}$, and a set of nodes M, $\mathcal{D}(M, \mathcal{F}) = \{X \in \mathcal{F} : X \cap M \neq \varnothing\}$ are the sets in $\mathcal{F}$ that are blocked (or *covered*) by M. The set M is called a *transversal* of $\mathcal{F}$, if $\mathcal{D}(M, \mathcal{F}) = \mathcal{F}$. The set of all transversals of $\mathcal{F}$ is denoted by $\mathcal{T}(\mathcal{F})$. Elements of $\mathcal{T}(\mathcal{F})$ with the smallest size are called *minimum* transversals of $\mathcal{F}$. Let $\tau(\mathcal{F})$ denote the *transversal number* of $\mathcal{F}$, i.e., the size of a minimum transversal of $\mathcal{F}$. Figures 3-4 illustrates the transversal in some well known networks.

Dziubiński and Goyal (2014) develop the following result on optimal defence and attack.

Proposition 2 *Consider a connected network $g \in \mathcal{G}(N)$ and suppose $c_a > \Delta f(n-1)$. Let (Δ^*, X^*) be an equilibrium.*

- $|\Delta^*| \leq \tau(\mathcal{E}(g, c_a))$ *and* Δ^* *is a minimum transversal of* $\mathcal{D}(\Delta^*, \mathcal{E}(g, c_a))$.
- $X^*(\Delta) = \varnothing$, *if* $\Delta \in \mathcal{T}(\mathcal{E}(g, c_a))$; $X^*(\Delta) \in \mathcal{E}(g, c_a)$ *with* $X^*(\Delta) \cap \Delta = \varnothing$, *otherwise.*

Optimal defence is characterized in terms of minimal transversal of the appropriate hypergraph of separators (or defence covers all nodes). If cost of attack is such that elimination of single nodes is not worthwhile, optimal attack is bounded above by the transversal number of the graph. Optimal attack is either empty or targets essential separators.

Example 1 above suggests that defence size is falling in defence costs and is non-monotonic in attack cost. The attack size is non-monotonic in both attack cost and defence cost. Dziubiński and Goyal (2014) show that these patterns are true more generally. The authors then study the relation between the network architecture and the *intensity of conflict*: this is the sum of expenditures of defence and attack. Their analysis characterizes minimal intensity of conflict and the corresponding networks that sustain it. This allows them to show how network architecture matter for the intensity of conflict.

They then turn to the problem of defence when nodes makes security choices: they show that the equilibrium in this decentralized defence game can also be characterized in terms of transversals and separators of the underlying network. Second, they find that defence exhibits properties of strategic substitutes and a threshold public good. Three, they show

that the welfare gap between decentralized equilibrium and first best outcomes is unbounded: interestingly, individual choice may lead to too little and to too much protection, relative to the choice of a single (centralized) defender.

2.2 The design of criminal networks

Illegal organizations, like other institutions, rely on cooperation and coordination among their members. As legal enforcement of formal contracts is problematic, such organizations are especially reliant on trust among members. Information sharing on identity and personal information may be an important factor in building internal trust and cohesion: but it can leave the organization vulnerable to 'serial' exposure. How does this trade-off affect the design of a criminal organization? In an early paper, Baccara and Bar-Isaac (2008) study this question.

The first point to note is that there is significant heterogeneity across the information structures of different criminal/illegal organizations. On the one hand there is the view that these organizations have a centralized information and enforcement structure. In the Mafia, there is the so-called Cupola that holds large amounts of information about the organization itself and carry out the enforcement needed for the organization to function. These crucial agents are shielded from the authorities since they are typically not directly involved in criminal activities. On the other hand, recent studies on modern terrorism suggest a decentralized organization characterized by the presence of independent "cells". These cells consist of agents who know each other and enforce each others actions but who have a very vague idea of how the organization looks outside the cell boundaries. Thus, even if authorities detect a cell, it is difficult to expand the detection further. This structure is similar to other organizations observed in history, including the anarchist and the revolutionary organizations in the late 19th century in Europe.

These empirical observations motivate a model with the following ingredients. Individuals are engaged in an infinitely repeated multi-person prisoners dilemma, augmented with the possibility of additional punishment, which can help encourage "good" behavior. The additional punishment of a player requires personal information about this specific person; this information makes the person vulnerable. Examples of this kind of information include identity, whereabouts, or some incriminating evidence about a person. They explore the trade-off between the enhancement in internal cohesion derived by exchanging internal information and the increase in vulnerability to detection that this exchange implies.

The model has $N = \{1, 2..., n\}$, $n \geq 2$ agents. Agents are engaged in an infinitely repeated prisoner's dilemma. A Designer attempts to sustain cooperation among the n agents. Links are directed, and if i is linked to j then he can inflict an *additional* punishment on j in case the latter fails to cooperate. This implies that the returns from connectedness are positive for the first link, but zero afterwards (as an agent cannot be punished more than once). Observe that in the absence of an Adversary a network made up of paired nodes is the optimal architecture.

The external authority, or the Adversary, attempts to inflict the most disruption possible on the network by allocating attack resources across the nodes. Contagion follows the direction of the link and is assumed to be unidirectional. The timing of the game is such that the Adversary moves first. The Designer observes the allocation of attack resources, and chooses links between the nodes.

Note that if nodes are sufficiently patient then cooperation can be sustained even without links between nodes. The empty network is in that case the optimal organization. If nodes are impatient, on the other hand, then even adding links between nodes will not suffice to induce cooperation. Again, the empty network is in that case the optimal organization. The case of interest is therefore that of intermediary values of the nodes' impatience. Let us now turn to this case.

Generally speaking, the agents probability of getting detected directly depends on the resources allocated on him and on his activity status. Baccara and Bar-Isaac (2008) study two polar cases, one, where detection probability is independent of activity in the organization and two, where detection is only possible if the agent is cooperating with the criminal organization. They provide characterize the optimal information structure within the organization. In the independent detection case, they find that if the probabilities of detection are sufficiently similar, either it is optimal to create no information links or the optimal structure consists of binary cells (pairs of agents with information about each other but with no information links with other members of the organization). Given this characterization, they then consider the optimal budget allocation for the Adversary. They show that there are circumstances in which allocating the budget symmetrically induces the organization to exchange no information. In these cases, a symmetric allocation is optimal. However, sometimes a symmetric allocation induces the agents to form a binary cell structure. Baccara and Bar-Isaac (2008) show that in this case, the authority optimizes by not investigating one of the agents at all while investigating the others equally.

In the latter cooperation-based detection case, since each agents probability of detection is a function of the level of cooperation within the organization, an optimal information structure

may require lower levels of cooperation from some of the agents to shield them from detection. Even though agents are ex ante symmetric, they show that the optimal information structure can be asymmetric, resembling a hierarchy with an agent who acts as an information hub, does not cooperate at all, and thus remains undetected. If each individual agents contribution to the organization is sufficiently high, the optimal organization can also be a binary cell structure. Moreover, the optimal strategy of the external agent is different under cooperation-based detection. For example, devoting considerable resources to scrutinizing a single agent makes that agent relatively likely to be detected whether linked or not under the agent-based cooperation model, thus making it cheap for the organization to link the agent and induce him to cooperate. In contrast, under cooperation-based detection, it is costly to make such a scrutinized agent cooperate (and thereby increase considerably the probability that he is detected).

The driving forces in these two detection approaches are thus very different. In the independent detection model, the Adversary chooses a strategy that makes it unappealing for agents to be vulnerable. In the cooperation-detection model, however, the external authoritys strategy of targeting someone makes it less attractive to have him cooperate.

We now briefly relate the findings of Goyal and Vigier (2014) and Baccara and Bar-Isaac (2008). In both papers there is trade-off between connections and vulnerability. However, the models differ along a number of dimensions and these differences serve to highlight the rich theoretical possibilities in this literature. In Goyal and Vigier (2014) the gains from large scale connectivity are key; by contrast, in Baccara and Bar-Isaac (2008) the size of the network plays no essential role in defining network value.[10] Two, the former paper studies conflict between defense and attack; by contrast, there are no defense resources in the latter. Three, the Designer moves first in the former model, while the Adversary moves first in the latter model. Four, links are undirected in the former, while they are directed in the latter. These differences are substantive and taken together lead to very different insights.

2.3 Open questions

The design and defence of networks that face threats is an important practical problem. Networks perform a variety of functions and this gives rise to different potential sources of network value. The papers we have surveyed approach the network value question in different

[10]This is best seen by comparing optimal networks in the absence of an Adversary in the two settings: in Baccara and Bar-Isaac (2008) linked pairs of players is an optimal criminal organization. By contrast, in Goyal and Vigier (2014) any optimal network must be connected.

ways, but connectivity and component size have been a prominent feature of many papers. The discussion of Baccara and Bar-Isaac (2008) highlights the key role of the network value function in shaping an answer to the design question. As research in this field matures we believe that closer attention to the source of network value would be important. In this section, we started with the first best scenario: where the design and defence are both controlled by a single player. In applications, individual nodes often have control of these variables. Our discussion of Cerdeiro et al. (2015) suggests that optimal networks with decentralized choice may be very different from first best networks. In important contexts such as epidemiology and cybersecurity, individuals choose links in addition to security. In future work, it would be important to study the impact of these choices.[11] Finally, we would like to comment on the nature of defence. Following on the early work of Aspnes et al. (2006) and others, most of the recent work surveyed in the section has assumed that defence is perfect. This is a natural first step, but clearly it is a strong assumption. The dynamics of contests on networks remains a poorly understood problem.

3 Resources, Conflict and Networks

In economics and in biology, we think of agents and organisms as seeking to expand their influence and to capture territory. One possible avenue through which to obtain resources is to appropriate them through conflict. However, agents may face constraints on whom they can target for conflict. The extensive literature on wars shows that a significant majority of them take place among physically proximate entities, Caselli et al. (2014). The traditional models of conflict have focused on bilateral conflicts or on groups of countries in conflict (Garfinkel and Skaperdas (2012)). As bilateral conflicts create spillovers to other conflicts and as the spillovers are mediated by the pattern of neighborhood relations, it is important to develop general models of conflict in networks. The literature surveyed below is a first step in this direction.

We start with a static conflict game on a network. The presentation draws on Franke and Öztürk (2009). There is a set $N = \{1, \ldots, n\}$, where $n \geq 3$ of agents that are located in an undirected network g. The set of rivals of agent i is given by $N_i(g)$, and so agent i is engaged in $n_i(g) = |N_i(g)|$ conflicts. The outcome of each bilateral conflict is probabilistic and depends on the investment in conflict by the respective rivals. For concreteness, we shall suppose that

[11] For a survey of the literature on co-evolution of networks and behavior, see chapter XX by Vega-Redondo (2015).

the conflict technology is the linear Tullock contest function. In a conflict between i and j, and given investments e_{ij} and e_{ji} the probability of winning for agent i is given by

$$p_{ij}(e_{ij}, e_{ji}) = \frac{e_{ij}}{e_{ij} + e_{ji}}, \tag{5}$$

so long as $e_{ij} + e_{ji} > 0$. In case $e_{ij} + e_{ji} = 0$, the probability of either player winning is $1/2$. Each agent i chooses a investment for each of his conflict links $\mathbf{e_i} = (e_{ij})_{j \in N_i}$. The cost of investment in conflict is given by the function $c(e_i)$. For simplicity, we assume that $c(e_i) = (\sum_{j \in N_i} e_{ij})^2$. The reward from winning a conflict is V, while the cost of losing is $-V$. We may now write the payoffs of agent i in network g, with investment profile $e = (e_1, \ldots, e_n)$, as

$$\pi_i(e) = V \sum_{j \in N_i} [p_{ij}(e_{ij}, e_{ji}) - p_{ji}(e)] - c(e_i). \tag{6}$$

The interest is in understanding how the network shapes conflict. We will focus on Nash equilibrium in conflict investments.

Define $e^*(g)$ to be an equilibrium for network g. Franke and Öztürk (2009) start by showing that there exists a unique equilibrium in this model and that it is interior. Define $E_i^*(g)$ to be the aggregate equilibrium investment by player i in network g. Equilibrium investments satisfy the following property: for each $i \in N$ and each $k \in N_i$,

$$V \frac{e_{ik}^*}{[e_{ik} + e_{ki}]^2} = E_i(g). \tag{7}$$

Let $e^*(g)$ be the equilibrium profile of investments in network g and let $E^*(g) = \sum_{i \in N} E_i^*(g)$. be an aggregate equilibrium investments or the conflict intensity.

Franke and Öztürk (2009) provide results on some well known special classes of networks. We present their results on regular networks and the star network.

Proposition 3 *Conflict equilibrium exhibit the following properties.*

1. *Regular networks: Conflict intensity is increasing in degree, d, and in number of agents n. Conflict intensity is higher in g_1 than in g_2 if and only if $n_1\sqrt{d}_1 > n_2\sqrt{d}_2$. Individual investment and expected payoff is decreasing in degree and does not depend on number of agents. Expected equilibrium payoff is negative for all agents.*

2. *Star network: Conflict intensity is increasing in the number of peripheral agents. For*

the center agent, link specific (aggregate) investment is decreasing (increasing) and the expected payoff is decreasing in number of peripheral agents. For the periphery agent, conflict investment is declining and payoffs are increasing.

Franke and Öztürk (2009) offer us an interesting first look at conflict in networks. Their results illustrate how the cost function and network creates spillovers and how these spillovers in turn shape behavior by different agents in a network. As the authors note, the problem of characterizing conflict in general networks remains an open problem.

In a recent paper, Konig et al. (2014) study conflict in a network setting where links may be positive (as between allies) or negative (as between enemies). They provide a characterization of conflict investments as a function of the network: investments by allies are strategic substitutes, while investments by enemies are strategic complements. They then show that equilibrium investments are proportional to Bonacich centrality of the allies and enemies networks, respectively. They then apply these results to understanding the nature of conflict in the Congo.

The authors assume a linear Tullock contest function and the conflict is static. In real world conflicts dynamics play an important role, as winners of current conflicts acquire more resources and power that they can use to subsequent conflicts. We examine the dynamics of conflict in the next section.

3.1 Dynamics of conflict

We now take up the study of conflict as a dynamic process with resource accumulation for the winner and elimination of the losers. By way of motivation, consider the example of a kingdom or a country seeking to expand its territory by means of military conquest. This drive toward expansion will typically be geographically constrained as it is difficult to conduct military campaigns far away from established territory. Indeed, empirical research shows that the vast majority of conflicts are amongst physically neighboring entities. Moreover, once a particular territory has been conquered and integrated, new territories close to the conquered territory become accessible. In addition, the resources of the newly acquired territory can be used for further conquest. Historians use archaeological evidence to argue that the Roman empire used resources from occupied territories around the Mediterranean to supply legions during the invasion of Western Europe and Britain.

Conflict may also take non-military forms, such as a company seeking to expand into new markets. It is easier for a company to expand into markets that are closely aligned to

its current markets, either geographically or in terms of product lines. Once a foothold has been established in a new market, this generates resources for further expansion. In addition, markets closely aligned to the newly entered market become more accessible.

The presentation here draws on De Jong et al. (2014), who study a framework where a number of agents seek to capture resources through conflict. At the start, individuals have resources. Each individual is located at a node of a network. As time goes by, opportunities arise for individuals to 'fight' and capture the resources of neighboring nodes. A conflict is modeled as a Tullock contest. The conflict yields a winner and a loser. The winner captures the resources of the loser and expands his influence in the network.

There are three ingredients in this framework: the initial resources of individuals, the network structure, and the technology of conflict (the parameters of the Tullock contest function). Their goal is to characterize the dynamics of conflict and the rise and fall of empires.

A set of players $P = \{1, 2, \dots n\}$ engage in conflict over a network with nodes $N = \{1, 2, \dots n\}$. Nodes have attached resources $r = (r_1, r_2, \dots, r_n)$. The set of all links form a connected network g.

Each node is controlled by one of the players. Let $S_i^t \in P$ denote the player in control of node i in period t, with $t = 0, 1, 2, ...$ Each player starts with ownership of their 'own' node, so that $S_i^0 = i$. Ownership of nodes may change during the game, depending on conflict outcomes. Let $G^t = \{g_{ij} \in g \mid S_i^t \neq S_j^t\}$. This is a sub-network of g containing all the links that connect nodes controlled by different players. Note that the value of G^0 is g. At the beginning of period t, a link $L^t \in G^t$ is selected with equal probability.

The players who control the nodes at two ends of the link each use the combined resources from their respective nodes. The winner of the contest gains control of the loser's nodes. Define $R_u^t = \sum_{S_k^t = u} r_k^t$, the total resources available to player u in period t. Let $g_{ij} = L^t$ be the selected link in G^t at round t. Then players S_i^t and S_j^t engage in a Tullock contest. Suppose, without loss of generality, that $S_i^t < S_j^t$. Then W_i^t is defined to be the binary variable describing the winner of the contest in period t, taking value 1 if player S_i^t wins and 0 if player S_j^t wins. The distribution of this variable is

$$P(W_i^t = 1) = \frac{(R_i^t)^\gamma}{(R_t^t)^\gamma + (R_j^t)^\gamma}$$

where $\gamma > 0$ is the parameter of the Tullock contest function.

The network is then updated depending on the value of W.

$$S_v^{t+1} = S_v^t \qquad \text{for v} \neq i, j$$
$$S_v^{t+1} = W^t S_i^t + (1 - W^t) S_j^t \qquad \text{for v} = i, j$$

The game ends when there is only player left, who is denoted the victor.

In this basic model, one player is eliminated in every period, so the dynamics must end in period $n - 1$. Moreover, *For $\gamma < +\infty$ and $r \in \mathbb{N}^n$, the game ends in $n - 1$ periods and the probability for any player to win the game is strictly positive.*

We now turn to how the probability of victory is affected by starting resources and network position. To make progress, De Jong et al. (2014) specialize the model and consider the case of linear Tullock function. Define $R = \sum_{i=1}^{n} r_i$. They establish:

Proposition 4 *Let $\gamma = 1$. Then the probability for player i to win the game is given by $P(i) = r_i/R$.*

The intuition behind this result is as follows. In order to win the game, a player must eventually capture all other resources. The player can do this in a single contest, fighting all other resources at the same time, in which case the probability of winning is as above. If the player engages in an intermediate contest, the increased probability of winning the final contest compensates exactly for the probability of losing the intermediate contest for γ equal to one. Network position influences the timing and frequency of contests, and therefore has no effect on win probability. For $\gamma < 1$, the Tullock contest function is everywhere concave in resources, and so resources gained in the intermediate contest do not compensate for the chance of losing the intermediate contest. If $\gamma > 1$, then the Tullock contest function is convex on part of its domain, so depending on resources, the resources gained from the intermediate contest may compensate for the chance of losing. In order to illustrate the effects of interaction between the technology of conflict and network structure, we consider a specific network, the star.

Proposition 5 *Let G be a star network with n peripheral nodes, and let resources be homogeneous among peripheral nodes, so that $r = (r_c, r_p, ...r_p)$. Then the win probabilities for central*

and peripheral nodes are given as follows.

$$P_c(r_c, r_p, \gamma) = \prod_{i=0}^{n-1} \frac{(r_c + r_p)^\gamma}{(r_c + ir_p)^\gamma + r_p^\gamma} \tag{8}$$

$$P_p(r_c, r_p, \gamma) = \frac{1}{n}(1 - P_c(r_c, r_p, \gamma)) \tag{9}$$

It is important to explore the interaction between resources, network and technology of conflict a bit more closely. To illustrate the richness of this relationship it is worth looking at the limiting case when $\gamma \to +\infty$. When $\gamma \to +\infty$, the Tullock contest reduces to the all-pay auction, where the player with higher resources wins with probability one. Consider a network with three nodes in a line, with resources r_1, r_2 and r_3. First, note that the player with the lowest resources has negligible probability of winning, regardless of network position. If any player has resources higher than the combined resources of the other two players, that player will win with probability close to 1, regardless of network position. So, the network position is irrelevant. Let $r_2 > r_1 = r_3$ and $r_2 < r_1 + r_3$. Then player 2 wins with probability one, and the marginal effect of resources is zero for all players. Now switch the location of player 2 and player 1. Then player 2 wins with probability $\frac{1}{2}$, and player 1 and 3 win with probability $\frac{1}{4}$. For players 1 and 3, adding any amount of resources increases win probability by a further $\frac{1}{4}$. To summarize, the network position can have either no effect or a very large effect, and a small amount of resources can have either no impact or a very large impact, depending on the network and current resource allocation.

These results suggest a very rich interaction between resources, networks and the technology of conflict in shaping conflict dynamics. A general analysis of this problem remains an open problem.

The framework presented above raises a number of interesting further questions. The network is taken as given. In a recent paper, Huremovic (2014) studies conflict in an evolving network. We have assumed that nodes engage in conflict, but a natural question is whether they have an incentive to engage in conflict. If the technology of conflict is very equalizing (γ close to 0) then nodes would prefer to not fight, as there is no gain in terms of additional resources, while there is a cost in terms of positive probability of elimination. Another issue relates to alliances: so far we have assumed that nodes remain independent. But alliances are a salient feature of international as well as civil conflict. We take up the role of alliances in shaping conflict next.

4 Alliances, networks and conflict

International and civil wars impose enormous direct costs on the parties involved and are have large indirect costs on third parties. Empirical work shows that around 40% of the wars with more than 1000 casualties involved more than 2 countries and large conflicts such as the World Wars and the Vietnam War involved alliances with many nation states. More generally, alliances have been a central element in violent conflict throughout history. These considerations motivate a study of alliance formation and how it shapes the intensity of conflict.[12]

We begin with a presentation of a recent paper by Jackson and Nei (2014).[13] They develop a model for the incentives of countries to attack each other, to form alliances, and to trade with each other. There is a set $N = \{1, ..., n\}$, where $n \geq 3$, of countries. Countries are linked through alliances, represented by a network of alliances g. If two countries are linked then they are allies. Let $g - i$ denote the network obtained by deleting all alliances that involve country i. Let $\mathcal{CL}(g)$ denote the set of cliques in network g. Each country $i \in N$ is endowed with a military strength $M_i \in \mathbb{R}_+$. For any subset of countries $C \subseteq N$, let $M(C) = \sum_{i \in C} M_i$ be their collective military strength. If there is a war between C_1 and C_2, with C_1 being the aggressor, then C_1 wins if $M(C_1) > \rho M(C_2)$. The parameter $\rho > 1$ reflects a relative advantage of being the defender and $\rho < 1$ reflects a relative advantage of being the aggressor.

The notion of 'vulnerability' plays a key role in the analysis. A country i is vulnerable at a network g if there exists a country j and a coalition $C \subseteq N_j(g) \cup \{j\}$ such that $j \in C$, $i \notin C$ and $M(C) > \rho M(i \cup (N_i(g) \cap C^c))$, where C^c is the complement of C. In this case, country j is said to be a potential aggressor at a network g. Thus, no country is vulnerable at a network g if for any coalition C of a potential aggressor j and any target country $i \notin C$, the aggressors cannot successfully attack the country. At this point, it is being assumed that winning is desirable and that losing a war is undesirable.

Jackson and Nei (2014) introduce the notion of war-stable networks to study the incentives of countries to form coalitions to defeat and conquer other countries. Define $E_i k(g, C)$ as the net gains to country k if country i is conquered by coalition C (of which k is a member), when country i is conquered by coalition given by $C' = \{i\} \cup (N_i(g) \cap C^c)$. It is assumed that there is a cost to maintaining a link $c_{ij} > 0$ between any pair of countries i, j. These costs will be

[12] There is an important body of research on groups in conflict, for a survey, see Garfinkel and Skaperdas (2012). In this survey, due to space constraints, we do not cover conflict among groups.

[13] For an early paper on network formation with antagonistic links see Hiller (2012).

taken to be small relative to the spoils from a successful war.

With this notation in place, a network g is war stable if the following conditions are satisfied:

1. no country is vulnerable at g.

2. $\forall g_{j,k} \notin g$ no country is vulnerable at g + jk,

3. $\forall g_{jk} \in g$, both j and k are vulnerable at $g - g_{jk}$.

Suppose that countries are ordered as follows: $M_1 \geq M_2 \geq .... \geq M_n$. Jackson and Nei (2014) establish the following result:

Proposition 6 *Let $n \geq 3$. There are no nonempty war-stable networks. The empty network is war-stable if and only if $\rho M_n \geq M_1 + M_2$.*

The intuition behind this result is as follows: For no country to be vulnerable and for every alliance to be productive (in terms of condition 3) networks to be sparse. However, sparse networks are susceptible to condition 2: allies of a country can join forces and defeat it. This tension suggests suggests rapidly shifting alliances and is reminiscent of the empirical patterns from the nineteenth century. Jackson and Nei (2014) report that during the nineteenth century and the first half of the twentieth century, roughly one-third of the alliances present at any time were dissolved within the next 5 years. By contrast, in the period from 1950 until 2000, this probability was around 0.05!

This sharp difference in the performance of alliances motivates a closer examination of other significant economic changes. Jackson and Nei (2014) focus on the changes in the size of international trade. They report that international trade has had two major periods of growth. The latter part of the nineteenth century and beginning of the twentieth saw a sharp rise in international trade. This rising trend was disrupted by the world wars. International trade picked up after the Second World War, recovering its pre-first world war level in the 1960's and then continuing to grow at an increasing rate thereafter. In particular, in 1850 international trade amounted to 5.1% of total world output, this share rose to 11.9% in 1913. It then remained below this level until the 1960's, picking up thereafter and reaching 25% in 2012. These changes lead Jackson and Nei (2014) to propose a richer model of alliances and wars, that incorporates the role of international trade.

They propose that a country gets a payoff $u_i(g)$ from network g, reflecting gains from trade. The notion of vulnerability is now adapted to take into account this additional consideration.

A country i is said to be *vulnerable despite trade* in a network g if there exists a country j and a coalition $C \subseteq N_j(g) \cup \{j\}$ such that $j \in C$, $i \notin C$ and (i) $M(C) > \rho M(i \cup (N_i(g) \cap C^c))$, and (ii) $u_k(g-i) + E_{ik}(g, C) \geq u_k(g)$, with some strict inequality.

The $u_k(g-i)$ reflects the trade implications of successful elimination of i: it is worth noting that a country k may stand to benefit or to lose from such a conquest. Taking this general effect into account, Jackson and Nei (2014) define network g to be *war and trade stable* if the following three conditions are met:

1. no country is vulnerable despite trade at g;
2. $\forall g_{jk} = 0$, if $u_j(g + g_{jk}) > u_i(g)$ then $u_k(g + g_{jk}) < u_k(g)$, and g_{jk} is not war-beneficial.
3. $\forall g_{jk} = 1$, either $u_j(g - g_{jk}) \leq u_j(g)$ or j is vulnerable despite trade at $g - g_{jk}$, and similarly for k.

In other words, a network of alliances is war and trade stable if no country is vulnerable despite trade, if no two countries can add an alliance that is mutually profitable (through economic or through war means), and either economic or war considerations prevent every country from severing any of its links.

For simplicity, suppose that

$$u_i(g) = f(d_i(g)) - cdi(g) \tag{10}$$

where $d_i(g)$ is the degree of i, f is concave, nondecreasing, and there is some $d \leq n-1$ such that $f(d) < cd$. Let $\bar{d}$ maximize $f(d)..cd$. In addition, let $E_{ij}(g; C) = E(d_i(g))/|C|$. Under these simplifying assumptions, Jackson and Nei (2014) establish the following existence result.

Proposition 7 *Consider the symmetric model with $d \geq 2$.*

- *If $E(d^*) \leq 2[f(d^*) - f(d^* - 1) - c]$, then any d-regular network (in any configuration), is war and trade stable network if $\rho \geq \frac{d^*+1}{d^*-1}$.*

The above proposition illustrates one route through which trade supports stable networks and thereby contains conflict. The condition provides sufficient gains from trade such that the potential spoils of a war are outweighed by the lost trade value: this in turns means that a country is never attacked by one of its own trading partners. Each country then has enough

alliances to protect itself against attacks from outside and this allows a wide range of networks to be sustained.

To summarize, the discussion above develops a simple model of network formation that yields two interesting insights. The first insight is that in a pure conflict setting individual attempts to form alliances and attack opponents leads to shifting and unstable alliances: this instability may make peace would be hard to sustain. The second insight is that the presence of large gains from trade can sustain stable alliance structures where no country is vulnerable to attack by a coalition of enemies.

In this model conflict is implicit: countries do not allocate resources and wage war on other countries. Thus the impact of alliances on the incentives to allocate resources for conflict are not explicitly considered. This public good aspect to individual contributions to a coalitional conflict are potentially important. Investing in conflict within an alliance has public good properties: the study of alliance formation in a setting where countries choose investments in conflict remains an open problem.[14]

5 Concluding Remarks

In recent years, a new literature has begun to study of the relation between conflict and networks. This paper provides a survey of this nascent literature.

In the first part, the focus was on settings where network connectivity is the key source of value. Motivated by cybersecurity and infrastructure applications the aim was to study the design and the defence of networks under threat. The basic framework involves two players: an Adversary and a Designer/defender. The Adversary uses resources to target nodes that maximize damage of the network, while the Designer/Defender uses defence resources and links to maximize the value of the residual network. We presented a number of results on optimal attack and defence targeting and on optimal design. The discussion reveals that the technology of conflict, the respective resources of the Adversary and Designer, and the network value function all play an important role in shaping conflict and in the design of the optimal network.

The second part of survey is motivated by the observation that most international conflict and civil unrest happens between physically proximate entities. Bilateral conflicts between two neighbors have spillovers on the neighbors of the neighbors. This motivates a study of

[14]For a survey on free riding and coalition formation among agents in conflict, see Bloch (2012).

conflict in networked environments. We started with a static model of conflicts and showed that aggregate conflict intensity and individual investments in conflict vary in interesting ways with the structure of the network. We then presented a model with a focus on the dynamics of conflict and conquest where winners captured the resources of the losers. Here we derived results on how the network and resources determine the winner for specific technologies of conflict and for specific networks.

In the third part, we moved to a study of alliance formation among competing nodes. The existing research provides us with insights into how gains from international trade are key to understanding the structure of alliances and the decline of international conflict in the last 50 years.

References

D. Acemoglu, A. Malekian, and A. Ozdaglar. Network security and contagion. NBER Working Paper 19174, National Bureau Of Economic Research, 2013.

D. Acemoglu, A. Ozdaglar, and A. Tahbaz-Salehi. Systemic risk and stability in financial networks. *American Economic Review*, 105:564–608, 2015.

R. Albert, H. Jeong, and A.-L. Barabási. Error and attack tolerance of complex networks. *Nature*, 406(6794):378–382, 2000.

T. Alpcan and T. Başar. *Network Security: A Decision and Game Theoretic Approach*. Cambridge University Press, Cambridge, England, 2011.

R. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, Inc., New York, NY, USA, 2001.

J. Arquilla and D. Ronfeldt. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Rand, Santa Monica, CA, 2001.

J. Aspnes, K. Chang, and A. Yampolskiy. Inoculation strategies for victims of viruses and the sum-of-squares partition problem. *Journal of Computer and System Sciences*, 72(6): 1077–1093, 2006.

M. Baccara and H. Bar-Isaac. How to organize crime? *Review of Economic Studies*, 75(4): 1039–1067, 2008.

V. Bala and S. Goyal. A noncooperative model of network formation. *Econometrica*, 68(5): 1181–1230, 2000.

F. Bloch. Endogenous formation of alliances in conflicts. In M. Garfinkel and S. Skaperdas, editors, *The Oxford Handbook of the Economics of Peace and Conflict*. Oxford University Press, 2012.

L. Blume, D. Easley, K. J., K. R., and T. T. Network formation in the presence of conatgion risk. In *Proc. 12th ACM Conference on Electronic Commerce*, 2011.

Y. Bramoulle and R. Kranton. In Y. Bramoulle, A. Galeotti, and B. Rogers, editors, *Oxford Handbook on Economics of Networks*. Oxford University Press, 2015.

A. Cabrales, P. Gottardi, and F. Vega-Redondo. Risk sharing and contagion in networks, 2010. Working Paper.

A. Cabrales, D. Gale, and P. Gottardo. In Y. Bramoulle, A. Galeotti, and B. Rogers, editors, *Oxford Handbook on Economics of Networks*. Oxford University Press, 2015.

F. Caselli, M. Morelli, and D. Rohner. The geography of inter-state resource wars, 2014. Working Paper, Columbia University.

D. Cerdeiro, M. Dziubiński, and S. Goyal. Contagion risk and network design. Cambridge-INET Institute 2015-04, 2015.

M. De Jong, A. Ghiglino, and S. Goyal. Resources, conflict and empire. mimeo, 2014.

Department of Homeland Security. *Office of Infrastructure ProtectionStrategic Plan: 2012-2016*. Washington, DC, 2012.

M. Dziubiński and S. Goyal. Network design and defence. *Games and Economic Behavior*, 79(1):30–43, 2013.

M. Dziubiński and S. Goyal. How to defend a network. Cambridge-INET Working Paper 2014-01, 2014.

M. Elliot, B. Golub, and M. Jackson. Financial networks and contagion. *American Economic Review*, 104:3115–53, 2014.

H. Eun. *Impact analysis of natural disasters on critical infrastructure, associated industries, and communities*. PhD thesis, Purdue University, West Lafayette, 2010.

J. Farrell and G. Saloner. Installed base and compatibility: Innovation, product preannouncements, and predation. *American Economic Review*, 76:940–955, 1986.

J. Franke and T. Öztürk. Conflict networks. Ruhr Economic Papers 116, University of Dortmund, 2009.

M. Garfinkel and S. Skaperdas. *The Oxford Handbook of the Economics of Peace and Conflict.* Oxford University Press, 2012.

S. Goyal. Sustainable communication networks. Tinbergen Institute Discussion Paper TI 93-250, Rotterdam-Amsterdam, 1993.

S. Goyal. *Connections: an introduction to the economics of networks*. Princeton University Press, 2007.

S. Goyal and A. Vigier. Attack, defence, and contagion in networks. *Review of Economic Studies*, 81(4):1518–1542, 2014.

F. Harary. The maximum connectivity of a graph. *Proceedings of the National Academy of Science*, 48(7):1142–1146, 1962.

T. Hiller. Friends and enemies: A model of signed network formation. Working paper, Bristol University, 2012.

K. Huremovic. Rent seeking and power hierarchies: A noncooperative model of network formation with antagonistic links. Nota di Lavoro 45.2014, Fondazione Eni Enrico Mattei, Milan, Italy, 2014.

India Today. Political agitations affect railway service. (March 26), 2011.

M. Jackson and S. Nei. Networks of military alliances, wars, and international trade. mimeo, 2014.

M. Katz and C. Shapiro. Network externalities, competition and compatibility. *American Economic Review*, 75(3):424–440, 1985.

K. Kliesen. The economics of natural disasters. *The Regional Economist*, April, 1995.

M. Konig, M. Rohner, D. Thoenig, and Zilibotti. Networks in conflict: theory and evidence from the great war of africa. mimeo, 2014.

H. Kunreuther and G. Heal. Interdependent security. *The Journal of Risk and Uncertainty*, 26(3):231–249, 2004.

G. Luft. Pipeline sabotage is terrorists weapon of choice. *Energy Security*, March 28, 2005.

R. B. Myerson. Graphs and cooperation in games. *Mathematics of Operations Research*, 2: 225–229, 1977.

M. Newman. *Networks: An Introduction*. Oxford University Press, Inc., New York, NY, USA, 2010.

S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu. A survey of game theory as applied to network security. In *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, pages 1–10, 2010.

S. Staniford, V. Paxson, and N. Weaver. How to own the internet in your spare time. In *Proceedings of the 11th USENIX Security Symposium*, pages 149–167, Berkeley, CA, USA, 2002. USENIX Association.

G. Tullock. *Efficient Rent Seeking*, pages 97–112. Texas A&M University Press, College Station, TX, 1980.

R. Vega-Redondo. In Y. Bramoulle, A. Galeotti, and B. Rogers, editors, *Oxford Handbook on Economics of Networks*. Oxford University Press, 2015.

S. Zhu and D. Levinson. Disruptions to transportation networks: A review. *Working Paper, University of Minnesota*, 2011.