EFFICIENT TERRORIST NETWORKS IN THE PRESENCE OF INFILTRATION[a]

[Job Market Paper]

Siddhartha Bandyopadhyay[*] **Tamoghna Bose**[†] **Sebastian Cortes-Corrales**[‡] **Aditya Goenka**[§]

July 12, 2025

Abstract

Abstract: Terrorist organisations face a dilemma: increased connectivity can enhance their benefits but also increase the risk of infiltration. In this paper, we examine how infiltration by law enforcement authorities affects the structure of terrorist networks. We model the network structure in the presence of infiltration and solve for an efficient network. The efficient network is determined by the probability of an individual terrorist being captured through direct and indirect connections. If capturing an individual terrorist is possible through both direct and indirect connections with equal probability, the efficient structure will form of maximally connected sub-structures i.e., 'components'. If the probability of an individual terrorist getting caught through direct connections is higher than indirect connections then non-maximally connected sub-structures may arise. The efficient network can have either symmetric or asymmetric components, depending on the probability of infiltration. For some parameter values the efficient network is composed of only symmetric components.

Keywords: infiltration, efficiency, components, non-maximally-connected, targeting-technology, law-enforcement.

JEL Classification : D02, D70, D85, L23.

[*]Department of Economics, University of Birmingham, s.bandyopadhyay@bham.ac.uk

[†]School of Liberal Arts, Bennett University, tamoghna.bose@bennett.edu.in

[‡]Department of Economics, University of Birmingham, s.cortescorrales@bham.ac.uk

[§]Department of Economics, University of Birmingham, a.goenka@bham.ac.uk

a We would like to thank participants at the Lancaster Game Theory Conference, 11th Warwick Economics PhD Conference, Birmingham Economic Theory Workshop, 2023, University of Calcutta 9th Research Scholar Workshop, 2024, Birmingham Business School Conference, 2024, as well as Kalyan Chatterjee, Antonio Cabrales and Michael Konig for helpful comments

1 Introduction

Law enforcement intelligence units often employ strategies to gather sensitive information aimed at dismantling terrorist plots. The Intelligence Handling Model (IHM), jointly developed by MI5 and Counter Terrorism (CT) policing in 2011, emphasizes gathering and analysing information to mitigate terrorist activities.[1] Using IHM, MI5 and CT policing thwarted 20 Islamist terrorist plots between 2013 and 2017. This strategy of gathering information to infiltrate is applicable to a wide range of organisations from terrorist groups to drug cartels, enabling the effective disruption of their activities through targeted intelligence gathering. In this chapter we aim to understand the efficient network structures of such organisations when law enforcement organisation can capture terrorists or other criminal networks using infiltration. For illustrative purposes we will continue to describe these as terrorist networks but they include these wider networks of interest to law enforcement.

We ask two main questions in this chapter: Given the presence of infiltration techniques like surveillance and electronic eavesdropping, how do terrorist organisations structure themselves? How do individual terrorists undertake productive activities within such organisational structures? These questions underscore the complexities and challenges in the fight against terrorism and organised crime.

While this matter pertains to the extensive body of literature on organisational structure, it does not center on infiltration, which is the primary focus of our chapter. Some papers discuss the internal efficiency of organisations, while others focus on external considerations. Baccara and Bar-Isaac (2008) combined both internal and external efficiencies in a crime setting. Their paper discusses the trade-off between concerns to increase internal efficiency (sustaining cooperation) against the threat of greater vulnerability to an external threat (increasing the probability of indirect detection) in an organisation

Our chapter differs from Baccara and Bar-Isaac (2008) in two key aspects. Firstly, we model the importance of interactions for the purpose of production, while they focus on interactions to enforce cooperation. For example, in a terrorist organisation, effective mutual support and resource sharing for production among members increase individual and total payoffs. Secondly, we determine the efficient network structure based on the probabilities of capturing players (i.e., terrorists) through direct and indirect connections. This is influenced by the 'precision' parameter used for targeting and the path length between terrorists, and it is independent of the level of information exchange. In contrast, Baccara and Bar-Isaac (2008) base their structure on whether detection depends on cooperation levels. Our approach considers the interconnectedness of terrorists and the associated capture risks, whereas theirs focuses on cooperation's impact on detection risks.

Our study seeks to answer the following research questions: What are the effort and utility for each member of a terrorist network, given a specific structure and the probability of infiltration? Furthermore, what constitutes an efficient terrorist network structure considering a given probability of infiltration?

In this chapter, we focus on understanding the efficient structure of the terrorist network designed. Terrorist networks often design multiple sub-structures, each sub-structure undertakes production cooperatively within those structures but independent of the other sub-structures. We model this as a terrorist network comprising of 'N' terrorists. There exists a head of the network, henceforth referred to as the 'Leader', who decides on these sub-structures of the terrorist network. The leader designs these networks keeping in mind the probability that an individual terrorist is captured directly or through direct and indirect connections. In our model, we focus on understanding these sub-structures inside the terrorist network and abstract away from the links between the leader and the terrorists inside the network. This leader operates from a concealed location, and his communication with other terrorists is assumed to be undecipherable by law enforcement authorities. He is cognizant of the potential for infiltration, understanding that law enforcement authorities can randomly target a terrorist through infiltration. Given this understanding, we model this as an extensive form game which we explain below.

In our chapter we explore the trade-offs terrorist organisations face: increased connectivity yields organisational benefits but also escalates the costs posed by infiltration. By examining how organisations navigate this balance, we seek to understand the architecture of efficient networks in the presence of infiltration threats. By an efficient network, we mean a terrorist organisation that maximizes the sum of utilities of its individual terrorists. We model this as a Stackelberg structure: the terrorist leader moves first, followed by the individual terrorists. The objective of the terrorist leader is to decide on the efficient network structure, given the possibility of infiltration. The in-

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664682/Attacks_in_London_and_Manchester_Open_Report.pdf

dividual terrorists then choose their effort to maximize their utilities within this network structure. In our model, the law enforcement authority is not modelled explicitly, instead, their presence is reflected in the utility functions of the individual terrorists, with each terrorist facing a random chance of being targeted. We solve this game by backward induction and solve for the Sub-game Perfect Nash Equilibrium (SPNE).

Our results show that if an individual terrorist can be captured through both direct and indirect connections with probability one if infiltration is successful, the efficient network consists of maximally connected sub-structures called 'components'. In the presence of infiltration, there is an optimal degree of separation within an efficient network depending on the probability of infiltration. Additionally, we also explore how structures within the network fluctuate with changes in infiltration probabilities. Our finding suggests that at low infiltration levels, the terrorist leader designs a single, complete structure. However, with increased infiltration risk, the network breaks down into smaller sub-structures. The components designed within these efficient networks can be either symmetric or asymmetric, depending on the probability of infiltration. For some parameter values, the efficient network consists only of symmetric components. When punishments in the form of fines are sufficiently high or when the degree of complementarity is low, we observe the emergence of symmetric components in our chapter. When an individual terrorist exerts maximal effort, even with high infiltration probability, an efficient network is not necessarily composed of empty sub-structures. We also conducted a series of comparative static analyses to understand how individual efforts and utilities vary in response to changes in key factors: the number of neighbours each terrorist has, the size of the terrorist network, the level of fine each terrorist faces, and the degree of complementarity between the efforts of terrorists. Our analysis shows that when the marginal cost of capture due to an increase in neighbours outweighs the marginal benefits from complementarity, the equilibrium effort decreases as the number of neighbours grows. The effect on equilibrium utilities is ambiguous: if the marginal change in equilibrium effort is non-positive, the marginal change in equilibrium utility is unambiguously negative. If the marginal change in equilibrium effort is positive, the effect on utilities remains ambiguous. If equilibrium effort is non-decreasing with the number of neighbours, the marginal change in complementarity between efforts is positively correlated with utility. Otherwise, it depends on the relative strength of the marginal benefit and cost. If the marginal change in equilibrium effort with respect to complementarity is non-positive, the marginal change in utility is negative. Otherwise, it depends on whether the benefits of increased complementarity outweigh the costs. We will discuss these comparative statics in more detail later.

Next, we focus on a second formulation where a terrorist can only be captured directly and not through any of its connections being infiltrated. In this case, the efficient network consists solely of symmetric components. At the end, we considered the formulation where the probability of capturing a terrorist through direct connections is higher than through indirect ones.[2] In this case, non-maximally connected sub-structures may emerge. Here, the likelihood of capturing a terrorist is inversely proportional to the distance between them and their connections.
Our model demonstrates that within a network, although there is a degree of separation between the sub-structures but within each sub-structure individual terrorists work closely i.e., they are maximally connected. This pattern is also observed in the analysis conducted by Krebs (2002).[3] Krebs (2002) uses publicly available data to construct a partial network map centred around the 19 hijackers. Examining the 9/11 terrorist network, we observe varying degrees of connectivity among the terrorists. Some were closely linked, while others had minimal connections. The 19 hijackers were divided into four groups, each responsible for crashing a plane at different locations. Although unfamiliar with each other before the attacks, they worked seamlessly together. Figure 1 illustrates the network of the 19 terrorists involved in the 9/11 attack. This is derived from mapping which terrorists were in which flight and from the sequence of events occurring within each flight which indicated there was close cooperation of the terrorists within each flight but not across flights. The diagram uses colour-coded blocks to represent the terrorists associated with each plane. Three planes had five terrorists onboard, while one had four. This suggests that the terrorists on each plane worked closely together, coordinating tasks such as subduing passengers but did to have any connections across the different planes. This pattern indicates that terrorists tend to operate in cohesive groups.

Although the primary motivation for this chapter is to analyse efficient terrorist networks and the resultant level of terrorising activities, the trade-offs and considerations discussed herein are also applicable to industrial espionage, spread of infections and systematic risk in banking models. Consequently, our findings can offer insights into the efficient network structure in contexts involving infiltration and other social networks where trust is a key factor in business proceedings. This will be discussed in more detail in the conclusion. In Section 2, we review the related literature, followed by the presentation of the general model in Section 3. In this section, we discuss the various cases of captures through connections. We characterise the equilibrium and do comparative statics of when the

[2] previously studied by Watts (2001) and Bala and Sanjeev Goyal (2000)

[3] https://www.aclu.org/sites/default/files/field_document/ACLURM002810.pdf

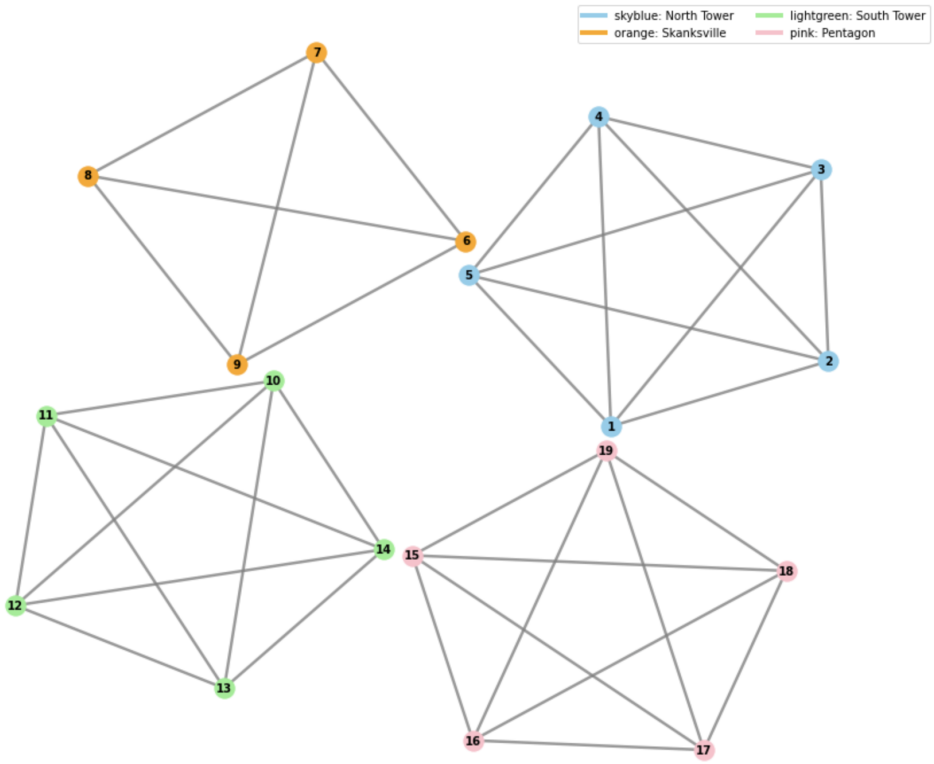

Figure 1: Network of 19 hijackers during execution of 9/11 attacks

probability of capture through connections is 1. Finally, Section 4 offers conclusions and potential directions for future research.

2 Related Literature

Our research contributes to the economic theory of networks[4], the literature on hide-and-seek [5] and related security games [6] by utilising peer effects models (see Durlauf (2004)), with a focus on centralized network design and defence strategies against the possibility of an attack.

Our chapter specifically focuses on crime, making it essential to review the literature associated to crime economics. The individual-level analysis of crime dates back to Becker (1968), who framed crime as an economic decision-making problem and provided insights into an individual's optimal response to the expected penalty of committing crime. The subsequent literature does not focus on how crime is committed when criminals work with their accomplices as a group and how such networks can be deterred.[7] Papers by Sarnecki (2001) and Warr (2002) suggest crime often originates within social networks, with criminals frequently having accomplices. In economics, studies like Glaeser, Sacerdote, and Scheinkman (1996) propose that crime-prone neighbourhoods can induce individuals to commit more crimes. Case and Katz (1991) found a ten percent increase in neighbourhood juvenile crime rate leads to a 2.3 percent increase in individual delinquency. According to Calvó-Armengol and Zenou (2004), delinquents engage in competition with each other in criminal activities but also derive benefits from having friendships with other criminals. These connections enable them to learn and acquire valuable know-how within the criminal domain. Our chapter also focuses how the marginal utility of an individual's action is influenced by the average level of that action taken by their peers.

[4]Network theory examines network formation, optimal structures, and the performance of social and economic networks under various conditions; see e.g., Vega-Redondo (2007); Jackson et al. (2008); Sanjeev Goyal (2012); Sanjeev Goyal (2023); Allen and Babus (2009); Cabrales, Gale, and Gottardi (2016).

[5]The first paper on hide-and-seek games was by Von Neumann (1953). Interestingly, the value of this 'hide-and-seek game' on a fixed arbitrary network can be computed using fractional graph theory, as shown by D. Fisher (1991).

[6]The literature on security explores the optimal allocation of limited security resources—such as guards or cybersecurity measures—to protect assets against threats (see e.g, Sinha et al. (2018), Kiekintveld et al. (2009) and Sanjeev Goyal and Vigier (2014)).

[7]See Ehrlich (1975); Ehrlich (1996); Heineke (1978); Brown and Reynolds (1973); Allingham and Sandmo (1972)

Notably, the works by Ballester, Calvó-Armengol, and Zenou (2006) and Ballester, Zenou, and Calvó-Armengol (2010), examines finite population non-cooperative games with linear-quadratic utilities, interpreting them as network games where each player's Nash equilibrium action is linked to her Bonacich centrality. It also analyses how aggregate equilibrium behavior varies with network size and density and introduces a policy for identifying and targeting the 'key-player' and 'key-group' whose removal optimally impacts aggregate activity. Their findings, when applied to the realm of crime, suggest that both a direct and an indirect effect on crime reduction. The insights gleaned from these papers can be considered as effective deterrence strategies when dealing with criminals operating as a cohesive group. Based on Ballester, Calvó-Armengol, and Zenou (2006) framework, we developed a model to study the efficient structure of terrorist networks in the presence of infiltration. In contrast to property crimes, these organisations are sometimes driven by non-profit motives, such as religious extremism, political ideology, or social and economic grievances. One can thus think of a leader who shares this ideology trying to maximize the sum of utilities of the members. Terrorist networks, being vulnerable to infiltration, give rise to various structures within the network. [8] Although these various structures function independently, the terrorists within each structure complement each other's roles (see e.g., Schorkopf (2003) and Baccara and Bar-Isaac (2008)) For instance, some members may specialise in bomb-making, others arrange resources, some know the right hideouts and some focus on attack preparations. This interdependence in their production and planning process creates a scenario where their efforts enhance each other's utility through collaboration. Our model suggests that different levels of infiltration, followed by appropriate punishment upon capture, can induce changes in the structure of a terrorist network. The connectivity within the structures and the number of structures varies depending on the probability of capture through direct and indirect connections. Understanding these structures is crucial for law enforcement authorities as it enables them to allocate their resources effectively, thereby enhancing their ability to combat crime more efficiently in the future.

Previous literature on centralized network design and defence often assumes homogeneity among nodes(see e.g., Bloch, Dutta, and Dziubiński (2020); Chen, Touati, and Zhu (2019); Gueye, Walrand, and Anantharam (2012)). Goyal et al. (2013) analysed a two-stage game where a designer selects and protects a network, and an attacker then targets nodes. They showed that optimal network formation varies with defence costs, favouring sparse networks when defence is affordable. Sanjeev Goyal and Vigier (2014) found that a centrally-protected star network often maximizes the designer's payoff. Cerdeiro, Dziubiński, and Sanjeev Goyal (2017) further explored decentralized defence, highlighting potential inefficiencies in security investment under this model. Stupak (2023) extends the literature on centralized network design and defence in three key directions: (1) by introducing heterogeneous vertices valued according to their degree centrality—the number of immediate neighbours a vertex has, (2) by modeling the simultaneous distribution of attacking and defensive resources by the Defender and Attacker and (3) by considering an adversary whose goal is to extract value from the network rather than merely disrupt it. They confirms that a centrally-protected star is the most secure formation, it also shows that it is the least efficient, appearing in equilibrium only when the cost of a single link is sufficiently high.

Drawing on prior research, our study makes three key contributions to network security models. In our chapter, we further extend the literature on centralized network design and defence by incorporating the Ballester, Calvó-Armengol, and Zenou (2006) framework. Unlike previous studies on defence, our chapter does not involve the allocation of defensive resources by the designer (referred to as the leader). Instead, the designer designs the network structure such that individual nodes (referred to as terrorists) work closely within a substructure, while maintaining separation between each substructures. Specifically, we introduce decision-making by individual terrorists for production activities within a substructure. The attacker in our model (referred to as law enforcement authorities) randomly targets a terrorist for capture. The number of terrorists captured through the links of the targeted terrorist is determined by the targeting technology. As in the existing literature, the attacker's objective is to disrupt the network. The designer, on the other hand, designs the network structure with the assumption of an external threat. We consider three distinct cases in our analysis. In the first case, the probability of capture through connections is 1. In the second case, the probability of capture through connections is 0. Finally, in the third case, we examine the case where there are unequal probabilities of capture through direct and indirect connections.

Our game is a variant of the hide-and-seek game, extensively studied in economics and computer science (see e.g., Bloch, Dutta, and Dziubiński (2020); Crawford and Iriberri (2007); Dziubiński and Roy (2018); David C Fisher (2002); Waniek, Michalak, Rahwan, et al. (2017); Waniek, Michalak, Wooldridge, et al. (2018)). Originat-

[8] The survey of non-judicial publications on terrorism suggests a shift in the characteristics of modern terrorism, marked by new actors, means, and ideologies, particularly the heightened role of religious fundamentalism. Fundamentalists, view the world as an eternal struggle between good and evil. Furthermore, the terrorist are now organized into small, durable cells within networks, making it more difficult for law-enforcement authorities to combat these organisations. https://www.ojp.gov/pdffiles1/nij/grants/208551.pdf

ing from Von Neumann (1953), these games have applications in security and auditing. While previous studies like Dziubiński and Roy (2018), Waniek, Michalak, Rahwan, et al. (2017) and Waniek, Michalak, Wooldridge, et al. (2018) focused on exogenously defined resources and non-strategic seeker responses, our approach builds on Stupak (2023), where the seeker (attacker) randomly selects a node to attack. However, in our model, the attack is non-strategic. Here, an individual node can be vulnerable both directly and through indirect connections, with vulnerability determined by exogenous probabilities of successful infiltration. The hider, aware of these vulnerabilities, designs the network structure accordingly. Within this structure, individual nodes maximize their payoffs by selecting optimal actions. Our focus is not only on network design but also on individual node decision-making within the designed network.

In addition to other strands of literature, our chapter relates to the financial contagion literature. Early models of counterparty risk, such as Rochet and Tirole (1996) and Allen and Gale (2000) explore the behaviour of banks and depositors. For instance, Allen and Gale (2000) analyses banks facing liquidity shocks, similar to the probability of infiltration in our model. To mitigate these shocks, banks can exchange deposits ex-ante. More recent studies (see e.g., Blume et al. (2013); Elliott, Golub, and Jackson (2014); Acemoglu, Ozdaglar, and Tahbaz-Salehi (2015)) examine interdependencies between banks, such as lending and liquidity provision, which can help distribute shocks and reduce the likelihood of individual failures. However, large shocks can still cause failures, with interdependencies transmitting the impact more widely. The extent of contagion depends on the model and the types of contracts between institutions. Our chapter is closely related to Cabrales, Gottardi, and Vega-Redondo (2017), who study optimal financial structures to minimize bank defaults. However, our research differs in three key ways: (1) we analyse the decision-making processes of individual terrorists within a pre-designed network structure designed by a terrorist leader, (2) we explore various cases of capture probability through direct and indirect connections, influenced by both law enforcement's targeting parameter values and the network's design and (3) we focus on a production network, examining contagion in a criminological context. Further details of the model and results are discussed in the next section.

3 Model

3.1 Network

There are $n \geq 3$ terrorists in the model. The terrorist network $\mathcal{G}$ is the pair $(N, \mathcal{E})$ consisting of a set of terrorists $N = \{1, 2, \ldots..n\}$ and a set of links $\mathcal{E} \subseteq N^2$ between them. Terrorists i and j are connected by a link if and only if $(ij) \in \mathcal{E}$. The neighbourhood of a terrorist $i \in N$ is represented by the set $N_i = \{j \in N : (ij) \in \mathcal{E}\}$. The degree d_i, gives the number of neighbours of terrorist $i \in N$, i.e., $d_i = |N_i|$. The terrorist network is undirected $(\forall\{i, j\} : (ij) \in \mathcal{E} \Leftrightarrow (ji) \in \mathcal{E})$ and reflexive $(\forall i : (ii) \in \mathcal{E})$, implying the connections between terrorists are mutual and terrorists can have self-loops. Let, P_i^j be a path from terrorist i to j defined as a sequence of distinct links $(i_1 i_2), (i_2 i_3), ...(i_{t-1} i_t)$ such that $(i_k i_{k+1}) \in \mathcal{E}$ for each $k \in \{1, ..., t-1\}$ with $i_1 = i$ and $i_t = j$. The length of the path P_i^j is defined as the number of links in the path, denoted by $L(P_i^j)$. The distance $d(i, j)$ between terrorists i and j is defined as the minimum length of all paths from i to j. Formally, $d(i, j) = \min\{L(P_i^j) \mid P_i^j = (i_1, i_2, \ldots, i_t),\ i_1 = i,\ i_t = j,\ (i_k, i_{k+1}) \in \mathcal{E}\ \forall k \in \{1, 2, \ldots, t-1\}\}$.[9] The sequence $(i_1, i_2, \ldots, i_t)$ defines a valid path, with $i_1 = i$ and $i_t = j$, and the edge condition $(i_k, i_{k+1}) \in \mathcal{E}$ ensures that each consecutive pair of vertices is connected by an edge in $\mathcal{E}$. The set of terrorists that has a path with terrorist i is denoted as $M_i = \{j \in N : d(i, j) \neq \infty\}$. The number of all path-connected terrorists of terrorist $i \in N$ is denoted by m_i, where $m_i = |M_i|$.Component is a subset $C(\mathcal{G}) \subset N$ that is maximally connected; that is, it is, itself, connected and no $C(\mathcal{G}') \supsetneq C(\mathcal{G})$ is also connected.[10]

3.2 Individual Choices

3.2.1 Terrorists

Terrorist $i \in N$ choose an effort $e_i \in [0, B]$, with $B < \infty$, for conducting terrorist activities. These terrorists are both self-sufficient $(g_{ii} = 1)$ as well as collaborate closely with their neighbours in the production process, and as a result, the outcome of each terrorist's output depends not only on their effort but also on the combined efforts with their neighbouring terrorists. Similar to Ballester, Calvó-Armengol, and Zenou (2006), producing output collaboratively indicates 'strategic complements', where the effort of terrorist j positively influences the output of terrorist i when there is a link between i and j i.e., $g_{ij} = 1$. The degree of this complementarity between

[9] If no path exists between terrorist i and j, then the $d(i, j) = \infty$, see Jackson et al. (2008).

[10] See Cabrales, Gottardi, and Vega-Redondo (2017).

the efforts of terrorists is denoted by $\beta \geq 0$. Since terrorists operate interdependently, they may be linked to one another within the network. In our chapter, we account for various possible cases on how a terrorist can be targeted.

3.2.2 Leader

The leader of the organisation holds the authority to decide the efficient network structure and operates from a concealed position and is not reflected in the terrorist network. In our model the leader is assumed to have an objective function that maximises the sum of utilities of members of the network. The leader is well aware of the possibility of infiltration and, accordingly, makes decisions regarding the network structure. This includes determining both the internal connectivity within a component and the degree of separation between different sub-structures.

3.2.3 Law Enforcement Authorities

The law enforcement authorities does not know the terrorist network structure. Although they are not explicitly modelled, they play a role in the expected payoff function of the terrorists and, consequently, in the decision-making process of the leader. Due to the unknown network structure, the authorities resort to random targeting of terrorists and attempt to gather evidence against them. We explain the general scenario. A terrorist denoted as i can be targeted with probability $\frac{\sum_{i\neq j,\ d(i,j)\neq\infty}\delta^{d(i,j)}+1}{n}$. This implies that out of the n possible terrorists, some terrorist i, is randomly targeted for infiltration, resulting in a targeting probability of $\frac{1}{n}$. However, terrorist i can also be targeted through its path-connected members depending on targeting technology $\delta \in [0,1]$, therefore the probability of targeting a terrorist is not just $\frac{1}{n}$ but $\frac{\sum_{i\neq j,\ d(i,j)\neq\infty}\delta^{d(i,j)}+1}{n}$. The probability of successful infiltration is denoted as $p \in [0,1]$. This can be interpreted as the likelihood of obtaining hard evidence against the terrorist after they have been randomly targeted. The probability of successful infiltration and the probability of terrorist i being targeted are considered independent events in the model. When terrorist i is targeted and the infiltration is successful, they incur a negative payoff referred to as 'fine' denoted by f, where $f \in (0,\infty)$.

3.3 Time-line

The game takes place sequentially and the timeline is as follows,

- At T=1, The leader decides on the network structure.[11]
- At, T=2, Individual terrorists choose efforts and maximize their own utilities given the network structure. level,
- At, T=3, The law enforcement authorities target a terrorist at random for capture.
- At, T=4, Payoffs are realised.

We analyse the above game in the next section.

3.4 Payoffs

All payoffs are realized at the end of the game. We adapted the model of Ballester, Calvó-Armengol, and Zenou (2006). The utility function for terrorist $i \in N$ is denoted as follows,

$$u_i = \frac{\sum_{i\neq j,\ d(i,j)\neq\infty}\delta^{d(i,j)}+1}{n}(1-p)e_i(g_{ii}+\beta\sum_{j\in N}g_{ij}e_j) + \frac{\sum_{i\neq j,\ d(i,j)\neq\infty}\delta^{d(i,j)}+1}{n}p(-f)+ \Big(1-\frac{\sum_{i\neq j,\ d(i,j)\neq\infty}\delta^{d(i,j)}+1}{n}\Big)e_i(g_{ii}+\beta\sum_{j\in N}g_{ij}e_j)-\frac{1}{2}e_i^2 \quad (1)$$

Now we will delve into a detailed explanation of the right-hand side (R.H.S) of equation 1. The R.H.S comprises four terms, each representing a specific aspect of the utility function of terrorist i: The first term denotes the payoff for terrorist i when, with a probability of $\frac{\sum_{i\neq j,\ d(i,j)\neq\infty}\delta^{d(i,j)}+1}{n}$, he was targeted, but the infiltration failed with a probability of $1-p$. In this scenario, the terrorist produces an output, which is influenced by both their own effort

[11] keeping in mind the probability of infiltration

and the joint efforts made in conjunction with their neighbours.[12] The second term signifies the payoff scenario in which the terrorist was targeted, and the infiltration was successful, resulting in a negative payoff of f. The third term represents the payoff when the terrorist was not targeted. This term is independent of the probability of infiltration. The output remains a combination of the terrorist's individual effort and the collaborative contributions of their neighbours. Lastly, the final term highlights the disutility of effort. To summarise, the R.H.S of equation 1.1 represents a model that considers various factors affecting terrorists actions and payoffs. It accounts for successful and unsuccessful law enforcement attempts, the collaboration between terrorists and their neighbours, the potential consequences of being caught, and the inherent cost and difficulty of engaging in terrorist activities.

Terrorists maximize their individual utilities by choosing their effort level given a network design. The leader of the terrorist network, who operates from a hidden position and whose communication is encrypted[13], then decides on the network structure given the probability of infiltration. The leader must decide both on the internal connectivity of components and the optimal degree of each component beyond which it is efficient to separate the components. The total welfare, denoted by W, is the summation of the utilities of individual terrorists. For a given p, the efficient terrorist network structure is the structure with maximized joint payoffs. The welfare function is defined as follows:

$$\max_{\mathcal{G}} W = \sum_{i=1}^{n} u_i \tag{2}$$

Moreover, the leader's decision problem revolves around deciding on a network structure that maximizes the collective utilities of the terrorists while minimising the cost of infiltration and disruption by law enforcement authorities. This approach ensures that terrorists operate as efficiently and covertly as possible, working together to achieve their objectives while evading detection and maximizing their individual utilities. The careful balance of network connectivity and the optimization of component degrees contribute to the creation of an effective and resilient terrorist network under the leader's direction.

For tractability reasons, we will focus for now on the scenario where the targeting technology parameter $\delta = 1$. This setting signifies that a terrorist can be targeted both directly and through all path-connected terrorists with certainty, i.e., with probability 1. Subsequently, in our chapter, we delve into scenarios where $\delta = 0$ and $\delta \in (0, 1)$ and examine the efficient network structures associated with different levels of infiltration.

3.5 Case 1: Probability of Capture through connections is One

With the targeting technology parameter $\delta = 1$ the utility of individual terrorist i can be written as,

$$u_i = \frac{m_i + 1}{n}(1-p)e_i(g_{ii} + \beta \sum_{j \in N} g_{ij}e_j) + \frac{m_i + 1}{n}p(-f) + (1 - \frac{m_i + 1}{n})e_i(g_{ii} + \beta \sum_{j \in N} g_{ij}e_j) - \frac{1}{2}e_i^2 \tag{3}$$

Note the leader welfare function is represented by equation 2. We denote the above game, as $\Gamma = \langle N, (e_i)_{i \in N}, (u_i(E, \mathcal{G})_{i \in N}) \rangle$, where $E = \times_{i \in N} e_i$. We solve the game using backward induction.

Before we proceed to the existence of a Nash Equilibrium, we rearrange the utility function of terrorist i as,

$$u_i = (1 - p\frac{m_i + 1}{n})e_i(1 + \beta \sum_{j \in N} g_{ij}e_j) - p\frac{m_i + 1}{n}f - \frac{1}{2}e_i^2 \tag{4}$$

for the convenience of demonstrating the existence of the Nash equilibrium in the strategic game.

Lemma 1: The game Γ admits a Nash equilibrium, if the following conditions for each terrorist $i \in N$ are satisfied,

- e_i is a nonempty compact and convex subset of the Euclidean space.
- u_i is continuous in e_{-i}.

[12] In essence, the terrorist exerts some effort on their own for production or planning, and there is additional collaborative input from their connected neighbours.

[13] This is not explicitly modelled but assumed to justify why the leader is never captured.

- u_i is continuous and concave in e_i,

Proof of Lemma 1: See the detailed proof in Appendix A.1. We used Debreu-Fan-Glicksberg Theorem [14] to show the existence of the equilibrium.

In a network, if any two terrorists are connected by a path, they share the same set of path-connected terrorists excluding the end node. When we examine the cardinality of these sets, we find that the number of path-connected terrorists is the same for both individuals. The cardinality solely considers the size or magnitude of the sets in a network. Therefore, regardless of which terrorist pair we consider, as long as there is a path connecting them, the number of path-connected terrorists will be the same. This observation highlights the symmetric aspect of indirect connections when any two terrorists are involved through the paths.

Lemma 2: For all $i \neq q \in N$, if a path P_i^q exists between terrorist i and q, then they have the same number of path-connected terrorists, i.e., $m_i = m_q$.

Proof of Lemma 2: Refer to Appendix A.2. We explain the intuition here below, with the help of an example.

Example 1: Consider two triads connected by a line as represented by Figure 2. Now, consider terrorist 2 and terrorist 5 where a path P_2^5 exists. The set of path-connected terrorists of terrorist 2 is denoted as $M_2 = \{3, 1, 5, 6, 4\}$, and the set of path-connected terrorists of terrorist 5 is denoted as $M_5 = \{3, 2, 1, 6, 4\}$. We observe that $M_2 \cap M_5 = \{1, 3, 6, 4\}$, and the only elements different in the sets are the nodes itself i.e., 2 in M_2 and 5 in M_5. However, when we look at the cardinality of the sets, then $m_2 = |M_2| = |M_5| = m_5$. Therefore, it can be said that when a path connects two terrorists, although the sets themselves are different, they have the same number of path-connected terrorists, i.e., the cardinality is the same. Generalizing to all $i \neq q \in N$, we explain Lemma 2.

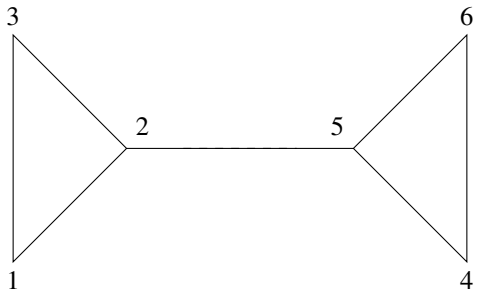

Figure 2: Two Connected Triads

In the presence of infiltration, the leader of the organisation design components (sub-networks) within the network. These components can vary from being a single complete structure to all empty sub-structures. However, specific properties of these components emerge due to certain conditions in our model. In this case, we have mentioned the use of targeting technology $\delta = 1$, that ensures if one terrorist is targeted, all the terrorists path-connected to them are also targeted.[15] This assumption enables law enforcement authorities to target terrorists not only directly but also through the targeting of their path-connected members with probability 1. Using this property, law enforcement can effectively disrupt the network operations. In Proposition 1, below we will elaborate on the connectivity in a network structure as a consequence of the assumption of the model.

Proposition 1: An efficient network is composed of components $C(\mathcal{G})$, where $d_i = m_i$ where d_i is the degree of i and m_i is the cardinality of path-connected members of i.

[14] See Debreu (1952), Fan (1952), and Glicksberg (1952).

[15] Alternatively, this can be explained as a terrorist being targeted directly and through all of their path-connected terrorists.

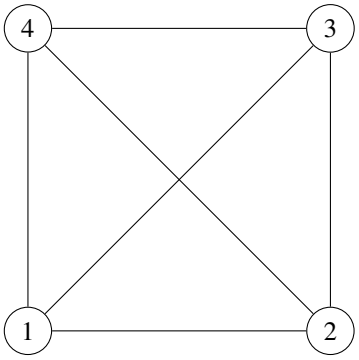

Figure 3: Complete Component

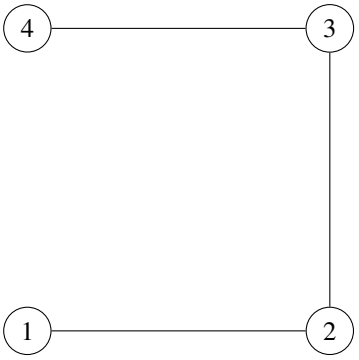

Figure 4: Line Component

Proof of Proposition 1: Please refer to Appendix A.3 for the proof.

This result highlights the strategic behaviour of the leader in designing maximally connected sub-structures i.e., components within the terrorist network. Within the designed component, individual terrorists maximize their own utilities by choosing their effort level for their illegal activities.

Discussion: To explain the rationale, we present two Figures (3 and 4), and use a proof by contradiction to demonstrate why Figure 3 represents the efficient network, as opposed to Figure 4.

Suppose the scenario where Figure 4 is regarded as the efficient network. In this case, terrorist 1 can be targeted in four different ways. They can be directly targeted, or through targeting terrorists 2, 3, and 4, as terrorist 1 is path-connected to all three of them. However, terrorist 1 receives benefits only from their direct connection, which, in this case, is terrorist 2. Now, if the leader had designed the network differently, such that terrorist 1 is connected to both terrorists 2 and 3, 1's benefits would have increased due to the additional neighbour, terrorist 3, while the risk of infiltration remains unchanged. Similarly, following the addition of a link with terrorist 3, if the leader had designed further a new structure structure where a link is present between terrorist 1 and terrorist 4, then terrorist 1's benefits would have been further enhanced while the cost from infiltration remains unchanged. The same intuition applies to other terrorists in the network. Having a terrorist located outside the direct neighbourhood but still within the component of the said terrorist only raises the cost of capture through infiltration. Thus, it is rational from the leader's point of view that in a component, all terrorists will have only neighbours and no non-neighbours, i.e., there will be no terrorist located outside the direct neighbourhood of any terrorist. This observation indicates that Figure 4 cannot be the efficient network. Therefore, we can conclude that in efficient networks, terrorists are maximally connected within their components. Thus, Figure 4 represents the efficient network.

By ensuring maximal connectivity within the components, the leader of the organisation efficiently designs the network structure to enhance benefits and reduce risks.

Lemma 3: Terrorists in a component have the same degree.

Proof of Lemma 3: From Lemma 2, we have shown that if a path P_i^q exists between terrorist i and q, then they share the same number of path-connected terrorists, denoted as $m_i = m_q$. Additionally, Proposition 1 indicates that due to $\delta = 1$, targeting a terrorist leads to the capture of all their path-connected terrorists if infiltration is successful. From the perspective of the leader, it is efficient to be maximally connected within a component, as this allows for the most complete utilisation of connections. As a direct consequence of proposition 1, for every terrorist in the network, the number of path-connected terrorists is equal to the number of neighbours, denoted as $m_i = d_i$. Otherwise, the benefits from connections would not be maximized, while cost from infiltration $p\frac{m_i+1}{n}$, are identical in both situations where $m_i > d_i^{'}$ and $m_i = d_i$.

Combining Lemma 2 and Proposition 1, we deduce that $d_i = d_q$. Looking at Figure 3 above, we can observe that all terrorists have the same degree inside the component. This implies that the terrorists in the efficient network, represented by Figure 3, are equally and maximally connected i.e., have components.

3.5.1 Equilibrium Characterization

Lemma 4: Terrorists in a component have same cardinality of path-connected terrorists and same degrees i.e., $m_i = m_j = d_i = d_j = \overline{d} \; \forall \; i \neq j \in C(\mathcal{G})$.

We formally combine, Proposition 1, Lemma 2 and 3 and present in Lemma 4. This emphasises the importance of the leader's decision-making regarding the maximal connectivity within a sub-structure (or structure) to design an efficient terrorist network.

Now we formalise the equilibrium characterisation of the model. Revisiting equation 4 for convenience,

$$u_i = \Big(1 - p\frac{m_i + 1}{n}\Big)e_i\Big(1 + \beta \sum_{j \in N} g_{ij}e_j\Big) - p\frac{m_i + 1}{n}f - \frac{1}{2}e_i^2$$

Using Lemma 4, equation 4 can be written as,

$$u_i = \Big(1 - p\frac{\overline{d} + 1}{n}\Big)e_i\Big(1 + \beta\overline{d}e_j\Big) - p\frac{\overline{d} + 1}{n}f - \frac{1}{2}e_i^2 \tag{5}$$

Assuming an interior solution, we maximize u_i with respect e_i and set it equal to 0:

$$\frac{\partial u_i}{\partial e_i} = \left(1 - p\frac{\overline{d} + 1}{n}\right)\left(1 + \beta\overline{d}e_j\right) - e_i = 0 \tag{6}$$

The F.O.C. of equation 6 can be re-written as,

$$e_i^* = \Big(1 - p\frac{\overline{d} + 1}{n}\Big)\Big(1 + \beta\overline{d}e_j^*\Big) \tag{7}$$

From Lemma 4, we know $m_i = m_j = d_i = d_j = \overline{d}$, therefore we can say it is an isomorphic decision problem and hence we are focusing on symmetric equilibrium, where $e_i = e_j = \overline{e} \; \forall \; i \neq j \in C(\mathcal{G})$.
Plugging $e_i = e_j = \overline{e}$ in equation 7, we can write, the interior equilibrium efforts as,

$$\overline{e^*} = \frac{n - p(\overline{d} + 1)}{n - \beta\overline{d}[n - p(\overline{d} + 1)]} \tag{8}$$

Plugging equilibrium efforts $\overline{e^*}$ from equation 8 in equation 5, we get the interior equilibrium utilities as,

$$\overline{u^*} = \frac{1}{2}\Big(\frac{n - p(\overline{d} + 1)}{n - \beta\overline{d}n + p\beta\overline{d}(\overline{d} + 1)}\Big)^2 - \frac{\overline{d} + 1}{n}pf \tag{9}$$

Proposition 2: There exists an interior Nash Equilibrium to the strategic game Γ.

For proving proposition 2 we need to prove the following Lemmas,

- The strategic form game Γ admits a Nash Equilibrium.
- There is an interior solution to the strategic game

The existence of the game Γ is proved using Debreu-Fan-Glicksberg Theorem. Refer to Lemma 1 in Appendix A.1.

Lemma 5: There is an interior solution to the strategic game Γ.

Proof of Lemma 5: Revisiting equation 8, we have:

$$\overline{e^*} = \frac{n - p(\overline{d} + 1)}{n - \beta\overline{d}[n - p(\overline{d} + 1)]}$$

To ensure that the denominator $n - \beta\overline{d}[n - p(\overline{d} + 1)] > 0$, we restrict the degree of complementarity between terrorist's efforts $\beta \in \Big(0, \frac{1}{n-1}\Big)$, ensuring that $\overline{e^*}$ remains finite. Henceforth in this chaper, we focus on $\beta \in$

$\left(0, \frac{1}{n-1}\right)$ to do our analysis. Now, consider the scenario where individual terrorists exert zero effort. In this case, equation 5 becomes,

$$u_i = -\frac{\overline{d}+1}{n} f \tag{10}$$

With equation 10 confirming $u_i < 0; \forall i \in N$, it can be deduced that terrorists will exert strictly positive effort i.e., $\boldsymbol{e} >> 0$. We considered $n \geq 3$ in our model, to rule out non-trivial component structure transition. Thus, provided the parameters β, p and $n \geq 3$, if $\overline{e^*} < B < \infty$, an interior solution to the game Γ is feasible.

Nevertheless, it is important to note that the strategic game can also give rise to a corner solution. A comprehensive overview of the equilibrium individual efforts, utilities, and the overall welfare of the network structure can be summarised through the following corollaries.

Corollary 1: Terrorists maximally connected in a component have the following equilibrium efforts and utilities,

$$\begin{aligned}
\overline{e^*} &= \begin{cases} \frac{n-p(\overline{d}+1)}{n-\beta\overline{d}[n-p(\overline{d}+1)]} & \text{if } \overline{e^*} < B \\ B & \text{otherwise} \end{cases} \\
\overline{u^*} &= \begin{cases} \frac{1}{2}\left(\frac{n-p(\overline{d}+1)}{n-\beta\overline{d}n+p\beta\overline{d}(\overline{d}+1)}\right)^2 - \left(\frac{\overline{d}+1}{n}\right)pf & \text{if } \overline{e^*} < B \\ (1-p\frac{\overline{d}+1}{n})B(1+\beta\overline{d}B) - \left(\frac{\overline{d}+1}{n}\right)pf - \frac{1}{2}B^2 & \text{otherwise} \end{cases}
\end{aligned} \tag{11}$$

Proof of Corollary 1: The calculations are shown in the Appendix A.4.

Referring to equation 8 and equation 9, we determine the interior equilibrium efforts and utilities. The equilibrium can also admit a corner solution when $e^* = B$. Similarly, the equilibrium utilities involving a corner solution, can be represented as $\overline{u^*} = (1-p\frac{\overline{d}+1}{n})B(1+\beta\overline{d}B) - \left(\frac{\overline{d}+1}{n}\right)pf - \frac{1}{2}B^2$, as provided by equation 11. The utility equilibrium at a given corner is negatively influenced by the probability of infiltration, the number of neighbours for each terrorist, and the fine faced upon capture, assuming all other parameters remain constant. On the other hand, it is directly proportional to the total size of the terrorist organisation.

Before delving into the comparative statics of the equilibrium conditions, directing our attention to the network's welfare becomes crucial. Examining welfare is of paramount importance as it offers insights into the network structures that emerge in respond to various levels of infiltration.

Corollary 2: The equilibrium welfare for the efficient network can be written as follows,

$$\overline{W^*} = \begin{cases} \sum_{k=1}^{K}\left(\overline{d_k}+1\right)\left[\frac{1}{2}\left(\frac{n-p(\overline{d_k}+1)}{n-\beta\overline{d_k}n+p\beta\overline{d_k}(\overline{d_k}+1)}\right)^2 - \left(\frac{\overline{d_k}+1}{n}\right)pf\right] & \text{if } \overline{e^*} < B \\ \sum_{k=1}^{K}\left(\overline{d_k}+1\right)\left[(1-p\frac{\overline{d_k}+1}{n})B(1+\beta\overline{d_k}B) - \left(\frac{\overline{d_k}+1}{n}\right)pf - \frac{1}{2}B^2\right] & \text{otherwise} \end{cases} \tag{12}$$

$\overline{d_k}$ is the degree of each terrorist in component k. Since all terrorists in a component have the same degree, it is denoted by an $\overline{d}$. K is the total number of components in an efficient Network. If $\overline{d_k} = d\ \forall k$, then components are symmetric and welfare can be written as,

$$\overline{W^*} = \begin{cases} \frac{n}{2}\left(\frac{n-p(\overline{d}+1)}{n-\beta\overline{d}n+p\beta\overline{d}(\overline{d}+1)}\right)^2 - (\overline{d}+1)pf & \text{if } \overline{e^*} < B \\ n\left(1-p\frac{\overline{d}+1}{n}\right)B(1+\beta\overline{d}B) - (\overline{d}+1)pf - \frac{n}{2}B^2 & \text{otherwise} \end{cases} \tag{13}$$

Proof of Corollary 2: The mathematical proof is shown in Appendix A.5.

The welfare of an efficient network can be determined by substituting the equilibrium utilities from equation 11 in terrorist leader problem i.e., equation 2. Upon examining these equilibrium welfare values, the leader designs the efficient network for a given probability of infiltration.

However, we focus on efficient networks, a common question emerges – whether the components within any efficient network exhibit symmetry or asymmetry. While equation 12 outlines the general welfare equation of an efficient network, equation 13 addresses the specific case of an efficient network with symmetric components. The subsequent section will delve into this topic, explaining that the presence of symmetric or asymmetric components

in an efficient network depends on the probability of infiltration, the degree of complementarity between terrorists efforts, fine and organisation size.

Characterisation of the Shapes and Sizes of Components: The efficient network may have symmetric or asymmetric components, depending on the value of p, n, β and f. We will demonstrate this, with the help of few examples.

Example 1: Consider a network comprising of 6 terrorists. In this context, the degree of complementarity characterising the synergy between the terrorist's efforts is denoted as $\beta = 0.19$, while the imposed fine is set at $f = 2$. The primary objective of this example is to highlight the potential for efficient networks to exhibit either symmetric or asymmetric components. To this end, two specific efficient network designs are of interest: one featuring all 6 terrorists in a complete component, and the other involving a configuration where 5 terrorists are in fully connected while one terrorist remains isolated.

Although various other efficient network arrangements are possible, it is worth noting that the leader of the organisation designs the network that yields the highest welfare for a given probability of infiltration. This decision ensures that the organisation's leader aims to maximize the network's overall efficiency while considering the potential risks associated with infiltration.

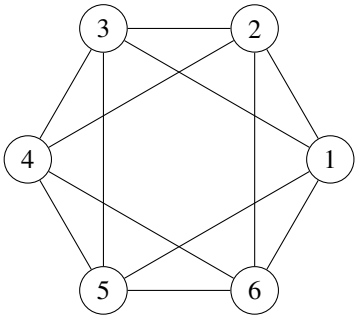

Figure 5: S.C. Efficient Network

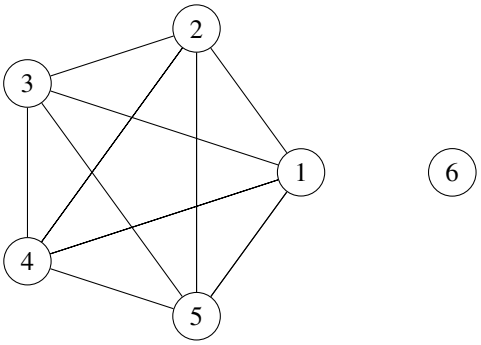

Figure 6: A.C. Efficient Network

The analysis was particularly focused on two levels of infiltration probability, specifically $p = 0.38$ and $p = 0.39$. The results revealed that at the infiltration probability of $p = 0.38$, the efficient network, depicted as Figure 5, showcases a single symmetric component. Conversely, at an infiltration probability of $p = 0.39$, the efficient network, illustrated as Figure 6, features asymmetric components. Notably, at this higher infiltration probability of $p = 0.39$, the leader opts to partition the network into two distinct components. This strategic decision is motivated by the intention to minimise the impact of infiltration-related costs.

As previously discussed in the chapter, the apprehension of terrorists leads to the capture of their path-connected terrorists. Consequently, as the level of infiltration probability escalates, these associated costs also increase gradually. In this context, the division of the network into separate components emerges as one among several efficient strategies to enhance the network's resilience against such escalating costs.

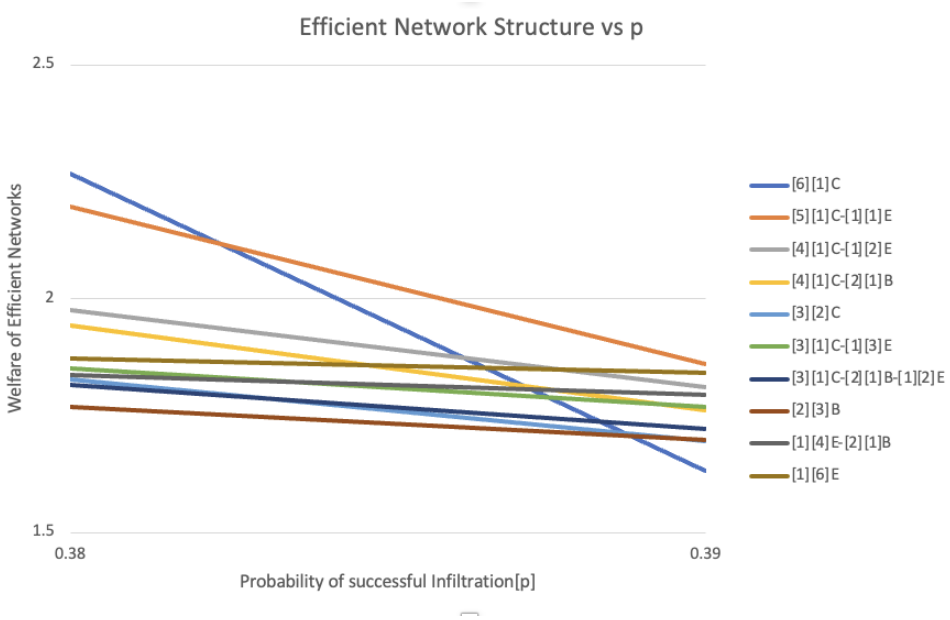

Figure 7: Transition of efficient Network with variation of p at $\beta = 0.19$ and $f = 2$
[16]

The scenario outlined in example 1 can be effectively depicted using figure 7. This visual aid captures the dynamic shift in the efficient network's structure – a transition occurring from a complete component consisting of all 6 terrorists to a new configuration featuring a complete component involving only 5 terrorists, with an accompanying empty component. This transition occurs within a specific range of infiltration probability, specifically between the values of 0.38 and 0.39. Within this range, the organisation's leader is tasked with making a strategic decision. The leader designs one of these two efficient network configurations based on a comparative assessment of their respective welfare values. The ultimate choice hinges upon identifying which among the two efficient networks offers greater welfare, given the specified parametric values.

Example 2: In a manner akin to example 1, a comparative analysis is conducted across four distinct efficient networks, considering varying values of the parameter p. The specific values chosen for this analysis are $\beta = 0.12$ and $f = 1$.

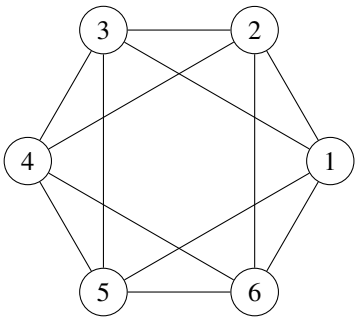

Figure 8: S.C. Efficient Network

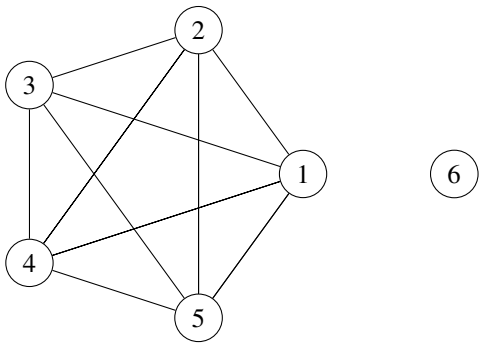

Figure 9: A.C. Efficient Network

[16][4][1]C-[2][1]B reads as 4 nodes comprising 1 complete component and 2 nodes comprising of 1 binary component.

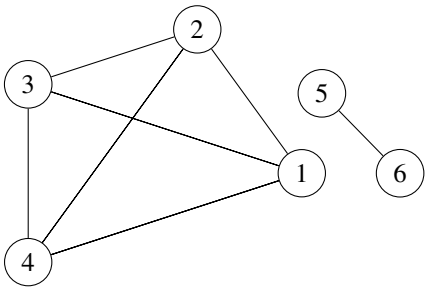

Figure 10: A.C. Efficient Network

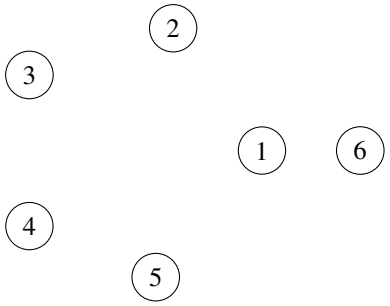

Figure 11: S.C. Efficient Network

Now consider a specific infiltration probability of $p = 0.29$. At this particular infiltration level, the efficient network that maximizes welfare is the one depicted in Figure 8. Upon increasing the infiltration probability by an increment of 0.1, a significant shift is observed in the nature of the efficient network. This transition is evident as the network transforms from having symmetric components, as shown in Figure 8, to possessing asymmetric components, which is represented in Figure 9. Continuing this analysis, at a slightly higher infiltration probability of $p = 0.31$, the efficient network maintains its configuration with asymmetric components. However, the relative sizes of these components experience alteration, leading to the arrangement depicted in Figure 10. Subsequently, when the infiltration probability reaches $p = 0.32$, a noteworthy change occurs. The efficient network undergoes disintegration, resulting in empty networks as illustrated in Figure 11. Consequently, the network once again exhibits symmetric components due to this breakdown.

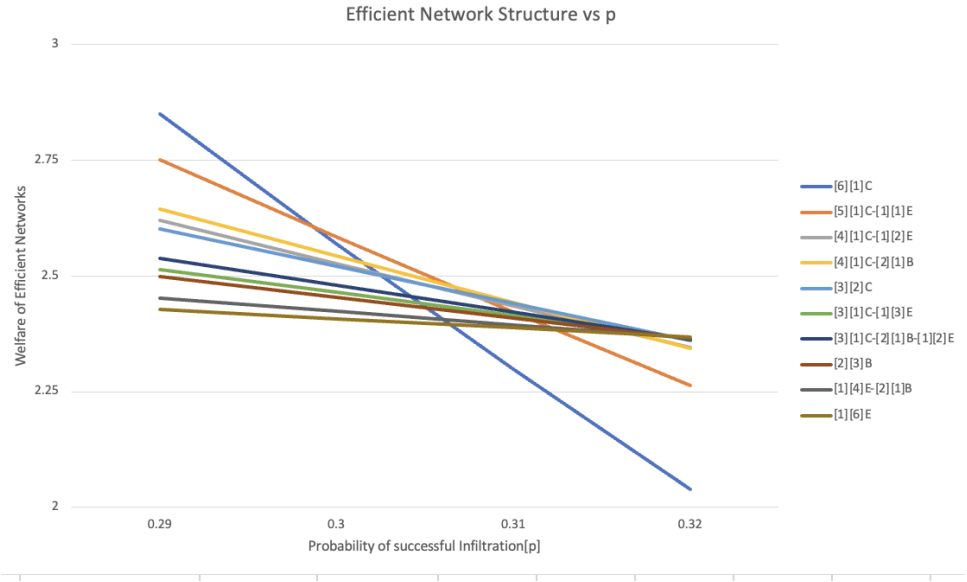

Figure 12: Transition of efficient Network with variation of p at $\beta = 0.12$ and $f = 1$

The sequence of network transitions is visually depicted in the figure 12 above. The corresponding welfare values associated with Figures 8,9, 10, and 11 are as follows: 2.85, 2.58, 2.44, and 2.37. Crucially, the leader of the organisation strategically design these specific network structures at different values of p, as indicated earlier. This decision is rooted in the fact that these chosen network configurations offer the highest possible welfare for the respective values of p.

So far, we have shown that efficient network may comprise of both sysmmetric and asymmetric components for small network size. However, in Example 3 we show this for larger network size.

Example 3: Our analysis is for a network size of $n = 100$. Due to the impracticality of comparing all possible network structures individually, particularly with larger network sizes, we aimed to discern the optimal component size for the given $n = 100$. In our investigation, we set parameters $\beta = 0.01$ and $f = 1$. We systematically varied p from 0 to 1 with increments of 0.01 and similarly varied $\overline{d}$ with increments of 1. Our objective was to determine, for each p value, the $\overline{d}$ that gives the maximum utility u for a terrorist i. We observed that for $p \in [0, 0.36]$, the u_i is maximized when $\overline{d}$ equals 99, indicating the efficient network structure is comprised of a single complete

component. However, for $p \in [0.37, 0.49]$, the efficient network comprises of asymmetric components. Notably, the optimal $\overline{d}$ is no longer 99 but begins to decrease, suggesting an inverse relationship between $\overline{d}$ and p. Finally, for $p \in [0.5, 1]$, the efficient network once again comprises of symmetric components, specifically, empty sub-structures are designed. Refer to the Table in Appendix B.1.

We now demonstrate that efficient networks is composed of symmetric components for some parameter values of fine.

Example 4: Our analysis focused on a network size of $n = 100$. As mentioned earlier, comparing all possible network structures individually is not feasible, especially with larger network sizes. Therefore, we aimed to discern the optimal neighbours for a terrorist for the given $n = 100$. In our investigation, we set the parameters $\beta = 0.01$ and $f = 4$. We systematically varied p from 0 to 1 with increments of 0.001 and similarly varied $\overline{d}$ with increments of 1. Our objective was to determine, for each p value, the $\overline{d}$ that gives the maximum utility u for a terrorist i.

We observed that for $p \in [0, 0.338]$, the u_i is maximized when $\overline{d}$ equals 99, indicating that each terrorist's utility is highest when the efficient network structure is a single complete component. Therefore, it is in the best interest of the leader to design an efficient network with a single complete component. However, for $p \in [0.339, 1]$, the optimal $\overline{d}$ is no longer 99 but drops down to 0. In this scenario, the efficient network comprises symmetric components, specifically, empty sub-structures are designed. In this case, no efficient networks are designed with asymmetric components.Refer to the Table in Appendix B.2.

Note that in the Table of Appendix B.2, we show a small range of p, where the transition from a single complete component to empty components occurs. We omitted the p values outside this range because for $p \in [0, 0.328]$, the efficient network is always a single complete component, and for $p \in [0.347, 1]$, the efficient network is always designed of only empty components.

Example 5: For $\beta = 0$, the efficient network is comprised of symmetric components.

For $\beta = 0$, the utility of an individual terrorist i can be written as below,

$$u_i = \frac{1}{2}\Big(\frac{n - p(\overline{d}+1)}{n - \beta\overline{d}(n - p(\overline{d}+1))}\Big)^2 - \Big(\frac{\overline{d}+1}{n}\Big)pf$$

$$= \frac{1}{2}\Big(\frac{n - p(\overline{d}+1)}{n}\Big)^2 - \Big(\frac{\overline{d}+1}{n}\Big)pf \tag{14}$$

From the above equation 14 we see that u_i has an inverse relationship with $\overline{d}$ for $p \in (0, 1]$. Hence, the efficient network is composed of only empty components. Therefore we can say the efficient network will be designed of symmetric components.

Now, we aim to explore the range of values for p where the network transitions from a single, fully-connected structure (i.e., component) to efficient networks with component sizes strictly smaller than a single complete component, yet strictly larger than empty components, and eventually to efficient networks composed entirely of empty components. Two threshold values of p, p^* and p^{**}, were obtained. Specifically, $\forall p \in [0, p^*]$, the efficient network consists of a single component. Conversely, $\forall p \in [p^{**}, 1]$, the network is designed with only empty components. Between these bounds, i.e., $\forall p \in (p^*, p^{**})$, various other efficient network designs may emerge. We will discuss this now with the help of some lemmas and propositions.

Lemma 6A: At $p = 0$, the efficient network structure is a complete component.

Proof of Lemma 6A: After substituting $p = 0$, in the interior equilibrium utility represented by equation 9 we get the following equation below,

$$\overline{u^*} = \frac{1}{2}\Big(\frac{1}{1 - \beta d}\Big)^2 \tag{15}$$

Upon examining the individual interior equilibrium utility, it becomes evident that a positive relationship exists between the utility and the number of neighbours a terrorist possesses. Consequently, when considering a degree denoted as d', where $d' < n - 1$ (with n representing the total number of terrorists), the resulting utility is lower than that derived from the utility equation 15 i.e., $u^{'} < u^*$.

Similarly, by substituting $p = 0$ into the corner equilibrium utility, as described in equation 11, we obtain the following equation:

$$\overline{u^*} = B(1 + \beta\overline{d}B) - \frac{1}{2}B^2 \tag{16}$$

As evident from the above equation, when we set $\overline{d} = n - 1$, the value of $\overline{u^*}$ is maximum.

This analysis prompts the conclusion that when the infiltration probability is set at $p = 0$, the optimal course of action for the leader is to design a single complete component as the efficient network.

Lemma 6B: At $p = 1$, the efficient network may not always comprise empty components.

1. When efforts exerted are non-maximal, the efficient network is always comprised of empty components at $p = 1$.
2. When efforts exerted are maximal, the efficient network is comprised of empty components if $e = B \leq B^*$, otherwise, it may be composed of some non-empty components.

Proof of Lemma 6B: At $p = 1$, the equilibrium utility can be written as,

$$\overline{u^*} = \frac{1}{2}\Big(\frac{n - (\overline{d} + 1)}{n - \beta\overline{d}n + \beta\overline{d}(\overline{d} + 1)}\Big)^2 - \frac{\overline{d} + 1}{n}f \tag{17}$$

Differentiating equation 17, with respect to $\overline{d}$ and simplifying we get,

$$\frac{\partial\overline{u^*}}{\partial\overline{d}} = \frac{n - (\overline{d} + 1)}{n - \beta\overline{d}n + \beta\overline{d}(\overline{d} + 1)}\Big[\frac{-n + \beta(n - \overline{d} - 1)^2}{(n - \beta\overline{d}n + \beta\overline{d}(\overline{d} + 1))^2}\Big] - \frac{1}{n}f$$

Given that the degree of complementarity between terrorist's efforts, denoted as β, is constrained by an upper limit of $\frac{1}{n-1}$, it follows that the term $-n + \beta(n - \overline{d} - 1)^2$ is inherently negative. As a result, $\frac{\partial\overline{u^*}}{\partial\overline{d}} < 0$, which signifies that when $p = 1$, the leader of the organisation deems it advantageous to design empty components inside the network

We will now demonstrate that similar empty components also arise in the corner utility function, when certain conditions on the corner effort are met. When setting $p = 1$ for the corner utility, the equation can be expressed as follows: $\overline{u^*} = \left(1 - \frac{\overline{d}+1}{n}\right) B(1 + \beta\overline{d}B) - \frac{\overline{d}+1}{n}f - \frac{1}{2}B^2$. Now, at $p = 1$, the utility associated with empty components is: $\overline{u^*} = \left(1 - \frac{1}{n}\right) B - \frac{1}{n}f - \frac{1}{2}B^2$. Now, we will consider a scenario where the leader intends to design one binary component while keeping $n-2$ empty components. The utility of the terrorist within the binary component can be written as: $\overline{u'} = \left(1 - \frac{2}{n}\right) B(1+\beta B) - \frac{2}{n}f - \frac{1}{2}B^2$. Comparing the $\overline{u'}$ and $\overline{u^*}$, if $B^* = \frac{1+\sqrt{1+4\beta f(n-2)}}{2\beta(n-2)} \geq B$ then at $p = 1$, the leader will design an efficient network with only empty components. Otherwise, an efficient network with some non-empty components will be designed.

We intuitively explain the above results. In the absence of infiltration risks, the lack of capture costs allows the terrorist leader to maximize welfare by designing a fully connected network. However, when the infiltration probability reaches 100 percent, the cost associated with infiltration surpasses the benefits gained from connections. Consequently, the terrorist networks become constituted solely of empty components.

However, when effort of terrorists exerts maximal effort, one can observe if B is smaller than B^*, then all components will be empty in the efficient network. However when B is greater than B^*, one can think that the benefits from connections (βB) is significantly higher as to allow non-empty components arising even when probability of infiltration is 1.

Drawing insights from Lemma $6A$ and $6B$ mentioned earlier, an inverse correlation between p and $\overline{d}$ becomes evident. The underlying logic is intuitive: as p rises, it becomes advantageous for the leader to refrain from increasing the number of neighbours of any terrorist, as doing so heightens the risk of infiltration. The mathematical analysis supporting this conclusion is relatively straightforward. By taking the derivative of equation 9 with respect to p, we arrive at the following result:

$$\frac{\partial u^*}{\partial p} = \frac{1}{2}\frac{[n - p(\overline{d} + 1)]}{[n - \beta\overline{d}(n - p(\overline{d} + 1)]}\frac{-n(\overline{d} + 1)}{[n - \beta\overline{d}(n - p(\overline{d} + 1)]^2} - \frac{\overline{d} + 1}{n}f \tag{18}$$

Examining equation 18, we observe that the sign of $\frac{\partial u^*}{\partial p}$ is negative. This is evident as, $[n-p(\overline{d}+1)]$, $[n-\beta\overline{d}(n-p(\overline{d}+1)]$, $n(\overline{d}+1)$ and $\frac{\overline{d}+1}{n}f$ is strictly positive. Delving into the marginal change in utility of any terrorist with respect to p, we see if the leader intends to augment the number of neighbours of a terrorist $\overline{d}$, it becomes evident that the utility of the terrorist diminishes even further. Consequently, it is not in the leader's best interest to increase the neighbours of any terrorist inside the network when the probability of infiltration rises. This establishes a clear monotonic non-increasing relationship between p and $\overline{d}$.

Proposition 3: There exists a lower bound p^* such that $\forall\ p \in [0, p^*]$, the efficient network is composed of a single complete component and an upper bound p^{**} such that $\forall\ p \in [p^{**}, 1]$, the efficient network may not always composed of all empty components.

For proving proposition 3 we need to prove the following lemmas,

1. **Lemma 7A**: There exists a value p^* such that for $\forall\ p \in [0, p^*]$, the efficient network is composed of a single complete component.
2. **Lemma 7B**: There exists a value p^{**} such that for $\forall\ p \in [p^{**}, 1]$, the efficient network may not necessarily be composed of empty components.

The proof of Lemma 7A and Lemma 7B is in the Appendix A.6.

We have proved Lemma 7A and Lemma 7B with the help of Bolzano's Theorem [17]. In Appendix A.6, we prove Proposition 3 under the assumption that terrorist's effort admits an interior equilibrium. A similar proof holds when the effort admits a corner solution. Since the proof is identical for both interior and corner solutions, we have omitted the latter. Here, we will discuss the implications.

From Lemma 6A and Lemma 6B, we observe that at $p = 0$, the efficient network is a single complete component regardless of whether the effort exerted is maximal or non-maximal. However, at $p = 1$, the efficient network may be composed of only empty components. This depends on the nature of the solution and other parameter values such as f, β, and n of the model.

By applying Bolzano's theorem in Lemma 7A and Lemma 7B, we show that there exist two probabilities of infiltration threshold values p^* and p^{**}, where for $p \in [0, p^*]$, the efficient network is composed of a single complete component. This is because the benefits of connections are higher than the cost of infiltration. However, for $p \in [p^{**}, 1]$, the efficient network associated with non-maximal effort is always composed of empty components. When terrorists exert maximal effort, depending on the level of this maximal effort, the efficient network may have all or some empty components. This indicates that even at high levels of infiltration, if the benefits of connections are sufficiently high, the network does not necessarily disintegrate into all empty components, but some non-empty components may still exist.

In the next section, we discuss the comparative statics of the model and examine how the equilibrium efforts and utilities vary with respect to network size, the degree of complementarity between the efforts of terrorists, the fines faced by terrorists, and the probability of infiltration.

3.5.2 Comparative Statics

In conducting comparative statics in this chapter, we restrict our attention to interior equilibrium efforts and utilities. Our focus is on understanding how these efforts and utilities change with variations in parametric values such as $\overline{d}$, n, p, f, and β. Although we recognise that $\overline{d}$ and n are discrete values, our primary interest lies in the signs of the comparative statics rather than their exact values. For convenience, we treat these parameters as continuous.

Variation with respect to $\overline{d}$: Upon calculating the derivative of equilibrium efforts (equation 8) with respect to $\overline{d}$, followed by simplifying the result, the resulting equation is as follows:

$$\frac{d\overline{e^*}}{d\overline{d}} = \frac{-np + \beta[n - p(\overline{d}+1)]^2}{[n - \beta\overline{d}[n - p(\overline{d}+1)]]^2} \tag{19}$$

[17] See Apostol (1991).

Given that the denominator of equation 19 is always positive, the direction of the sign of $\frac{d\overline{e^*}}{d\overline{d}}$ can be understood by focusing on the numerator.

$$\frac{d\overline{e^*}}{d\overline{d}} \begin{cases} \geq 0 & \text{if } -np + \beta[n - p(\overline{d}+1)]^2 \geq 0 \\ < 0 & \text{otherwise} \end{cases} \tag{20}$$

The term present in equation 20, namely $-np + \beta[n - p(\overline{d}+1)]^2$, can be rewritten as $-\frac{p}{n} + \beta[1 - p(\frac{\overline{d}+1}{n})]^2$. The transformed expression can be explained in the following manner: When the number of neighbours for a terrorist increase, the marginal cost of getting captured increases by $\frac{p}{n}$. However, the marginal benefits will also rise due to the degree of complementarity β, provided the terrorist remains uncaptured with probability $\left(1 - \frac{p(d+1)}{n}\right)$. If the marginal cost of getting captured outweighs the marginal benefits from complementarity, given that the terrorist remains uncaptured, the equilibrium effort decreases as the number of neighbours increases.

Consider the scenario, where the probability of successful infiltration $p = 1$, the number of nodes $n = 4$ and the degree of complementarity between the efforts of terrorists $\beta = 0.001$. In this context, the expression $-\frac{p}{n} + \beta[1 - p(\frac{\overline{d}+1}{n})]^2$ yields a negative value, as the cost of getting captured is higher than benefits of not getting captured. Conversely, when $p = 0$, the expression becomes positive. Thus, the sign of $\frac{d\overline{e^*}}{d\overline{d}}$ can be influenced by the specific values of the parameters. Consequently, in principle, the sign becomes uncertain due to the variability of these parameter values.

The equilibrium utility (equation 9) can be reformulated as:

$$\overline{u^*} = \frac{1}{2}\overline{e^*}^2 - \frac{\overline{d}+1}{n}pf \tag{21}$$

Upon calculating the derivative of equation 21 with respect to $\overline{d}$ and further simplifying, the result is as follows:

$$\frac{d\overline{u^*}}{d\overline{d}} = \overline{e^*}\frac{d\overline{e^*}}{d\overline{d}} - \frac{1}{n}pf \tag{22}$$

When the number of neighbours of a terrorist increase, the effect on their equilibrium utilities is ambiguous. If the marginal change in equilibrium effort is non-positive with respect to the number of neighbours $\overline{d}$, then the marginal change in equilibrium utility is unambiguously negative, as evident from the expression above. However, when the marginal change in equilibrium effort is strictly positive, the marginal effect on equilibrium utilities is ambiguous. If the increase in the marginal effort of a terrorist with respect to $\overline{d}$ is greater than or equal to the marginal cost of capture and subsequent fines, then the equilibrium utilities increase or remain constant, otherwise they decrease.

Variation with respect to n: Applying a similar approach as mentioned above, by calculating the derivative of equation 8 in relation to the size of the terrorist network n and then simplifying the outcome, the resulting equation is as follows:

$$\frac{d\overline{e^*}}{dn} = \frac{\frac{d\overline{d}}{dn}[-np + \beta(n - p(\overline{d}+1))^2] + \frac{d\beta}{dn}\overline{d}(n - p(\overline{d}+1))^2 + p(\overline{d}+1)}{[n - \beta\overline{d}(n - p(\overline{d}+1))]^2} \tag{23}$$

We know from the above expression that the denominator is strictly positive, so the sign of $\frac{de}{dn}$ depends on the sign of the numerator. In our chapter, we considered that the sign of $\frac{d\beta}{dn}$ is negative. This implies that with a greater number of terrorists, the marginal increase in complementarity decreases. However, the number of neighbours for a terrorist can increase or decrease with the size of the network. If the marginal benefit of an increase in effort with an increase in $\overline{d}$ is positive, then $\frac{d\overline{d}}{dn}$ is positive otherwise it is negative. Therefore, the sign of $\frac{de}{dn}$ is the interplay of these forces mentioned above. If the marginal benefit from increasing network size is greater than the marginal cost, then $\frac{de}{dn} > 0$, otherwise it can remain constant or decrease as well.

Using equation 21 and taking derivative with respect to n, we get,

$$\frac{d\overline{u^*}}{dn} = \overline{e^*}\frac{d\overline{e^*}}{dn} + \frac{pf}{n}\left[\frac{\overline{d}+1}{n} - \frac{d\overline{d}}{dn}\right] \tag{24}$$

The term $\left[\frac{\overline{d}+1}{n} - \frac{d\overline{d}}{dn}\right]$ in equation 24 can be represented as $\varepsilon_{\overline{d},n} = \frac{n}{\overline{d}+1} * \frac{d(\overline{d}+1)}{dn}$, where $\varepsilon_{\overline{d},n}$ signifies the proportionate change in the number of neighbours of terrorists resulting from a proportionate change in the terrorist

network size. If $\varepsilon_{\overline{d},n}$ falls within the range of 0 and 1, it signifies that due to the reduction in the cost of capture through infiltration with an increase in network size, the equilibrium utility of an individual terrorist increases alongside the expansion of the network. Nevertheless, when $\varepsilon_{\overline{d},n}$ is more than 1, the sign of $\frac{d\overline{u^*}}{dn}$ becomes uncertain. Specifically, the sign of $\frac{d\overline{u^*}}{dn}$ turns negative only when the penalties post-apprehension are considerably substantial, causing the utility of terrorists to decline as the network size grows.

Variation with respect to p: We now explore how effort and utility of inidividual terrorists vary with the probability of infiltration. Upon calculating the derivative of equation 8 with respect to p and then simplifying the obtained expression, the outcome is as follows:

$$\frac{d\overline{e^*}}{dp} = \Big[\frac{-n(\overline{d}+1) + \Big(\frac{d\overline{d}}{dp}\Big)\Big(-np + \beta[n - p(\overline{d}+1)]^2\Big)}{[n - \beta\overline{d}[n - p(\overline{d}+1)]]^2}\Big] \tag{25}$$

Examining the impact of varying the probability of successful infiltration, the sign of $\frac{d\overline{e^*}}{dp}$ can be determined by focusing on the numerator, given the denominator is always positive in equation 25. It is plausible to consider that the network leader might reduce the number of neighbours for certain for some terrorists, if not for all. The numerator of equation 25 can be restated as $-\frac{\overline{d}+1}{n} + (\frac{d\overline{d}}{dp})[-\frac{p}{n} + \beta[1 - p(\frac{\overline{d}+1}{n})]^2]$.

Particular attention is drawn to the sign of $-\frac{p}{n} + \beta[1 - p(\frac{\overline{d}+1}{n})]^2$. From equation 20 we know the sign of $\frac{d\overline{e^*}}{d\overline{d}}$ can be positive, negative or equal to 0, depending on the interplay of the cost of getting captured and the benefits of not getting captured. Nonetheless, as the leader decreases $\overline{d}$ with the increase in p, the sign of $\frac{d\overline{e^*}}{dp}$ is unambiguously negative if $-\frac{p}{n} + \beta[1 - p(\frac{\overline{d}+1}{n})]^2 > 0$. However, when the term $-\frac{p}{n} + \beta[1 - p(\frac{\overline{d}+1}{n})]^2$ is negative, the sign of $\frac{d\overline{e^*}}{dp}$ becomes ambiguous. In such a scenario, the sign of $\frac{d\overline{e^*}}{dp}$ can only be positive when the leader can effectively increase the benefits by reducing the number of neighbours for each terrorist.

Similarly as above, taking derivative of equation 21, with respect to p, we get,

$$\frac{d\overline{u^*}}{dp} = \overline{e^*}\frac{d\overline{e^*}}{dp} - \frac{f}{n}\Big[(\overline{d}+1) + p\frac{d\overline{d}}{dp}\Big] \tag{26}$$

In cases where the sign of $\frac{d\overline{e^*}}{dp}$ is negative and the term within the parenthesis is positive, the sign of $\frac{d\overline{u^*}}{dp}$ becomes conclusively negative. Additionally, sizeable fines following apprehension can also lead to a decrease in the utility of terrorists. However, it is important to note that the sign of $\frac{d\overline{u^*}}{dp}$ can also be positive based on the marginal benefit from increasing efforts and the marginal cost of capture.

Variation with respect to f: We now focus how the equilibrium efforts and utilities of terrorists responds to changes in f. Taking derivative of equation 8 with respect to f and subsequently simplifying the expression, the outcome is as follows:

$$\frac{d\overline{e^*}}{df} = \Big[\frac{\Big(\frac{d\overline{d}}{df}\Big)\Big(-np + \beta[n - p(\overline{d}+1)]^2\Big)}{[n - \beta\overline{d}[n - p(\overline{d}+1)]]^2}\Big] \tag{27}$$

Given that the denominator of equation 27 is positive and understanding that the degree of each terrorist is inversely related to fines, the equation presents some insights. Even if the term $-\frac{p}{n} + \beta[1 - p(\frac{\overline{d}+1}{n})]^2$ is positive, the influence of $(\frac{d\overline{d}}{df})$ contributes to the decline of equilibrium efforts. Conversely, when $[-\frac{p}{n} + \beta\left(1 - p\frac{\overline{d}+1}{n}\right)^2] < 0$, the equilibrium effort increases with fines. This can be explained by the fact that as fines increase, the leader reduces the number of connections each individual terrorist has to minimise the risk of infiltration. This results in an increase in the number of components within the network. However, within these components, the individual efforts will increase. Thus the sign of $\frac{d\overline{e^*}}{df}$ is dependent on the sign of $\frac{d\overline{e^*}}{d\overline{d}}$.

Similar to the previous discussions, calculating the derivative of equation 21 with respect to f yields:

$$\frac{d\overline{u^*}}{df} = \overline{e^*}\frac{d\overline{e^*}}{df} - \frac{p}{n}\Big[(\overline{d}+1) + f\frac{d\overline{d}}{df}\Big] \tag{28}$$

Much like the explanation for the equilibrium utility variation concerning p, the implications of changes in f can be understood. When $\frac{d\overline{e^*}}{df}$ takes a negative value and the term within the parenthesis remains positive, the sign of

$\frac{d\overline{e^*}}{df}$ is unequivocally negative. However, when $\frac{d\overline{e^*}}{df} > 0$, the actual sign of $\frac{d\overline{u^*}}{df}$ is depends on the interplay of the marginal benefit from increasing efforts and the marginal cost of capture.

Variation with respect to β: Lastly, we explore how the equilibrium efforts and utilities of individual terrorists changes with changes in β (represents the degree of complementarity between terrorists efforts). Calculating the derivative with respect to β and then simplifying, we obtain:

$$\frac{d\overline{e^*}}{d\beta} = \Big[\frac{\Big(\frac{d\bar{d}}{d\beta}\Big)\Big(-np + \beta[n - p(\bar{d}+1)]^2\Big) + \bar{d}(n-(\bar{d}+1))^2}{[n - \beta\bar{d}[n - p(\bar{d}+1)]]^2}\Big] \tag{29}$$

From the above equation we can see the denominator is strictly positive. Therefore, the sign of $\frac{d\overline{e^*}}{d\beta}$ depends on the sign of the numerator. Intuitively, we understand that an increase in the degree of complementarity between the efforts of terrorists β leads to an increase in the number of neighbours, as it increases payoffs for individual terrorists. However, an increase in neighbours does not necessarily lead to an increase in effort (see the comparative statics of changes in effort with the changes in number of neighbours for a terrorist). If the equilibrium effort is non-decreasing with the number of neighbours, then the above equation becomes unambiguously positive. Otherwise, it depends on the relative strength of the marginal benefit and the marginal cost in the expression above.

Now we look at the terrorist utility. Taking derivative of equation 21, with respect to β, we get,

$$\frac{d\overline{u^*}}{d\beta} = \overline{e^*}\frac{d\overline{e^*}}{d\beta} - \frac{pf}{n}\Big[\frac{d\bar{d}}{d\beta}\Big] \tag{30}$$

If $\frac{d\overline{e^*}}{d\beta}$ is non-positive, the sign of $\frac{d\overline{u^*}}{d\beta}$ is unambiguously negative. Otherwise, it is ambiguous and depends on whether the marginal benefits from the increase in complementarity between the efforts of terrorists are higher than the marginal costs of increased connections designed due to the increase in complementarity.

The comparative statics governing the welfare of the network mirror the properties observed in the utility of individual terrorists, as the welfare of the network is a scalar addition of the utilities of individual terrorists. Given this relationship this section is skipped.

3.6 Case 2: No Probability of capture through connections

In this section, we revisit the general formulation of the utility function of individual terrorist (equation 1) and discuss the efficient network structures of the model where the probability of capture through connections are 0. Previously, we explored the scenario where a terrorist is captured with probability 1 (i.e., $\delta = 1$), both through direct and indirect connections. Now, we shall consider the cases: when a terrorist cannot be captured through direct or indirect connections ($\delta = 0$). By simplifying and rewriting equation 1, we obtain:

$$u_i = \Big(1 - p\frac{\sum_{i\neq j, d(i,j)\neq\infty}\delta^{d(i,j)}+1}{n}\Big)e_i(g_{ii} + \beta\sum_{j\in N} g_{ij}e_j) - p\frac{\sum_{i\neq j, d(i,j)\neq\infty}\delta^{d(i,j)}+1}{n}f - \frac{1}{2}e_i^2 \tag{31}$$

Lemma 8: For $\delta = 0$, terrorist network is designed of components.

Proof of Lemma 8: By plugging $\delta = 0$ into equation 31, we observe that u_i increases with the number of neighbours of terrorist i and is independent of the level of infiltration. Therefore, the efficient network is a complete component. Intuitively, this implies that when a terrorist can only be captured directly and not through any connections, the leader then designs maximally connected or complete components that maximize the utility for any individual terrorist. In this case, the equilibrium effort and the associated utility can be computed straightforwardly.

Corollary 3: Terrorists maximally connected in a component when $\delta = 0$, have the following equilibrium efforts and utilities,

$$\begin{aligned}
\overline{e^*} &= \begin{cases} \frac{1}{1-\beta[n-1]} & \text{if } \overline{e^*} < B \\ B & \text{otherwise} \end{cases} \\
\overline{u^*} &= \begin{cases} \frac{1}{2}\Big(\frac{1}{1-\beta[n-1]}\Big)^2 & \text{if } \overline{e^*} < B \\ B(1+\beta(n-1)B) - \frac{1}{2}B^2 & \text{otherwise} \end{cases}
\end{aligned} \tag{32}$$

The equilibrium efforts and utilities of individual terrorists are independent of the level of infiltration. In this scenario, the total welfare of the network is $n \times \overline{u^*}$.

3.7 Case 3: Unequal Probability of Capture through Connections

In this section, we consider the final case where a terrorist has an unequal probability of capture through connections i.e., $\delta \in (0, 1)$. This implies that a terrorist is captured with a higher probability through direct connections compared to indirect connections. In this scenario, an efficient network may consist of non-maximally connected sub-structures, depending on the level of infiltration. We illustrate this with an example. Consider the parameter values $n = 6$, $\beta = 0.11$, $\delta = 0.75$, and $f = 0.5$, while varying the level of infiltration. We have focused on $p \in [0.4, 0.6]$, as outside this range, the efficient network is composed of maximally connected sub-structures.

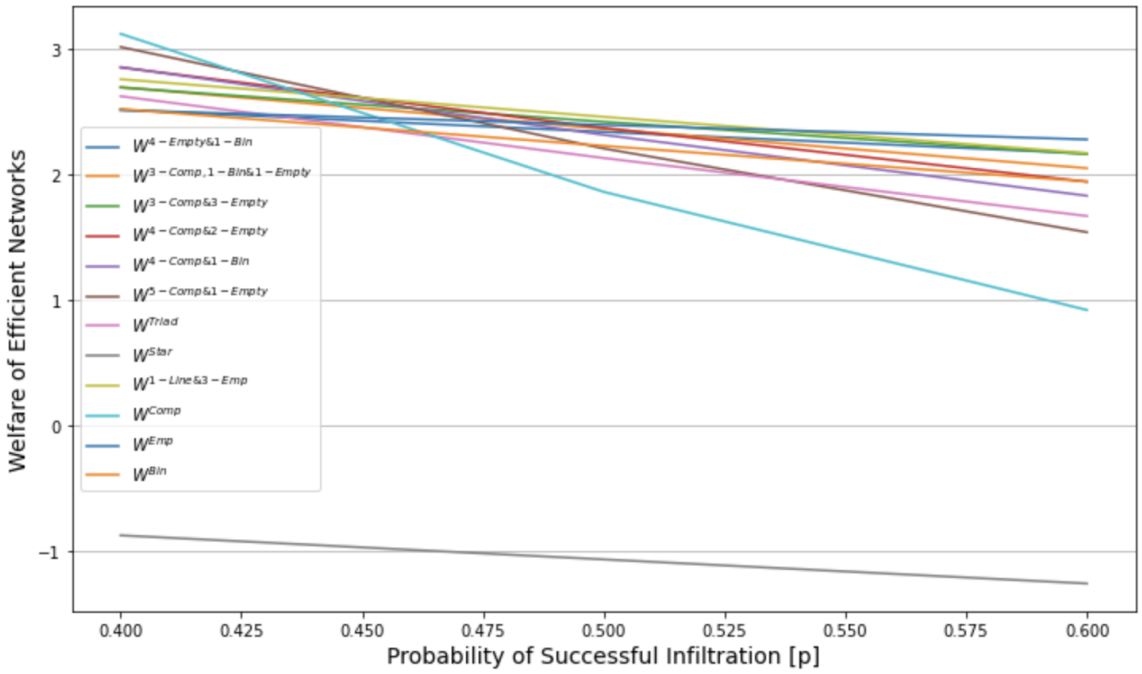

Figure 13: Transition of efficient Network with variation of p at $n = 6$, $\beta = 0.11$, $\delta = 0.75$ and $f = 0.5$

In the Figure 13 above, we considered all the efficient networks with maximally connected sub-structures for $n = 6$ and compared them with two efficient networks with non-maximally connected sub-structures: one where three nodes are designed as a line sub-structure and three are empty sub-structure, and another where the nodes are designed to have a star structure. We found that for some $p \in (0.45, 5.25]$, the efficient network is composed of non-maximally connected sub-structure. While we are not asserting that the specific configuration of three nodes designed as a line sub-structure and three empty sub-structure is the most efficient, we can conclude with certainty that for $\delta \in (0, 1)$, $p \in (0.45, 5.25]$, $n = 6$, $\beta = 0.11$, $\delta = 0.75$, and $f = 0.5$, an efficient network cannot be designed of maximally connected sub-structures i.e., components.

Therefore, we can say for a given p, f and β, for $\delta = 0$ and $\delta = 1$ the efficient terrorist network is designed of maximally connected components and $\delta \in (0, 1)$ the efficient terrorist network maybe be designed of non-maximally connected components.

4 Conclusion and Future Extensions

We developed a game-theoretic model of terrorism to gain insights into the sub-structures of efficient terrorist networks in the presence of infiltration. Our analysis reveals that, with infiltration, there are conditions under which there is a degree of separation between the various sub-structures in the network. We considered various cases regarding how a terrorist can be captured. If a terrorist is captured with probability one through both direct and indirect connections, the efficient network is composed of components. The shape and number of components within the efficient network vary with the probability of infiltration, the degree of complementarity between terrorists efforts, the network size and the fines. We observe that these components can be either symmetric or

asymmetric depending on the probability of infiltration. We also observe that, at low infiltration levels, the efficient network is a single complete component. However, when infiltration is high, the efficient network is composed of smaller, multiple components. Even when the probability of successful infiltration is 1, the efficient network is not necessarily composed of empty components. We identify two threshold values of the probability of infiltration below and above which the efficient network is composed of symmetric components. Using simulation, we showed that when fine is above a certain value, the efficient network is composed only of symmetric components. If a terrorist is captured only directly and not through any connections, the efficient network is composed of a single complete component. This complete component is independent of the probability of infiltration. However, if a terrorist is captured with a higher probability through direct connections than through indirect connections, an efficient network may be complete, empty or have non-maximally connected sub-structures.

For future research, there are several promising directions for extending our model. In our current model, we focused on how terrorists can benefit from their connections in carrying out terrorist activities. One intriguing direction for exploration is to consider how these connections may also aid terrorists in evading capture during infiltration efforts. Another direction of research could involve relaxing the assumption of an exogenous network structure to exploring the evolution of networks influenced by the probability of infiltration. Such a dynamic perspective could provide valuable insights into how terrorist networks adapt and grow over time. In our existing model, we assumed that the terrorist leader operates from a concealed location. A fascinating extension of this work would be to investigate scenarios where the leader is situated within the network and analyse the optimal position for the leader within the network structure. Furthermore, empirical research can play a crucial role in enhancing our understanding of terrorist networks in the presence of infiltration. Gathering data from sources such as the Global Terrorism Database can provide valuable insights and opportunities for real-world validation. These are the avenues of research that we intend to explore in our future work, and they hold the potential to further enrich our understanding of the dynamics of terrorist networks in the face of infiltration.

References

Acemoglu, Daron, Asuman Ozdaglar, and Alireza Tahbaz-Salehi (2015). "Systemic risk and stability in financial networks". In: *American Economic Review* 105.2, pp. 564–608.

Allen, Franklin and Ana Babus (2009). "Networks in finance". In: *The network challenge: strategy, profit, and risk in an interlinked world* 367.

Allen, Franklin and Douglas Gale (2000). "Financial contagion". In: *Journal of political economy* 108.1, pp. 1–33.

Allingham, Michael G and Agnar Sandmo (1972). "Income tax evasion: A theoretical analysis". In: *Journal of public economics* 1.3-4, pp. 323–338.

Apostol, Tom M (1991). *Calculus, Volume 1*. John Wiley & Sons.

Baccara, Mariagiovanna and Heski Bar-Isaac (2008). "How to organize crime". In: *The Review of Economic Studies* 75.4, pp. 1039–1067.

Bala, Venkatesh and Sanjeev Goyal (2000). "A noncooperative model of network formation". In: *Econometrica* 68.5, pp. 1181–1229.

Ballester, Coralio, Antoni Calvó-Armengol, and Yves Zenou (2006). "Who's who in networks. Wanted: The key player". In: *Econometrica* 74.5, pp. 1403–1417.

Ballester, Coralio, Yves Zenou, and Antoni Calvó-Armengol (2010). "Delinquent networks". In: *Journal of the European Economic Association* 8.1, pp. 34–61.

Becker, Gary S (1968). "Crime and punishment: An economic approach". In: *Journal of political economy* 76.2, pp. 169–217.

Bloch, Francis, Bhaskar Dutta, and Marcin Dziubiński (2020). "A game of hide and seek in networks". In: *Journal of Economic Theory* 190, p. 105119.

Blume, Lawrence et al. (2013). "Network formation in the presence of contagious risk". In: *ACM Transactions on Economics and Computation (TEAC)* 1.2, pp. 1–20.

Brown, William W and Morgan O Reynolds (1973). "Crime and "punishment": Risk implications". In: *Journal of economic theory* 6.5, pp. 508–514.

Cabrales, Antonio, Douglas Gale, and Piero Gottardi (2016). "Financial contagion in networks". In.

Cabrales, Antonio, Piero Gottardi, and Fernando Vega-Redondo (2017). "Risk sharing and contagion in networks". In: *The Review of Financial Studies* 30.9, pp. 3086–3127.

Calvó-Armengol, Antoni and Yves Zenou (2004). "Social networks and crime decisions: The role of social structure in facilitating delinquent behavior". In: *International Economic Review* 45.3, pp. 939–958.

Case, Anne and Lawrence F Katz (1991). *The company you keep: The effects of family and neighborhood on disadvantaged youths*.

Cerdeiro, Diego A, Marcin Dziubiński, and Sanjeev Goyal (2017). "Individual security, contagion, and network design". In: *Journal of Economic Theory* 170, pp. 182–226.

Chen, Juntao, Corinne Touati, and Quanyan Zhu (2019). "A dynamic game approach to strategic design of secure and resilient infrastructure network". In: *IEEE Transactions on Information Forensics and security* 15, pp. 462–474.

Crawford, Vincent P and Nagore Iriberri (2007). "Fatal attraction: Salience, naivete, and sophistication in experimental "hide-and-seek" games". In: *American Economic Review* 97.5, pp. 1731–1750.

Debreu, Gerard (1952). "A social equilibrium existence theorem". In: *Proceedings of the National Academy of Sciences* 38.10, pp. 886–893.

Durlauf, Steven N (2004). "Neighborhood effects". In: *Handbook of regional and urban economics* 4, pp. 2173–2242.

Dziubiński, Marcin and Jaideep Roy (2018). "Hide and seek game with multiple resources". In: *International Symposium on Algorithmic Game Theory*. Springer, pp. 82–86.

Ehrlich, Isaac (1975). "Deterrence: evidence and inference". In: *Yale. LJ* 85, p. 209.

— (1996). "Crime, punishment, and the market for offenses". In: *Journal of economic perspectives* 10.1, pp. 43–67.

Elliott, Matthew, Benjamin Golub, and Matthew O Jackson (2014). "Financial networks and contagion". In: *American Economic Review* 104.10, pp. 3115–3153.

Fan, Ky (1952). "Fixed-point and minimax theorems in locally convex topological linear spaces". In: *Proceedings of the National Academy of Sciences* 38.2, pp. 121–126.

Fisher, David C (2002). "Fractional dominations and fractional total dominations of graph complements". In: *Discrete applied mathematics* 122.1-3, pp. 283–291.

Fisher, DC (1991). "Two person zero sum games and fractional graph parameters". In: *Congressus Numerantium*, pp. 9–9.

Glaeser, Edward L, Bruce Sacerdote, and Jose A Scheinkman (1996). "Crime and social interactions". In: *The Quarterly journal of economics* 111.2, pp. 507–548.
Glicksberg, Irving L (1952). "A further generalization of the Kakutani fixed theorem, with application to Nash equilibrium points". In: *Proceedings of the American Mathematical Society* 3.1, pp. 170–174.
Goyal, S et al. (2013). "Network design and defence". In: *Games and Economic Behavior* 79.1, pp. 30–43.
Goyal, Sanjeev (2012). *Connections: an introduction to the economics of networks*. Princeton University Press.
— (2023). *Networks: An economics approach*. MIT Press.
Goyal, Sanjeev and Adrien Vigier (2014). "Attack, defence, and contagion in networks". In: *The Review of Economic Studies* 81.4, pp. 1518–1542.
Gueye, Assane, Jean C Walrand, and Venkat Anantharam (2012). "How to choose communication links in an adversarial environment?" In: *Game Theory for Networks: 2nd International ICST Conference, GAMENETS 2011, Shanghai, China, April 16-18, 2011, Revised Selected Papers 2*. Springer, pp. 233–248.
Heineke, John M (1978). *Economic models of criminal behavior*. North-Holland Amsterdã, Holanda.
Jackson, Matthew O et al. (2008). *Social and economic networks*. Vol. 3. Princeton university press Princeton.
Kiekintveld, Christopher et al. (2009). "Computing optimal randomized resource allocations for massive security games". In.
Krebs, Valdis E (2002). "Mapping networks of terrorist cells". In: *Connections* 24.3, pp. 43–52.
Rochet, Jean-Charles and Jean Tirole (1996). "Interbank lending and systemic risk". In: *Journal of Money, credit and Banking* 28.4, pp. 733–762.
Sarnecki, Jerzy (2001). *Delinquent networks: Youth co-offending in Stockholm*. Cambridge University Press.
Schorkopf, Frank (2003). "Behavioral and Social Science Perspectives on Political Violence". In: *Terrorism as a Challenge for National and International Law*. Springer Verlag, pp. 3–22.
Sinha, Arunesh et al. (2018). "Stackelberg security games: Looking beyond a decade of success". In: IJCAI.
Stupak, Oleh (2023). "Secure and efficient networks". In.
Vega-Redondo, Fernando (2007). *Complex social networks*. 44. Cambridge University Press.
Von Neumann, John (1953). "A certain zero-sum two-person game equivalent to the optimal assignment problem". In: *Contributions to the Theory of Games* 2.0, pp. 5–12.
Waniek, Marcin, Tomasz P Michalak, Talal Rahwan, et al. (2017). "On the construction of covert networks". In: *Proceedings of the 16th conference on autonomous agents and multiagent systems*, pp. 1341–1349.
Waniek, Marcin, Tomasz P Michalak, Michael J Wooldridge, et al. (2018). "Hiding individuals and communities in a social network". In: *Nature Human Behaviour* 2.2, pp. 139–147.
Warr, Mark (2002). *Companions in crime: The social aspects of criminal conduct*. Cambridge University Press.
Watts, Alison (2001). "A dynamic model of network formation". In: *Games and Economic Behavior* 34.2, pp. 331–341.

A Appendix: Proofs

A.1 Proof of Lemma 1:

We begin by observing that the action space for each terrorist can be restricted to the interval $[0, B]$, where B is a finite upper bound. This restriction ensures that the action spaces of all terrorists are convex (by definition) and compact subsets of the Euclidean space. Next, let us examine equation 4, which reveals that the utility function of a terrorist is continuous in the product of their actions $(e_1, e_2, \ldots, e_n)$. Now, consider the payoff function of terrorist $i \in N$, denoted as $(1 - p\frac{m_i+1}{n})e_i(1 + \beta \sum_{i \in N} g_{ij}e_j)$. This function is linear in e_i, making it quasi-concave in e_i. The second term $p\frac{m_i+1}{n}f$ is constant with respect to changes in e_i. Additionally, the quadratic cost function is convex in e_i. Hence, by analysing the utility function of terrorist i, we can conclude that it is a concave function in e_i and, therefore, quasi-concave. Since all the assumptions of the Debreu-Fan-Glicksberg Theorem [18] are satisfied – including the quasi-concavity of the utility functions, the convexity of the strategy spaces, and the compactness of the strategy sets – the game admits a Nash equilibrium.

A.2 Proof of Lemma 2:

By the definition of the path stated earlier, we can express it as:

$$|M_i \cup \{i\}| = |M_q \cup \{q\}|$$

Using the set union formula, we can rewrite the above equation as:

$$|M_i| + 1 - |M_i \cap \{i\}| = |M_q| + 1 - |M_q \cap \{q\}|$$

Since both sets $\{i\}$ and $\{q\}$ contain only one element, their cardinality is 1. Additionally, by the definition of path-connected members, M_i and $\{i\}$ are mutually exclusive sets. Therefore, $|M_i \cap \{i\}| = 0$. Similarly, M_q and $\{q\}$ are also mutually exclusive sets, so $|M_q \cap \{q\}| = 0$. Therefore, the equation can be simplified to:

$$|M_i| + 1 = |M_q| + 1$$

By the network definition, the cardinality of path-connected members is written as $|M_i| = m_i$ for all $i \in N$. Hence, the above equation can be rewritten as: $m_i + 1 = m_q + 1$. Therefore, we have successfully proven Lemma 2.

A.3 Proof of Proposition 1:

We maximise equation 4 with respect to the effort of individual terrorist e_i and set it equal to 0. Simplifying, we can write the equilibrium effort of individual terrorist in terms of equilibrium efforts of their neighbours,

$$e_i^* = \Big(1 - p\frac{m+1}{n}\Big)\Big(1 + \beta \sum_{j \in N} g_{ij}e_j\Big) \tag{33}$$

Substituting this implicit equilibrium efforts in equation 4 (the general utility function associated with $\delta = 1$) we can write the utility of individual terrorist implicitly as,

$$u_i = \frac{1}{2}\Big(1 - p\frac{m_i+1}{n}\Big)\Big(1 + \beta \sum_{j \in N} g_{ij}e_j\Big)^2 - p\frac{m_i+1}{n}f \tag{34}$$

To prove Proposition 1, we know from equation 4 that terrorist $i \in N$ will never choose zero efforts, as that would lead to $u_i < 0$. We then examine the first partial derivative of equation 33 and 34, where $\frac{\partial e_i}{\partial e_j}$ and $\frac{\partial u_i}{\partial e_j}$ will always be strictly greater than zero if $g_{ij} = 1 \; \forall \; \{i \neq j \in N\}$, given that $\boldsymbol{e} >> 0$ and $\beta \in (0, \frac{1}{n-1})$. In the network definition subsection, we defined m_i as the number of path-connected terrorists to i. Let u_i be the corresponding utility for terrorist i with degree $d_i = m_i$, where $d_i = \sum_{j \in N_i} g_{ij}$. We disregard scenarios where terrorist i has a degree $d_i > m_i$ since $d_i \subseteq m_i$. Revisiting equation 4, if terrorist i has a degree $d_i^{'} < d_i = m_i$, then $u_i^{'} < \hat{u}_i$ since $d_i^{'} < d_i$ and $e_j^{'} < e_j$ [19]. However, the cost of infiltration, given by $\Big(p\frac{m_i+1}{n}\Big)$, remains the same in both scenarios. Therefore, we can deduce that the leader designs a network where terrorists are maximally connected within a substructure (i.e., components are designed), and thus, the proposition is proved.

[18] See Debreu (1952),Fan (1952) and Glicksberg (1952).

[19] as $\frac{\partial e_i}{\partial e_j} > 0$ and $\frac{\partial u_i}{\partial e_j} > 0$ if $g_{ij} = 1 \; \forall \; i \neq j \in N, \beta \in (0, \frac{1}{n-1})$ and $\boldsymbol{e} >> 0$

A.4 Proof of Corollary 1

A.4.1 Proof of Interior Equilibrium Effort

Looking back at the equilibrium conditions (equation 6), we know,

$$e_i^* = \Big(1 - p\frac{\overline{d}+1}{n}\Big)\Big(1 + \beta\overline{d}e_j^*\Big)$$

Given the model parameters, its a isomorphic decision problem, so we are focussing on the symmetric equilibrium, therefore $e_i^* = e_j^* = \overline{e^*}$, hence we can write the above equation as,

$$\overline{e^*} = \Big(1 - p\frac{\overline{d}+1}{n}\Big)\Big(1 + \beta\overline{d}\overline{e^*}\Big) \tag{35}$$

Simplifying the equation 35, we can write,

$$\overline{e^*} = \Big(1 - p\frac{\overline{d}+1}{n}\Big) + \Big(1 - p\frac{\overline{d}+1}{n}\Big)\beta\overline{d}\overline{e^*}$$

$$\overline{e^*}\Big[1 - \Big(1 - p\frac{\overline{d}+1}{n}\Big)\beta\overline{d}\overline{e^*}\Big] = \Big(1 - p\frac{\overline{d}+1}{n}\Big)$$

Hence the interior equilibrium effort can be written as,

$$\overline{e^*} = \frac{n - p(\overline{d}+1)}{n - \beta\overline{d}(n - p(\overline{d}+1))}$$

A.4.2 Proof of Equilibrium Utility

Plugging equilibrium effort equation (equation 7) in the individual utility function (equation 5), we can write the equilibrium utility as,

$$\overline{u^*} = \frac{1}{2}\Big(1 - p\frac{\overline{d}+1}{n}\Big)^2\Big(1 + \beta\overline{d}\overline{e^*})^2 + \frac{\overline{d}+1}{n}p(-f) \tag{36}$$

Now substituting equilibrium effort in equation 36, we get,

$$\overline{u^*} = \frac{1}{2}\Big(1 - p\frac{\overline{d}+1}{n}\Big)^2\Big(1 + \beta\overline{d}\Big(\frac{n - p(\overline{d}+1)}{n - \beta\overline{d}[n - p(\overline{d}+1)]}\Big)\Big)^2 + \frac{\overline{d}+1}{n}p(-f)$$

We now simplify the equilibrium utility step by step,

$$\overline{u^*} = \frac{1}{2}\Big(1 - p\frac{\overline{d}+1}{n}\Big)^2\Big(1 + \beta\overline{d}\Big(\frac{n - p(\overline{d}+1)}{n - \beta\overline{d}[n - p(\overline{d}+1)]}\Big)\Big)^2 + \frac{\overline{d}+1}{n}p(-f)$$

$$\overline{u^*} = \frac{1}{2}\Big(1 - p\frac{\overline{d}+1}{n}\Big)^2\Big(1 + \Big(\frac{n\beta\overline{d} - p\beta\overline{d}(\overline{d}+1)}{n - \beta\overline{d}n + p\beta\overline{d}(\overline{d}+1)}\Big)\Big)^2 + \frac{\overline{d}+1}{n}p(-f)$$

$$\overline{u^*} = \frac{1}{2}\Big(1 - p\frac{\overline{d}+1}{n}\Big)^2\Big(\frac{n - \beta\overline{d}n + p\beta\overline{d}(\overline{d}+1) + n\beta\overline{d} - p\beta\overline{d}(\overline{d}+1)}{n - \beta\overline{d}n + p\beta\overline{d}(\overline{d}+1)}\Big)^2 + \frac{\overline{d}+1}{n}p(-f)$$

$$\overline{u^*} = \frac{1}{2}\Big(1 - p\frac{\overline{d}+1}{n}\Big)^2\Big(\frac{n}{n - \beta\overline{d}n + p\beta\overline{d}(\overline{d}+1)}\Big)^2 - \frac{\overline{d}+1}{n}pf$$

The simplified interior equilibrium utility can be written as,

$$\overline{u^*} = \frac{1}{2}\Big(\frac{n - p(\overline{d}+1)}{n - \beta\overline{d}n + p\beta\overline{d}(\overline{d}+1)}\Big)^2 - \frac{\overline{d}+1}{n}pf$$

When the equilibrium effort admits a corner solution i.e. $\overline{e^*} = B$, the corresponding equilibrium utility can be written as,

$$\overline{u^*} = \Big(1 - p\frac{\overline{d}+1}{n}\Big)B\Big(1 + \beta\overline{d}B\Big) - \frac{\overline{d}+1}{n}pf - \frac{1}{2}B^2 \tag{37}$$

A.5 Proof of Corollary 2

Substituting the equilibrium utilities in the welfare function (equation 2), we can obtain the equilibrium welfare of an efficient network. The welfare corresponding to the interior equilibrium effort can be written as,

$$\overline{W^*_{int}} = \sum_{k=1}^{K}\Big(\overline{d_k}+1\Big)\Big[\frac{1}{2}\Big(\frac{n-p(\overline{d_k}+1)}{n-\beta\overline{d_k}n+p\beta\overline{d_k}(\overline{d_k}+1)}\Big)^2-\Big(\frac{\overline{d_k}+1}{n}\Big)pf\Big]$$

Similarly, the welfare corresponding to the corner equilibrium effort, can be written as,

$$\overline{W^*_{cor}} = \sum_{k=1}^{K}\Big(\overline{d_k}+1\Big)\Big[(1-p\frac{\overline{d_k}+1}{n})B(1+\beta\overline{d_k}B)-\Big(\frac{\overline{d_k}+1}{n}\Big)pf-\frac{1}{2}B^2\Big]$$

When the components in the efficient network are symmetric, the corresponding utilities are:

$$\overline{W^*_{int}} = n\Big[\frac{1}{2}\Big(\frac{n-p(\overline{d}+1)}{n-\beta\overline{d}n+p\beta\overline{d}(\overline{d}+1)}\Big)^2-\frac{\overline{d}+1}{n}pf\Big]$$

and,

$$\overline{W^*_{cor}} = n\Big[(1-p\frac{\overline{d_k}+1}{n})B(1+\beta\overline{d_k}B)-\Big(\frac{\overline{d_k}+1}{n}\Big)pf-\frac{1}{2}B^2\Big]$$

A.6 Proof of Proposition 3

We will prove Proposition 3 with the help of Lemma 7A and Lemma 7B:

Proof of Lemma 7A: Based on Lemma 6A, we have shown that at $p=0$, the terrorist network comprises a single component. Comparing $\overline{W}(p=0,\overline{d}=n-1)=\frac{n}{2}\left(\frac{n}{n-\beta(n-1)}\right)^2$ and $\overline{W}(p=1,\overline{d}=n-1)=-nf$, it becomes evident that $\overline{W}(p=0,\overline{d}=n-1)>\overline{W}(p=1,\overline{d}=n-1)$. Our focus lies in determining the existence of p^*, such that $\forall p\in[0,p^*]$, the efficient network maintains a single maximally connected component. To show this, we need to demonstrate that for such p's the following condition holds,

$$\overline{W}(p,\overline{d}=n-1)>\widehat{W}=\max_{\mathcal{G}}\sum_{k=1}^{K}(\overline{d_k}(\mathcal{G})+1)u_k(p,\overline{d_k}(\mathcal{G})) \tag{38}$$

Beyond p^*, the efficient network no longer exhibits a single complete component.

Consider a function $g(p)$ defined as follows: $g(p)=\overline{W}(p,\overline{d}=n-1)-\widehat{W}(p)$. We understand that $g(p)$ is continuous since $\overline{W}(p,\overline{d}=n-1)$ and $\widehat{W}(p)$ are continuous functions. We want to analyse $g(p)$ at $p=0$ and $p=1$.

1. At $p=0$, we find $g(p=0)=\overline{W}(p=0,\overline{d}=n-1)-\widehat{W}(p=0)>0$. This inequality is based on Lemma 6A, which tells us that when $p=0$, the efficient network is comprised of a single component.
2. At $p=1$, we have $g(p=1)=\overline{W}(p=1,\overline{d}=n-1)-\widehat{W}(p=1)<0$. Given that $\frac{\partial\overline{u}}{\partial p}<0$ and considering that $\overline{W}$ is a linear transformation of $\overline{u}$, we can infer that $\frac{\partial\overline{W}}{\partial p}<0$. We also understand that there is a monotonic non-increasing relationship between p and $\overline{d}$. This suggests when p increases, the efficient network transitions from being a single component to other efficient network structures.

By applying Bolzano's Theorem [20], we can conclude that there exists a $p\in(0,1)$ such that $g(p)=0$. Consequently, $\overline{W}(p,\overline{d}=n-1)=\widehat{W}(p)$, and we can identify a p^*, such that $\forall p\in[0,p^*]$, the efficient network remains a single maximally connected complete component. Beyond p^*, this single complete component is no longer the efficient network.

Proof of Lemma 7B: Similarly, from Lemma 6B we know that at $p=1$, the terrorist network will have n empty components. We are interested in discussing the existence of p^{**}, such that $\forall p\in[p^{**},1]$, the efficient

[20] See Apostol 1991

network will have n empty components. To establish this, we need to demonstrate that for such p's the following condition holds,

$$\overline{W}(p, \overline{d} = 0) > \widehat{W} = \max_{\mathcal{G}} \sum_{k=1}^{K} (\overline{d_k}(\mathcal{G}) + 1) u_k(p, \overline{d_k}(\mathcal{G})) \tag{39}$$

Below p^{**}, the efficient network comprises of components which larger component size compared to empty networks.

Consider a function $h(p)$ defined as follows: $h(p) = \overline{W}(p, \overline{d} = 0) - \widehat{W}(p)$. We understand $h(p)$ is continuous since $\overline{W}(p, \overline{d} = 0)$ and $\widehat{W}(p)$ are continuous functions. We want to analyze $h(p)$ at $p = 0$ and $p = 1$.

1. At $p = 0$, we find $h(p = 0) = \overline{W}(p = 0, \overline{d} = 0) - \widehat{W}(p = 0) < 0$. Given that $\frac{\partial \overline{u}}{\partial p} < 0$ and considering that $\overline{W}$ is a linear transformation of u, we can infer that $\frac{\partial \overline{W}}{\partial p} < 0$. We also understand that there is a monotonic non-increasing relationship between p and $\overline{d}$. This suggests that when p is low, the efficient network will comprise of larger connected components compared to empty components, and the welfare of these efficient networks with larger connected components is higher than efficient networks with empty components.

2. At $p = 1$, we have $h(p = 1) = \overline{W}(p = 1, \overline{d} = 0) - \widehat{W}(p = 1) > 0$. This inequality is based on Lemma 6B, which tells us that when $p = 1$, the efficient network is comprised of only empty components.

By applying Bolzano's Theorem, we can conclude that there exists an $p \in (0, 1)$ such that $h(p) = 0$. Consequently, $\overline{W}(p, d = 0) = \widehat{W}(p)$, and we can identify a p^{**}, such that $\forall p \in [p^{**}, 1]$, the efficient network comprises of only empty components. Below p^{**}, the efficient network comprises of components with larger connected components compared to empty networks.

B Appendix: Tables

B.1 Optimal degree with changes in p when $n = 100$, $f = 1$ and $\beta = 0.01$

For	p	=	0.00,	d	where	u	is	maximum:	99.0000
For	p	=	0.01,	d	where	u	is	maximum:	99.0000
For	p	=	0.02,	d	where	u	is	maximum:	99.0000
For	p	=	0.03,	d	where	u	is	maximum:	99.0000
For	p	=	0.04,	d	where	u	is	maximum:	99.0000
For	p	=	0.05,	d	where	u	is	maximum:	99.0000
For	p	=	0.06,	d	where	u	is	maximum:	99.0000
For	p	=	0.07,	d	where	u	is	maximum:	99.0000
For	p	=	0.08,	d	where	u	is	maximum:	99.0000
For	p	=	0.09,	d	where	u	is	maximum:	99.0000
For	p	=	0.10,	d	where	u	is	maximum:	99.0000
For	p	=	0.11,	d	where	u	is	maximum:	99.0000
For	p	=	0.12,	d	where	u	is	maximum:	99.0000
For	p	=	0.13,	d	where	u	is	maximum:	99.0000
For	p	=	0.14,	d	where	u	is	maximum:	99.0000
For	p	=	0.15,	d	where	u	is	maximum:	99.0000
For	p	=	0.16,	d	where	u	is	maximum:	99.0000
For	p	=	0.17,	d	where	u	is	maximum:	99.0000
For	p	=	0.18,	d	where	u	is	maximum:	99.0000
For	p	=	0.19,	d	where	u	is	maximum:	99.0000
For	p	=	0.20,	d	where	u	is	maximum:	99.0000
For	p	=	0.21,	d	where	u	is	maximum:	99.0000
For	p	=	0.22,	d	where	u	is	maximum:	99.0000
For	p	=	0.23,	d	where	u	is	maximum:	99.0000
For	p	=	0.24,	d	where	u	is	maximum:	99.0000
For	p	=	0.25,	d	where	u	is	maximum:	99.0000
For	p	=	0.26,	d	where	u	is	maximum:	99.0000
For	p	=	0.27,	d	where	u	is	maximum:	99.0000
For	p	=	0.28,	d	where	u	is	maximum:	99.0000
For	p	=	0.29,	d	where	u	is	maximum:	99.0000
For	p	=	0.30,	d	where	u	is	maximum:	99.0000
For	p	=	0.31,	d	where	u	is	maximum:	99.0000
For	p	=	0.32,	d	where	u	is	maximum:	99.0000
For	p	=	0.33,	d	where	u	is	maximum:	99.0000
For	p	=	0.34,	d	where	u	is	maximum:	99.0000
For	p	=	0.35,	d	where	u	is	maximum:	99.0000
For	p	=	0.36,	d	where	u	is	maximum:	99.0000
For	p	=	0.37,	d	where	u	is	maximum:	98.0000
For	p	=	0.38,	d	where	u	is	maximum:	92.0000
For	p	=	0.39,	d	where	u	is	maximum:	86.0000
For	p	=	0.40,	d	where	u	is	maximum:	80.0000
For	p	=	0.41,	d	where	u	is	maximum:	74.0000
For	p	=	0.42,	d	where	u	is	maximum:	69.0000
For	p	=	0.43,	d	where	u	is	maximum:	63.0000
For	p	=	0.44,	d	where	u	is	maximum:	57.0000
For	p	=	0.45,	d	where	u	is	maximum:	52.0000
For	p	=	0.46,	d	where	u	is	maximum:	46.0000
For	p	=	0.47,	d	where	u	is	maximum:	40.0000
For	p	=	0.48,	d	where	u	is	maximum:	34.0000
For	p	=	0.49,	d	where	u	is	maximum:	26.0000

For	p	=	0.50,	d	where	u	is	maximum:	0.0000
For	p	=	0.51,	d	where	u	is	maximum:	0.0000
For	p	=	0.52,	d	where	u	is	maximum:	0.0000
For	p	=	0.53,	d	where	u	is	maximum:	0.0000
For	p	=	0.54,	d	where	u	is	maximum:	0.0000
For	p	=	0.55,	d	where	u	is	maximum:	0.0000
For	p	=	0.56,	d	where	u	is	maximum:	0.0000
For	p	=	0.57,	d	where	u	is	maximum:	0.0000
For	p	=	0.58,	d	where	u	is	maximum:	0.0000
For	p	=	0.59,	d	where	u	is	maximum:	0.0000
For	p	=	0.60,	d	where	u	is	maximum:	0.0000
For	p	=	0.61,	d	where	u	is	maximum:	0.0000
For	p	=	0.62,	d	where	u	is	maximum:	0.0000
For	p	=	0.63,	d	where	u	is	maximum:	0.0000
For	p	=	0.64,	d	where	u	is	maximum:	0.0000
For	p	=	0.65,	d	where	u	is	maximum:	0.0000
For	p	=	0.66,	d	where	u	is	maximum:	0.0000
For	p	=	0.67,	d	where	u	is	maximum:	0.0000
For	p	=	0.68,	d	where	u	is	maximum:	0.0000
For	p	=	0.69,	d	where	u	is	maximum:	0.0000
For	p	=	0.70,	d	where	u	is	maximum:	0.0000
For	p	=	0.71,	d	where	u	is	maximum:	0.0000
For	p	=	0.72,	d	where	u	is	maximum:	0.0000
For	p	=	0.73,	d	where	u	is	maximum:	0.0000
For	p	=	0.74,	d	where	u	is	maximum:	0.0000
For	p	=	0.75,	d	where	u	is	maximum:	0.0000
For	p	=	0.76,	d	where	u	is	maximum:	0.0000
For	p	=	0.77,	d	where	u	is	maximum:	0.0000
For	p	=	0.78,	d	where	u	is	maximum:	0.0000
For	p	=	0.79,	d	where	u	is	maximum:	0.0000
For	p	=	0.80,	d	where	u	is	maximum:	0.0000
For	p	=	0.81,	d	where	u	is	maximum:	0.0000
For	p	=	0.82,	d	where	u	is	maximum:	0.0000
For	p	=	0.83,	d	where	u	is	maximum:	0.0000
For	p	=	0.84,	d	where	u	is	maximum:	0.0000
For	p	=	0.85,	d	where	u	is	maximum:	0.0000
For	p	=	0.86,	d	where	u	is	maximum:	0.0000
For	p	=	0.87,	d	where	u	is	maximum:	0.0000
For	p	=	0.88,	d	where	u	is	maximum:	0.0000
For	p	=	0.89,	d	where	u	is	maximum:	0.0000
For	p	=	0.90,	d	where	u	is	maximum:	0.0000
For	p	=	0.91,	d	where	u	is	maximum:	0.0000
For	p	=	0.92,	d	where	u	is	maximum:	0.0000
For	p	=	0.93,	d	where	u	is	maximum:	0.0000
For	p	=	0.94,	d	where	u	is	maximum:	0.0000
For	p	=	0.95,	d	where	u	is	maximum:	0.0000
For	p	=	0.96,	d	where	u	is	maximum:	0.0000
For	p	=	0.97,	d	where	u	is	maximum:	0.0000
For	p	=	0.98,	d	where	u	is	maximum:	0.0000
For	p	=	0.99,	d	where	u	is	maximum:	0.0000

B.2 Optimal degree with Variation in p when $n = 100$, $f = 4$, and $\beta = 0.01$

For	p	=	0.328,	d	where	u	is	maximum:	99.0000
For	p	=	0.329,	d	where	u	is	maximum:	99.0000
For	p	=	0.330,	d	where	u	is	maximum:	99.0000
For	p	=	0.331,	d	where	u	is	maximum:	99.0000
For	p	=	0.332,	d	where	u	is	maximum:	99.0000
For	p	=	0.333,	d	where	u	is	maximum:	99.0000
For	p	=	0.334,	d	where	u	is	maximum:	99.0000
For	p	=	0.335,	d	where	u	is	maximum:	99.0000
For	p	=	0.336,	d	where	u	is	maximum:	99.0000
For	p	=	0.337,	d	where	u	is	maximum:	99.0000
For	p	=	0.338,	d	where	u	is	maximum:	99.0000
For	p	=	0.339,	d	where	u	is	maximum:	0.0000
For	p	=	0.340,	d	where	u	is	maximum:	0.0000
For	p	=	0.341,	d	where	u	is	maximum:	0.0000
For	p	=	0.342,	d	where	u	is	maximum:	0.0000
For	p	=	0.343,	d	where	u	is	maximum:	0.0000
For	p	=	0.344,	d	where	u	is	maximum:	0.0000
For	p	=	0.345,	d	where	u	is	maximum:	0.0000
For	p	=	0.346,	d	where	u	is	maximum:	0.0000
For	p	=	0.347,	d	where	u	is	maximum:	0.0000