# Protection optimale des réseaux logistiques contre des attaques

**Thèse**

**Naji Bricha**

**Doctorat en génie mécanique**

**Philosophiae doctor (Ph.D.)**

Québec, Canada

# Résumé

L’évolution des réseaux logistiques s'accompagne du risque inquiétant d'attaques intentionnelles et ils deviennent de plus en plus des cibles potentielles. Il est donc essentiel de les protéger contre ces attaques. Cette thèse développe une méthode d’allocation optimale des ressources de défense des entités de réseaux logistiques contre des attaques intentionnelles, dans le contexte de l’optimisation de la localisation des installations. Cette méthode permet de calculer les dégâts, d’évaluer la valeur d'une cible critique et de répartir de façon optimale des ressources limitées de défense, et ce, en tenant compte de la stratégie de l’attaquant. Trois cas de réseaux logistiques sont étudiés dans cette thèse. Nous considérons tout d’abord le contexte de localisation d’installations *à capacité illimitée* où une stratégie de protection optimale est sélectionnée. Ensuite, la notion de *capacité supplémentaire* est utilisée comme moyen de protection *indirecte*, permettant de réduire le dommage encouru. Enfin, comme l'efficacité d’un réseau logistique est largement déterminée par le bon fonctionnement des *entrepôts*, ces derniers sont également protégés de la même façon que les usines. Alors que l’objectif du défendeur est de minimiser les dégâts, l’attaquant va chercher à maximiser ces dégâts. Dans les trois cas considérés, le problème sera défini comme un jeu non coopératif min-max à deux périodes dans lequel le défendeur joue en premier. Cela signifie que le défendeur choisit une stratégie à la première période qui minimise le dégât maximal que l’attaquant pourrait causer à la seconde période. Dans le but d’estimer les utilités des joueurs, la méthode proposée évalue l’espérance mathématique de plusieurs coûts : le coût nécessaire à la restauration des installations endommagées, les coûts encourus en raison de l'augmentation possible des coûts de transport suite à des attaques, et le coût dû à une rupture de stock. Un algorithme est développé afin de déterminer la solution d'équilibre et la stratégie de défense optimale. Dans chacun des cas étudiés, notre méthode est comparée à d'autres stratégies. Les résultats obtenus montrent clairement l’efficacité de notre modèle et l’apport de la capacité supplémentaire comme moyen de protection indirecte, ainsi que l’importance de protéger les entrepôts.

# Abstract

The evolution of logistic networks is accompanied by the worrisome risk of intentional attacks and these networks increasingly become potential targets. It is essential to protect them against these attacks. This thesis develops a method for the optimal allocation of defensive resources among the entities' logistic networks to protect against intentional attacks in the context of facility location optimization. This method is developed to calculate the expected damage, evaluate the value of a critical target and optimally distribute the limited defensive resources, taking the attacker's strategy into account. Three cases of logistics networks are studied in this thesis. We first of all consider the context of the uncapacitated fixed-charge location where a strategy of optimal protection is selected. Then, extra-capacity is used as a means for indirect protection, allowing the reduction of the expected damage. Lastly, as the efficiency and effectiveness in any logistics network is largely determined by the correct operation of the warehouses, the latter are also protected in the same way as the plants. Whereas the defender's objective is to minimize the damage, the attacker seeks to maximize this damage. In the three cases considered the problem formulation as a two-period game where the defender invests in the first period. This means that the defender selects a strategy in the first period that minimizes the maximum loss the attacker may cause in the second period. A method is developed to evaluate the utilities of the players. This method evaluates many expected costs, including the cost needed to restore disabled facilities, the backorder cost, and the cost incurred because of the change in transportation costs after attacks. An algorithm is developed to find the equilibrium solution and the optimal defence strategy. Our method is compared to other suggested strategies. Obtained results clearly indicate the effectiveness of our model and the indirect protection by extra-capacity deployment, as well as the importance of protecting the warehouses.

# Table des matières

# Liste des tableaux

# Liste des figures

*À ma chère épouse Sanaa qui m'a appuyé, encouragé et soutenu durant cette période*

*À mes enfants et à mes frères à qui j'ai promis d'aller jusqu'au bout*

*À tous mes proches et amis.*

# Remerciements

Je tiens à exprimer ma reconnaissance chaleureuse et sincère à mon directeur de recherche, le professeur Mustapha Nourelfath, pour sa participation, son soutien et ses encouragements tout le long de cette thèse. La grande qualité de son encadrement m'a permis de mener à bien cette thèse et m'a toujours aidé à aller de l'avant et à ne jamais abandonner.

Je tiens à exprimer toute ma reconnaissance et ma gratitude à messieurs Daoud Ait-Kadi, professeur au département de génie mécanique de la Faculté des sciences et de génie de l'Université Laval; Farouk Yalaoui, professeur à l'Université de Technologie Troyes (France); Masoumeh Kazemi Zanjani professeur à l'université Concordia (Montréal) pour l'intérêt qu'ils ont porté à ce travail en acceptant d'être membres de mon jury et pour le temps qu'ils ont consacré à l'évaluation de cette thèse.

Un grand merci à ma chère épouse Sanâa pour son soutien inconditionnel et sa patience durant mes études. J'espère qu'elle trouve ici l'expression de mon éternelle reconnaissance.

Merci aussi à mes collègues du Centre interuniversitaire de recherche sur les réseaux d'entreprise, la logistique et le transport (CIRRELT).

# Avant-propos

Cette thèse a été effectuée sous la direction du Pr. Mustapha Nourelfath au département de génie mécanique de la faculté des sciences et de génie de l'Université Laval, au sein Centre interuniversitaire de recherche sur les réseaux d'entreprise, la logistique et le transport **(**CIRRELT). Rédigée selon le principe d'insertion d'articles, elle se compose de trois articles qui ont été tous cosignés avec Pr. Mustapha Nourelfath. Pour chacun de ces articles, j'ai agi à titre de chercheur principal dans le développement des approches proposées, la conception des algorithmes, l'implantation informatique, l'analyse des résultats, ainsi que la rédaction de la première version de chacun des trois articles.
Le premier article intitulé « *Critical supply network protection against intentional attacks: a game-theoretical model* » a été publié en 2013 dans le journal « *Reliability Engineering & System Safety* ». La version présentée dans cette thèse est identique à la version publiée.

Le second article intitulé « *Extra-capacity versus protection for supply networks under attack*» a été publié en 2014 dans le journal « *Reliability Engineering & System Safety* ». La version présentée dans cette thèse est identique à la version publiée.

Le troisième article intitulé «*Protection of warehouses and plants under capacity constraint* » a été acceptée (avec modifications mineures) pour publication dans le journal « *Reliability Engineering and System Safety* ». Il a été révisé suite aux recommandations des évaluateurs et il est présentement soumis pour approbation finale. La version présentée dans cette thèse est identique à la dernière version révisée et resoumise.

Notons que la revue *Reliability Engineering and System Safety* est l'une des revues les plus lues dans le domaine de la fiabilité ; elle cible comme public à la fois les chercheurs fiabilistes et les industriels. Avec un facteur d'impact relativement élevé, elle demeure incontestablement une excellente revue dans le domaine de sûreté de fonctionnement. Nous avons choisi d'y soumettre les trois articles dans un souci de continuité, sachant que c'est dans cette revue qu'ont paru plusieurs travaux pionniers sur la thématique émergente de la protection des infrastructures critiques.

# Chapitre 1

# Introduction

## 1.1 Motivation

Un réseau logistique comprend un ensemble de nœuds connectés entre eux par des liens. Ces nœuds représentent des sources d'approvisionnement (fournisseurs), des usines, des entrepôts, des points de vente, des marchés (clients), etc. Les principales activités logistiques (production, manutention, entreposage, …) sont effectuées au niveau des nœuds de cette chaîne. Entre les nœuds, on trouve des activités de transport de marchandises (routier, ferroviaire, aérien, maritime), d'échange d'information et de données, de dédouanement, etc.

L'importance de ces réseaux logistiques n'est plus à démontrer. D'après le 23$^{ème}$ état annuel du rapport logistique (*23$^{rd}$ Annual State of Logistics Report*), aux États-Unis, les coûts logistiques d'affaires en 2011 se sont élevés à 1,28 trillions de dollars, ce qui représente 8.5 % du produit intérieur brut (PIB) américain. Cela signifie que le fonctionnement efficace du réseau logistique est une question cruciale pour la société. Les conséquences des perturbations affectant son fonctionnement normal peuvent être catastrophiques.
Les installations des réseaux logistiques constituent des infrastructures vulnérables à différentes perturbations pouvant affecter leur performance : accidents, pannes d'équipements, incendies, catastrophes naturelles, attaques intentionnelles, sabotage, etc. Parmi les facteurs ayant contribué à l'augmentation de la vulnérabilité des réseaux logistiques de notre société moderne, on peut citer par exemple les risques liés à l'utilisation des nouvelles technologies de l'information et de la communication, l'augmentation de leur complexité et la mondialisation des échanges.

Les catastrophes causées par l'homme et par la nature ont augmenté en nombre et en intensité au cours des dernières années (les événements du 11 septembre 2001 étant parmi les plus connus du grand public). Des événements récents ont montré que si une ou plusieurs entités critiques d'un réseau logistique (installations clés, goulets d'étranglement, liaisons critiques, etc.) sont endommagées à cause d'un accident ou d'une attaque intentionnelle, le réseau est paralysé et les dégâts sont énormes. Ceci entraîne un impact négatif sur le plan social, politique et économique. L'usine d'un fournisseur unique pour les pièces essentielles ravagée par le feu étant un exemple. C'est le cas de la foudre qui a frappé l'usine de semi-conducteurs de Philips au Nouveau Mexique (Sheffi, 2005). Le four

d'une ligne de production prend feu et une production des milliers de téléphones portables est annulée. Les deux géants de la téléphonie mobiles Nokia et Ericsson, totalisent 40% des commandes de cette usine. Nokia tout seul a obtenu l'utilisation de toutes les réserves de capacités de production de Philips. La perte annuelle pour Philips est estimée à 40 millions de dollars. Celle d'Ericsson s'élève à environ 464 millions de dollars et aucune perte pour Nokia.

En 2005, dans l'océan atlantique nord des États-Unis, l'ouragan Katrina, l'un des ouragans les plus puissants a causé des dégâts estimés à plus de 108 milliards de dollars (Knabb, 2005). Les américains étaient incapables de gérer la crise comme il faut. Cet ouragan a dévoilé la vulnérabilité de leur dispositif de sécurité intérieure.

En Octobre 2001, des traces d'anthrax ont été découverts dans des installations de traitement à Brentwood (Washington, DC) au service postal gouvernemental des États-Unis (*United States Postal Service*: *USPS*) (Sheffi, 2005). Les actes terroristes ont été soupçonnés d'être responsables de cet incident. Cela a conduit à la fermeture de l'usine de 633,000 pieds carrés et l'USPS a perdu la capacité d'un grand établissement.

Dans (Hausken, 2010), l'auteur considère le cas de l'attentat au gaz sarin dans le métro de Tokyo, le 20 mars 1995. Lors de cinq attaques coordonnées, du gaz sarin a été libéré sur les lignes Chiyoda, Marunouchi et Hibiya du métro de Tokyo tuant douze personnes, blessant gravement cinquante personnes et causant des problèmes de vision temporaires à un millier d'autres. C'est l'attentat le plus grave au Japon depuis la fin de la seconde guerre mondiale. Le nombre très élevé de victimes est directement lié à la localisation (lignes de métro), à l'heure choisie (heure de pointe) et au moyen d'attaque utilisé (gaz sarin) qui peut atteindre son efficacité optimale dans le contexte de rassemblement de foules (lignes de métro, stade, concert, …). La localisation, l'heure choisie et le type d'attaque constituent la stratégie choisie par l'attaquant pour causer le plus grand dégât possible. Il est extrêmement coûteux de protéger au maximum, toutes les lignes du métro de Tokyo contre toutes les menaces. Mais la sécurité des passagers doit être assurée en considérant par exemple une mesure telle que l'interdiction des liquides et des gels au-dessus de 100 ml de volume dans le métro. Une telle mesure ne ferait que compliquer l'attaque puisque 1350 ml qui ont été utilisées dans la

ligne Naka-Meguro Hibiya, 900 ml dans le sud-ouest de la ligne liée à Chiyoda, etc. L'interdiction des liquides et des gels au-dessus de 100 ml nécessiterait l'installation du même équipement qui existe dans les aéroports. L'inconvénient de l'installation de ce matériel serait la réduction du nombre de passagers qui pourraient voyager par unité de temps et l'augmentation du nombre de files d'attente dans les stations. Une telle mesure a été mise en œuvre dans les aéroports après une découverte 2006 par les services de sécurité britanniques d'un complot visant à faire exploser des explosifs sur les avions transatlantiques. Après l'installation des appareils de dépistage dans les aéroports américains en janvier 1973, les terroristes ne pouvaient pas facilement contourner cet obstacle. En conséquence, le nombre d'attentat terroristes à partir des aéroports des États-Unis avait diminué. Par analogie, si une mesure interdisant les liquides et les gels supérieurs à 100 ml par les compagnies aériennes ont été mises en place sur le métro de Tokyo, l'attaquant peut envisager d'autres solutions telles que choisir un nouveau mode d'attaque ou abandonner l'attaque; on aurait pu décider d'assumer les coûts de la libération de grandes quantités de sarin pour maximiser les pertes, et de le faire de manière plus 'professionnelle'. L'attaque aurait eu plus de succès si les hôpitaux ne fonctionnaient pas de manière fiable. On aurait ciblé les hôpitaux, par exemple en coupant l'électricité. D'autres mesures pour assurer la défense d'un système de transport souterrain : l'installation de caméras vidéo ; de capteurs qui détectent le feu, les gaz et les bruits ; la mise en place de mesures plus contraignantes (déshabillage et décontamination des victimes par exemple).
On voit bien dans cet exemple (Hausken, 2010) qu'il est nécessaire de développer des stratégies permettant d'optimiser la défense de l'infrastructure (lignes du métro), en tenant compte du fait que les antagonistes peuvent adapter leurs actions afin d'exploiter les faiblesses de ces infrastructures.

Ainsi, dans le monde actuel, déterminer la meilleure façon de protéger les infrastructures critiques devient de plus en plus important. La protection de ces infrastructures contre des attaques stratégiques et intentionnelles est en fait devenue un sujet important pour les concepteurs.

Les installations des réseaux logistiques font partie des infrastructures critiques qui sont potentiellement vulnérables à des attaques intentionnelles par des adversaires intelligents (terroristes ou autres). Il est donc crucial de les protéger contre ce type d'attaques.
Or, la protection contre de telles attaques intentionnelles est fondamentalement différente de la protection contre des accidents aléatoires ou des désastres naturels (Bier et al., 2007). Certains types de protection ne sont efficaces que contre les attaques intentionnelles, ou seulement contre les catastrophes naturelles. Par exemple, les barrières autour des bâtiments, les caméras ou les agents de sécurité ne les protègent que contre les attaques intentionnelles (terrorisme). De même, l'amélioration de la zone humide (zone de terre qui est saturé avec de l'eau) le long d'une côte ne la protège que contre les ouragans et d'autres types de risques naturels.

Un attaquant ou un terroriste est un adversaire intelligent qui peut par exemple choisir d'attaquer la partie la plus vulnérable du réseau de façon à causer le maximum de dégâts, ou encore essayer de contourner les moyens de sécurité mis en place et d'adapter ses tactiques en exploitant tous les points faibles de l'infrastructure. La protection contre des attaques intentionnelles est ainsi fondamentalement différente de la protection contre des accidents aléatoires ou des désastres naturels (Hausken et al., 2009).

Les méthodes classiques de conception basées sur l'analyse des défaillances aléatoires des composantes ne tiennent pas directement compte de la possibilité d'attaques intentionnelles. L'attaquant est avantagé par rapport au défendeur dans le sens qu'il peut choisir le temps, la place et les moyens d'attaque. Il en résulte que les méthodes d'allocation des ressources de protection contre ces attaques doivent tenir compte de la nature intelligente et adaptative de la menace. Ce constat a motivé la problématique formulée dans cette thèse. Sachant en fait que les méthodes d'allocation des ressources de défense contre ces attaques doivent tenir compte de la nature intelligente et adaptative de la menace, notre objectif principal est de développer une méthode d'allocation optimale des ressources de défense qui tient compte de la stratégie de l'attaquant.

## 1.2 Problématique

Les travaux de cette thèse de doctorat s'inscrivent dans le cadre d'une problématique générale de conception robuste des réseaux logistiques en tenant compte du risque d'attaques intentionnelles, de la stratégie de l'attaquant et de la valeur des entités ciblées. Sachant qu'il est essentiel de développer des méthodes qui permettent d'optimiser la protection des composantes critiques, la problématique de cette thèse peut être formulée par les questions de recherche suivantes :

**Question 1**

*Comment calculer les dégâts et évaluer la valeur d'une cible critique dans un réseau logistique ?*

Nous allons chercher à évaluer la perte possible d'une ou plusieurs entités logistiques. Parmi les éléments à prendre en compte pour évaluer cette perte, on peut citer le temps nécessaire à la restauration de l'installation attaquée, l'augmentation possible des coûts de transport, la dégradation causée au niveau du service, etc. Il est nécessaire d'évaluer quantitativement ce type de dégâts. Ne pas évaluer convenablement ces dégâts peut conduire à une mauvaise protection, causant ainsi des dommages considérables.

**Question 2**

*Comment répartir de façon optimale des ressources limitées de protection en tenant compte de la stratégie de l'attaquant ?*

Sachant que la protection de toutes les installations d'un réseau logistique exposées à des attaques intentionnelles serait trop coûteuse, on considère le cas dans lequel le concepteur doit répartir un budget limité pour protéger le réseau logistique. Une telle protection doit tenir compte non seulement de la valeur des installations ciblées, mais aussi de la stratégie de l'attaquant.

Cette problématique sera étudiée dans le contexte de plusieurs configurations typiques du réseau générique de la figure 1.1. Ce réseau logistique couvre l'ensemble d'usines, d'entrepôts et clients. Sa structure dépend de combien d'usines et d'entrepôts une entreprise

devrait implanter pour satisfaire ses besoins évolutifs, où devraient-ils être localisés, quelle devrait être leur mission et quelles devraient être leurs capacités ?
Cela peut se traduire par exemple par le problème de localisation-allocation (choix des installations et détermination des flux), qui est souvent appelé simplement problème de localisation d'installations.

La localisation fait référence au choix de sites, en répondant entre autres aux questions suivantes : Où faut-il localiser les sites de production et de distribution ? De quel nombre et de quelle taille ?
L'allocation fait référence aux décisions d'affectation des activités de production/distribution aux sites choisis : À partir de chaque site, quelle demande devrait être servie ?

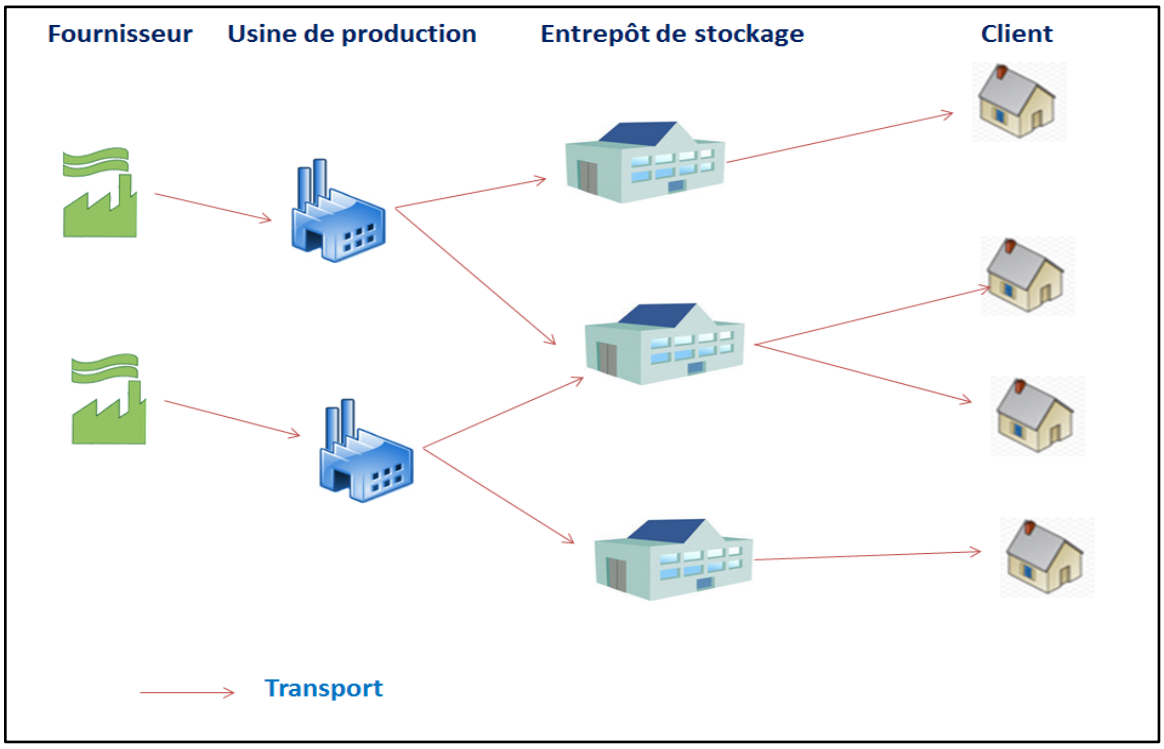


**Figure 1.1- Réseau logistique**

Ainsi, l'objectif de la localisation des installations est d'aider les entreprises à situer leurs installations pour répondre de façon optimale aux demandes de leurs clients.

Nous allons présenter ci-dessous, les problèmes de localisation d'installations les plus connus dans la littérature scientifique et les plus utilisés en pratique.

**Problème médian (*P-median problem*)**

Ce problème consiste à déterminer la localisation des installations afin de minimiser la somme des distances entre ces installations et les points de demande. Les distances sont pondérées selon l'importance de la demande. L'une des premières références introduisant ce problème est (Hakimi, 1964).

**Problèmes de couverture (*Covering problems*)**

Ce problème est décomposé en deux sous problèmes: le problème de recouvrement (*Set Covering Problem*) et le problème de couverture maximale (*Maximal Covering Problem*). Le premier problème (Toregas et al., 1971) consiste à déterminer un nombre d'installations à condition qu'aucun point de demande ne soit à une distance supérieure à la distance de couverture (seuil maximum) de l'installation la plus proche. Le deuxième problème (Church et ReVelle, 1974) consiste à maximiser les demandes couvertes pour un nombre d'installations fixe.

**Problème du centre (*Center problem*)**

Ce problème modélisé par Hakimi (1964), consiste à minimiser la distance maximale entre les points de demande et les installations les plus proches en exigeant que toutes les demandes soient satisfaites.

Dans les problèmes de conception des réseaux logistiques, le coût fixe d'ouverture d'une installation devient un objectif additionnel à la minimisation de la distance. Plusieurs modèles déterministes à charge fixe avec ou sans capacité ont été développé.

**Problème de localisation d'installations à capacité non limitée (*Uncapacitated Facility Location Problem: UFLP*)**

Dans ce problème classique (Balinski, 1965), un ensemble de sites potentiels et un ensemble des clients à servir sont considérés. Chaque site potentiel a un coût fixe d'ouverture et un coût variable d'exploitation. Le problème consiste à déterminer les

installations (capacité non limitée) à ouvrir, leurs emplacements et les flux des produits de façon à minimiser le coût total, composé du coût fixe des installations, du coût de production et/ou du coût de possession des stocks et du coût de transport.

**Problème de localisation d'installations avec capacités limitées et d'acquisition de la capacité (*Capacitated facility location and capacity acquisition problem*: *CFL & CAP*)**
Dans ce problème (Verter et Dincer, 1995), on associe à chaque site potentiel une capacité, un coût fixe d'ouverture sans le coût d'acquisition de la capacité et un coût variable d'exploitation. Ce problème consiste à décider de la localisation et de la taille des installations (capacité limitée) à ouvrir de façon à minimiser le coût total, composé du coût fixe des installations, du coût d'acquisition de la capacité, du coût de production et/ou du coût de possession des stocks et du coût de transport.

Dans cette thèse, nous avons considéré trois modèles de localisation d'installations correspondant à des configurations différentes de réseaux logistiques. Le premier modèle est celui de la localisation d'installations à capacité non limitée (*Uncapacitated Facility Location Problem: UFLP*). Le second modèle considère le problème de localisation d'installations et d'acquisition de la capacité (*Capacitated facility location and capacity acquisition problem*: *CFL & CAP*). Le troisième modèle considère est une version plus riche du second modèle que nous avons proposée afin d'inclure les entrepôts dans un contexte de capacité limitée, avec une possibilité d'étendre les capacités des usines et des entrepôts afin de contrer les effets des attaques.

## 1.3 Objectifs

L'objectif général de la thèse est de développer une méthode d'allocation optimale des ressources de défense qui tient compte de la stratégie de l'attaquant. Dans le contexte de l'optimisation de la localisation des installations, cette méthode sera ainsi développée afin de répondre aux objectifs suivants :

**Objectif 1**

*Il consiste à calculer les dégâts, évaluer la valeur d'une cible critique et répartir de façon optimale des ressources limitées de protection, en tenant compte de la stratégie de l'attaquant dans un contexte de localisation d'installations à capacité illimitée.*

Quand une usine qui doit servir un ensemble de clients donnés est hors service suite à une attaque, ces clients devront être servis par une autre usine qui se trouve plus loin. Il en résulte que les coûts engendrés vont correspondre non seulement aux coûts de restauration, mais aussi aux coûts de transport additionnels. Notre objectif ici est de proposer un modèle d'évaluation du dégât engendré par l'attaque d'une ou plusieurs installations, et de répartir un budget limité de façon optimale entre les différentes installations, tout en intégrant le caractère stratégique de l'attaquant.

**Objectif 2**

*Il consiste à étudier l'impact de la capacité supplémentaire sur la réduction du dommage dans un contexte de localisation d'installations à capacités limitées.*

Le but ici est d'étudier l'importance de la capacité supplémentaire sur la réduction des dommages des installations. Notre objectif est d'améliorer éventuellement l'allocation des ressources de protection en investissant dans des capacités supplémentaires d'usines.

**Objectif 3**

*Il s'agit d'étendre nos travaux au contexte de localisation d'usines et d'entrepôts à capacités limitées.*

Notre objectif ici est de proposer un modèle d'évaluation du dégât et de répartir de façon optimale un budget limité pour la protection d'un réseau logistique incluant des usines et des entrepôts. En plus de moyens de protection directement disponibles, la notion de capacité supplémentaire comme moyen de protection sera utilisée, aussi bien pour les usines que pour les entrepôts. Inclure ainsi les entrepôts permet d'élargir l'applicabilité de nos travaux, tout en donnant plus de possibilités pour une meilleure allocation du budget de protection. Notons aussi que l'aversion au risque d'attaque d'un entrepôt peut différer de celle associée à une usine.

## 1.4 Revue de la littérature

La protection des réseaux logistiques contre des attaques stratégiques est un domaine qui a été abordé par des communautés de recherche différentes. Notre revue de littérature va porter sur les axes complémentaires suivants :

1) Analyse de risque et sécurité des réseaux logistiques.
2) Conception robuste des réseaux logistiques.
3) Fortification et protection des réseaux logistiques.

### 1.4.1 Analyse de risque et sécurité

Les interactions complexes entre l'environnement et la société humaine exposent cette dernière à une multitude de risques. Les perturbations causées par les différentes catastrophes, ou par le terrorisme pouvant porter sur les atteintes aux personnes, les dommages aux biens physiques, mettent bien en évidence la complexité de ces interactions et l'ampleur des conséquences qui peuvent en découler.

- Avril 1912: Grosse catastrophe du Titanic.
- Janvier 1986: Désintégration de la navette spatiale américaine Challenger.
- Décembre 1984: Un gaz nocif est échappé dans une usine de pesticides de l'entreprise américaine *Union Carbide* au centre de l'Inde à Bhopal. Cet accident a coûté la vie à 8 000 personnes mortes en 3 jours. Mais le nombre total de morts est estimé jusqu'à aujourd'hui à plus de 20 000, sans compter le nombre colossal de victimes invalides à vie.
- Mars 2011: Grave accident nucléaire de la centrale *Fukushima* au Japon à cause d'un tremblement de terre suivi d'un tsunami.
- 2010: Déversement pétrolier dans le Golfe du Mexique.

Dans (Garrick et al., 2004), les auteurs proposent une méthodologie pour évaluer quantitativement les risques terroristes. Le but de la méthode est d'aider à choisir efficacement une décision pour combattre le terrorisme. L'accent est mis sur les attaques terroristes qui pourraient avoir des conséquences catastrophiques. L'objectif est d'implanter un processus des décisions résultantes de l'évaluation des risques. Ce processus comprend

(1) une compréhension de la nature de la menace, (2) un système d'information directement liée à «l'intelligence» contre le terrorisme, et (3) les structures organisationnelles qui peuvent prendre en temps opportun des actions coordonnées et efficaces.

Les auteurs Apostolakis et Lemon (2005) ont présenté une méthodologie pour l'identification et la hiérarchisation des vulnérabilités des infrastructures interconnectés. Ils ont employé la théorie des graphes pour identifier les scénarios qui sont obtenus selon la sensibilité des composants de ces infrastructures à une attaque terroriste.
La méthodologie de hiérarchisation développée est basée sur la théorie de l'utilité multi-attributs. L'impact de la perte des services d'une infrastructure est évalué à l'aide d'un arbre de décision. Les résultats obtenus, qui sont conditionnels à une menace spécifique, sont fournis au décideur pour une utilisation dans la gestion des risques. La méthodologie est développée par la présentation d'une partie de l'analyse menée sur le campus du *Massachusetts Institute of Technology*.

La vulnérabilité des réseaux logistiques dépend des éléments exposés, de leurs résistances et de leurs comportements face à une perturbation interne ou externe. Afin de pouvoir gérer les risques, il faut au préalable identifier les vulnérabilités de des réseaux logistiques.
Dans (Sheffi, 2005), l'auteur explique que le risque est la probabilité qu'un phénomène dangereux (perturbation) se produise et se transforme en un dommage d'une certaine gravité pour la santé des personnes, des biens et de l'environnement. Les risques n'ont pas tous le même niveau d'impact. Pour déterminer ce niveau d'impact, on caractérise un risque par deux grandeurs : sa fréquence, qui détermine la probabilité d'occurrence de l'événement ; et sa gravité, qui est fonction de l'ampleur des conséquences négatives. Le niveau d'impact du risque est appelé criticité et est fonction de la fréquence et de la gravité (Criticité = Fréquence × Gravité). L'analyse de risque est l'une des premières étapes et forme le principal moyen d'optimiser la sécurité. Si optimiser signifie faire le maximum, cela signifie aussi le faire avec le minimum de ressources possibles. Ayant tous intérêt à avoir une sécurité appropriée et à réduire au minimum les coûts, l'analyse de risque est donc de première importance pour tous les environnements. Quatre solutions ont été identifiées par les auteurs Martz et Johnson (1987) pour réduire la criticité des risques d'une attaque stratégique qui sont l'évitement, la prévention, la protection et le transfert.

L’évitement est une méthode radicale qui permet de réduire les risques associés à l’attaque stratégique. La prévention consiste à mettre en place des mesures limitant la fréquence des risques liés à une attaque stratégique. La protection agit sur la gravité des risques. Les mesures de protection visent à modifier le déroulement des attaques stratégiques lorsqu’elles surviennent de façon à limiter leur impact. Le transfert est un artifice permettant de ne plus assumer la responsabilité d’un risque, au profit d’un tiers. Le risque n’est pas supprimé, il est simplement déplacé.

Les premières applications de l'analyse de risque pour assurer la sécurité et lutter contre le terrorisme, ont été réalisées dans (Cox, 1990). Plusieurs autres travaux (Haimes et Roadmap., 2002; Ezell et al., 2000) ont été aussi réalisés avant même le 11 Septembre, spécifiquement sur les menaces contre les infrastructures sensibles. Après le 11 Septembre, plusieurs analystes ont proposé l’utilisation de l'analyse de risque pour la sécurité interne d’un pays (Cornell et Guikema., 2002). L'accent a été mis principalement sur la prise de décisions fondée sur des analyses de risque pour cibler la sécurité des investissements et isoler les menaces les plus importantes. Dans (Haimes et al., 1998), l’auteur a développé des méthodes de protection d’infrastructures, en regroupant les contre-mesures en quatre catégories:

- Sécurité : restreindre l'accès aux sites critiques des installations.
- Redondance : fournir d'autres moyens d'exercer les fonctions clés.
- Robustesse : rendre les systèmes plus forts ou moins sensibles aux perturbations.
- Résilience : veiller à ce que les principaux systèmes puissent être restaurés rapidement.

Les publications citées ci-dessus (et plusieurs autres) confirment que l'analyse de risque est très importante pour identifier les menaces et les vulnérabilités les plus significatives de la sécurité face aux attaques stratégiques, particulièrement pour des systèmes complexes tels que les réseaux logistiques. Les vulnérabilités de ces derniers dépendent en fait des interdépendances qui ne peuvent pas être aisément identifié sans analyse détaillée. La section suivante sera consacrée à une revue des principaux travaux sur la conception robuste des réseaux logistiques.

### 1.4.2 Conception robuste des réseaux logistiques

#### 1.4.2.1 Modèles de conception d'un réseau logistique

La conception d'un réseau logistique concerne la détermination de sa structure. En d'autres termes, la définition des liens entre les différents processus et activités d'approvisionnement, de production et de distribution. Il s'agit de déterminer le type, le nombre et la localisation des sites, de même que leurs relations d'affaires. Différents modèles peuvent être envisagés pour la résolution de tels problèmes comme les modèles de programmation mathématique déterministes et stochastiques. Un modèle de programmation mathématique, qu'il soit déterministe ou stochastique, est un outil d'optimisation. Il propose la configuration des réseaux logistiques adaptée au contexte de fonctionnement d'une organisation sur l'horizon de planification considéré, suivant les besoins à rencontrer, les capacités utilisées et les coûts ou les revenus engendrés.

Le problème de conception d'un réseau logistique peut être caractérisé comme un problème d'allocation-localisation (Martel, 2005). Les modèles déterministes fournissent une base pour la conception d'un réseau logistique qui exige des décisions stratégiques sur le nombre, l'endroit, la capacité et la mission d'équipements de production et de distribution (Owen et Daskin, 1998; Daskin et al., 2005).

Dans (Vidal et Goetschalckx, 1997; Vidal et Goetschalckx, 2000), les auteurs ont fait une synthèse de ces travaux et ont montré que la tendance et le défi portent sur la considération de l'incertitude et des perturbations dans les modèles de configuration des réseaux logistiques.

#### 1.4.2.2 Conception de réseaux logistiques fiables, robustes et résilients

Un réseau logistique est robuste (Klibi et al., 2010) s'il peut continuer à créer de la valeur, quels que soient les événements aléatoires et périlleux qui surviennent en mettant en place des politiques de réponse et des stratégies de résilience. Ces dernières permettent au réseau de retomber rapidement sur pied lorsque des ruptures se produisent. Lorsque la résilience est atteinte, l'organisation est alors plus performante ce qui devient un avantage concurrentiel face à l'environnement instable qui auparavant était susceptible d'ébranler le réseau logistique. Dans ce contexte, le critère fiabilité est un critère très pertinent parce

qu'il permet d'évaluer la robustesse des configurations du réseau. La notion de fiabilité d'un réseau logistique est liée à la théorie de la fiabilité d'un réseau quelconque. Dans (Shier, 1991), l'auteur a développé un ensemble de méthodes permettant de maximiser la probabilité qu'un graphe reste longtemps connecté après une défaillance. En règle générale, on considère la défaillance des liens du réseau. Portant principalement sur la connectivité, les modèles d'optimisation de la fiabilité des réseaux considèrent le coût de construction du réseau, et non le coût qui résulte d'une rupture. Notons aussi qu'il s'agit souvent d'une fiabilité a posteriori du réseau logistique qui est une évaluation des performances enregistrées par le réseau. Elle est mesurée après la réalisation de l'affaire contractée avec le client. Plusieurs travaux existants portent ainsi sur la conception des réseaux logistiques en tenant compte de la fiabilité (Goetschalckx et al., 2002), la robustesse (Snyder, 2006) et la réactivité (Christopher et Peck., 2004). Dans (Walid et al., 2010), l'auteur présente une méthodologie générale pour la conception de réseaux logistiques efficaces et robustes dans un environnement incertain.

L'objectif de cette méthodologie est de définir une structure réseau qui assure, de façon permanente, la création de valeur pour l'entreprise, pour faire face aux aléas associés aux opérations d'affaires normales et se prémunir contre des risques de ruptures. Elle est basée sur le cadre de prise de décision distribuée et sur une modélisation mathématique qui intègre la programmation stochastique multi-étapes, l'analyse de risque et la programmation robuste. L'anticipation de l'univers futur de l'entreprise se fait à l'aide de scénarios, grâce à une méthode Monte-Carlo. La génération des conceptions possibles est réalisée à partir d'échantillons de scénarios. Finalement, ces conceptions sont évaluées selon une approche multicritère.

### 1.4.3 Fortification et protection des réseaux logistiques

Ces modèles permettent d'identifier les investissements importants de protection et les mesures de sécurité afin d'améliorer la fiabilité des réseaux logistiques et leurs fortifications. Le premier modèle de base est dit RIMF (*R-Interdiction Median model with Fortification*). Il est basé sur le problème *P*-médian. C'est un problème de programmation en nombres entiers mixtes à deux niveaux (niveau du défendeur et niveau de l'attaquant)

qui vise la répartition optimale des ressources limitées de protection pour un ensemble d'installations, afin de minimiser les coûts de transport (Scaparra et Church, 2012).

Il existe relativement peu de travaux traitant de l'allocation optimale des ressources de défense contre des attaques intentionnelles. Dans le domaine de la fiabilité, la majorité des travaux existants mettent l'emphase sur l'identification des risques, la fortification des cibles vulnérables et l'augmentation de la probabilité de survie du système. La détermination de stratégies de réduction du risque suppose souvent que la menace est statique (Levitin, 2003). Alors que ces travaux sont très importants et essentiels, ils ignorent la nature intelligente et dynamique d'une menace (Cox, 1990; Bier et al., 2007). Le problème d'optimisation ainsi considéré ne tient pas compte de la stratégie de l'attaquant.

Dans le passé, c'est uniquement dans le domaine de la défense militaire que ce type de question a été étudié, en utilisant des concepts issus de la théorie des jeux (Berkovitz et Dresher, 1959). La contribution de notre thèse consiste à étendre et adapter ces concepts au domaine de la protection des réseaux logistiques.

En effet, la prise en considération à la fois des points de vue du défendeur et de l'attaquant, dans la protection d'infrastructures critiques, constitue actuellement un thème de recherche en pleine émergence dans la communauté des fiabilistes. Dans un travail récent (Hausken, 2011), l'auteur montre l'importance d'utiliser la théorie des jeux comme cadre conceptuel pour tenir compte des actions d'adversaires intelligents. Au début, la théorie des jeux a été appliquée pour résoudre des problèmes liés à des applications militaires. Dans (Haywood, 1954; Berkovitz et Dresher, 1960), les auteurs ont appliqué la théorie des jeux à l'emploi optimal des tactiques de guerre dans l'armé de l'air sous forme d'un jeu à multi- périodes entre les deux côtés opposés. Dans ce jeu, chaque côté cherche le plus grand profit possible. Sachant que les probabilités de comportement attendu de l'attaquant peuvent être calculées, il est normal d'appliquer les techniques de la théorie des jeux pour développer des stratégies permettant d'optimiser la défense de l'infrastructure, en tenant compte du fait que les antagonistes peuvent adapter leurs actions afin d'exploiter les faiblesses des infrastructures.

Dans (Levitin et Hausken., 2009a; Levitin et Hausken., 2009b; Levitin et Hausken., 2009c), les auteurs ont développé plusieurs méthodes permettant d'affecter des ressources parmi les composantes d'infrastructures critiques pour les défendre contre des antagonistes intelligents en tenant compte de la nature intelligente et adaptative de la menace, ainsi d'autres méthodes pour la protection contre des accidents et des phénomènes naturels.

Plusieurs autres travaux existants se concentrent sur les jeux probabilistes traitant des modèles qui ne considèrent que les probabilités de succès d'attaques, étant donné que les attaquants semblent prendre la probabilité de succès en considération dans leur choix de cibles (ressources les plus précieuses). En combinant la théorie de la fiabilité des systèmes et les techniques de la théorie des jeux, les auteurs (Levitin et Hausken, 2010) ont développé un ensemble de méthodes et d'algorithmes permettant l'allocation optimale des ressources de protection (défense) contre des attaques stratégiques pour des structures séries et parallèles. L'interaction entre joueurs conflictuels (défendeur et attaquant) est modélisée dans (Levitin et Hausken, 2010; Hausken, 2011) en introduisant le concept de fonction de succès de compétition (*contest sucess function*) (Nitzan, 1994). Dans une compétition, chaque joueur exerce des efforts afin d'augmenter sa probabilité de gagner cette compétition. Certains travaux (Hausken et Levitin, 2009a; Levitin et Hausken, 2009b) ont analysé l'amélioration de la stratégie de défense par le déploiement des fausses cibles dans le système.

## 1.5 Méthodologie

### 1.5.1 Méthodologie pour l'objectif 1

dans un contexte de localisation d'installations à capacité illimitée, nous développons une méthode pour calculer les dégâts, évaluer la valeur d'une cible critique et répartir de façon optimale des ressources limitées de protection en tenant compte de la stratégie de l'attaquant. Il s'agit de développer un modèle basé sur la théorie du jeu pour protéger les installations d'un réseau logistique contre les attaques intentionnelles, et ce, dans le contexte de localisation d'installations à capacité illimitée. Étant donné un ensemble d'alternatives d'investissement pour protéger les installations contre les menaces identifiées, l'objectif est de sélectionner la stratégie de défense optimale en tenant compte de la

stratégie de l'attaquant ; ce dernier étant considéré comme un joueur qui cherche à maximiser les dégâts. Une méthode est développée pour évaluer les utilités des deux joueurs (le défendeur et l'attaquant). Cette méthode évalue l'espérance mathématique de plusieurs coûts : le coût nécessaire à la restauration des installations endommagées, le coût due à une rupture de stock et les coûts encourus en raison de l'augmentation des coûts de transport suite à des attaques. Alors que l'objectif du défendeur est de minimiser les dégâts, l'attaquant va chercher à maximiser ces dégâts. Le problème sera défini comme un jeu non coopératif min-max à deux périodes dans lequel le défendeur joue en premier. Cela signifie que le défendeur choisit une stratégie à la première période qui minimise le dégât maximal que le défendeur pourrait causer à la seconde période. Cette façon de faire permet de tenir compte du point de vue de l'attaquant dans l'allocation optimale des ressources par le défendeur. La vulnérabilité d'une usine est définie par sa probabilité de destruction. Le conflit sur les vulnérabilités des usines est modélisé en utilisant le concept de fonction de succès de compétition, qui détermine la probabilité de gagner ou perdre dépendamment des efforts du défendeur et de l'attaquant et des caractéristiques de la compétition. Un algorithme est développé afin de déterminer la solution d'équilibre et la stratégie de défense optimale. La méthode ainsi proposée est comparée à d'autres stratégies susceptibles d'être utilisées en pratique. Les résultats obtenus montrent clairement l'efficacité de notre modèle.

### 1.5.2 Méthodologie pour l'objectif 2

La méthode développée permet d'étudier l'impact de la capacité supplémentaire sur la réduction du dommage. Nous développons un modèle sous forme d'un jeu non coopératif à deux périodes entre le défendeur et l'attaquant, qui permet la protection des installations d'un réseau logistique contre les attaques intentionnelles dans le contexte de localisation d'installations à capacités limitées.

*Le concept de capacité excédentaire (ou supplémentaire) est introduit comme moyen de protection indirecte.*

Le problème de localisation d'installations et d'acquisition de la capacité consiste à décider de la localisation, de la taille et de la date de mise en œuvre de la capacité afin de servir l'ensemble des clients. Dans (Verter et Dincer, 1995), une approche intégrée pour le problème de localisation d'installations et d'acquisition de la capacité a été étudiée dont le

but est de déterminer simultanément la localisation optimale et la taille de chaque nouvelle installation puisque dans de nombreux projets d'investissement, les décisions concernant la localisation et la taille d'une nouvelle installation sont étroitement liées car les coûts d'acquisition de la capacité dépendent de l'emplacement de la nouvelle installation. Dans (Dasci et Laporte, 2005), une approche analytique de localisation d'installations et d'acquisition de la capacité dans le contexte de la demande incertaine a été étudiée. Dans (Verter et Dincer, 1992), les auteurs ont développé une évaluation intégrée de la localisation d'installations, de l'acquisition de la capacité et du choix de la technologie pour l'élaboration de stratégies de fabrication. Les auteurs Rajagopalan et Soteriou (1994) ont développé une formulation mathématique pour modéliser l'ensemble des caractéristiques principales de l'acquisition, de la cession et des décisions de remplacement de la capacité. La capacité est souvent achetée sous forme de matériel qui correspond à une taille discrète. Une partie ou la totalité de la capacité peut être remplacé périodiquement en raison de la disponibilité des équipements moins chers et de meilleure qualité ou en raison de la détérioration et de l'augmentation des coûts d'exploitation des équipements plus âgés. Certaines capacités peuvent être éliminées en raison de la baisse de la demande. Une formulation mathématique a été développée pour modéliser l'ensemble de ces caractéristiques.

*Dans notre cas, étant donné un ensemble d'alternatives d'investissement pour défendre les installations contre des menaces, l'objectif est de sélectionner la stratégie de défense optimale (choix de capacités supplémentaires et de moyens de protection) en tenant compte de la stratégie de l'attaquant, qui cherche à maximiser le dommage*.

Une méthode et un algorithme sont développés pour évaluer les utilités des joueurs et pour déterminer la solution d'équilibre et la stratégie de défense optimale. Des résultats numériques montrent l'apport de la capacité supplémentaire comme moyen de protection indirecte.

### 1.5.3 Méthodologie pour l'objectif 3

La méthode développée dans cette étape permet d'étendre nos travaux au contexte de localisation d'usines et *d'entrepôts* avec capacités limitées. La prise en compte de la protection des entrepôts augmente la complexité du problème de protection. Pour répondre

à cet objectif, nous avons développé une méthode qui tient compte de l'importance des entrepôts. Bien que très importants, ces derniers sont souvent moins bien protégés que les usines. Cette négligence relative des entrepôts peut être justifiée par le fait que les usines contiennent plus d'équipement de production souvent plus chers.

Les entrepôts sont couramment utilisés par les fabricants pour la conservation des stocks à des fins de production ou de distribution. Il est évident que l'efficacité de fonctionnement d'un réseau logistique est liée au bon fonctionnement des entrepôts. Ils jouent un rôle vital pour le succès ou l'échec des entreprises d'aujourd'hui (Frazelle, 2002a) et dans la détermination de la compétitivité d'une entreprise. Il existe en effet de nombreuses situations où il n'est pas approprié de fournir directement aux clients. Par exemple, certains clients exigent d'être servis à partir des entrepôts qui peuvent répondre à leurs besoins la même journée ou le lendemain (Baker, 2004). Les délais de livraison des entrepôts sont courts et à moindre coût (Harrison et Hoek, 2005). Les entrepôts doivent être en mesure de recevoir correctement la marchandise et l'expédier aussi efficacement que possible, en respectant les dates de livraison promises aux clients qui sont de plus en plus exigeants ( Frazelle, 2002b). Ils permettent de réaliser des économies d'échelle dans l'achat et/ou la production et ils ont un impact critique non seulement au niveau de service à la clientèle, mais aussi sur les coûts de la logistique (Baker, 2004; Baker et Canessa, 2009; ELA European, 2004). Les entrepôts font partie intégrante du système classique de production-distribution. Dans la littérature, le problème de la conception du système classique de production-distribution est abordé par plusieurs auteurs Vidal et Goetschalckx (1997), Beamon (1998), Erenguc et al. (1999), Sarmiento et Nagi (1999), Verter et al. (2001). Le problème de la conception des entrepôts est abordé par Baker et Canessa (2009). L'auteur Syam (2000) traite le problème de localisation des entrepôts à multi périodes. L'auteur Revelle (1986) propose le modèle du problème de la localisation des entrepôts avec deux objectifs : minimiser les coûts et maximiser la demande. Dans un réseau logistique, si un ou plusieurs entrepôts ne sont pas disponibles, les pertes peuvent être importantes. Donc, il est impératif pour le succès des entreprises que les entrepôts soient conçus et protégés de façon à ce qu'ils fonctionnent de manière fiable. Même s'il existe une riche littérature sur la conception d'un réseau logistique face à des risques, la possibilité d'utiliser la capacité supplémentaire des installations (usines et entrepôts) en cas d'attaques intentionnelles n'est pas normalement

prise en compte par une telle conception. De plus, les problèmes d'optimisation considérés ne tiennent pas compte de la stratégie de l'attaquant.

La méthode que nous proposons pour la protection conjointe des usines et des entrepôts est basée sur un jeu de compétition a deux périodes, et ce, de façon similaire aux méthodes développées pour répondre aux objectifs 1 et 2. Les résultats numériques obtenus montrent l'importance de protéger les entrepôts. ,

Comme illustré à la figure 1.2, la méthodologie proposée est appliquée pour la protection des réseaux logistiques dans le cadre d'une problématique générale de conception robuste des réseaux logistiques en tenant compte du risque d'attaques, de la stratégie de l'attaquant et de la valeur des entités ciblées.

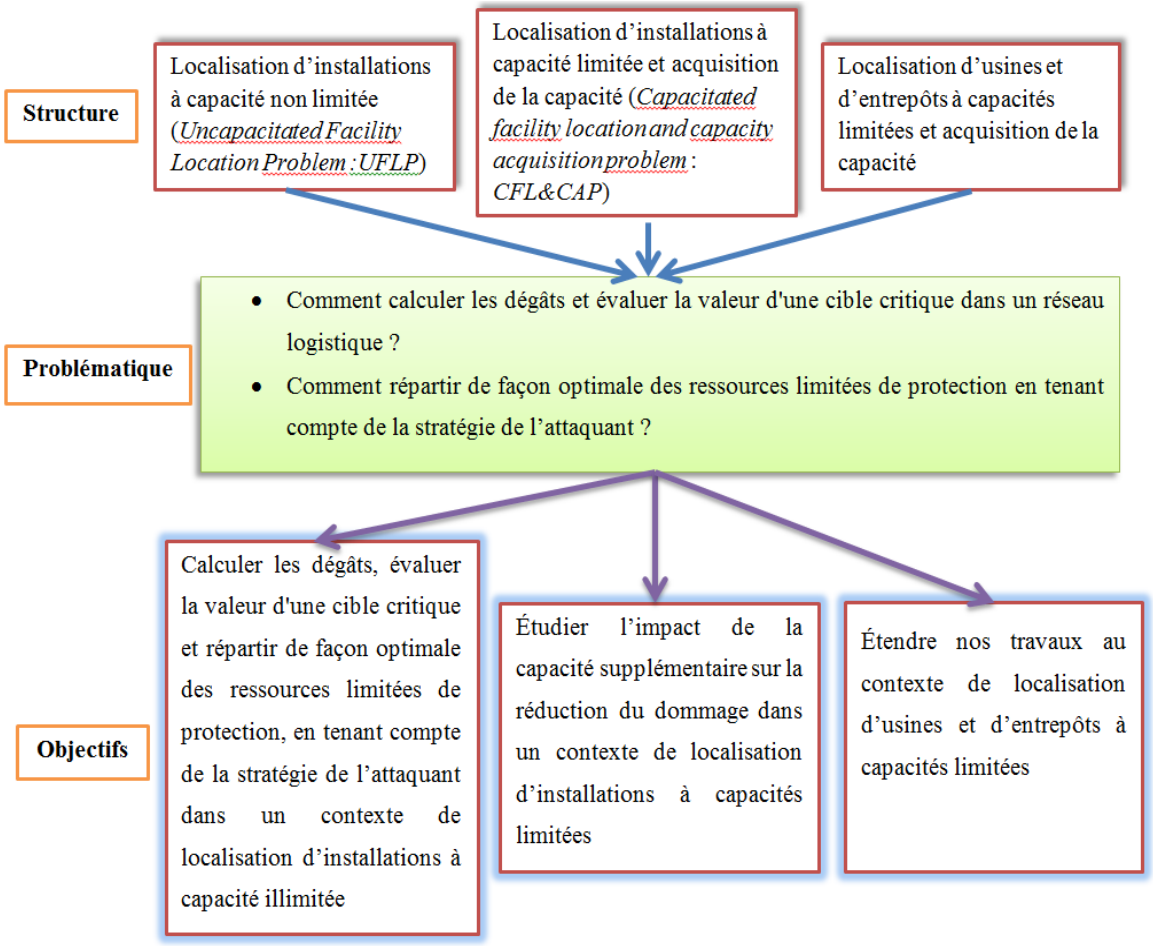


**Figure 1.2- Structure, problématique et objectifs de la thèse**

Avant de conclure ce chapitre, nous allons résumer ici les étapes méthodologiques de chacun des trois problèmes étudiés.

**Problème 1 (Contribution 1)**

*Protection du réseau logistique contre les attaques intentionnelles dans le contexte de localisation d'installations à capacités illimitées*

**Étape 1**

Résoudre le problème de localisation d'installations à capacités illimitées pour avoir la solution optimale dans une situation normale.

**Étape 2**

Formuler le problème comme un jeu non coopératif à deux périodes entre le défendeur et l'attaquant et proposer un ensemble d'alternatives de protection et un ensemble d'alternatives d'attaque.

**Étape 3**

Développer la méthode qui évalue de nombreux coûts estimés, le coût nécessaire pour restaurer les installations endommagées, le coût encouru par la rupture des stocks, et les coûts engendrés en raison de l'augmentation des coûts de transport suite aux attaques. En fonction de ces coûts, cette méthode évalue les utilités du défendeur et de l'attaquant.

**Étape 4**

Développer un algorithme qui détermine la solution d'équilibre et la stratégie de défense optimale.

**Problème 2 (Contribution 2)**

*L'impact de la capacité supplémentaire sur la réduction du dommage dans le contexte de localisation d'installations à capacités limitées*

**Étape 1**

Résoudre le problème de localisation d'installations et acquisition de la capacité pour avoir la solution optimale dans une situation normale.

**Étape 2**

Formuler le problème comme un jeu non coopératif à deux périodes entre le défendeur et l'attaquant. Proposer un ensemble d'alternatives pour la protection directe et indirecte par la capacité supplémentaire et un ensemble d'alternatives d'attaque.

**Étape 3**

Développer la méthode qui évalue de nombreux coûts estimés, le coût nécessaire pour restaurer les installations endommagées, le coût encouru par la rupture des stocks, et les coûts engendrés en raison de la variation des coûts de transport suite aux attaques. En fonction de ces coûts, cette méthode évalue les utilités du défendeur et de l'attaquant.

**Étape 4**

Développer un algorithme qui détermine la solution d'équilibre et la stratégie optimale de protection directe et indirecte par la capacité supplémentaire.

**Problème 3 (Contribution 3)**

*L'importance des entrepôts dans le contexte de localisation d'usines et d'entrepôts à capacités limitées*

**Étape 1**

Résoudre le problème de localisation d'usines et d'entrepôts à capacités limitées pour avoir la solution optimale dans une situation normale.

**Étape 2**

Formuler le problème comme un jeu non coopératif à deux périodes entre le défendeur et l'attaquant. Proposer un ensemble d'alternatives pour la protection directe et indirecte par la capacité supplémentaire, d'usines et d'entrepôts et un ensemble d'alternatives d'attaque.

**Étape 3**

Développer la méthode qui évalue de nombreux coûts estimés, le coût nécessaire pour restaurer les installations endommagées, le coût encouru par la rupture des stocks, et les coûts engendrés en raison de l'augmentation des coûts de transport suite aux attaques. En fonction de ces coûts, cette méthode évalue les utilités du défendeur et de l'attaquant.

**Étape 4**

Développer un algorithme qui détermine la solution d'équilibre et la stratégie optimale de protection directe et indirecte par la capacité supplémentaire, d'usines et d'entrepôts.

## 1.6 Conclusion

Dans ce chapitre, après avoir motivé notre étude de la protection des réseaux logistiques contre des attaques intentionnelles, nous avons détaillé la problématique et les objectifs de cette thèse. Ensuite, nous avons effectué une revue de littérature. Nous avons enfin résumé la méthodologie des travaux réalisés. Les trois prochains chapitres représenteront avec plus de détail les trois contributions de la thèse.

## Bibliographie


Apostolakis, G.E., Lemon, D.M., 2005. A Screening Methodology for the identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism. Risk Analysis 25 (2), 361-376.

Balinski, M., 1965. Integer programming: methods, uses, computation. Management Science 12, 254-313.

Baker, P., 2004. Aligning distribution center operations to supply chain strategy. International Journal of Logistics Management 15 (1), 111–123.

Baker, P., Canessa, M., 2009. Warehouse design: A structured approach. European Journal of Operational Research, 193(2), 425–436.

Beamon, B., 1998. Supply chain design and analysis: Models and methods. Internat. J. Production Econom. 55, 281–294.

Berkovitz, L., Dresher, M., 1959. A game-theory analysis of tactical air war. Military Operations Research 7, 599–620.

Berkovitz, L., Dresher, M., 1960. Allocation of two types of aircraft in tactica. Military Operations Research 8, 694–706.

Bier, V., Oliveros, S., Samuelson, L., 2007. Choosing What to Protect: Strategic defensive Allocation Against an Unknown Attacker. Journal of Public Economic Theory 9 (4), 563-587.

Cornell, P.E., Guikema, S., 2002. Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures. Military Operations Research 7 (4), 5–20.

Church, R., ReVelle, C., 1974. The maximal covering location problem. Papers of the Regional Science Association 32, 101-1018.

Cox, L., 1990. A probabilistic risk assessment program for analyzing security risks. In New risks: Issues and management, New York, Plenum Press.

Christopher, M., Peck, H., 2004. Building the resilient supply chain. International Journal of Logistics Management 15 (2), 1–13.

Dasci, A. and G. Laporte 2005. An Analytical Approach to the Facility Location and Capacity Acquisition Problem under Demand Uncertainty. Journal of the Operational Research Society 56, 397-405.

Daskin, M., Snyder, L., Berger, R., 2005. Facility Location in Supply Chain Design. Logistics Systems: Design and Operation. Springer, New York, 39–66.

Ezell, B., Farr, J. and Wiese, I., 2000. An infrastructure risk analysis of municipal water distribution system. Journal of Infrastructure Systems 6 (3), 118–122.

ELA European, 2004. Logistics Association/AT Kearney Management Consultants. Differentiation for Performance, Deutscher Verkehrs-Verlag GmbH, Hamburg.

Erenguc, S. S., Simpson, N. C., Vakharia, A. J., 1999. Integrated production/distribution planning in supply chains: An invited review. Eur. J. Oper. Res. 115, 219–236.

Frazelle, E., 2002a. Supply Chain Strategy: The Logistics of Supply Chain Management. McGraw-Hill, New York.

Frazelle, E., 2002b. World-class Warehousing and Material Handling. McGraw-Hill, New York.

Garrick, B.J., James, E.H, Max, K., McDonald, J.C, Tara, O., Peter, S.P., Elizabeth, R.P., Rosenthal, R., Alvin, W.T., Lee, A.V., Edwin, L.Z., 2004. Confronting the risks of terrorism: making the right decisions. Reliability Engineering and System Safety 86, 129-176.

Goetschalckx, M., Vidal, C. and Dogan, K., 2002. Modeling and design of global logistics systems: A review of integrated strategic and tactical models and design algorithms. European Journal of Operational Research 143, 1–18.

Haimes, Y., Matalas, N., Lambert H., Jackson, and Fellows, A., 1998. Reducing vulnerability of water supply systems to attack. Journal of Infrastructure Systems 4 (4), 164–177.

Haimes, Y. Roadmap, Y., 2002. For modeling risks of terrorism to the homeland. Journal of Infrastructure Systems 8 (2), 35–41.

Hakimi, S.L., 1965. Optimum distribution of switching centers in a communication network and some related graph theoretic problems. Operations Research 13, 462–475.

Harrison, A., Van Hoek, R., 2005. Logistics Management and Strategy, second ed. Pearson, Harlow.

Hausken, K., Bier, V., Zhuang, J., 2009. Defending against Terrorism, Natural Disaster, and All Hazards. Game Theoretic Risk Analysis of Security Threats. Springer, New York, 65-97.

Hausken, K., Levitin, G., 2009. Protection vs. False Targets in Series Systems. Reliability Engineering and System Safety 94 (5), 973-981.

Hausken, K., 2010. Defense and attack of complex and dependent systems. Journal of Reliability Engineering and System Safety 95 (1), 29–42.

Hausken, K., 2011. Protecting complex infrastructures against multiple strategic attackers, International Journal of Systems Science, 42 (1), 11-29.

Haywood, O., 1954. Military decision and game theory. Journal of the Operations Research Society of America, 365–385.

Klibi, W., Martel, A., Guitouni, A., 2010. The design of robust value-creating supply chain networks: A critical review. European Journal of Operational Research 203 (2), 283–293.

Knabb, R.D, 2005. Tropical Cyclone Report: Hurricane Katrina: 23–30.

Levitin, G., 2003. Optimal multilevel protection in series-parallel systems, Reliability Engineering and System Safety 81, 93-102.

Levitin, G., Hausken, K., 2009a. Redundancy Vs. Protection in Defending Parallel Systems Against Unintentional and Intentional Impacts. IEEE Transactions on Reliability 58 (4), 679-690.

Levitin, G., Hausken, K., 2009b. False Targets Efficiency in Defense Strategy. European Journal of Operational Research 5 (5), 155-162.

Levitin, G., Hausken, K., 2009c. Intelligence and impact contests in systems with redundancy, false targets, and partial protection. Reliability Engineering and System Safety 25, 1927–1941.

Levitin, G., Hausken, K., 2010. Defence and attack of systems with variable attacker system structure detection probability. Journal of the Operational Research Society 61, 124-133.

Martel, A., 2005. The design of production-distribution networks: A mathematical programming approach. In: Geunes, J., Pardalos, P. (Eds.), Supply Chain Optimization. Springer, 265–306.

Martz, H., Johnson, M., 1987. Risk analysis of terrorist attacks. Risk Analysis 35–47.

Nitzan, S. (1994). Modelling rent-seeking contests. European Journal of Political Economy 10(1):41–60.

Owen S., Daskin M., 1998. Strategic Facility Location: A Review. European Journal of Operational Research 111 (3), 423-447.

Rajagopalan, Soteriou, A. 1994. Capacity Acquisition and Disposal with Discrete Facility Sizes. Management Science 40 (7), 903-917.

ReVelle, C., 1986. The maximum capture or sphere of influence location problem: Hotelling revisited on a network. Journal of Regional Science 26, 343–358.

Sarmiento, A. M., Nagi, R., 1999. A review of integrated analysis of production-distribution systems. IIE Trans. 31, 1061–1074.

Syam, S.S., 2000. Multiperiod capacity expansion in globally dispersed regions, Decision Sciences 31(1), 173-196.

Scaparra, M.P., Church, R.L., 2012. Protecting supply systems to mitigate potential disaster: a model to fortify capacitated facilities. International Regional Science Review 35 (2), 188-210.

Sheffi, Y., 2005. The Resilient Enterprise, Cambridge, Mass: MIT Press.

Shier, D., 1991. Network Reliability and Algebraic Structures. Clarendon Press, Oxford, England.

Snyder, L., 2006. Facility location under uncertainty: A review. IIE Transactions 38 (7), 537–554.

Toregas, C., Swain, R., ReVelle, C., Bergman, L. 1971. The location of emergency service facilities. Operations Research 19, 1363-1373.

Verter, V., Dasci, A., Bulgak., M., 2001. The production-distribution system design problem. C. Floudas, P. Pardalos, eds. Encyclopedia of Optimization. Kluwer Academic Publishers, Boston, MA.

Verter, V., Dincer., C., 1995. Facility Location and Capacity Acquisition: An Integrated Approach. Naval Research Logistics 42, 1141-1160.

Verter, V., Dincer, C., 1992. An Integrated Evaluation of Facility Location, Capacity Acquisition and Technology Selection for Designing Global Manufacturing Strategies, European Journal of Operational Research 60 (1), 1-18.

Vidal, C., Goetschalckx, M., 1997. Strategic Production Distribution Models: A critical Review with Emphasis on Global Supply Chain Models. European Journal of Operational Research 98, 1-18.

Vidal, C., Goetschalckx, M., 2000. Modeling the Effect of Uncertainties on Global Logistics Systems. Journal of Business Logistics 21 (1), 95-120.

# Chapitre 2

# Critical supply network protection against intentional attacks: a game-theoretical model

L'article intitulé « Critical supply network protection against intentional attacks: a game-theoretical model » est inclus dans ce chapitre. Il a été publié dans le journal « Reliability Engineering and System Safety » en 2013. La version présentée dans ce chapitre est identique à la version publiée.

# Résumé

Le sujet le plus important pour les chaînes logistiques d'aujourd'hui est comment protéger ses installations contre des attaques intentionnelles, car il est devenu inacceptable d'ignorer l'impact élevé des perturbations à faible probabilité causées par ces attaques.

Cet article développe un modèle basé sur la théorie du jeu pour la protection des installations dans le contexte du problème de localisation d'installations à capacité illimitée. Étant donné un ensemble d'alternatives d'investissement pour protéger les installations contre les menaces identifiées, l'objectif est de choisir la stratégie de défense optimale. L'attaquant est considéré comme un joueur qui cherche à maximiser les dégâts attendus. Le conflit entre le défendeur et l'attaquant sur la vulnérabilité des installations est modélisé en introduisant le concept de fonction de succès de compétition. La vulnérabilité d'une installation est définie par la probabilité de sa destruction. La fonction de succès de compétition détermine la vulnérabilité de chaque installation en fonction des investissements relatifs du défendeur et de l'attaquant et des caractéristiques de la compétition. Une méthode est développée pour évaluer les utilités du défendeur et de l'attaquant. Cette méthode évalue de nombreux coûts estimés, le coût nécessaire pour restaurer les installations endommagées, le coût encouru par la rupture des stocks, et les coûts engendrés en raison de l'augmentation des coûts de transport suite aux attaques. En effet, lorsqu'une ou plusieurs installations ne sont pas disponibles, les coûts de transport vont augmenter puisque les clients des installations endommagées peuvent être servis à partir d'autres installations en service et qui sont plus éloignées. Le modèle considère un jeu non coopératif à deux périodes entre les joueurs, et un algorithme est présenté pour déterminer la solution d'équilibre et la stratégie de défense optimale. Un exemple illustratif est présenté. La stratégie de défense optimale obtenue par la méthode développée dans cet article est comparée à d'autres stratégies.

## 2.1 Abstract

A crucial issue in today's critical supply chains is how to protect facilities against intentional attacks, since it has become unacceptable to ignore the high impact of low probability disruptions caused by these attacks. This article develops a game-theoretical model to deal with the protection of facilities, in the context of the uncapacitated fixed-charge location problem. Given a set of investment alternatives for protecting the facilities against identified threats, the objective is to select the optimal defence strategy. The attacker is considered as a player who tries to maximise the expected damage while weighing against the attacks expenditures. The conflict on facilities vulnerability is modelled using the concept of contest. The vulnerability of a facility is defined by its destruction probability. Contest success functions determine the vulnerability of each facility dependent on the relative investments of the defender and the attacker on each facility, and on the characteristics of the contest. A method is developed to evaluate the utilities of the players (*i.e.*, the defender and the attacker). This method evaluates many expected costs, including the cost needed to restore disabled facilities, the backorder cost, and the cost incurred because of the increase in transportation costs after attacks. In fact, when one or several facilities are unavailable, transportation costs will increase since reassigned customers may receive shipments from facilities which are farther away. The model considers a non-cooperative two-period game between the players, and an algorithm is presented to determine the equilibrium solution and the optimal defence strategy. An illustrative example is presented. The approach is compared to other suggested strategies, and some managerial insights are provided in the context of facility location.

### Nomenclature

| | |
|---|---|
| $n$ | number of facilities in the system |
| $j$ | $j$th potential facility location, $j = 1, 2, \ldots, n$ |
| $i$ | $i$th demand location, $i = 1, 2, \ldots, u$ |
| $h_i$ | demand at customer location $i$ |
| $f_j$ | fixed cost of locating a facility at site $j$ |
| $\rho_{ij}$ | unit cost of shipping between facility site $j$ and customer location $i$ |

| | |
|---|---|
| $X_j$ | binary variable, which is equal to 1 if a facility is to be located at candidate site $j$, and 0 otherwise |
| $Y_{ij}$ | fraction of demand at customer location $i$ which is served by a facility at site $j$ |
| $\beta_j$ | type of protection for facility $j$ |
| $p$ | index of protection type, $p = 1, 2, \ldots, \beta_j$ |
| $B_{jp}$ | investment effort to protect a facility located at site $j$ using protection type $p$ |
| $b_{jp}$ | unit cost of effort to protect a facility located at site $j$ using protection type $p$ |
| $\overline{B_{jp}}$ | investment expenditure to protect a facility located at site $j$ using protection type $p$ |
| $\pi_j$ | value from $p = 1, 2, \ldots, \beta_j$ |
| $\pi_j^{opt}$ | optimal defence strategy value from $p = 1, 2, \ldots, \beta_j$ |
| $\mathbf{P}$ | vector of protection strategy, $\mathbf{P}=\left(\pi_j\right)$ |
| $\mathbf{P}_{\text{opt}}$ | vector of the optimal protection strategy, $\mathbf{P}_{\text{opt}} = \left(\pi_j^{opt}\right)$ |
| $\mathbf{B}$ | vector of investments to protection strategy $\mathbf{P}$, $\mathbf{B}= \left(B_{j\pi_j}\right)$ |
| $\mathbf{B}_{\text{opt}}$ | vector of investments to protection strategy $\mathbf{P}_{\text{opt}}$, $\mathbf{B}_{\text{opt}} = \left(B_{j\pi_j^{opt}}\right)$ |
| $B_{j\pi_j}$ | element of investments vector $\mathbf{B}$ |
| $B_{j\pi_j^{opt}}$ | element of investments vector $\mathbf{B}_{\text{opt}}$ |
| $\lambda_{jp}$ | binary variable $\lambda_{jp}$ which is equal to 1 if a protection of type $p$ is used for facility $j$ |
| $\boldsymbol{\lambda}$ | matrix, $\boldsymbol{\lambda} = \left(\lambda_{jp}\right)$ |
| $\alpha_j$ | attack type against any facility $j$ |
| $m$ | index of attack type ($m = 0, 1, \ldots, \alpha_j$) |
| $Q_{jm}$ | attack effort to attack facility located at site $j$ using attack action $m$ |
| $q_{jm}$ | unit cost to attack facility located at site $j$ using attack action $m$ |

| | |
|---|---|
| $\overline{Q_{jm}}$ | investment expenditure to attack facility located at site *j* using attack action *m* |
| $\omega_j$ | value from $m = 0, 1, \ldots, \alpha_j$ |
| $\omega_j^{opt}$ | value from *m* of the optimal attack strategy |
| **M** | vector of attack strategy, $\mathbf{M}=\left(\omega_j\right)$ |
| $\mathbf{M}_{\text{opt}}$ | vector of the optimal attack strategy, $\mathbf{M}_{\text{opt}}= \left(\omega_j^{opt}\right)$ |
| $\mathbf{Q}_{\text{opt}}$ | vector of attack effort of the optimal attack strategy, $\mathbf{Q}_{\text{opt}} = \left(Q_{j\omega_j^{opt}}\right)$ |
| $Q_{j\omega_j^{opt}}$ | element of attack effort vector $\mathbf{Q}_{\text{opt}}$ |
| $\mu_{jm}$ | binary variable which is equal to 1 if a type *m* attack is used for facility *j* |
| $\boldsymbol{\mu}$ | matrix, $\boldsymbol{\mu} = \left(\mu_{jm}\right)$ |
| $\boldsymbol{\mu}_{\text{opt}}$ | matrix, $\boldsymbol{\mu}_{\text{opt}} = \left(\mu_{jm}\right)$ |
| $\nu_{pm}(j)$ | destruction probability of a facility *j* |
| $\nu_{p\omega_j^{opt}}(j)$ | destruction probability of a facility *j* for the optimal defence strategy |
| $\nu(\mathbf{P},\mathbf{M})$ | matrix, $\nu(\mathbf{P},\mathbf{M}) = \left(\nu_{pm}(j)\right)$ |
| $\nu(\mathbf{P},\mathbf{M}_{\text{opt}})$ | matrix, $\nu(\mathbf{P},\mathbf{M}_{\text{opt}}) = \left(\nu_{p\omega_j^{opt}}(j)\right)$ |
| $c_j$ | parameter that expresses the intensity of the contest concerning facility *j* |
| $C_R(\mathbf{P},\mathbf{M})$ | expected cost required to restore the attacked facilities which depends on **P** and **M** |
| $C_R(\mathbf{P},\mathbf{M}_{\text{opt}})$ | expected cost required to restore the attacked facilities which depends on **P** and $\mathbf{M}_{\text{opt}}$ |
| $R_j$ | cost required to restore the attacked facility *j* |
| $k$ | combinations index, $(k = 0,\ldots,2^n - 1)$ |
| $S_k$ | combinations of disabled and functional facilities for the facilities |

| | |
|---|---|
| S | set of combinations of disabled and functional facilities, S = $\{S_k\}$ |
| $T_k$ | cost incurred because of the increase in transportation cost when the combination is $S_k$ |
| $B$ | backorder cost |
| $\Delta C_{pm}(k)$ | attack outcomes of combination $k$, |
| $TCI(\mathbf{P},\mathbf{M})$ | expected value of the transportation cost increase which depends on **P** and **M** |
| $TCI(\mathbf{P},\mathbf{M}_{opt})$ | expected value of the transportation cost increase which depends on **P** and $\mathbf{M}_{opt}$ |
| $D(\mathbf{P},\mathbf{M})$ | expected damage which depends on **P** and **M** |
| $U_d(\mathbf{P},\mathbf{M})$ | defender expected utility which depends on **P** and **M** |
| $U_d(\mathbf{P},\mathbf{M}_{opt})$ | defender expected utility which depends on **P** and $\mathbf{M}_{opt}$ |
| $U_a(\mathbf{P},\mathbf{M})$ | attacker expected utility which depends on **P** and **M** |
| $U_{min}$ | defender minimal utility |
| $U_{max}$ | attacker maximal utility |

## 2.2 Introduction

Many governments have identified critical infrastructures that are, by default, potential targets of terrorist attacks. These infrastructures include critical supply chains, such as those of medical material and subsistence (food or food-related supplies, including bottled water), bulk petroleum, and petro-chemicals. Therefore, a crucial issue in today's supply chains is to protect vulnerable facilities against malevolent acts. Examples of such acts are cybercrimes, destruction, theft, and manipulation of information. The cost of protecting against malevolent acts on critical infrastructures has increased during recent years. However, planning for possible intentional attacks is an enormous financial and logistical challenge. When facilities are critical, industries face a new financial allocation dilemma. On the one hand, the implementation of all the security and protection recommendations when designing new facilities or fortifying existing ones would impose a huge financial burden on industries. On the other hand, it has become unacceptable to ignore the high impact of low probability disruptions caused by intentional attacks. Since it is generally

impractical to secure all assets, it is important to optimise the protection of key supply chain facilities.

This article considers the uncapacitated fixed-charge location problem (UFLP) to deal with defence resource allocation. The facility location decisions are very important in supply chain design. The UFLP is a classical location problem and forms the basis of several location models. In this problem, we are given a set of customer locations with known demands and a set of potential facility locations. If we choose to locate a facility at a site, we incur a known fixed location cost. There is a known unit cost of shipping between each facility site and each customer location. The problem is to find the locations of the facilities, and the shipment pattern between the facilities and the customers, to minimise the sum of the facility location and shipment costs, subject to a requirement that all customer demands be satisfied. The additional strategic decision dealt with here is how to allocate optimally the protective resources among the facilities, knowing that these facilities are exposed to external intentional attacks. In other words, given a set of investment alternatives for protecting the facilities, we want to determine how much to invest optimally in defending each facility, while taking into account that both the defender and the attacker are fully optimising agents.

The traditional UFLP assumes that, once constructed, the facilities chosen will always operate as planned. However, if a facility is attacked, it may become unavailable and customers must be served from other facilities that are farther away than their regular facilities. This may lead to excessive additional transportation costs, while it is possible to increase significantly the resilience of the system when attacked by protecting a few key facilities. As major threats in today's world involve strategic attackers, accounting for the viewpoints of both the defender and the attacker has become a necessity.

Even if there is a mature literature on facility design with probabilistic failure of components [3], the possibility of intentional strikes or attacks is not normally taken into account by such a design. Previous papers on facility location and supply chain design models under uncertainty have missed taking into account the attacker as a fully strategic optimising agent. In a pioneering work, the authors of [17] formulated reliability models for facility location to hedge against facility "failures" due, for example, to inclement weather,

labour actions, sabotage, terrorism, or changes in ownership. In this model, the critical difference between intentional and non-intentional acts is however neglected. A broad range of models for designing supply chains that are resilient to disruptions is presented in a tutorial by Ref. [18], which reviews more than one hundred papers on the subject. For other reviews on facility location and supply chain design models under uncertainty, see Ref. [12]. The multi-level optimisation model presented in [15] aims at identifying the optimal allocation of limited protective resources across facilities by considering the event of a worst-case loss of a number of facilities. These types of protection models against worst-case disruptions are formulated as tri-level mixed integer programs: the top level problem involves the system planner's decisions about which facilities to secure (defender problem); the intermediate level problem models the worst-case scenario loss of unprotected facilities (attacker model); the bottom level problem reflects the fact that the system users try to operate within the system in an optimal way after the disruption (user model).

Historically, the military has had a long-term interest in identifying critical targets [6, 7, 20]. Many of these models are based on game theory to allocate resources in order to cause the greatest harm to an enemy. The use of game theory for the optimal defence of infrastructures has become more prominent in recent research in the domain of reliability theory, e.g. [2, 9, 10, 13, 30-32]. Note that in [30-32] both intentional and non-intentional impacts are taken into account.

This article accounts for these developments in reliability design, in using a way of thinking which is new in the context of facility location and supply chain design. The proposed model takes into account the discrete nature of protection and attack alternatives. To simplify the analysis, the article deals only with intentional attacks like terrorism, ignoring the existence of natural disasters and other non-intentional sources of uncertainty. Unlike the existing models for facility location and supply chain design models under uncertainty, this article develops a game-theoretical model where the defender and the attacker are considered as two strategic players. Such a model does not omit the strategic behaviour of the attacker in making decisions about defensive investments on facilities. This attacker is

considered as an intelligent and adaptable adversary player who chooses optimally how fiercely to attack facilities.

The remainder of the paper is organised as follows. Section 2 presents the mathematical model of the fixed charge facility location problem. Section 3 formulates the studied problem as a two-period game. Section 4 evaluates the players' utilities. Section 5 develops an algorithm to solve the game. Section 6 presents a numerical example. Section 7 concludes the paper.

### 2.3 The fixed-charge facility location problem

In this problem we are given a set of customer locations with known demands and a set of potential facility locations. If we choose to locate a facility at a site, we incur a known fixed location cost. Once a certain facility has been located, it can provide an unlimited amount of supply to the various customers. There is a known unit cost of shipping between each facility site and each customer location. A customer has a demand that must be shipped from one of the open facilities. The goal is to find the locations of the facilities, and the shipment pattern between the facilities and the customers, to minimise the sum of the facility location and shipment costs, subject to a requirement that all customer demands be satisfied.

The following notations are used in the mathematical model:

$i$ $i$th demand location, $i = 1, 2, \ldots, u$

$j$ $j$th potential facility location, $j = 1, 2, \ldots, n$

$h_i$ demand at customer location $i$

$f_j$ fixed cost of locating a facility at site $j$

$\rho_{ij}$ unit cost of shipping between facility site $j$ and customer location $i$

The decision variables are the binary variable $X_j$ , which is equal to 1 if a facility is to be located at site $j$ (and 0 otherwise), and $Y_{ij}$ representing the fraction of demand at customer location $i$ which is served by a facility at site $j$.

The mathematical formulation for the fixed-charge facility location model is given in Ref. [1]:

Minimise $$\sum_{j=1}^{n} f_j X_j + \sum_{j=1}^{n}\sum_{i=1}^{u} h_i \rho_{ij} Y_{ij}, \quad (2.1)$$

Subject to $$\sum_{j=1}^{n} Y_{ij} = 1 \quad i = 1,\ 2,\ ...,\ u, \quad (2.2)$$

$$Y_{ij} \le X_j \quad i = 1,\ 2,\ ...,\ u,\ \ j = 1,\ 2,\ ...,\ n, \quad (2.3)$$

$$X_j \in \{0,\ 1\} \quad j = 1,\ 2,\ ...,\ n, \quad (2.4)$$

$$Y_{ij} \ge 0 \quad i = 1,\ 2,\ ...,\ u,\ \ j = 1,\ 2,\ ...,\ n. \quad (2.5)$$

The objective function (2.1) minimises the sum of the fixed facility location costs and the shipments or transportation costs. Constraint (2.2) requires each customer to be assigned to a certain facility. Constraint (2.3) prohibits a customer from being assigned to a facility that has not been opened. Constraint (2.4) requires the location variables to be binary, and constraint (2.5) is a simple non-negativity constraint.

The decision variables $X_j$ and $Y_{ij}$ are related, respectively, to the locations of the facilities, and the shipment pattern between the facilities and the customers. While the demand $h_i$ (at customer location $i$) is determined according to the customer's need, the variables $X_j$ and $Y_{ij}$ are both decided by the defender. Note however that the decisions on $X_j$ and $Y_{ij}$ are not part of the game. In fact, we consider that the supply network has already been designed (by determining $X_j$ and $Y_{ij}$), then the defender protects the facilities using the theoretical game model presented in the next section.

The formulation given above assumes that facilities have unlimited capacity; the problem is sometimes referred to as the uncapacitated fixed charge location problem (UFLP). The UFLP is NP-hard [5], and a number of solution approaches have been proposed to solve it. For a comprehensive review of the UFLP, the reader is referred to Ref. [4]. In this paper, the UFLP will be solved using CPLEX optimisation software.

### 2.4 Problem formulation as a two-period game

Consider a system containing $n \ge 1$ facilities subjected to intentional attacks. Our model considers two players: the defender and the attacker. Between these two antagonist players,

there is a conflict over facilities' vulnerability. A set of critical threats is first identified. For each possible threat, our problem consists in optimally allocating the protective resources among the facilities, knowing that these facilities are exposed to external intentional attacks. In other words, given a set of investment alternatives for protecting the facilities against the identified threat, we want to determine how much to invest optimally in defending each facility, while taking into account that both the defender and the attacker are fully optimising agents. The attacker is considered as an intelligent and adaptable adversary player who chooses optimally how fiercely to attack facilities. The model developed in this section has to take into account such strategic behaviour of the attacker when making decisions about defensive investments on facilities.

More precisely, we consider a system containing $n$ facilities (targets) designed using the optimisation model (2.1)-(2.5). The defender minimises the expected damage of the system and the investment expenditure incurred to protect the system, which is formulated as a utility that can be maximised. The attacker maximises his utility also, measured as the expected damage minus the attacks expenditures. For each facility $j$, the defender chooses an investment effort $B_{jp} \in \left\{B_{j1},\ B_{j2},\ ...,\ B_{j\beta_j}\right\}$ and the attacker chooses an attack effort $Q_{jm} \in \left\{Q_{j0},\ Q_{j1},\ ...,\ Q_{j\alpha_j}\right\}$. Therefore, the defender has $n$ strategic choice variables and the attacker has $n$ strategic choice variables. $Q_{j0} = 0$ corresponds to the absence of an attack. We consider a two-period game where the defender determines its $n$ free choice variables simultaneously and independently in the first period, and the attacker thereafter determines its $n$ free choice variables simultaneously and independently in the second period. The game as well as the defence and attack choices are detailed in what follows.

### 2.4.1 The defender

For each facility $j$, we consider that there exists a set of $\beta_j$ available types of protections against the identified threat. Each protection type is indicated by index $p$ ($p$ = 1, 2, …, $\beta_j$). The defender incurs an investment effort $B_{jp}$ (investment, for short) at unit cost $b_{jp}$ ($b_{jp}$>0) to protect a facility located at site $j$ using protection type $p$. Lower $b_{jp}$ means greater

defence efficiency: $1/b_{jp}$ is the efficiency. We consider that the investment expenditure $\overline{B_{jp}}$, measured in dollar terms, is given by $\overline{B_{jp}} = b_{jp}B_{jp}$.

We represent a protection strategy of the $n$ facilities by a vector $\mathbf{P} = (\pi_j)$, $\pi_j$ takes values from $p = 0, 1, \ldots, \beta_j$. For example, $\mathbf{P} = (1 \quad 1 \quad 1)$ means that there are 3 facilities that are protected using type 1 protection.

To each protection strategy **P**, corresponds a vector of investments $\mathbf{B} = (B_{j\pi_j})$. For example, when $\mathbf{P} = (1 \quad 1 \quad 1)$, we have $\mathbf{B} = (B_{11} \quad B_{21} \quad B_{31})$.

Let us introduce a binary variable $\lambda_{jp}$ which is equal to 1 if a protection of type $p$ is used for facility $j$. Assuming that one type of protection is used, we have:

$$\sum_{p=1}^{\beta_j} \lambda_{jp} = 1, \ \forall j. \tag{2.6}$$

### 2.4.2 The attacker

Conversely, the attacker seeks to attack the system to ensure that it does not function reliably. He (she) has a set of $\alpha_j$ available attack actions against any facility $j$. Each attack type is indicated by index $m$ ($m = 0, 1, \ldots, \alpha_j$). $m = 0$ indicates the absence of an attack. Analogously, the attacker incurs an effort $Q_{jm}$ at unit cost $q_{jm}$ to attack facility located at site $j$ using attack action $m$. The inefficiency of investment is $q_{jm}$, and $1/q_{jm}$ is the efficiency. Its investment expenditure, in dollar terms, is $\overline{Q_{jm}} = q_{jm}Q_{jm}$, where $q_{jm} > 0$.

We represent an attack strategy against the $n$ facilities by a vector $\mathbf{M} = (\omega_j)$, $\omega_j$ takes values from $m = 0, 1, \ldots, \alpha_j$. For example, $\mathbf{M} = (2 \quad 2 \quad 2)$ means that there are 3 facilities that can be attacked using attacks of type 2.

We introduce a binary variable $\mu_{jm}$ which is equal to 1 if an attack of type $m$ is used for facility $j$. Assuming that one type of attack is used, we have:

$$\sum_{m=0}^{\alpha_j} \mu_{jm} = 1, \ \forall j. \tag{2.7}$$

### 2.4.3 Conflict over vulnerability of facilities

The vulnerability of a facility *j* is defined by its destruction probability $v_{pm}(j)$. There is a conflict over this vulnerability between the defender and the attacker. To model this conflict, we use the concept of *contest* commonly used in rent-seeking literature [19, 14, 11, 16, 8]. In rent seeking, there is a conflict over a rent between contending agents, just as there is a conflict over this vulnerability between the defender and the attacker. The most common functional form is the ratio form [19]. This is used in this paper to formulate the vulnerability of any facility *j* by a contest success function as follows:

$$v_{pm}(j) = \frac{(Q_{jm})^{c_j}}{(B_{jp})^{c_j} + (Q_{jm})^{c_j}}, \tag{2.8}$$

where $\partial v_{pm}(j)/\partial Q_{jm} > 0$, $\partial v_{pm}(j)/\partial B_{jp} < 0$, and $c_j \geq 0$ is a parameter that expresses the intensity of the contest. It is assumed that $c_j$ does not depend on *p* and *m*.

Figure 2.1 shows the successful attack probability $v_{pm}(j)$ as a function of $B_{jp}/Q_{jm}$ for various $c_j$. From Equation (8) and Figure 2.1, many remarks can be formulated as explained in [10]. We observe that with an infinite amount of defensive effort, and finite offensive effort, facility *j* is 0% vulnerable. The same result follows with finite defensive effort and zero offensive effort. On the other hand, with an infinite amount of offensive effort, and finite defensive effort, facility *j* is 100% vulnerable. The same result follows with finite offensive effort and zero defensive effort. We also observe that [10]:

- When $c_j$=0, the efforts $Q_{jm}$ and $B_{jp}$ have no impact on the vulnerability regardless of their size, which gives 50% vulnerability.
- When $c_j$=1, the efforts have proportional impact on the vulnerability.
- $c_j$=∞ gives a step function where "winner-takes-all".

- $0<c_j<1$ gives a disproportional advantage of exerting less effort than one's opponent.
- $c_j>1$ gives a disproportional advantage of exerting more effort than one's opponent.

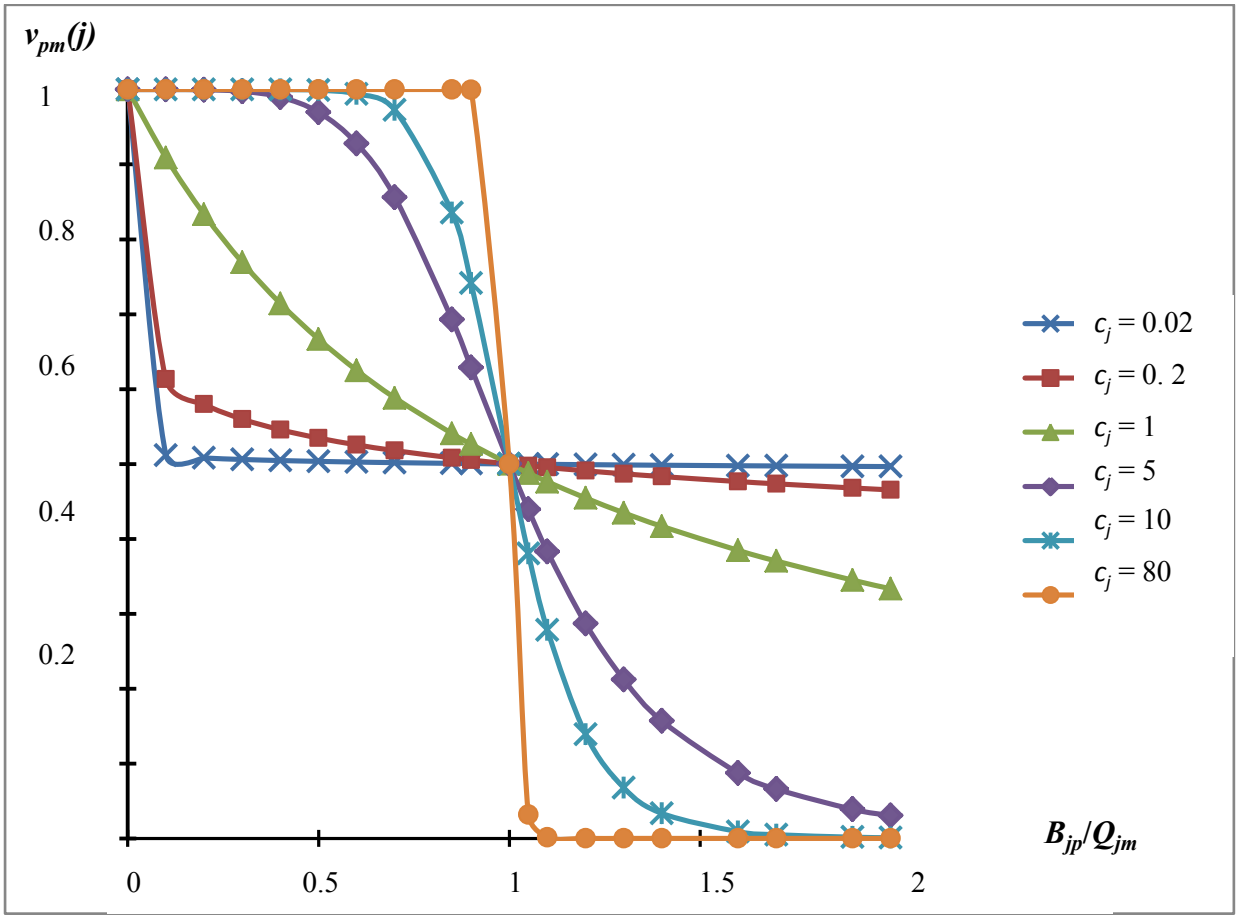


**Fig. 2.1-** Successful attack probability $v_{pm}(j)$ as a function of $\frac{B_{jp}}{Q_{jm}}$ for various $c_j$ (adapted from [10])

### 2.4.4 The game

Having the vulnerabilities of facilities as functions of the attacker's and the defender's efforts, both agents can estimate the expected damage caused by the attack for any possible distribution of these efforts. The defender's objective is to maximise his utility function by minimising the expected damage and weighing against protection expenditures. The attacker's objective is to maximise the expected damage while weighing against the attacks expenditures. Facilities are usually built over time by the defender. The attacker takes it as

given when he (she) chooses his (her) attack strategy. Therefore, as indicated before, we consider a two-period game where the defender invests in the first period, and the attacker moves in the second period. This means that the defender selects a strategy in the first period that maximizes his utility, considering that the attacker will maximize also his utility in the second period. After evaluating the utilities of each player in the next subsection, the game will be solved with backward induction, in which the second period is solved first.

### 2.5 Players utilities evaluation

We assume that attacks against different facilities succeed or fail independently. We also assume that the attacker can attack each facility $j$ only once, and that many facilities can be attacked at the same time. The damage caused by an attack is associated with two terms:

- The expected cost $C_R$ required for restoring the attacked facilities. If $R_j$ is the cost required to restore the attacked facility, this cost depends on the defence and attack strategies **P** and **M**, and it is given by:

$$C_R(\mathbf{P},\mathbf{M}) = \sum_{j=1}^{n} \sum_{m=0}^{\alpha_j} \sum_{p=1}^{\beta_j} \lambda_{jp} \mu_{jm} \nu_{pm}(j) R_j . \tag{2.9}$$

- The expected cost incurred because of the increase in transportation cost after attacks. When one or several facilities are unavailable, the transportation cost will increase since reassigned customers may receive shipments from facilities which are farther away. When the entire system is disabled, *i.e.* when *all* facilities are disabled, the demands cannot be satisfied (we have assumed that facilities have unlimited capacity).

  Each facility can be either Disabled or Functional. Let us define by S = $\{S_k\}$ the set of possible combinations when considering all facilities. For $n$ facilities, there are $2^n$ possible combinations. As an illustrative example, Table 2.1 presents all possible combinations for three facilities denoted by F1, F2 and F3. In this case, there are 8 possible combinations for the facilities ($k$ = 0, 1, …, 7).

Let us denote by $T_k$ the cost incurred because of the increase in transportation cost when the combination is $S_k$, *i.e.* the cost under combination $S_k$ minus the cost in a normal situation.

The evaluation of the costs $T_k$ for all combinations may require the solution of $\left(2^n - 2\right)$ UFLP; the other two combinations are combination 0 where all facilities are functional, and combination $\left(2^n - 1\right)$ where all facilities are disabled and a backorder cost $B$ is incurred ($T_7$ = B). Each UFLP corresponds to a combination $S_k$, and requires the solution of the optimisation model (2.1)-(2.5) under this combination. In the example above (with three facilities), if we consider attack combination 1, the model (2.1)-(2.5) is solved considering that only facilities 2 and 3 are operational, to determine the cost $T_1$.

**Table 2.1-** Possible combinations: case of three facilities

| Combination $S_k$ | Index $k$ |
|---|---|
| All facilities are functional | 0 |
| F1 is disabled and the others facilities are functional | 1 |
| F2 is disabled and the others facilities are functional | 2 |
| F3 is disabled and the others facilities are functional | 3 |
| F1 and F2 are disabled, and F3 is functional | 4 |
| F1 and F3 are disabled, and F2 is functional | 5 |
| F2 and F3 are disabled, and F1 is functional | 6 |
| F1, F2 and F3 are disabled | 7 |

The increase of the transportation cost is related to all the possible outcomes. Attack outcomes are denoted by $\Delta C_{pm}(k)$, with $p$ and $m$ given and $k$ varying from 0 to $2^n - 1$. Considering that each facility can be either attacked or not, there are also $2^n$ possibilities of attacks for $n$ facilities, for given strategies **P** and **M**. Table 2.2 illustrates, for an example of 3 facilities, the calculation of the expected cost incurred because of the increase in transportation cost after attacks.

**Table 2.2-** Combination of attacked facilities and outcomes

| Combination | Attack outcome $\Delta C_{pm}(k)$ |
|---|---|
| No facility is attacked | $\Delta C_{pm}(0) = 0$ |

| | |
|---|---|
| Only F1 is attacked | $\Delta C_{pm}(1) = T_1 \nu_{pm}(1)$ |
| Only F2 is attacked | $\Delta C_{pm}(2) = T_2 \nu_{pm}(2)$ |
| Only F3 is attacked | $\Delta C_{pm}(3) = T_3 \nu_{pm}(3)$ |
| F1 and F2 are attacked, F3 not attacked | $\Delta C_{pm}(4) = T_1 \nu_{pm}(1)(1-\nu_{pm}(2)) + T_2 \nu_{pm}(2)(1-\nu_{pm}(1)) + T_4 \nu_{pm}(1)\nu_{pm}(2)$ |
| F1 and F3 are attacked, F2 not attacked | $\Delta C_{pm}(5) = T_1 \nu_{pm}(1)(1-\nu_{pm}(3)) + T_3 \nu_{pm}(3)(1-\nu_{pm}(1)) + T_5 \nu_{pm}(1)\nu_{pm}(3)$ |
| F2 and F3 are attacked, F1 not attacked | $\Delta C_{pm}(6) = T_2 \nu_{pm}(2)(1-\nu_{pm}(3)) + T_3 \nu_{pm}(3)(1-\nu_{pm}(2)) + T_6 \nu_{pm}(2)\nu_{pm}(3)$ |
| All facilities are attacked | $\Delta C_{pm}(7) = T_1 \nu_{pm}(1)(1-\nu_{pm}(2))(1-\nu_{pm}(3)) + T_2 \nu_{pm}(2)(1-\nu_{pm}(1))(1-\nu_{pm}(3)) + T_3 \nu_{pm}(3)(1-\nu_{pm}(1))(1-\nu_{pm}(2)) + T_4 \nu_{pm}(1)\nu_{pm}(2)(1-\nu_{pm}(3)) + T_5 \nu_{pm}(1)\nu_{pm}(3)(1-\nu_{pm}(2)) + T_6 \nu_{pm}(2)\nu_{pm}(3)(1-\nu_{pm}(1)) + B\,\nu_{pm}(1)\nu_{pm}(2)\nu_{pm}(3)$ |

The expected value of the transportation cost increase is given by:

$$TCI(\mathbf{P},\mathbf{M}) = \sum_{k=1}^{2^n-1} \Delta C_{pm}(k). \tag{2.10}$$

The expected damage is then:

$$D(\mathbf{P},\mathbf{M}) = \sum_{j=1}^{n}\sum_{m=0}^{\alpha_j}\sum_{p=1}^{\beta_j}\lambda_{jp}\mu_{jm}\nu_{pm}(j)R_j + \sum_{k=1}^{2^n-1}\Delta C_{pm}(k) \tag{2.11}$$

The defender expected utility is:

$$\begin{aligned} U_d(\mathbf{P},\mathbf{M}) &= -D(\mathbf{P},\mathbf{M}) - \sum_{j=1}^{n}\sum_{p=1}^{\beta_j}\lambda_{jp}\overline{B_{jp}} \\ &= -\left(\sum_{j=1}^{n}\sum_{m=0}^{\alpha_j}\sum_{p=1}^{\beta_j}\lambda_{jp}\mu_{jm}\nu_{pm}(j)R_j + \sum_{k=1}^{2^n-1}\Delta C_{pm}(k)\right) - \sum_{j=1}^{n}\sum_{p=1}^{\beta_j}\lambda_{jp}\overline{B_{jp}} \end{aligned} \tag{2.12}$$

The attacker expected utility is:

$$\begin{aligned} U_a(\mathbf{P},\mathbf{M}) &= D(\mathbf{P},\mathbf{M}) - \sum_{j=1}^{n}\sum_{m=0}^{\alpha_j}\mu_{jm}\overline{Q_{jm}} \\ &= \sum_{j=1}^{n}\sum_{m=0}^{\alpha_j}\sum_{p=1}^{\beta_j}\lambda_{jp}\mu_{jm}\nu_{pm}(j)R_j + \sum_{k=1}^{2^n-1}\Delta C_{pm}(k) - \sum_{j=1}^{n}\sum_{m=0}^{\alpha_j}\mu_{jm}\overline{Q_{jm}} \end{aligned} \tag{2.13}$$

## 2.6 Solving the game

This is a two-period game where the defender invests in the first period, and the attacker moves in the second period [10, 13]. This means that the defender selects a strategy in the first period that maximizes his utility, considering that the attacker will maximize his utility in the second period. The following algorithm is used for finding the equilibrium solution, by solving the game with backward induction in which the second period is solved first:

**1) Inputs:**

- A system of $n$ facilities ($j$ = 1, 2, …, $n$) located by solving the optimisation model (1)-(5).

• A set of $\beta_j$ protection types for each facility $j$ ($p = 1, 2, \ldots, \beta_j$).

• A set of $\alpha_j$ attack types per facility $j$ ($m = 0, 1, \ldots, \alpha_j$).

• *Parameters*:

- Protection investment efforts $B_{jp}$;
- Unit costs of protection efforts $b_{jp}$;
- Attack investment efforts $Q_{jp}$;
- Unit costs of attack efforts $q_{jp}$;
- Contest intensities $c_j$;
- Restoration costs $R_j$; and
- Backorder cost $B$.

**2) Evaluation of the costs $T_k$ for all combinations**

For each combination $k = 1, 2, \ldots, 2^n - 2$

**3.1.** Solve the model (2.1)-(2.5) to determine the cost $T_k$;

**3) Initialization**

Assign $U_{\min} = \infty$ ($U_{\min}$ is the defender minimal utility);

Assign $U_{\max} = 0$ ($U_{\max}$ is the attacker maximal utility).

**4) Determination of the optimal attack strategy** (*i.e.*, the strategy that maximises the attacker utility)

For each protection strategy $\mathbf{P} = \left(\pi_j\right)$

**4.1.** For each attack strategy $\mathbf{M} = \left(\omega_j\right)$

**4.1.1.** Construct a matrix $\boldsymbol{\lambda} = \left(\lambda_{jp}\right)$ such as

$$\lambda_{jp} = \begin{cases} 1 & if \ \ \pi_j = p \\ 0 & otherwise \end{cases}, \text{ and } \sum_{p=1}^{\beta_j} \lambda_{jp} = 1, \ \ \forall j ;$$

**4.1.2.** Construct a matrix $\boldsymbol{\mu} = \left(\mu_{jm}\right)$ such as

$$\mu_{jm} = \begin{cases} 1 & if \ \ \omega_j = m \\ 0 & otherwise \end{cases}, \text{ and } \sum_{m=0}^{\alpha_j} \mu_{jm} = 1, \ \ \forall j \, ;$$

**4.1.3.** Determine the matrix $\boldsymbol{\nu}(\mathbf{P},\mathbf{M}) = \left(\nu_{pm}(j)\right)$ such as each element $\nu_{pm}(j)$ is evaluated by using equation (2.8);

**4.1.4.** Calculate the costs $C_R(\mathbf{P},\mathbf{M})$ by using equations (2.9);

**4.1.5.** Calculate the expected value of the transportation cost increase $TCI(\mathbf{P},\mathbf{M})$ by using equation (2.10);

**4.1.6.** Calculate the attacker utility $U_a(\mathbf{P},\mathbf{M})$ by using equation (2.13);

**4.1.6.1.** If $U_a(\mathbf{P},\mathbf{M}) > U_{max}$ assign $U_{max} = U_a(\mathbf{P},\mathbf{M})$, $\mathbf{M}_{\text{opt}} = \mathbf{M} = \left(\omega_j^{opt}\right)$, $\mathbf{Q}_{\text{opt}} = \left(Q_{j\omega_j^{opt}}\right)$;

**5) Determination of the optimal defence strategy** (*i.e.*, maximising the defender utility)

For each protection strategy $\mathbf{P} = \left(\pi_j\right)$

**5.1.** Assign $\boldsymbol{\mu}_{\text{opt}} = \left(\mu_{jm}\right)$ such as

$$\mu_{jm} = \begin{cases} 1 & if \ \ \omega_j^{opt} = m \\ 0 & otherwise \end{cases};$$

**5.2.** Determine the matrix $\boldsymbol{\nu}(\mathbf{P},\mathbf{M}_{\text{opt}}) = \left(\nu_{p\omega_j^{opt}}(j)\right)$ such as each element $\nu_{pm}(j)$ is evaluated by using equation (2.8) with $\boldsymbol{\lambda}=\left(\lambda_{jp}\right)$ and under attack strategy $\mathbf{M}_{\text{opt}}$, *i.e.*, $\nu_{p\omega_j^{opt}}(j) = \dfrac{\left(Q_{j\omega_j^{opt}}\right)^{c_j}}{\left(B_{jp}\right)^{c_j} + \left(Q_{j\omega_j^{opt}}\right)^{c_j}}$;

**5.3.** Calculate the costs $C_R(\mathbf{P},\mathbf{M}_{\text{opt}})$ by using equations (2.9) (under attack strategy $\mathbf{M}_{\text{opt}}$);

**5.4.** Calculate the expected cost $TCI(\mathbf{P},\mathbf{M}_{\text{opt}})$ by using equation (2.10);

**5.5.** Calculate the defender utility $U_d(\mathbf{P}, \mathbf{M}_{\text{opt}})$ by using equation (2.12);

**5.5.1.** If $-U_d(\mathbf{P}, \mathbf{M}_{\text{opt}}) < U_{min}$ assign $U_{min} = -U_d(\mathbf{P}, \mathbf{M}_{\text{opt}})$,

$$\mathbf{P}_{\text{opt}} = \mathbf{P} = \left(\pi_j^{opt}\right), \mathbf{B}_{\text{opt}} = \left(B_{j\pi_j^{opt}}\right).$$

## 2.7 Illustrative example

In this section, we consider a simple example for a step-by-step illustration of the algorithm above. Then, the protection strategy obtained is compared to other defence strategies. The issues of limited budgets and the influence of contest intensities are also discussed.

### 2.7.1 Input data

Let us consider 5 facilities and 10 demand nodes. Table 2.3 provides the fixed costs of location facilities. Table 2.4 gives the yearly demand, and Table 2.5 presents the unit costs of shipping between facility sites and customer locations.

**Table 2.3-** Fixed cost of locating a facility at site

| Site *j* | Fixed cost (in $ million) |
|---|---|
| 1 | 42 |
| 2 | 48 |
| 3 | 24 |
| 4 | 32 |
| 5 | 17 |

**Table 2.4-** Demand per year at customer location

| Customer location *i* | Demand |
|---|---|
| 1 | 750 |
| 2 | 50 |
| 3 | 40 |
| 4 | 900 |
| 5 | 35 |
| 6 | 100 |
| 7 | 600 |
| 8 | 45 |
| 9 | 1,400 |
| 10 | 650 |

**Table 2.5-** Unit cost (in $) of shipping between facility site *j* and customer location *i*

| | Site *j* | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| Customer location *i* | 1 | 1,600 | 6,100 | 6,300 | 7,800 | 7,400 |
| | 2 | 1,000 | 5,600 | 6,000 | 7,200 | 7,000 |
| | 3 | 4,200 | 1,900 | 4,200 | 7,500 | 5,600 |
| | 4 | 5,000 | 1,700 | 4,400 | 6,100 | 4,900 |
| | 5 | 6,600 | 4,900 | 3,100 | 7,600 | 2,800 |
| | 6 | 5,800 | 4,800 | 1,300 | 6,600 | 2,900 |
| | 7 | 6,000 | 5,100 | 900 | 4,800 | 2,700 |
| | 8 | 7,000 | 7,900 | 3,800 | 600 | 3,100 |
| | 9 | 7,600 | 8,200 | 5,100 | 700 | 4,100 |
| | 10 | 7,500 | 7,100 | 4,600 | 6,900 | 800 |

In a normal situation (*i.e.*, when there is no attack), the optimal solution for the UFLP is shown in Figure 2.2. This entails a fixed cost of $163 million, and a transportation cost of $103.02 million over 20 years.

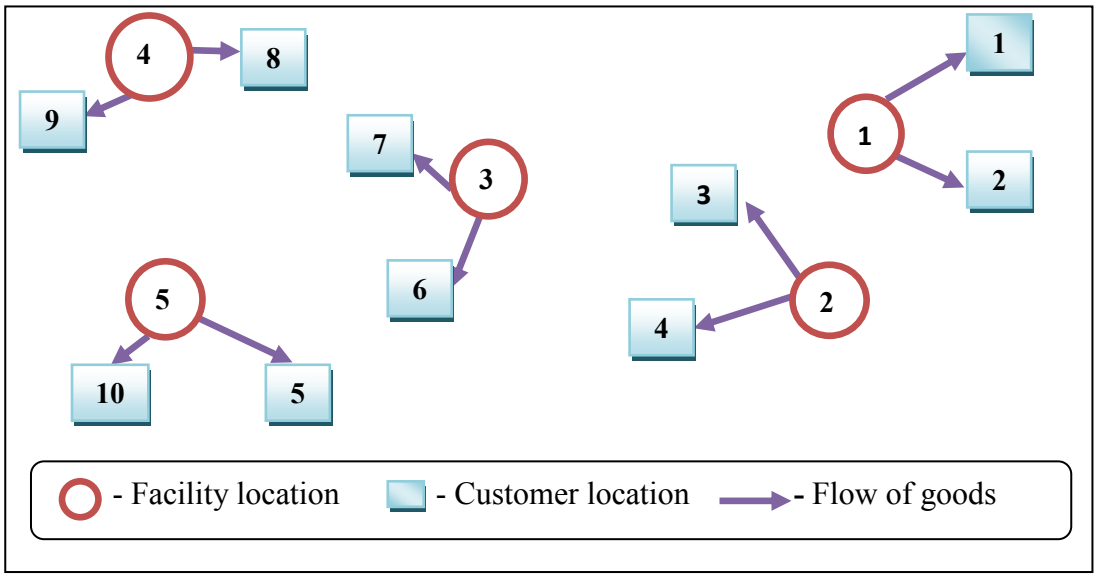


**Fig. 2.2-** The optimal UFLP solution

Table 2.6 gives the protection investment efforts $B_{jp}$, and the unit costs of protection efforts $b_{jp}$ (to protect a facility located at site $j$ using protection type $p$). The corresponding

investment expenditures $\overline{B_{jp}}$ are also shown. Analogously, Table 2.7 presents the attack investment efforts $Q_{jm}$, the unit costs of attack efforts $q_{jp}$ (to attack facility located at site $j$ using attack action $m$), and the corresponding investment expenditures $\overline{Q_{jm}}$. The restoration costs $R_j$ are given in Table 2.8, while the time required to restore each disabled facility, at the given cost, is one week. We consider that the backorder cost is \$1.6 million. Since such a backorder situation happens only when the entire system is disabled, the indicated cost corresponds to the incurred loss when all facilities are disabled during one week. We consider that all contest intensities are equal to 1, which means that the efforts have proportional impact on the vulnerability.

**Table 2.6-** Defense parameters

| Protection types $p$ | Unit costs $b_{jp}$ | Protection efforts $B_{jp}$ | Investment expenditures (in \$) $\overline{B_{jp}}$ |
|---|---|---|---|
| 1 | 100 | 70 | 7,000 |
| 2 | 130 | 200 | 26,000 |
| 3 | 135 | 250 | 33,750 |
| 4 | 280 | 555 | 155,400 |

**Table 2.7-** Attacker parameters

| Attack types $m$ | Unit costs $q_{jm}$ | Attack efforts $Q_{jm}$ | Investment expenditures $\overline{Q_{jm}}$ (in \$) |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 30 | 220 | 6,600 |
| 2 | 25 | 150 | 3,750 |
| 3 | 35 | 270 | 9,450 |
| 4 | 54 | 350 | 18,900 |

**Table 2.8-** Restoration costs of disabled facilities (in \$)

| Disabled facility $j$ | Restoration costs $R_j$ |
|---|---|
| 1 | 180,000 |
| 2 | 175,000 |
| 3 | 165,000 |
| 4 | 166,000 |
| 5 | 190,000 |

### 2.7.2 Evaluation of the costs $T_k$ for all combinations

If, for example, facility 1 is disabled by an attack, the transportation cost over 20 years becomes $175.12 million, which corresponds to an increase of 70%. Figure 2.3 shows the new optimal UFLP solution when facility 1 is attacked.

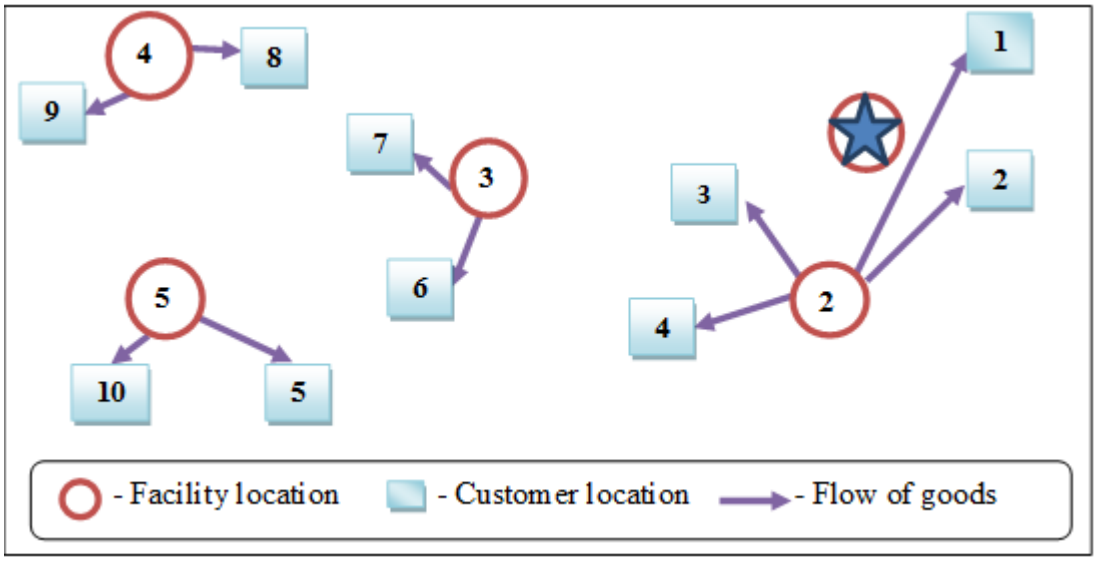


**Fig. 2.3-** The optimal UFLP solution if facility 1 is disabled

Table 2.9 presents the costs Tk for all possible combinations. Recall that Tk is the cost incurred because of the increase in transportation cost when the combination is Sk, i.e. the cost under combination Sk minus the cost in a normal situation. Since the restoration time is one week, each cost Tk is evaluated as the excess in transportation cost during this week. For example, when facility 1 is disabled, the cost T1 is given by the cost under combination $S_1$ minus the cost in a normal situation during one week. That is, $T_1$ (in $ million) is equal to (175.12 - 103.02)/1024. Here, 1024 is the number of weeks during 20 years.

**Table 2.9-** The costs $T_k$ for all possible combinations $S_k$

| $k$ | Disabled facilities | $T_k$ (in $) |
|---|---|---|
| 1 | 1 | 69,330 |
| 2 | 2 | 48,500 |
| 3 | 3 | 23,850 |
| 4 | 4 | 93,700 |
| 5 | 5 | 47,700 |

| | | |
|---|---|---|
| 6 | 1, 2 | 121,100 |
| 7 | 1, 3 | 93,170 |
| 8 | 1, 4 | 163,030 |
| 9 | 1, 5 | 117,030 |
| 10 | 2, 3 | 81,000 |
| 11 | 2, 4 | 142,200 |
| 12 | 2, 5 | 96,130 |
| 13 | 3, 4 | 117,550 |
| 14 | 3, 5 | 129,390 |
| 15 | 4, 5 | 168,930 |
| 16 | 1, 2, 3 | 171,500 |
| 17 | 1, 2, 4 | 214,800 |
| 18 | 1, 2, 5 | 168,800 |
| 19 | 1, 3, 4 | 186,870 |
| 20 | 1, 3, 5 | 198,720 |
| 21 | 1, 4, 5 | 238,260 |
| 22 | 2, 3, 4 | 174,700 |
| 23 | 2, 3, 5 | 191,350 |
| 24 | 2, 4, 5 | 217,430 |
| 25 | 3, 4, 5 | 412,190 |
| 26 | 1, 2, 3, 4 | 265,200 |
| 27 | 1, 2, 3, 5 | 310,520 |
| 28 | 1, 2, 4, 5 | 290,030 |
| 29 | 1, 3, 4, 5 | 412,920 |
| 30 | 2, 3, 4, 5 | 404,000 |

### 2.7.3 Determination of the optimal attack strategy (i.e., the strategy that maximises the attacker utility)

By applying step 4 of the algorithm, the most harmful attack corresponds to the following strategy: $\mathbf{M}_{opt} = (4 \quad 4 \quad 3 \quad 3 \quad 4)$. This means that facilities 1, 2 and 5 are disabled using type 4 attacks; and facility 3 and 4 are disabled using type 3 attacks. The maximum loss is \$1,547,342 and the corresponding attacker utility is $U_{max}$ = \$1,452,842.

### 2.7.4 Determination of the optimal defence strategy (i.e., maximising the defender utility)

The last step of the algorithm allows us to allocate optimally the protective resources among the facilities, without missing the strategic behaviour of the attacker. This attacker is

in fact considered as an intelligent and adaptable adversary player who chooses optimally how fiercely to attack facilities. To make decisions about defensive investments on facilities, the defence strategy suggested by our method is the strategy that maximises the defender utility considering that the attacker will maximize his utility also. The obtained solution corresponds to the following strategy: $\mathbf{P}_{opt}$ = (3 3 2 2 3). This means that facilities 1, 2 and 5 are protected using type 3 protections; and facility 3 and 4 are protected using type 2 protections. The loss is \$689,081 and the corresponding defender utility is $U_{min}$ = \$857,831.

### 2.7.5 Comparison

The protection strategy obtained by the proposed game-theoretical model is compared to some defence strategies that could be used in practice. This comparison allows us to measure, for the example above, how much our method is better than others, when the attacker tries to maximize his utility (calculated as the expected damage of an attack minus the attack expenditure). The strategies considered in this comparison are as follows:

- *Strategy 1: Facilities with higher fixed costs are protected by more expensive protection types*

In our example, the facilities that have higher fixed costs are ranked as follows (see Table 2.4): F2, F1, F4, F3, F5. On the other hand, the protection types ($p$) are ranked according to their investment expenditures as follows (see Table 2.7): 4, 3, 2, 1. In this strategy, we consider that facilities 2 and 1 are protected using type 4 protection; facilities 4, 3 and 5 are protected using, respectively, protections of types 3, 2 and 1. That is, this protection strategy corresponds to $\mathbf{P}_1$ = (4 4 2 3 1).

- *Strategy 2: We use a more expensive protection type for a facility that, when disabled, yields more increase in transportation costs*

In our example, ranking the facilities that, when disabled, yield more increase in transportation costs can be based on the first five lines of Table 2.9. In fact, a facility with higher $T_k$ is more critical according to this strategy. As a result, the ranking of facilities is as follows: F4, F1, F2, F5, F3. On the other hand, the protection types ($p$) are ranked according to their investment expenditures as follows (see Table 2.6): 4, 3, 2, 1. Therefore,

we consider that facilities 4 and 1 are protected using type 4 protection; facilities 2, 5 and 3 are protected using, respectively, protections of types 3, 2 and 1. That is, this protection strategy corresponds to $\mathbf{P}_2 = (4 \quad 3 \quad 1 \quad 4 \quad 2)$.

Considering that the attacker seeks to maximize his utilities, the defender utilities corresponding to strategies 1 and 2 are \$1,065,294 and \$1,033,170, respectively. We remark that the protection strategy obtained by our model is 24.18% better than strategy 1 and 20.44 % better than strategy 2.

### 2.7.6 Limited defence budget

The defence strategy optimisation problem has been solved for a limited defender's budget. The obtained solutions for different budgets are presented in Table 2.10. We remark from this table that the expected damage is indeed higher for a lower defence budget. The relationship between the investment sizes and the effect on facilities protection provides important managerial information for decision makers. In fact, for each increase in the defence budget, it is important to quantify the resulting reduction in the expected damage, in order to decide if it is worth investing more in protecting facilities.

**Table 2.10-** Obtained defense strategies for different budgets ($c_j = 1$)

| Defense budget (in \$) | Defense cost (in \$) | Expected damage (in \$) | Defense strategy $\mathbf{P}_{opt}$ |
|---|---|---|---|
| 35,000 | 35,000 | 1,392,044 | ( 1 1 1 1 1 ) |
| 60,000 | 54,000 | 1,209,085 | ( 1 1 1 1 2 ) |
| 80,000 | 73,000 | 1,070,835 | ( 1 1 2 1 2 ) |
| 100,000 | 99,750 | 931,820 | ( 1 1 2 2 3 ) |
| 120,000 | 118,750 | 842,051 | ( 2 1 2 2 3 ) |
| 130,000 | 130,000 | 792,571 | ( 2 2 2 2 2 ) |
| 140,000 | 137,750 | 767,004 | ( 2 2 2 2 3 ) |
| 150,000 | 145,500 | 745,249 | ( 2 2 2 3 3 ) |
| 160,000 | 153,250 | 725,359 | ( 2 2 3 3 3 ) |
| 170,000 | 168,750 | 689,081 | ( 3 3 3 3 3 ) |
| 180,000 | 168,750 | 689,081 | ( 3 3 3 3 3 ) |

The expected damage cost as a function of the defence budget is presented in Figure 2.4. This curve is drawn by evaluating the optimal defence strategy for each budget, considering that the attacker chooses the harmful strategy. This curve shows graphically the relationship

between the investment sizes and the effect on facilities protection. From this curve, one can also see that the budget greater than $168,750 makes no sense for the given set of available protections, since additional investment cannot reduce the expected damage.

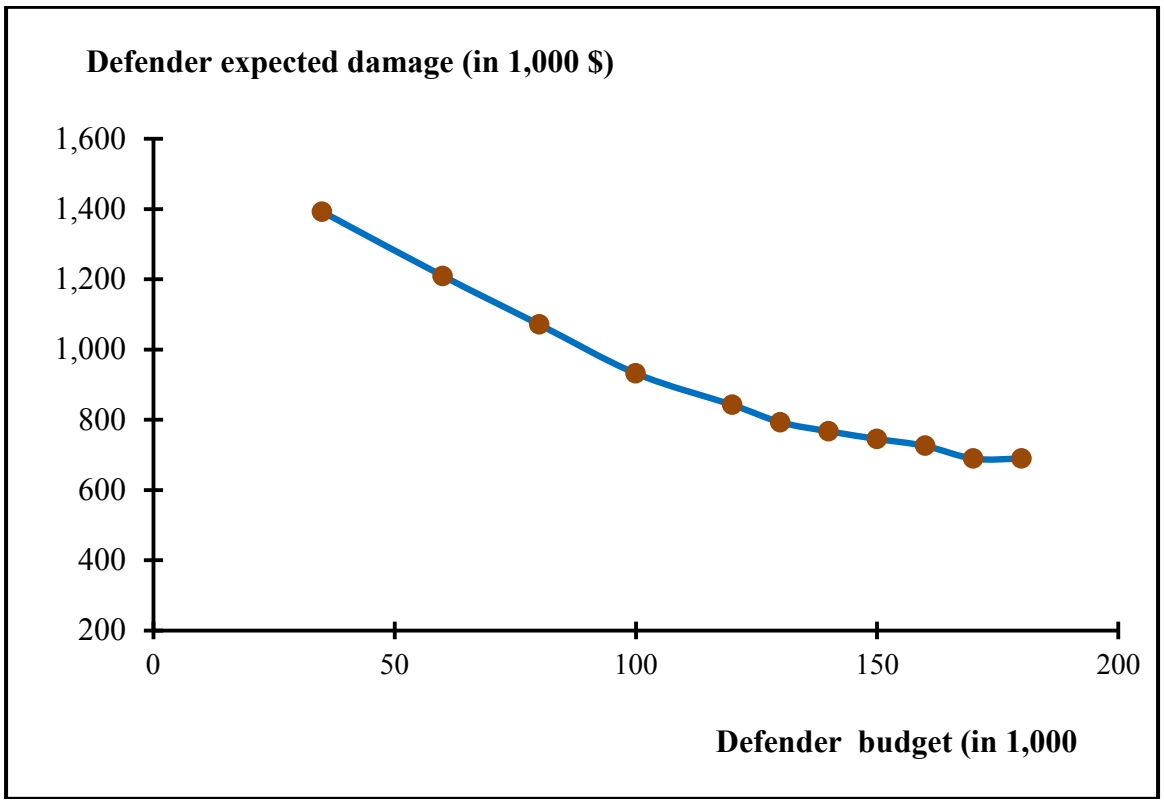


**Fig. 2.4**- Expected damage costs as function of defense budget ($c_j = 1$)

### 2.7.7 Limited defence and attack budgets

Figs. 2.5-2.8 present the optimal strategies of the defender and the attacker as functions of the contest intensity, when the defence and the attacks are both limited. Four pairs of defence and attack budgets are considered. We remark that when the attacker's budget is relatively low (cases of Figures 2.5 and 2.6), the defender benefits from the greatest contest intensity. But, when the attacker's budget is high (cases of Figures 2.7 and 2.8) the defender benefits instead from the lowest contest intensity.

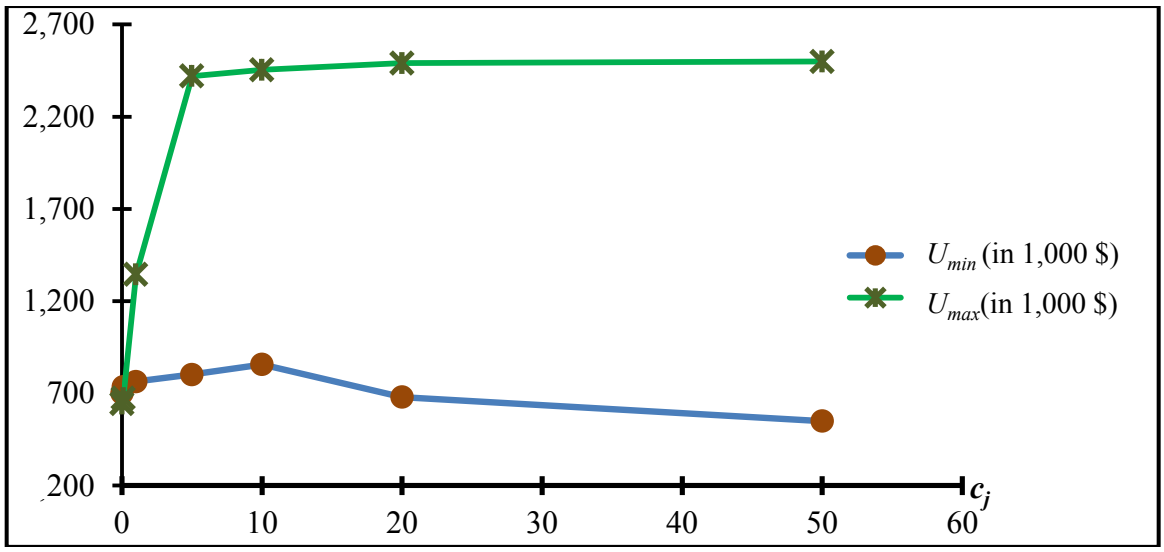


**Fig. 2.5-** Defender utility as a function of the contest intensity, when the defense budget is $100,000 and the attack budget is $50,000

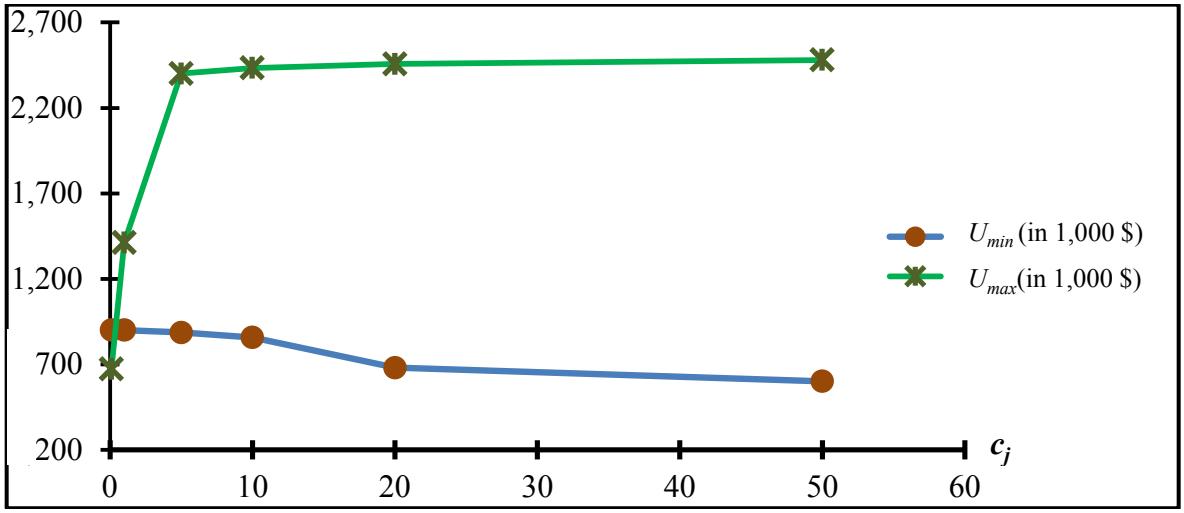


**Fig. 2.6-** Defender utility as a function of the contest intensity, when the defense budget is $100,000 and the attack budget is $80,000

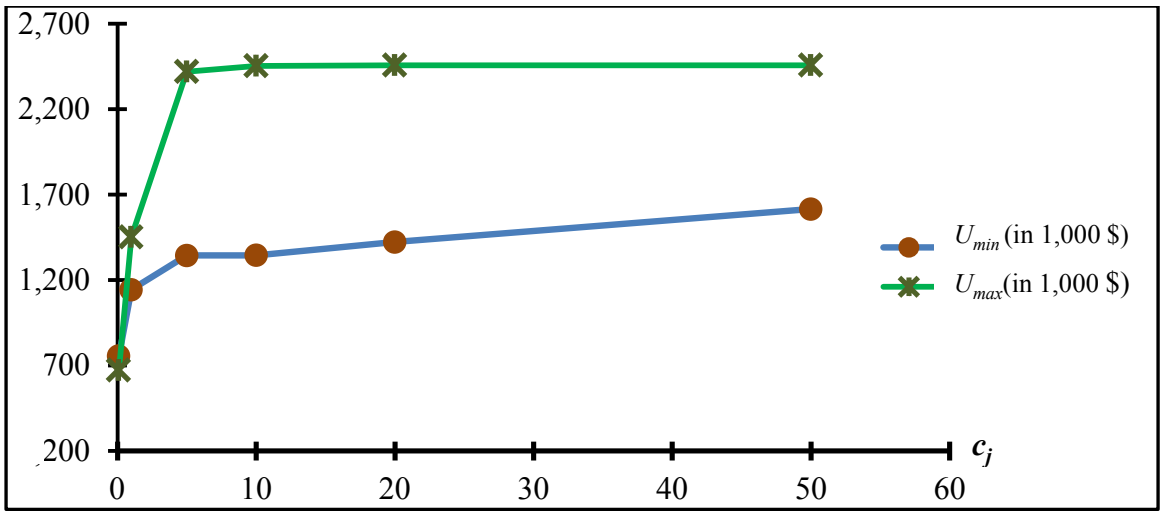


**Fig. 2.7-** Defender utility as a function of the contest intensity, when the defense budget is $80,000 and the attack budget is $140,000

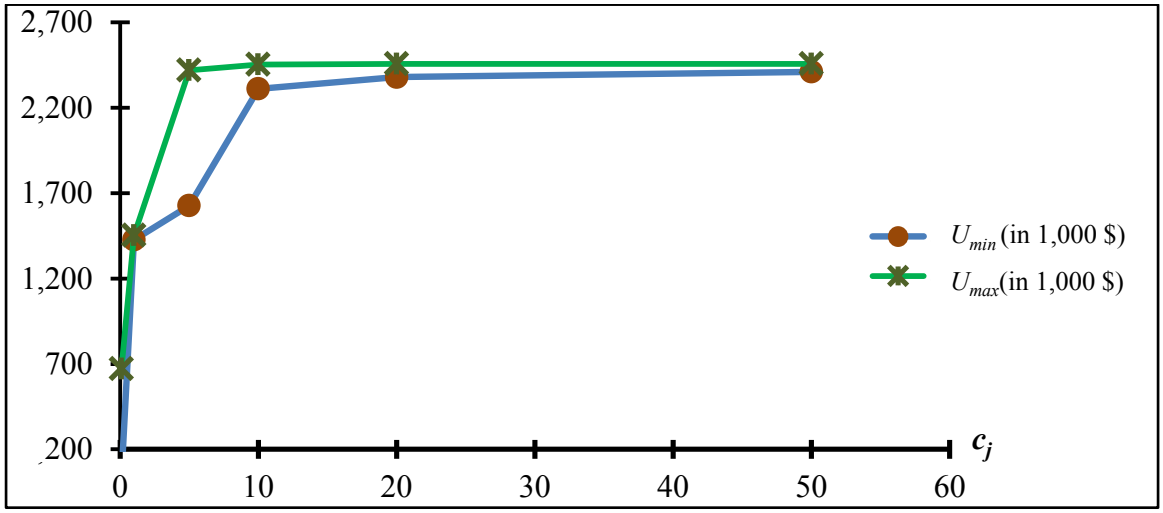


**Fig. 2.8-** Defender utility as a function of the contest intensity, when the defense budget is $50,000 and the attack budget is $140,000

## 2.8 Conclusion

Facility location literature has failed to take into account the attacker as a fully strategic optimising agent. The use of game theory for the optimal defence of infrastructures has

become more prominent in recent research in the domain of reliability theory, e.g. [2, 9, 10, 13]. This article accounts for these developments in reliability design and introduces a way of thinking which can be considered as new in the context of facility location and supply chain design. The conflict on facilities vulnerability is modelled using the concept of contest [19, 8]. In the uncapacitated fixed charge location context, when one or several facilities are unavailable, the transportation cost will increase since reassigned customers may receive shipments from facilities which are farther away. A method is developed to evaluate the utilities of the players. The expected costs evaluated by our method include the cost incurred because of the increase in transportation costs after attacks, the backorder cost, and the cost necessary to restore disabled facilities. The model considers a non-cooperative two-period game between the players, and an algorithm is presented for determining the equilibrium solution and the optimal defence strategy. The approach gives important managerial insights for the protection of located facilities. Future work is required to deal with many problems related for example to:

- The incomplete information on facilities and on attacker strategies; it was assumed in this paper that the players have full knowledge about the parameters of the game. As in practice this information can be uncertain, it is necessary to characterise the probability distribution of each parameter. When this is impossible or difficult, using subjective probabilities is an interesting alternative [29].
- The possibility of multiple attacks by several attackers against the facilities; this will consist in extending our supply networks protection model to the case when several attackers perform many consecutive attacks on different facilities. In this case, the attackers, and the defender may adapt their strategies based on the results of previous attacks. The issue will then be to find the optimal dynamic strategy for the facilities defence.

Solving these problems should help bridge the gap between our game-theoretical model analysis, and the application in real-life supply chains.

On the other hand, even if the computation time required to solve the game for the example problem did not exceed 15 minutes, it remains that the proposed method will be time-consuming if larger problems are considered. It is necessary to solve exponentially large numbers of NP-hard problems; and all of them for every instance of the problem. One way

to reduce the computation time to solve larger problems is to solve transportation problems instead of more complicated UFLP models. In fact, as the facilities are not capacitated, we only need to assign each demand point to the functioning facilities and that can easily be done by assigning the demand to the closest open facility. This means that we only need to solve a simple greedy assignment problem given the facilities that are functioning. Another way to reduce the computation time is to use meta-heuristics to reduce the number of NP-hard problems that need to be run to solve the game.

Finally, our future research will address the capacitated fixed charge location problem (CFLP), *i.e.*, with limited capacity. When the capacity is limited, planned losses should be included with decisions on backorder acceptance. Planned losses have been introduced in Ref. [28] where the authors state that this may occur when the backorder cost is acceptable, or the production costs to meet the demand are high. A common practice in supply chain management consists in using extra-capacity options as a recourse. In this case, it is important to find the best trade-off between extra-capacity options and defence strategies.

**Acknowledgements**

The authors would like to thank the editor, and the anonymous referees for their constructive comments and recommendations which have improved the presentation of this paper. They would also like to thank the *Natural Sciences and Engineering Research Council of Canada* (NSERC) for their financial support of the project, and the *Fonds québécois de la recherche sur la nature et les technologies* (FQRNT) for their assistance in providing a doctoral research scholarship for the Ph.D. thesis of the first author.

**References**

[1] Balinski, M., 1965. Integer programming: methods, uses, computation. Management Science 12 (3), 254–313.

[2] Bier, V., Azaiez, N., 2009. Game theoretic risk analysis of security threats. Springer, New York.

[3] Colbourn, C. J., 1987. The Combinatorics of Network Reliability. New York: Oxford University Press.

[4] Cornuéjols, G., Nemhauser, G.L., Wolsey, L.A., 1990. The uncapacitated facility location problem. In: Mirchandani, P.B., Francis, R.L. (Eds.), Discrete Location Theory, 119–171.

[5] Garey, M., Johnson, D., 1979. Computers and Intractability. A Guide to the Theory of NP-Completeness. Freemann, San Francisco.

[6] Ghare, P.M., Montgomery, D.C., Turner, W.C., 1971. Optimal Interdiction Policy for a Flow Network. Naval Research Logistics Quarterly 18 (1), 37–45.

[7] Golden, B., 1978. A Problem of Network Interdiction. Naval Research Logistics Quarterly 25 (4), 711–713.

[8] Hausken, K., 2005. Production and Conflict Models versus Rent-Seeking Models, Public Choice, Springer 123 (1), 59–93.

[9] Hausken, K., Levitin, G., 2009. Protection vs. False Targets in Series Systems. Reliability Engineering and System Safety 94 (5), 973–981.

[10] Hausken, K., Levitin, G., 2009. Minmax defense strategy for complex multi-state systems. Reliability Engineering and System Safety 94 (2), 577–587.

[11] Hirshleifer, J., 1995. Theorizing about conflict. In: K. Hartley and T. Sandler, Editors, Handbook of Defense Economics. Elsevier Science, Amsterdam, Netherlands.

[12] Klibi, W., Martel, A., Guitouni, A., 2010. The design of robust value-creating supply chain networks: A critical review. European Journal of Operational Research 203 (2), 283–293.

[13] Levitin, G., Hausken, K., 2009. Redundancy vs. Protection vs. False Targets for Systems under Attack. IEEE Transactions on Reliability 58 (1), 58–68.

[14] Nitzan, S., 1994. Modelling rent-seeking contests. European Journal of Political Economy 10 (1), 41–60.

[15] Scaparra, M., Church, R., 2008. A bilevel mixed-integer program for critical infrastructure protection planning. Computers and Operations Research 35 (6), 1905–1923.

[16] Skaperdas S., 1996. Contest success functions. Econ Theory 7 (2), 283–290.

[17] Snyder, L.V., Daskin, M., 2005. Reliability Models for Facility Location: The Expected Failure Case. Transportation Science 39 (3), 400–416.

[18] Snyder, L.V., 2006. Facility location under uncertainty: a review. IIE Transactions 38 (7), 547–564.

[19] Tullock, G., 1980. Efficient rent seeking. In: Buchanan, M., Robert, D., Tullock, G. (Eds.), Toward a theory of the rent seeking society. Texas A&M University Press, 97–112.

[20] Whiteman, P.S., 1999. Improving Single Strike Effectiveness for Network Interdiction. Military Operations Research 4 (4), 15–30.

[21] Garrick, B.J *et al.*, 2004. Confronting the risks of terrorism: making the right decisions. Reliability Engineering and System Safety 86, 129–176.

[22] Hausken, K., 2002. Probabilistic Risk Analysis and Game Theory. Risk Analysis 22, 17–27.

[23] Kunreuther, H., Heal, G., 2003. Interdependent Security. The Journal of Risk and Uncertainty 26, 231–249.

[24] Zhuang, J., Bier, V., Gupta, A., 2007. Subsidies in Interdependent Security with Heterogeneous Discount Rates. Engineering Economist 52, 1–19.

[25] Hausken, K., 2006. Income, Interdependence, and Substitution Effects Affecting Incentives for Security Investment. Journal of Accounting and Public Policy 25, 629–665.

[26] Bier, V., Abhichandani, V. Optimal Allocation of Resources for Defense of Simple Series and Parallel Systems from Determined Adversaries, Proceedings of the Engineering Foundation Conference on Risk-Based Decision Making in Water Resources X, Santa Barbara, CA: American Society of Civil Engineers; 2002.

[27] Bier, V., Nagaraj, A., Abhichandani, V., 2005. Protection of Simple Series and Parallel Systems with Components of Different Values. Reliability Engineering and System Safety 87, 315–323.

[28] Hausken, K., Levitin, G., 2009. Meeting a Demand vs. Enhancing Protections in Homogeneous Parallel Systems. Reliability Engineering and System Safety 94 (11), 1711–1717.

[29] Hausken, K., 2011. Protecting complex infrastructures against multiple strategic attackers. International Journal of Systems Science 42 (1), 11–29.

[30] Hausken, K., Bier, V., Zhuang, J., 2008. Defending against terrorism, natural disaster, and all hazards. In Game Theory and Reliability, Springer Series on Reliability Engineering, V. Bier and N. Azaiez, Eds.

[31] Levitin, G., Peng, R., Xie, M., Ng, S-H., Ben Haim, H., 2012. False target vs. protection in defending parallel systems against unintentional and intentional impacts. International Journal of Performability Engineering 8 (5), 465–478.

[32] Levitin, G., Hausken, K., 2009. Redundancy vs. protection in defending parallel systems against unintentional and intentional impacts. IEEE Transactions on Reliability 58 (4), 679–690.

# Chapitre 3

# Extra-capacity versus protection for supply networks under attack

L'article intitulé « Extra-capacity versus protection for supply networks under attack» est inséré dans ce chapitre. Il a été publié dans le journal « Reliability Engineering and System Safety » en 2014. La version présentée dans ce chapitre est identique à la version publiée.

# Résumé

Cet article développe un modèle basé sur la théorie du jeu pour la protection des installations d'un réseau logistique, et ce dans le contexte de localisation d'installations à capacités limitées. En plus d'un ensemble d'alternatives de protection directe des installations, la capacité supplémentaire des installations voisines en fonctionnement peut être utilisée suite aux attaques intentionnelles afin de livrer à temps et d'éviter les pénalités de retard. Le modèle proposé considère un jeu non coopératif à deux périodes entre deux joueurs (le défendeur et l'attaquant), et un algorithme est présenté pour déterminer la solution d'équilibre et la stratégie optimale de défense sous contraintes de la capacité. Une méthode est développée pour évaluer les utilités du défendeur et de l'attaquant. L'approche proposée est illustrée à l'aide d'un exemple numérique. La stratégie de défense de notre modèle est comparée à d'autres stratégies, et les résultats obtenus indiquent clairement l'efficacité de notre modèle à obtenir le meilleur compromis entre l'investissement dans la protection directe et le déploiement de la capacité supplémentaire.

## 3.1 Abstract

This article develops a game-theoretical model to deal with the protection of facilities, in the context of the capacitated fixed-charge location and capacity acquisition problem. A set of investment alternatives is available for direct protection of facilities. Furthermore, extra-capacity of neighbouring functional facilities can be used after attacks to avoid the backlog of demands and backorders. The proposed model considers a non-cooperative two-period game between the players, and an algorithm is presented to determine the equilibrium solution and the optimal defender strategy under capacity constraints. A method is developed to evaluate the utilities of the defender and the attacker. The benefit of the proposed approach is illustrated using a numerical example. The defence strategy of our model is compared to other strategies, and the obtained results clearly indicate the superiority of our model in finding the best trade-off between direct protection investment and extra-capacity deployment.

**Nomenclature**

| | |
|---|---|
| $n$ | number of customers in the system |
| $m$ | number of facilities in the system |
| $i$ | $i$th potential facility location, $i = 1, 2, \ldots, m$ |
| $j$ | $j$th demand location, $j = 1, 2, \ldots, n$ |
| $\psi_i$ | fixed cost of locating a facility at candidate site $i$ |
| $h_i$ | function representing the total capacity acquisition cost at facility $i$ |
| $c_{ij}$ | unit cost of shipping between candidate facility site $i$ and customer location $j$ |
| $D_j$ | demand at customer location $j$ |
| $\text{CAP}_i$ | maximum capacity that can be built-in at candidate site $i$ |
| $Z_{ij}$ | quantity shipped from candidate facility site $i$ to customer location $j$ |
| $Y_i$ | binary variable, which is equal to 1 if a facility is to be located at candidate site $i$, and 0 otherwise |
| $\beta_i$ | number of protection types for facility $i$ |
| $p$ | index of protection type, $p = 1, 2, \ldots, \beta_i$ |
| $F_{ip}$ | investment effort to protect a facility located at site $i$ using protection type $p$ |
| $f_{ip}$ | unit cost of effort to protect a facility located at site $i$ using protection type $p$ |
| $\overline{F_{ip}}$ | investment expenditure to protect a facility located at site $i$ using protection type $p$ |
| $\pi_i$ | value from $p = 1, 2, \ldots, \beta_i$ |
| $\pi_i^{opt}$ | optimal defence strategy value from $p = 1, 2, \ldots, \beta_i$ |
| $\mathbf{P}$ | vector of protection strategy, $\mathbf{P}=(\pi_i)$ |
| $\mathbf{P}_{\text{opt}}$ | vector of the optimal protection strategy, $\mathbf{P}_{\text{opt}} = \left(\pi_i^{opt}\right)$ |
| $\mathbf{F}$ | vector of investments to protection strategy $\mathbf{P}$, $\mathbf{F}= \left(F_{i\pi_i}\right)$ |
| $\mathbf{F}_{\text{opt}}$ | vector of investments to protection strategy $\mathbf{P}_{\text{opt}}$, $\mathbf{F}_{\text{opt}} = \left(F_{i\pi_i^{opt}}\right)$ |
| $F_{i\pi_i}$ | element of investments vector $\mathbf{F}$ |

| | |
|---|---|
| $F_{i\pi_i^{opt}}$ | element of investments vector $\mathbf{F}_{\text{opt}}$ |
| $\lambda_{ip}$ | binary variable which is equal to 1 if a protection of type $p$ is used for facility $i$ |
| $\boldsymbol{\lambda}$ | matrix, $\boldsymbol{\lambda} = \left(\lambda_{ip}\right)$ |
| $\rho_i$ | number of extra-capacity options for each facility $i$ |
| $e$ | index of extra-capacity options, $e = 1, 2, \ldots, \rho_i$ |
| $\tau_{ie}$ | proportion of the acquired capacity associated with the facility located at site $i$ using extra-capacity option $e$ |
| $C_i^*$ | capacity acquired associated with the facility located at site $i$ |
| $Ac_i$ | capacity acquisition cost at facility location $i$ per unit |
| $CE_{ie}$ | investment of extra-capacity associated with the facility located at site $i$ using extra-capacity option $e$, $CE_{ie} = Ac_i \tau_{ie} C_i^*$ |
| $\mathbf{E}$ | vector of extra-capacity strategy, $\mathbf{E} = \left(\theta_i\right)$ |
| $\theta_i$ | values from $e = 0, 1, \ldots, \rho_i$ |
| $\mathbf{T}$ | vector of investments to each extra-capacity strategy $\mathbf{E}$, $\mathbf{T} = \left(\tau_{i\theta_i}\right)$ |
| $\xi_{ie}$ | binary variable which is equal to 1 if an extra-capacity option $e$ is selected for facility $i$ |
| $\alpha_i$ | number of attack types against any facility $i$ |
| $g$ | index of attack type ($g = 0, 1, \ldots, \alpha_i$) |
| $Q_{ig}$ | attack effort to attack facility located at site $i$ using attack action $g$ |
| $q_{ig}$ | unit cost to attack facility located at site $i$ using attack action $g$ |
| $\overline{Q_{ig}}$ | investment expenditure to attack facility located at site $i$ using attack action $g$ |
| $\omega_i$ | value from $g = 0, 1, \ldots, \alpha_i$ |
| $\omega_i^{opt}$ | value from $g$ of the optimal attack strategy |
| $\mathbf{G}$ | vector of attack strategy, $\mathbf{G}=\left(\omega_i\right)$ |

$\mathbf{G}_{\text{opt}}$ vector of the optimal attack strategy, $\mathbf{G}_{\text{opt}} = \left(\omega_i^{opt}\right)$

$\mathbf{Q}_{\text{opt}}$ vector of attack effort of the optimal attack strategy, $\mathbf{Q}_{\text{opt}} = \left(Q_{i\omega_i^{opt}}\right)$

$Q_{i\omega_i^{opt}}$ element of attack effort vector $\mathbf{Q}_{\text{opt}}$

$\mu_{ig}$ binary variable which is equal to 1 if a type $g$ attack is used for facility $i$

$\boldsymbol{\mu}$ matrix, $\boldsymbol{\mu} = \left(\mu_{ig}\right)$

$\boldsymbol{\mu}_{\text{opt}}$ matrix, $\boldsymbol{\mu}_{\text{opt}} = \left(\mu_{ig}\right)$

$\nu_{pg}(i)$ destruction probability of a facility $i$

$\nu_{p\omega_i^{opt}}(i)$ destruction probability of a facility $i$ for the optimal defence strategy

$\boldsymbol{\nu}(\mathbf{P},\mathbf{G})$ matrix, $\boldsymbol{\nu}(\mathbf{P},\mathbf{G}) = \left(\nu_{pg}(i)\right)$

$\boldsymbol{\nu}(\mathbf{P},\mathbf{G}_{\text{opt}})$ matrix, $\boldsymbol{\nu}(\mathbf{P},\mathbf{G}_{\text{opt}}) = \left(\nu_{p\omega_i^{opt}}(i)\right)$

$\varepsilon_i$ parameter that expresses the intensity of the contest concerning facility $i$

$C_R(\mathbf{P},\mathbf{G})$ expected cost required to restore the attacked facilities which depends on **P** and **G**

$C_R(\mathbf{P},\mathbf{G}_{\text{opt}})$ expected cost required to restore the attacked facilities which depends on **P** and $\mathbf{G}_{\text{opt}}$

$R_i$ cost required to restore the attacked facility $i$

$k$ combinations index, $(k = 0,\ldots,2^m - 1)$

$S_k$ combinations of disabled and functional facilities for the facilities

S set of combinations of disabled and functional facilities, $S = \{S_k\}$

$Ct_k$ cost incurred because of the change in transportation cost when the combination is $S_k$

$\overline{Ac}$ average of the capacity acquisition costs per unit

$B_{img}$ brand image of the company

$YD_k$ annual unmet demand

$B_k$ backorder cost when the combination is $S_k$

| | |
|---|---|
| $\Delta C_{pg\mathrm{E}}(k)$ | attack outcomes of combination $k$ which depend on $p$, g and **E** |
| $TB$(**P**,**G**,**E**) | expected cost associated with the transportation cost change and the backorder cost which depends on **P, G** and **E** |
| $D$(**P**,**G**,**E**) | expected damage which depends on **P, G** and **E** |
| $U_d$(**P**,**G**,**E**) | defender expected utility which depends on **P, G** and **E** |
| $U_d$(**P**,$\mathbf{G}_{\mathrm{opt}}$,**E**) | defender expected utility which depends on **P,** $\mathbf{G}_{\mathrm{opt}}$ and **E** |
| $U_a$(**P**,**G**,**E**) | attacker expected utility which depends on **P, G** and **E** |
| $U_{\min}$ | defender minimal utility |
| $U_{\max}$ | attacker maximal utility |

## 3.2 Introduction

Critical infrastructures such as supply networks represent enormous investments devoted to the distribution of goods and services. These investments require large capital outlays. Even a minor disruption can degrade the system performance. Reductions of capacity can introduce significant delays in getting back to the planned production schedule and inflict substantial losses. Such supply networks can be the victim of threats of different kinds, such as accidental failures, natural catastrophes, terrorist attacks and sabotages, fire, industrial accidents, tsunamis, earthquakes, floods and cyclones. Recent events have shown that if one or more entities of a critical logistical network (key facilities, bottlenecks, critical links, etc.) are damaged due to an accident or an intentional attack, the network is paralysed and the damage would be enormous, resulting in a negative impact at the social, political and economic levels. Attacks can also have a serious impact on health and safety or the effective functioning of the system.

There is a relevant literature on the defence of network infrastructures against intentional attacks. In [1], the authors analyse the strategic defence and attack of complex networks and systems with components in series, parallel, interlinked, interdependent, independent, or combinations of these. The authors of [2] have recently developed a method based on a Monte Carlo simulation approach for evaluating the expected damage related to nodes deprivation of supply of commodities in multi-commodity networks as a consequence of intentional attack on arbitrarily chosen network links. In [3], the authors showed that scale-

free networks are robust against random failures but fragile to intentional attacks. In [4], critical locations susceptible to terrorist attacks are determined by decision makers on the basis of geographic regions classification. In [24] the authors study the effects of intentional attacks on transportation networks of two arcs that are subject to traffic congestion. The authors of [27] provide optimal protection configurations for a network with components vulnerable to an interdictor with potentially different attacking strategies. Ref. [28] develops an ordinal optimisation-based method to identify top contributors to power networks failure when considering cascade failure events.

There is also a mature literature on facility design with probabilistic failure of components [5,29,30]. However, the possibility of intentional strikes or attacks is not normally taken into account in this literature, except in [6] where the authors developed a game-theoretical model to protect facilities against intentional attacks in the context of the *uncapacitated* fixed-charge location problem. This article deals with the protection of network logistic facilities in the context of the *capacitated* fixed-charge location and capacity acquisition problem (CFL & CAP). Facility location and capacity acquisition are of vital importance for supply chain management [7-9]. Here, we consider the CFL & CAP to deal with resource allocation of protection and allocation of extra-capacity among facilities.

The aim of the CFL & CAP is to decide simultaneously on the optimal location and capacity size of each new facility to be established [8-13]. In this problem, we are given a set of customer locations with known demands and a set of potential facility locations. If we decide to locate a facility with a chosen capacity at a candidate site, we incur a known fixed location cost. There is a known unit cost of shipping between each candidate facility site and each customer location. The problem is to find the locations of the facilities and the shipment pattern between the facilities and the customers, to minimise the sum of the facility location and shipment costs, subject to the constraints that all demands must be served, facilities capacities must not be exceeded, and customers can only be served from open facilities.

For the protection of network logistic facilities in the context of the CFL & CAP, we consider that not only a set of investment alternatives are available for “direct” protection of facilities, but also extra-capacities of neighbouring functional facilities can be used after

attacks for “indirect” protection. Extra-capacity is among the different strategies to deal with the risk of uncertain production capacity. It can be used, after a capacity shock, to quickly bring production back on schedule and to avoid the backlog of demands [14]. In the case of demand growth, facilities of supply network might hold extra-capacity against demand variability [15]. In our case, extra-capacity of neighbouring functional facilities is used after attacks in order to satisfy all customer demands and to avoid backorders.

In supply chains, the backorder unit cost is always higher than the capacity acquisition unit cost. Consequently, the cost of any strategy using only direct protection (without extra-capacities) will be higher than that of our model. By acquiring extra-capacities to hedge against expensive backorders, we introduce an indirect but effective means to protect the supply network against attacks.

The idea of deploying extra-capacities to indirectly protect facilities is similar in spirit to the use of redundant system elements in the defence literature [21,26,31].The redundancy is aimed at providing the system with the ability to perform its task when part of the system elements is destroyed by an attack. Similarly, in our model, the extra-capacity of neighbouring functional facilities is used after attacks to avoid the backlog of demands and backorders.

The CFL & CAP problem assumes that, once constructed, the facilities chosen will always operate as planned. However, if a facility is attacked, it may become unavailable and customers must be served from other functional facilities of the supply network that can be farther than their regular facilities, but subject to constraints that functional facilities capacities must not be exceeded. To satisfy customer demands and to avoid backorders, the amount produced by disabled facility must be allocated optimally among the functional facilities. This reduces the cost of delayed production after attacks, but may lead to additional costs. The strategic decision dealt with here is how to allocate optimally the protective resources and the extra-capacity among the facilities, knowing that these facilities are exposed to external intentional attacks. In other words, given a set of investment alternatives for protecting the facilities and a set of extra capacities, we want to determine how much to invest optimally in direct protection of facilities and in indirect

protection by extra-capacity, while taking into account that both the defender and the attacker are fully optimising agents. The idea of using extra-capacity to indirectly protect supply networks against intentional attack is used in this paper to develop a game-theoretic model with the objective of finding the best trade-off between direct investments in protection and indirect protection by extra-capacities deployment.

The remainder of the paper is organised as follows. Section 2 presents the mathematical model of capacitated fixed-charge location and capacity acquisition problem. Section 3 formulates the studied problem as a two-period non-cooperative game. Section 4 evaluates the players' utilities. Section 5 develops an algorithm to solve the game. Section 6 presents a numerical example. Section 7 concludes the paper.

### 3.3 The facility location and capacity acquisition problem

The CFL & CAP considers the problem of locating facilities to minimise the sum of the facility location costs, the costs of capacity acquisition associated with the size of open facility and the shipping costs from open facilities to customers subject to constraints that all demands must be served, facility capacities must not be exceeded, and customers can only be served from open facilities [9]. The CFL &CAP has been widely studied in the literature and applied in a variety of domains, and is known to be *NP*-hard [16].

The decision variables are $Z_{ij}$ representing the quantity shipped from candidate facility site $i$ to customer location $j$; and $Y_i$ which is equal to 1 if a facility is to be located at candidate site $i$, and 0 otherwise.

Using the notation in the nomenclature, the problem can be modelled as follows:

$$\text{Minimize} \qquad \sum_{i=1}^{m}\left[\psi_i Y_i + h_i\left(\sum_{j=1}^{n} Z_{ij}\right) + \sum_{j=1}^{n} c_{ij} Z_{ij}\right], \tag{3.1}$$

$$\text{Subject to} \qquad \sum_{i=1}^{m} Z_{ij} = D_j \quad j = 1,\ 2,\ ...,\ n, \tag{3.2}$$

$$0 \le Z_{ij} \le Y_i D_j \quad i = 1,\ 2,\ ...,\ m,\ \ j = 1,\ 2,\ ...,\ n, \tag{3.3}$$

$$\sum_{j=1}^{n} Z_{ij} \le \mathrm{CAP}_i \quad i = 1,\ 2,\ ...,\ m. \tag{3.4}$$

$$Y_i \in \{0,\ 1\} \quad i = 1,\ 2,\ ...,\ m. \tag{3.5}$$

The objective function (3.1) minimises the sum of the fixed facility location costs, the costs of capacity acquisition associated with open facility, and the shipments or transportation costs. Constraint (3.2) ensures that each customer's demand will be fully satisfied. Constraint (3.3) is a simple non-negativity constraint and it guarantees that customers receive shipments only from open facilities. Capacity constraint (3.4) ensures that an open facility $i$ does not supply more than its capacity $\mathrm{CAP}_i$, and constraint (3.5) requires the location variables to be binary.

If we assume that $h_i$ is a linear function, the form of the objective function becomes $\sum_{i=1}^{m}\left[\psi_i Y_i + Ac_i \sum_{j=1}^{n} Z_{ij} + \sum_{j=1}^{n} c_{ij} Z_{ij}\right]$, where $Ac_i$ is the capacity acquisition cost at facility location per unit.

To hedge against facilities unavailability, it is possible at the beginning to acquire capacities that are higher than the optimal values obtained from the model (3.1)-( 3.5). Our objective is to find the best defence and capacity acquisition strategies, knowing that the facilities are subject to intentional attacks. As already explained in the introduction, given a set of investment alternatives for protecting the facilities and set of extra capacities, we want to determine how much to invest optimally in direct protection of facilities and in indirect protection by extra-capacity, while taking into account that both the defender and the attacker are fully optimising agents.

In the proposed model the defender first locates the facilities; then, she (he) decides on protections types and extra-capacities for these already located facilities. The decision variables $Z_{ij}$ and $Y_i$ are related to the location model. For each facility $i$ ($i$ = 1, 2, …, $m$) the

defender decides on a protection type and on an extra-capacity option. As a result, for the $m$ facilities we have $2m$ free choice variables ($m$ protection types and $m$ extra-capacity options).

The next section presents our game-theoretic model developed to find the best trade-off between direct investments in protection and indirect protection by extra-capacities deployment.

## 3.4 Problem formulation using game theory

We consider a system containing $m$ facilities (targets) designed using the optimisation model (3.1)-( 3.5). Our model considers two players: the defender and the attacker. We are given a set of investment alternatives for protecting the facilities (we call this direct protection), and a set of extra-capacity options for each facility (we call this indirect protection). The objective is to determine how to allocate optimally (direct) protective resources and (indirect) extra-capacities among the facilities taking into account the attacker strategy.

For the attacker, there are also many ways to attain the facilities performance with a set of investment alternatives. We consider a two-period game between the defender who selects a strategy in the first period that minimises the maximum loss that the attacker may cause in the second period. This means that in the first period the defender determines its $2m$ free choice variables simultaneously and independently, and in the second period the attacker determines its $m$ free choice variables simultaneously and independently. For each player strategy, a utility function is associated with each game conclusion.

The defender maximises his utility by minimising the expected damage of the system and the investment expenditure incurred to extra-capacity and to protect the system. The attacker maximises his utility also, calculated as the expected damage minus the attacks expenditures. To better understand the game, the defence and attack choices are detailed in what follows.

### 3.4.1 The defender

We consider that for each facility $i$ there exists a set of $\beta_i$ available types of protections against the identified threat. Each protection type is indicated by index $p$ ($p$ = 0, 1, 2, …, $\beta_i$). $p$ = 0 means that no defence is used. Let $\overline{F_{ip}}$ be the defender investment expenditure in dollar terms. We express $\overline{F_{ip}}$ as the product of two parts, $F_{ip}$ and $f_{ip}$ . That is, $\overline{F_{ip}} = f_{ip}F_{ip}$ where $F_{ip}$ is an investment effort incurred by the defender at unit cost $f_{ip}$ ($f_{ip}$>0) to protect a facility located at site $i$ using protection type $p$.

We consider a vector **P** = $(\pi_i)$ which represents a protection strategy of the $m$ facilities such as $\pi_i$ takes values from $p$ = 1, 2, …, $\beta_i$. For example, **P** = $(2 \quad 1 \quad 3)$ means that we have facility 1 protected using type 2 protection, facility 2 is protected using type 1 protection and facility 3 is protected using type 3 protection. To each protection strategy **P**, corresponds a vector of investments **F** = $\left(F_{i\pi_i}\right)$. For example, when P =$(2 \quad 1 \quad 3)$, we have **F** = $(F_{12} \quad F_{21} \quad F_{33})$.

Let $\lambda_{ip}$ be a binary variable which is equal to 1 if a protection of type $p$ is selected for facility $i$, and 0 otherwise. We assume that only one type of protection of facility $i$ is used:

$$\sum_{p=1}^{\beta_i} \lambda_{ip} = 1, \ \forall i. \tag{3.6}$$

Let $\rho_i$ be the number of available extra-capacity options for each facility $i$. Let $e$ ($e$ = 1, 2, …, $\rho_i$ ) be an index that indicates each extra-capacity option. The defender incurs an investment of proportion of the capacity acquired $\tau_{ie}$ associated with the facility located at site $i$ using extra-capacity option $e$. Let $C_i^*$ denote the capacity acquired. We assume that $h_i(.)$ the capacity acquisition cost at facility location is a linear function. We then consider that the investment of extra-capacity $CE_{ie}$ associated with the facility located at site $i$ using extra-capacity option $e$, measured in dollar terms, is given by $CE_{ie} = Ac_i\tau_{ie}C_i^*$ , where $Ac_i$ is the capacity acquisition cost at facility location $i$ per unit.

We represent an extra-capacity strategy of the $m$ facilities by a vector **E** = $(\theta_i)$, $\theta_i$ takes values from $e$ = 0, 1, …, $\rho_i$. For example, **E** = $(2 \quad 2 \quad 2)$ means that option 2 extra-capacity is selected for the 3 facilities.

To each extra-capacity strategy **E**, corresponds a vector of investments **T** = $\left(\tau_{i\theta_i}\right)$. For example, when **E** = $(2 \quad 2 \quad 2)$, we have **T**=$\{\tau_{12},\ \tau_{22},\ \tau_{32}\}$.

Let us introduce a binary variable $\xi_{ie}$ which is equal to 1 if an extra-capacity of type $e$ is selected for facility $i$. Assuming that one type of extra-capacity is used, we have:

$$\sum_{e=0}^{\rho_i} \xi_{ie} = 1, \ \forall i. \tag{3.7}$$

### 3.4.2 The attacker

The attacker seeks to attack the system to ensure that it does not function reliably. He (she) has a set of $\alpha_i$ available attack actions against any facility $i$. Each attack type is indicated by index $g$ ($g$ = 0, 1, 2, …, $\alpha_i$). $g$ = 0 indicates the absence of an attack. Analogously, the attacker incurs an effort $Q_{ig}$ at unit cost $q_{ig}$ to attack facility located at site $j$ using attack action $g$. The inefficiency of investment is $q_{ig}$, and $1/q_{ig}$ is the efficiency. Its investment expenditure, in dollar terms, is $\overline{Q_{ig}} = q_{ig}Q_{ig}$,, where $q_{ig}$>0.

We consider a vector **G** = $(\omega_i)$ which represents an attack strategy against the $m$ facilities, $\omega_i$ takes values from $g$ = 1, 2, …, $\alpha_i$. For example, **G** = $(3 \quad 1 \quad 3)$ means that we have two facilities that can be attacked using attacks of type 3 and facility 2 that can be attacked using attack of type 1.

Let $\mu_{ig}$ be a binary variable which is equal to 1 if an attack of type $g$ is used for facility $i$, and 0 otherwise. We assume that only one type of attack of facility $i$ is used:

$$\sum_{g=1}^{\alpha_i} \mu_{ig} = 1, \ \forall i. \tag{3.8}$$

We suppose that successful or failed attacks against different facilities are independent. We also assume that each facility can be attacked by the attacker only once, and that many facilities can be attacked at the same time.

### 3.4.3 Vulnerability of facilities

In game theory, interaction between two conflicted players (here the defender and the attacker) can be modelled by introducing the concept of the contest success function commonly used in the rent seeking literature [17, 18, 19, 20]. The vulnerability or the probability of a successful attack on facility *i* is defined by its destruction probability $\nu_{pg}(i)$. The vulnerability of the attacked facility is usually determined by the ratio form of the attacker–defender contest success function [21, 22, 23]. The vulnerability of any facility *i* by a contest success function is:

$$\nu_{pg}(i) = \frac{\left(Q_{ig}\right)^{\varepsilon_i}}{\left(F_{ip}\right)^{\varepsilon_i} + \left(Q_{ig}\right)^{\varepsilon_i}}, \tag{3.9}$$

where $\partial \nu_{pg}(i) / \partial Q_{ig} > 0$, $\partial \nu_{pg}(i) / \partial F_{ip} < 0$, and $\varepsilon_i \geq 0$ is a parameter that expresses the intensity of the contest. We assume that $\varepsilon_i$ does not depend on *p* and *g*.

On the one hand, if the attacker exerts high offensive effort, it is likely to win the contest which is expressed by high vulnerability; on the other hand, if the defender exerts high defensive effort, it is likely to win the contest which is expressed by low vulnerability [18, 19, 21, 23].

### 3.4.4 The game

Having the vulnerabilities of facilities as functions of the attacker's and the defender's efforts, both agents can estimate the expected damage caused by the attack for any possible

distribution of these efforts. The defender's objective is to maximise its utility function by minimising the expected damage and weighing against protection and extra-capacity expenditures. The attacker's objective is to maximise the expected damage while weighing against the attacks expenditures [25]. Facilities are usually built over time by the defender. The attacker takes it as given when he (she) chooses his (her) attack strategy. Therefore, we consider a two-period min-max game where the defender invests in the first period, and the attacker moves in the second period. This means that the defender selects a strategy in the first period that minimises the maximum loss that the attacker may cause in the second period. The utilities of each player are evaluated in the next section, while the game will be solved with backward recursion, in which the second period is solved first in Section 5.

### 3.5 Evaluation of the players' utilities

The damage caused by an attack is associated with the following terms:

***Damage 1***: **The expected cost required for restoring the attacked facilities**

If $R_i$ is the cost required to restore the attacked facility $i$, this cost depends on the defence and attack strategies **P** and **G**, and it is given by:

$$C_R(\mathbf{P},\mathbf{G}) = \sum_{i=1}^{m} \sum_{g=0}^{\alpha_i} \sum_{p=1}^{\beta_i} \lambda_{ip} \mu_{ig} \nu_{pg}(i) R_i . \tag{3.10}$$

***Damage 2*: The cost incurred because of the backorder and the change in transportation**

On the one hand, a backorder cost is incurred when the demands cannot be satisfied. This will happen either when the entire system is disabled, or when even the available extra-capacities are not enough to fulfil the demands. On the other hand, there is a change in transportation cost after attacks. When one or several facilities are unavailable, to avoid the backlog of demands and backorders, available extra-capacities of neighbouring functional facilities are used. Adding the available extra-capacity to initial capacity, customers could be served and may receive shipments from these facilities, which can sometimes be farther

away (subject to constraints that their total capacity must not be exceeded). As a matter of fact, the transportation cost will change as customers are reassigned.

While damage 1 has been expressed by equations (3.10), the evaluation of damage 2 is provided in what follows.

Each facility can be either Disabled or Functional. Let S = $\{S_k\}$ be a set of possible combinations when considering all facilities. For $m$ facilities, there are $2^m$ possible combinations. Table 3.1 presents all possible combinations for three facilities denoted by Fac1, Fac2 and Fac3, In this case, there are eight possible combinations for the facilities ($k$ = 0, 1, …, 7).

**Table 3.1-** Possible combinations: case of three facilities.

| Combination $S_k$ | Index $k$ |
|---|---|
| All facilities are functional | 0 |
| Fac 1 is disabled and the others facilities are functional | 1 |
| Fac 2 is disabled and the others facilities are functional | 2 |
| Fac 3 is disabled and the others facilities are functional | 3 |
| Fac1 and Fac 2 are disabled, and Fac 3 is functional | 4 |
| Fac1 and Fac 3 are disabled, and Fac 2 is functional | 5 |
| Fac 2 and Fac 3 are disabled, and Fac 1 is functional | 6 |
| Fac1, Fac 2 and Fac 3 are disabled | 7 |

Let us denote by $Ct_k$ the cost incurred because of the change in transportation cost, *i.e.* the cost under combination $S_k$ minus the cost in a normal situation. We also denote by $B_k$ the backorder cost when the combination is $S_k$. As $Ct_k$ and $B_k$ depend on the vector **E** of extra-capacity strategy, they are rather written $Ct_k(\mathbf{E})$ and $B_k(\mathbf{E})$. Let us denote by $T_k(\mathbf{E})$ the sum of the backorder cost and the cost incurred because of the change in transportation cost when the combination is $S_k$. That is,

$$T_k(\mathbf{E}) = Ct_k(\mathbf{E}) + B_k(\mathbf{E}). \quad (3.11)$$

The evaluation of $Ct_k(\mathbf{E})$ and $B_k(\mathbf{E})$ requires the development of a new optimisation model to analyse the supply network after attacks. This is a variant of model (3.1)-( 3.5) to take into account the following two remarks.

**Remark 1**:

The capacity of each facility is equal to the capacity acquired according to the optimal solution of model (3.1)-( 3.5), plus the extra-capacity deployed according to the vector strategy **E**. That is, if we denote by $MC_{ie}$ the modified (eventually extended) capacity, we have

$$MC_{ie} = C_i^* \left(1 + \tau_{ie}\right). \quad (3.12)$$

**Remark 2**:

A backorder cost must be taken into account whenever the total demand is higher than the total quantity shipped. Note that in the context of supply networks, the backorder cost is relatively high. Knowing that $Z_{ij}$ is the quantity shipped from candidate facility site $i$ to customer location $j$, the annual unmet demand $YD_k(\mathbf{E})$ is given by

$$YD_k(\mathbf{E}) = Max\left(0,\ \sum_{j=1}^{n} D_j - \sum_{i=1}^{m}\sum_{j=1}^{n} Z_{ij}\right). \quad (3.13)$$

Let us denote by $B_{img}$ the brand image of the company, and $\overline{Ac}$ the average of the capacity acquisition costs per unit. We consider here that the backorder is computed per year, based on 20% of the average of the capacity acquisition costs. Using a function $\delta(x)$ is equal to 1 if $x$ is strictly positive and 0 otherwise, we have

$$B_k(\mathbf{E}) = \delta\left(\sum_{j=1}^{n} D_j - \sum_{i=1}^{m}\sum_{j=1}^{n} Z_{ij}\right)\left[B_{img} + 0.2 \times \overline{Ac} \times \left(\sum_{j=1}^{n} D_j - \sum_{i=1}^{m}\sum_{j=1}^{n} Z_{ij}\right)\right]. \quad (3.14)$$

Equation (3.14) expresses the fact that there is a backorder cost only when the total demand is higher than the total quantity shipped (*i.e.*, $\sum_{j=1}^{n} D_j - \sum_{i=1}^{m}\sum_{j=1}^{n} Z_{ij}$ is strictly positive).

Taking into account remarks 1 and 2 above, the modified optimisation model is as follows:

Minimise $$\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}Z_{ij} + \delta\left(\sum_{j=1}^{n} D_j - \sum_{i=1}^{m}\sum_{j=1}^{n} Z_{ij}\right)\left[B_{img} + 0.2 \times \overline{Ac} \times \left(\sum_{j=1}^{n} D_j - \sum_{i=1}^{m}\sum_{j=1}^{n} Z_{ij}\right)\right], \quad (3.15)$$

Subject to $$\sum_{i=1}^{m} Z_{ij} \le \mathrm{D}_j \qquad j = 1,\ 2,\ ...,\ n, \quad (3.16)$$

$$\sum_{j=1}^{n} Z_{ij} \le C_i^{*}\left(1 + \tau_{ie}\right) \qquad i = 1,\ 2,\ ...,\ m,\ e = 0, 1, \ldots,\ \rho_i, \quad (3.17)$$

$$Z_{ij} \ge 0 \qquad i = 1,\ 2,\ ...,\ m,\ \ j = 1,\ 2,\ ...,\ n. \quad (3.18)$$

The decision variables of the model (3.15)-(3.18) are $Z_{ij}$ representing the quantity shipped from candidate facility site $i$ to customer location $j$. The objective function (3.15) minimises the sum of the transportation costs and the backorder costs. Constraint (3.16) is a non-negativity constraint and it guarantees that each customer receives shipments less or equal to the demand. Capacity constraint (3.17) ensures that a facility $i$ does not supply more than its capacity. Constraint (3.18) is a simple non-negativity constraint.

Let us consider for example combination 2 in Table 3.1, where only facilities 1 and 3 are operational. For a given extra-capacity strategy (**E**), the modified capacities $MC_{ie}$ are evaluated (for each facility using Equation (3.12)), and used in constraint (3.17). The model (3.15)-(3.18) must be solved to determine the decision variables $Z_{ij}$. This optimal solution is characterised by a new transportation cost and a backorder cost $B_2$(**E**). The cost $Ct_2$(**E**) is the cost incurred because of the change in transportation cost, *i.e.* the cost under combination $S_2$ minus the cost in a normal situation.

To solve the model (3.15)-(3.18), two cases are considered.

**Case 1**: $\sum_{i=1}^{m} MC_{ie} \geq \sum_{j=1}^{n} D_j$

As the total capacity is larger than the total demand, no backorder is incurred. Since the backorder cost is relatively high, the demand should be fully satisfied. In this case, the problem can be solved by rewriting the objective function and constraint (3.16) as follows:

Minimise $\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij} Z_{ij},$ (3.19)

Subject to $\sum_{i=1}^{m} Z_{ij} = D_j \quad j = 1,\ 2,\ ...,\ n,$ (3.20)

$\sum_{j=1}^{n} Z_{ij} \leq C_i^{*}\left(1+\tau_{ie}\right) \quad i = 1,\ 2,\ ...,\ m,\ e = 0, 1, \ldots,\ \rho_i,$ (3.21)

$Z_{ij} \geq 0 \qquad i = 1,\ 2,\ ...,\ m,\ \ j = 1,\ 2,\ ...,\ n.$ (3.22)

**Case 2**: $\sum_{i=1}^{m} MC_{ie} < \sum_{j=1}^{n} D_j$

When the total capacity is less than the total demand, a backorder cost is inevitably incurred. Knowing that the backorder cost is relatively high, the overall capacity is used to fulfil the demand. Thus, the backorder quantity can be calculated, without solving the optimisation model, as $\left(\sum_{j=1}^{n} D_j - \sum_{i=1}^{m} MC_{ie}\right)$. The resulting backorder cost is then $B_{img} + 0.2 \times \overline{Ac} \times \left(\sum_{j=1}^{n} D_j - \sum_{i=1}^{m}\sum_{j=1}^{n} Z_{ij}\right)$.

To find the modified transportation cost, the problem can be solved by rewriting constraint (3.17) to state that the overall capacity must be used. The resulting model is as follows:

Minimise $\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij} Z_{ij},$ (3.23)

Subject to $\sum_{i=1}^{m} Z_{ij} \leq \mathrm{D}_j \quad j = 1,\ 2,\ ...,\ n,$ (3.24)

$\sum_{j=1}^{n} Z_{ij} = C_i^{*}\left(1+\tau_{ie}\right) \quad i = 1,\ 2,\ ...,\ m,\ e = 0, 1, \ldots,\ \rho_i.$ (3.25)

$$Z_{ij} \geq 0 \qquad i = 1,\ 2,\ ...,\ m,\ \ j = 1,\ 2,\ ...,\ n. \tag{3.26}$$

The following algorithm summarises the solution method used to solve the model (3.15)-(3.18):

For each extra-capacity strategy **E**

For each combination $k = 1, 2, \ldots, 2^m - 1$

If $\sum_{i=1}^{m} MC_{ie} \geq \sum_{j=1}^{n} D_j$

$B_k(\mathbf{E}) = 0$;

Solve the model (3.19)-(3.22) to determine the cost $Ct_k(\mathbf{E})$;

If $\sum_{i=1}^{m} MC_{ie} < \sum_{j=1}^{n} D_j$

$$B_k(\mathbf{E}) = B_{img} + 0.2 \times \overline{Ac} \times \left( \sum_{j=1}^{n} D_j - \sum_{i=1}^{m} \sum_{j=1}^{n} Z_{ij} \right);$$

Solve the model (3.23)-(3.26) to determine the cost $Ct_k(\mathbf{E})$.

The evaluation of the costs $Ct_k(\mathbf{E})$ may require the solution of $(2^m - 2)$ optimisation models. In fact, this should be done for all combinations $k$, except combination 0 where all facilities are functional, and for combination $(2^m - 1)$ where all facilities are disabled. Each solution of the optimisation model corresponds to a combination $S_k$. Note that $Ct_k(\mathbf{E})$ can be negative; but as the backorder costs are relatively high, there will be a damage $T_k(\mathbf{E})$ all the time.

The backorder costs and the changes of the transportation costs are related to all the possible outcomes. Each attack outcome $T_k(\mathbf{E})$ is multiplied by the probability of the corresponding combination to calculate $\Delta C_{pg\mathbf{E}}(k)$, with $p$, $g$ and **E** given and $k$ varying from 0 to $2^m - 1$. Considering that each facility can be either attacked or not, there are also $2^m$ possibilities of attacks for $m$ facilities, for given strategies **P** and **G**. Table 3.2 illustrates, for an example of three facilities, the calculation of the expected cost incurred because of the change in cost after attacks.

**Table 3.2-** Combination of attacked facilities and outcomes.

| Combination of disabled facilities | $\Delta C_{pg\mathbf{E}}(k)$ |
|---|---|
| All facilities are Functional | $\Delta C_{pg\mathbf{E}}(0) = 0$ |
| Only Fac1 is Disabled | $\Delta C_{pg\mathbf{E}}(1) = T_1(\mathbf{E})\nu_{pg}(1)$ |
| Only Fac2 is Disabled | $\Delta C_{pg\mathbf{E}}(2) = T_2(\mathbf{E})\nu_{pg}(2)$ |
| Only Fac3 is Disabled | $\Delta C_{pg\mathbf{E}}(3) = T_3(\mathbf{E})\nu_{pg}(3)$ |
| Fac1 and Fac2 are Disabled, Fac3 is Functional | $\Delta C_{pg\mathbf{E}}(4) = T_1(\mathbf{E})\nu_{pg}(1)(1-\nu_{pg}(2)) + T_2(\mathbf{E})\nu_{pg}(2)(1-\nu_{pg}(1)) + T_4(\mathbf{E})\nu_{pg}(1)\nu_{pg}(2)$ |
| Fac1 and Fac3 are Disabled, Fac2 is Functional | $\Delta C_{pg\mathbf{E}}(5) = T_1(\mathbf{E})\nu_{pg}(1)(1-\nu_{pg}(3)) + T_3(\mathbf{E})\nu_{pg}(3)(1-\nu_{pg}(1)) + T_5(\mathbf{E})\nu_{pg}(1)\nu_{pg}(3)$ |
| Fac2 and Fac3 are Disabled, Fac1 is Functional | $\Delta C_{pg\mathbf{E}}(6) = T_2(\mathbf{E})\nu_{pg}(2)(1-\nu_{pg}(3)) + T_3(\mathbf{E})\nu_{pg}(3)(1-\nu_{pg}(2)) + T_6(\mathbf{E})\nu_{pg}(2)\nu_{pg}(3)$ |
| All facilities are Disabled | $\Delta C_{pg\mathbf{E}}(7) = T_1(\mathbf{E})\nu_{pg}(1)(1-\nu_{pg}(2))(1-\nu_{pg}(3)) + T_2(\mathbf{E})\nu_{pg}(2)(1-\nu_{pg}(1))(1-\nu_{pg}(3)) + T_3(\mathbf{E})\nu_{pg}(3)(1-\nu_{pg}(1))(1-\nu_{pg}(2)) + T_4(\mathbf{E})\nu_{pg}(1)\nu_{pg}(2)(1-\nu_{pg}(3)) + T_5(\mathbf{E})\nu_{pg}(1)\nu_{pg}(3)(1-\nu_{pg}(2)) + T_6(\mathbf{E})\nu_{pg}(2)\nu_{pg}(3)(1-\nu_{pg}(1)) + T_7(\mathbf{E})\nu_{pg}(1)\nu_{pg}(2)\nu_{pg}(3)$ |

The expected value of the cost incurred because of the backorder and the change in transportation cost (damage 2) is given by:

$$TB(\mathbf{P},\mathbf{G},\mathbf{E}) = \sum_{k=1}^{2^m-1} \Delta C_{pg\mathbf{E}}(k). \tag{3.27}$$

The expected damage is then the sum of damages 1 and 2 given by equations (3.10) and (3.27):

$$D(\mathbf{P},\mathbf{G},\mathbf{E}) = \sum_{i=1}^{m}\sum_{g=0}^{\alpha_j}\sum_{p=1}^{\beta_j}\lambda_{ip}\mu_{ig}\nu_{pg}(i)R_i + \sum_{k=1}^{2^m-1}\Delta C_{pg\mathbf{E}}(k). \quad (3.28)$$

The total protection cost (*TPC*) is:

$$TPC(\mathbf{P},\mathbf{G},\mathbf{E}) = \sum_{i=1}^{m}\sum_{p=1}^{\beta_i}\lambda_{ip}\overline{B_{ip}} + \sum_{i=1}^{m}\sum_{e=0}^{\rho_i}\xi_{ie}CE_{ie}. \quad (3.29)$$

The defender expected utility is:

$$\begin{aligned} U_d(\mathbf{P},\mathbf{G},\mathbf{E}) &= -D(\mathbf{P},\mathbf{G},\mathbf{E}) - \sum_{i=1}^{m}\sum_{p=1}^{\beta_i}\lambda_{ip}\overline{B_{ip}} - \sum_{i=1}^{m}\sum_{e=0}^{\rho_i}\xi_{ie}CE_{ie} \\ &= -\left(\sum_{i=1}^{m}\sum_{g=0}^{\alpha_i}\sum_{p=1}^{\beta_i}\lambda_{ip}\mu_{ig}\nu_{pg}(i)R_i + \sum_{k=1}^{2^m-1}\Delta C_{pg\mathbf{E}}(k)\right) - \sum_{i=1}^{m}\sum_{p=1}^{\beta_i}\lambda_{ip}\overline{B_{ip}} - \sum_{i=1}^{m}\sum_{e=0}^{\rho_i}\xi_{ie}CE_{ie}. \end{aligned} \quad (3.30)$$

The attacker expected utility is:

$$\begin{aligned} U_a(\mathbf{P},\mathbf{G},\mathbf{E}) &= D(\mathbf{P},\mathbf{G},\mathbf{E}) - \sum_{i=1}^{m}\sum_{g=0}^{\alpha_i}\mu_{ig}\overline{Q_{ig}} \\ &= \sum_{i=1}^{m}\sum_{g=0}^{\alpha_i}\sum_{p=1}^{\beta_i}\lambda_{ip}\mu_{ig}\nu_{pg}(i)R_i + \sum_{k=1}^{2^m-1}\Delta C_{pg\mathbf{E}}(k) - \sum_{i=1}^{m}\sum_{g=0}^{\alpha_i}\mu_{ig}\overline{Q_{ig}}. \end{aligned} \quad (3.31)$$

## 3.6 Solution of the game

We analyse a two-period game where the defender moves in the first period, and the attacker moves in the second period [18, 26]. This means that the defender selects a strategy in the first period that minimises the maximum loss that the attacker may cause in the second period. In order to find the equilibrium, the game is solved with backward induction in which the second period is solved first using the following algorithm, which is an adaptation of the algorithm in [6] to take into account the extra-capacity dimension as a means for indirect protection:

**1) Inputs**

• A system of $m$ facilities ($i$ = 1, 2, …, $m$) located by solving the optimisation model (3.1)-( 3.5).

• A set of $\beta_i$ protection types for each facility $i$ ($p$ = 1, 2, …, $\beta_i$).

• A set of $\alpha_i$ attack types per facility $i$ ($g$ = 0, 1, …, $\alpha_i$).

• A set of $\rho_i$ extra-capacity options per facility $i$ ($e$ = 0, 1, 2, …, $\rho_i$ ).

• *Parameters*:

- Protection investment efforts $F_{ip}$;
- Unit costs of protection efforts $f_{ip}$;
- Attack investment efforts $Q_{ig}$;
- Unit costs of attack efforts $q_{ig}$;
- Capacity acquired $C_i^*$;
- Capacity acquisition cost per unit $Ac_i$;
- Proportion of the capacity acquired $\tau_{ie}$;
- Contest intensities $\varepsilon_i$;
- Restoration costs $R_i$; and
- Brand image of the company $B_{img}$.

**2) Initialisation**

Assign $U_{\min} = \infty$ ($U_{\min}$ is the defender's minimal utility);

Assign $U_{\max} = 0$ ($U_{\max}$ is the attacker's maximal utility).

**3) Determination of the optimal attack strategy** (*i.e.*, the strategy that maximises the attacker's utility)

For each protection strategy **P** = $(\pi_i)$

**3.1.** For each attack strategy **G** = $(\omega_i)$

**3.1.1.** Construct a matrix $\boldsymbol{\lambda} = (\lambda_{ip})$ such as

$$\lambda_{ip} = \begin{cases} 1 & if \quad \pi_i = p \\ 0 & otherwise \end{cases}, \text{ and } \sum_{p=1}^{\beta_i} \lambda_{ip} = 1, \ \forall i ;$$

**3.1.2.** Construct a matrix $\boldsymbol{\mu} = (\mu_{ig})$ such as

$$\mu_{ig} = \begin{cases} 1 & if \ \ \omega_i = g \\ 0 & otherwise \end{cases}, \text{ and } \sum_{g=0}^{\alpha_i} \mu_{ig} = 1, \ \ \forall i \, ;$$

**3.1.3.** Determine the matrix $\boldsymbol{\nu}(\mathbf{P},\mathbf{G}) = \left(\nu_{pg}(i)\right)$ such as each element $\nu_{pg}(i)$ is evaluated by using equation (3.9);

**3.1.4.** Calculate the costs $C_R(\mathbf{P},\mathbf{G})$ by using equations (3.10);

**3.1.5.** For each extra-capacity strategy $\mathbf{E} = \left(\theta_i\right)$

**3.1.5.1.** For each combination $k = 1, 2, \ldots, 2^m - 1$

**3.1.5.1.1.** Solve the model (3.15)-(3.18), using the algorithm presented in Section 4, to determine the cost $T_k(\mathbf{E}) = Ct_k(\mathbf{E}) + B_k(\mathbf{E})$;

**3.1.5.2.** Calculate the expected cost $TB(\mathbf{P},\mathbf{G},\mathbf{E})$ by using equation (3.27);

**3.1.5.3.** Calculate the attacker's utility $U_a(\mathbf{P},\mathbf{G},\mathbf{E})$ by using equation (3.31);

**3.1.5.3.1.** If $U_a(\mathbf{P},\mathbf{G},\mathbf{E}) > U_{max}$ assign $U_{max} = U_a(\mathbf{P},\mathbf{G},\mathbf{E})$,

$$\mathbf{G}_{\text{opt}} = \mathbf{G} = \left(\omega_i^{opt}\right), \ \mathbf{Q}_{\text{opt}} = \left(Q_{i\omega_i^{opt}}\right);$$

**4) Determination of the optimal defence strategy** (*i.e.*, maximising the defender's utility)

For each protection strategy $\mathbf{P} = \left(\pi_i\right)$

**4.1.** Assign $\boldsymbol{\mu}_{\text{opt}} = \left(\mu_{ig}\right)$ such as

$$\mu_{ig} = \begin{cases} 1 & if \ \ \omega_i^{opt} = g \\ 0 & otherwise \end{cases};$$

**4.2.** Determine the matrix $\boldsymbol{\nu}(\mathbf{P},\mathbf{G}_{\text{opt}}) = \left(\nu_{p\omega_i^{opt}}(i)\right)$ such as each element $\nu_{pg}(i)$ is evaluated by using equation (3.9) with $\boldsymbol{\lambda}=\left(\lambda_{ip}\right)$ and under attack strategy $\mathbf{G}_{\text{opt}}$,

$$i.e.,\ \ \nu_{p\omega_i^{opt}}(i) = \frac{\left(Q_{i\omega_i^{opt}}\right)^{\varepsilon_i}}{\left(F_{ip}\right)^{\varepsilon_i} + \left(Q_{i\omega_i^{opt}}\right)^{\varepsilon_i}};$$

**4.3.** Calculate the costs $C_R(\mathbf{P},\mathbf{G}_{\text{opt}})$ by using equations (3.10) (under attack strategy $\mathbf{G}_{\text{opt}}$);

**4.4.** For each extra-capacity strategy $\mathbf{E} = \left(\theta_i\right)$

**4.4.1.** For each combination $k = 1, 2, \ldots, 2^m - 1$

**4.4.1.1.** Solve the model (3.15)-(3.18), using the algorithm presented in Section 4, to determine the cost $T_k(\mathbf{E}) = Ct_k(\mathbf{E}) + B_k(\mathbf{E})$;

**4.4.2.** Calculate the expected cost $TB(\mathbf{P},\mathbf{G}_{\text{opt}},\mathbf{E})$ by using equation (3.27);

**4.4.3.** Calculate the defender utility $U_d(\mathbf{P},\mathbf{G}_{\text{opt}},\mathbf{E})$ by using equation (3.30);

**4.4.4.** If $-U_d(\mathbf{P},\mathbf{G}_{\text{opt}},\mathbf{E}) < U_{min}$ assign $U_{min} = -U_d(\mathbf{P},\mathbf{G}_{\text{opt}},\mathbf{E})$,

$$\mathbf{P}_{\text{opt}} = \mathbf{P} = \left(\pi_i^{opt}\right),\ \mathbf{F}_{\text{opt}} = \left(F_{i\pi_i^{opt}}\right),\ \mathbf{E}_{\text{opt}} = \mathbf{E} = \left(\theta_i^{\ opt}\right),$$

$$\mathbf{T_{opt}} = \mathbf{T} = \left(\tau_{i\theta_i}^{\ opt}\right).$$

The presented methodology presumes solving a large number of optimisation problems that are N-P hard. In general, this leads to enormous computational effort. One way to reduce the computational complexity of the algorithm is to use heuristics to reduce the number of N-P hard problems that need to be run to solve the game. Another possible way to reduce the computation time consists in using an efficient heuristic to solve each N-P hard problem. Finally, if different combinations of attack and defence can lead to the same subsets of disabled facilities, there is no need to calculate the same damage each time. Using all these techniques together should significantly reduce the complexity of the algorithm.

## 3.7 Illustrative example

In this section, a simple example is presented to illustrate the model. The defender's optimal strategy obtained is compared to some defence strategies. The issues of limited budgets and the influence of contest intensities are also discussed. The model is used to find the best trade-off between direct investments in protection and extra-capacities deployment.

### 3.7.1 Input data

We consider three facilities and five demand nodes. Table 3.3 presents the maximum capacity and the fixed costs of locating facilities. Table 3.4 provides the yearly demands, and Table 3.5 gives the unit costs of producing and shipping between facility sites and customer locations. We assume that the total capacity acquisition cost at facility location, $h_i(.)$, is a linear function. Table 3.6 gives the capacity acquisition cost at facility location per unit. We assume that the cost of the brand image of the company ($B_{img}$) is \$200,000.

When there is no attack, the optimal CFL & CAP solution for this instance is shown in Table 3.7 and pictured in Figure 3.1. This solution entails a fixed cost of \$6,300,000, a capacity acquisition cost of \$898,000 and a transportation cost of \$3,812,000 over one year.

**Table 3.3-** Maximum capacity and fixed cost of locating a facility at candidate site *i*.

| Site *i* | Fixed cost (in \$) | Maximum Capacity |
|---|---|---|
| 1 | 2100,000 | 45,000 |
| 2 | 2400,000 | 61,200 |
| 3 | 1800,000 | 38,700 |

**Table 3.4-** Demand per year at customer location.

| Customer location *j* | Demand |
|---|---|
| 1 | 25,000 |
| 2 | 21,000 |
| 3 | 13,000 |
| 4 | 11,000 |
| 5 | 10,500 |

**Table 3.5-** Unit cost (in $) of shipping from candidate facility site *i* to customer location *j*.

| | Site *i* | 1 | 2 | 3 |
|---|---|---|---|---|
| Customer location *j* | 1 | 48 | 62 | 72 |
| | 2 | 55 | 50 | 66 |
| | 3 | 60 | 44 | 52 |
| | 4 | 65 | 58 | 48 |
| | 5 | 70 | 65 | 44 |

**Table 3.6-** Capacity acquisition cost at facility location per unit.

| Site *i* | Cost (in $) per unit ($Ac_i$) |
|---|---|
| 1 | 11 |
| 2 | 12 |
| 3 | 10 |

**Table 3.7-** Optimal CFL & CAP solution.

| | Site *i* | 1 | 2 | 3 |
|---|---|---|---|---|
| Customer location *j* | 1 | 25,000 | 0 | 0 |
| | 2 | 0 | 21,000 | 0 |
| | 3 | 0 | 13,000 | 0 |
| | 4 | 0 | 0 | 11,000 |
| | 5 | 0 | 0 | 10,500 |
| Capacity acquired $C_i^*$ | | 25,000 | 34,000 | 21,500 |
| Cost (in $) of capacity acquired | | 275,000 | 408,000 | 215,000 |

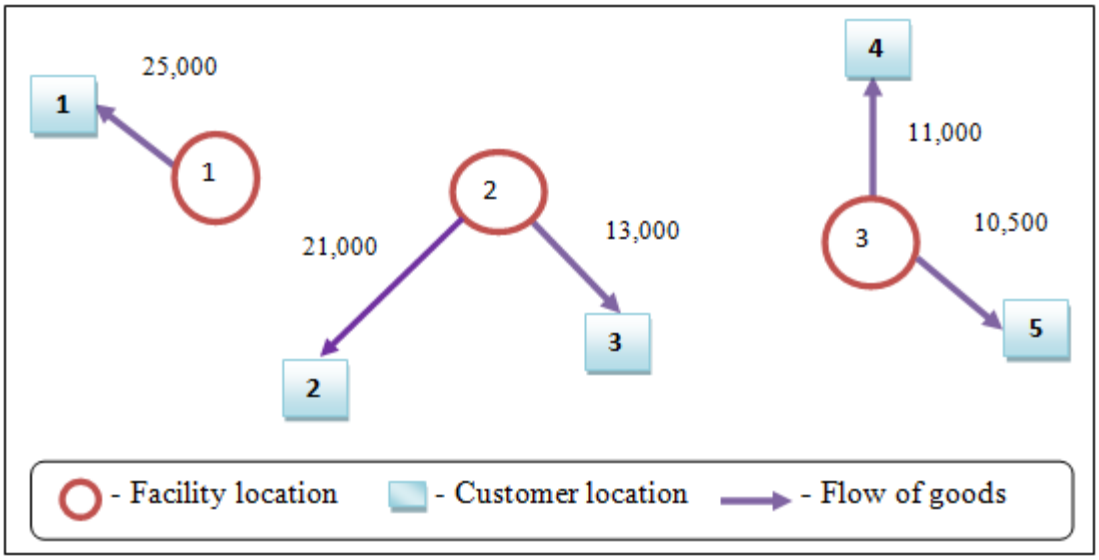


**Fig. 3.1-** The optimal CFL & CAP solution.

Table 3.8 provides the protection investment efforts $F_{ip}$, and the unit costs of protection efforts $f_{ip}$. Analogously, the attack investment efforts $Q_{ig}$ and the unit costs of attack efforts are given in Table 3.9. Table 3.10 presents the extra-capacity parameters. The restoration costs $R_i$ are given in Table 3.11, while the time to restore each disabled facility, at the given cost, is one week. We consider (except in Section 6.5) that all contest intensities are equal to 1, which means that the efforts have proportional impact on the vulnerability.

**Table 3.8-** Defence parameters.

| Protection types $p$ | Unit costs $f_{ip}$ | Protection efforts $F_{ip}$ |
|---|---|---|
| 1 | 70 | 100 |
| 2 | 555 | 280 |
| 3 | 200 | 130 |

**Table 3.9-** Attacker parameters.

| Attack types $m$ | Unit costs $q_{ig}$ | Attack efforts $Q_{ig}$ |
|---|---|---|
| 1 | 220 | 30 |
| 2 | 150 | 25 |
| 3 | 350 | 54 |

**Table 3.10-** Extra-capacity parameters.

| Extra-capacity options $e$ | Proportion of the capacity acquired $\tau_{ie}$ |
|---|---|
| 1 | 32% |
| 2 | 68% |
| 3 | 80% |

**Table 3.11-** Restoration costs of disabled facilities (in $).

| Disabled facility $i$ | Restoration costs $R_i$ |
|---|---|
| 1 | 16,000 |
| 2 | 18,000 |
| 3 | 11,000 |

### 3.7.2 Evaluation of the costs $Ct_k(\mathbf{E})$ and $B_k(\mathbf{E})$ for all combinations of disabled facilities

To illustrate the evaluation of the costs $Ct_k(\mathbf{E})$ and $B_k(\mathbf{E})$, let us consider the extra-capacity strategy $\mathbf{E}$ = (2 1 3). This means that the capacities $C_1^*$, $C_2^*$ and $C_3^*$ are extended by 68%, 32% and 80%, respectively (see Table 3.10), and the modified capacities are:

$MC_{12} = C_1^*(1+0.68) = 42{,}000$; $MC_{21} = C_2^*(1+0.32) = 44{,}880$; and

$MC_{33} = C_3^*(1+0.8) = 38{,}700$.

Table 3.12 presents the costs $Ct_k(\mathbf{E})$ and $B_k(\mathbf{E})$ for all possible combinations for $\mathbf{E}$ = (2 1 3). Since the restoration time is one week, each cost in Table 3.12 is evaluated for one week; the number of weeks during one year is considered equal to 52.

Let us illustrate the calculation of $Ct_k(\mathbf{E})$ for $k$=1 and $\mathbf{E}$ = (2 1 3). If facility 1 is disabled by an attack, there is no backorder ($B_k(\mathbf{E})$ = 0 since the total capacity is larger than the total demand). However, the quantity shipped from disabled facility 1 to customers is assigned to functional facilities 2 and 3. By solving the model (3.19)-(3.22), the transportation cost is evaluated under the considered situation (facility 1 disabled and extra-capacity options 1 and 3 for facilities 2 and 3). Fig. 3.2 shows the new optimal solution. Recall that $Ct_k(\mathbf{E})$ is the cost incurred because of the change in transportation cost when the extra-capacity

strategy is **E** and the combination is $S_k$, *i.e.* the cost under combination $S_k$ minus the cost in a normal situation. Since the restoration time is one week, each cost $Ct_k$ is evaluated as the change in transportation cost during this week. The cost $Ct_1(\mathbf{E})$ is given by the cost under combination $S_1$ (for **E** = (2 1 3)) minus the cost in a normal situation during one week. That is, $Ct_1(\mathbf{E})$ is (\$4,277,200-\$3,812,000)/52, which is equal to \$8,946. Recall here that 52 is the number of weeks during one year.

**Table 3.12-** The costs $T_k(\mathbf{E})$ (in \$) for all possible combinations $S_k$ per week for **E** = (2 1 3).

| $k$ | Disabled facilities | **E** = (2 1 3) | | |
|---|---|---|---|---|
| | | $B_k(\mathbf{E})$ | $Ct_k(\mathbf{E})$ | $T_k(\mathbf{E})$ |
| 1 | 1 | 0 | 8,946 | 8,946 |
| 2 | 2 | 0 | 4,865 | 4,865 |
| 3 | 3 | 0 | 7,377 | 7,377 |
| 4 | 1, 2 | 211,508 | -35,938 | 175,57 |
| 5 | 1, 3 | 209,807 | -29,980 | 179,827 |
| 6 | 2, 3 | 210,600 | -32,250 | 178,35 |
| 7 | 1, 2, 3 | 222,163 | -73,308 | 148,855 |

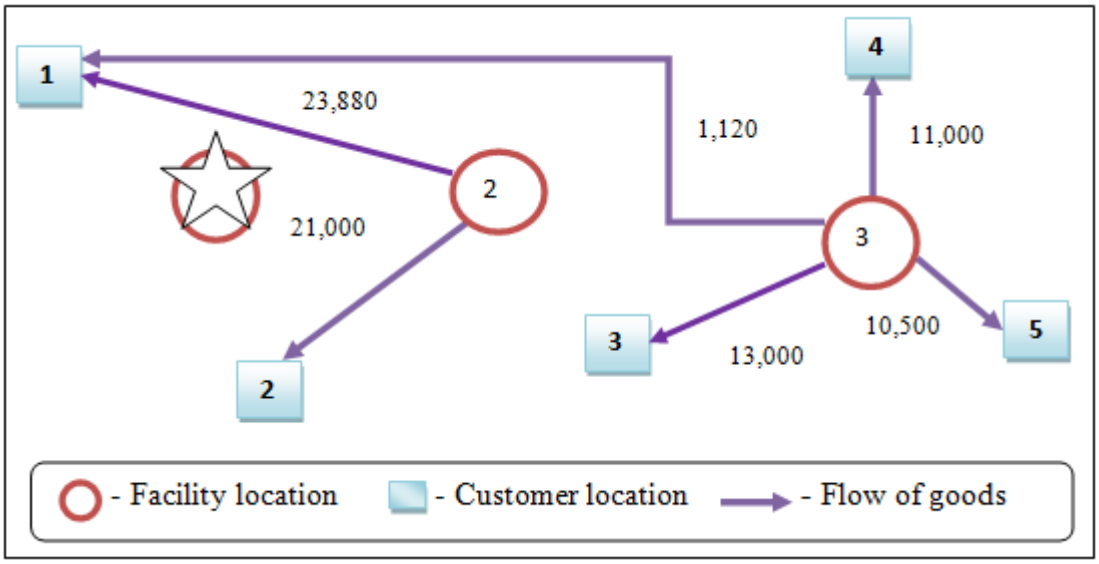


**Fig. 3.2-** The Optimal solution if facility 1 is disabled and the extra-capacity option is **E** = (2 1 3).

### 3.7.3 Determination of the optimal attack strategy

The attacker strategy that maximises his utility by applying step 3 of the algorithm (*i.e*, the second period of the game is solved first) is $\mathbf{G}_{opt}$ = (3 3 1). This means that facilities 1 and 2 are disabled using type 3 attacks; and facility 3 is disabled using type 1 attack. The maximum loss is \$1109,778 and the corresponding attacker utility is $U_{max}$ = \$ 1065,378.

### 3.7.4 Determination of the optimal defender strategy

By applying step 4 of the algorithm and to find the equilibrium, taking into account the attacker strategy above (where the attacker maximises his utility), the first period of the game is solved in order to maximise the defender utility, and consequently to allocate optimally the protective resources and extra-capacity among the facilities. The obtained solution corresponds to the following strategy:

- $\mathbf{P}_{opt}$ = (3 1 3): this means that facilities 1 and 3 are protected using type 3 protections; and facility 2 is protected using type 1 protection; and
- $\mathbf{E}_{opt}$ = (2 1 3): this means that the extra-capacities are 68%, 32% and 80% for facilities 1, 2 and 3 (respectively). The total cost of extra-capacity is \$489,560.

The loss is \$358,901 and the corresponding defender utility is $U_{min}$ = \$907,461.

### 3.7.5 The optimal defender and attacker strategy as a function of the contest intensity

Figs. 3.3 and 3.4 show graphically the defender and attacker utility as a function of the contest intensity, when the defence and the attack budgets are both limited. Two pairs of defence and attack budgets are considered. We remark that when the attacker's budget is relatively low (case of Fig. 3.3), the defender benefits from the greatest contest intensity. However, when the attacker's budget is high (case of Fig. 3.4), the defender benefits instead from the lowest contest intensity.

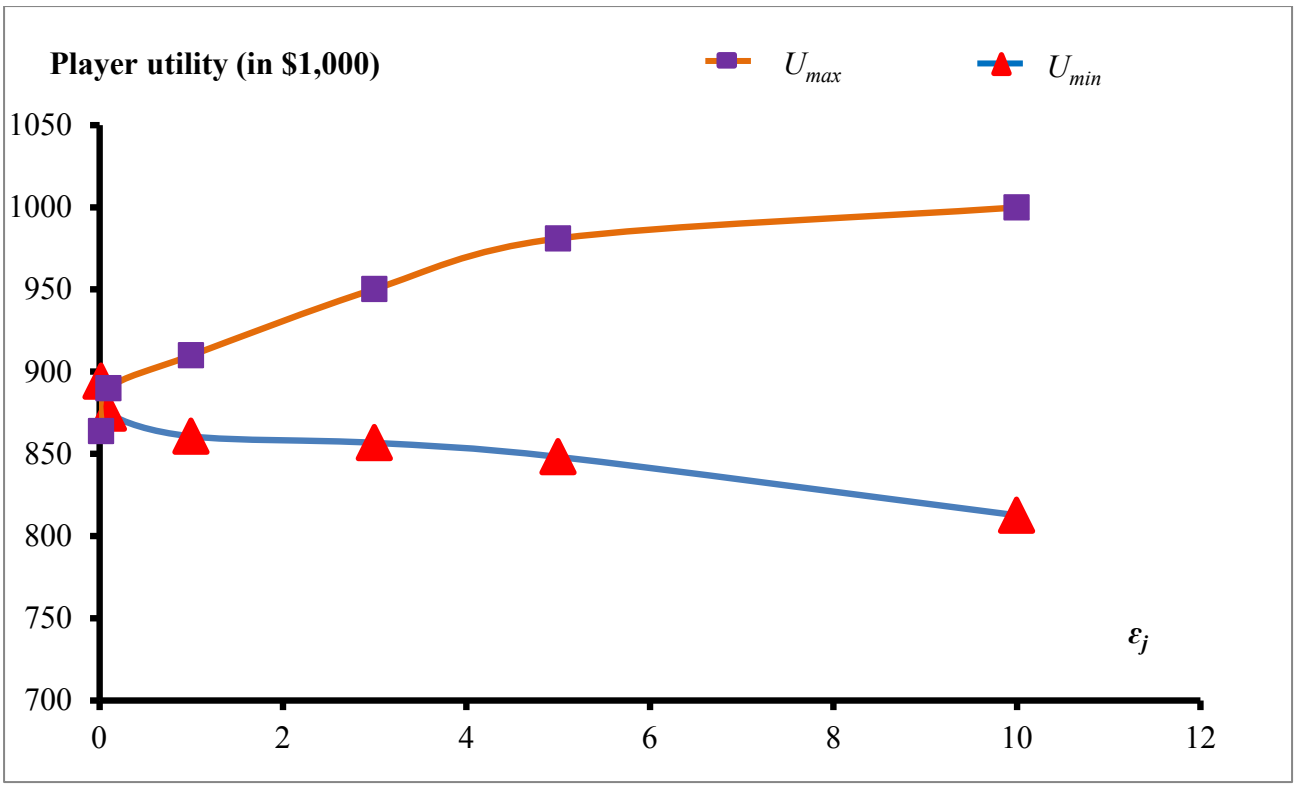


**Fig. 3.3-** Defender utility as a function of the contest intensity, when the defence budget is $600,000 and the attack budget is $12,000.

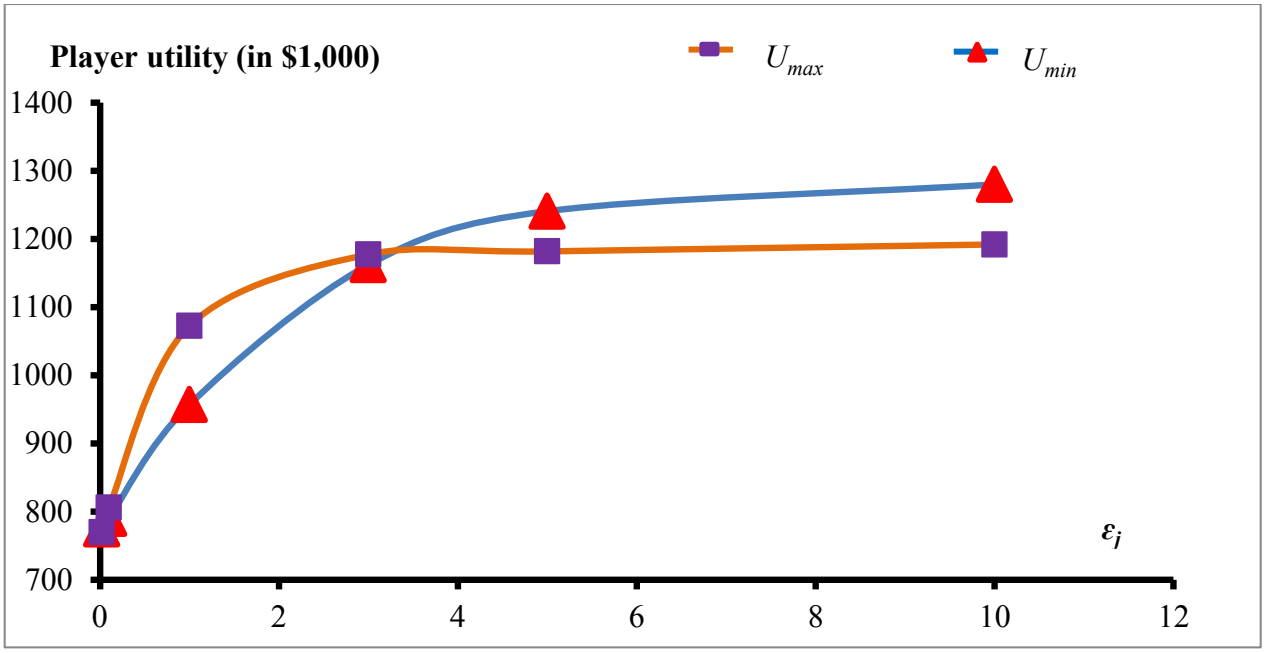


**Fig. 3.4-** Defender utility as a function of the contest intensity, when the defence budget is $600,000 and the attack budget is $56,700.

### 3.7.6 Comparison

We compare the defender optimal strategy obtained by our model to some defence strategies. The objective is to measure, for the example above, how much our method is better than others, when the attacker tries to maximise his utility. To define strategies that could be used in practice, we rank the facilities, the protection types, and the extra-capacity options. A facility with higher fixed cost has higher rank; from Table 3.3, the ranking is then: Fac2, Fac1 and Fac3. On the other hand, the protection types are ranked according to their investment expenditures as follows (see Table 3.8): 2, 3, 1. Also, the extra-capacity options are ranked according to their investment expenditures as follows: 3, 2, 1 (see Table 3.10). The strategies considered in this comparison are as follows:

- *Strategy 1: Protection of all facilities by the most expensive protection type and the highest extra-capacities available*

  In this strategy, we consider that each facility is protected using type 2 protection and the highest extra-capacity available. That is, the protection strategy corresponds to **P** = (2 2 2) and the extra-capacity strategy corresponds to **E** = (3 3 3). The corresponding defender utility is $U_{min}$ = $1253,978.

- *Strategy 2: Protection of all facilities by the most expensive protection types and the lowest extra-capacities available*

  We consider that each facility is protected using type 2 protection and the lowest extra-capacity available. That is, the protection strategy corresponds to **P** = (2 2 2) and the extra-capacity strategy corresponds to **E** = (1 1 1). The corresponding defender utility is $U_{min}$ = \$1409,814.

- *Strategy 3: Protection of all facilities by the cheapest protection types and the highest extra-capacities available*

  We consider here that all facilities are protected using type 1 protections and using the lowest extra-capacities. That is, the protection strategy corresponds to **P** = (1 1 1) and the extra-capacity strategy corresponds to **E** = (3 3 3). The corresponding defender utility is $U_{min}$ = \$1222,057.

- *Strategy 4: Protection of all facilities by the cheapest protection types and the lowest extra-capacities available*

  We consider that all facilities are protected using type 1 protections and using the lowest extra-capacities available. That is, the protection strategy corresponds to **P** = (1 1 1) and the extra-capacity strategy corresponds to **E** = (1 1 1). The corresponding defender utility is $U_{min}$ = \$1471,266.

- *Strategy 5: Facilities with higher fixed costs are protected by more expensive protection types and using lower extra-capacities*

  Facility 1 is protected using type 3 protection and using extra-capacity option 2; Facility 2 is protected using type 2 protection and extra-capacity option 1; and Facility 3 is protected using type 1 protection and extra-capacity option 3. That is, the protection strategy corresponds to **P** = (3 2 1) and the extra-capacity strategy corresponds to **E** = (2 1 3). The corresponding defender utility is $U_{min}$ = \$1020,337.

- *Strategy 6: Facilities with higher fixed costs are protected by more expensive protection types and using higher extra-capacities*

  Facility 1 is protected using type 3 protection and using extra-capacity option 2; Facility 2 is protected using type 2 protection and extra-capacity option 3; and Facility 3 is protected using type 1 protection and extra-capacity option 1. That is, the protection strategy corresponds to **P** = (3 2 1) and the extra-capacity strategy corresponds to **E** = (2 3 1). The corresponding defender utility is $U_{min}$ = \$1277,042.

The obtained results indicate that the defender strategy obtained by our model is:

- 31% better than Strategy 1;
- 47% better than Strategy 2;
- 28 % better than Strategy 3;
- 54% better than Strategy 4;
- 6.57% better than Strategy 5; and
- 33% better than Strategy 6.

Our model gives better results as it is designed to find the best trade-off between direct protection investment and extra-capacity deployment, unlike the above strategies.

The first three strategies are characterised by a 'fearful' attitude of the defender who is 'risk averse' in the sense that she (he) prefers to use one of the most expensive protection types and/or extra-capacities for all facilities.

In contrast, Strategy 4 corresponds to an 'inapprehensive' behaviour (as the defender prefers to use the least expensive protection types and extra-capacities for all facilities).

From the above results, we remark that for the considered numerical example, the 'risk averse' strategies 1, 2 and 3 are better than the 'inapprehensive' strategy 4.

Strategies 5 and 6 are more 'rational' than the others, in the sense that they take into account the fixed costs of facilities in the defence allocation. However, as the costs of extra-capacities are much higher than the direct protection costs in our numerical example, strategy 5 gives the best results, but less than the strategy resulting from our game-theoretical model.

### 3.7.7 Limited budget

Here, we solve the defence strategy optimisation problem for a limited defender's budget. Table 13 presents the best trade-off between extra-capacity options and protection strategies for different budgets. We remark from this table that for a lower defence budget, the expected damage is indeed higher. The relationship between the investment sizes and the effect on facilities protection provides important managerial information for decision makers. In fact, for each increase in the defence budget, it is important to quantify the resulting reduction in the expected damage, in order to decide if it is worth investing more in protecting facilities and using extra-capacities.

**Table 3.13-** Obtained defence and extra-capacity strategies for different budgets ($\varepsilon_j = 1$).

| Defender budget (in $) | Protection cost (in $) | Extra capacity Cost (in $) | Expected damage (in $) | Defender utility $U_{min}$ (in $) | Defence strategy $\mathbf{P}_{opt}$ | Extra-capacity strategy $\mathbf{E}_{opt}$ |
|---|---|---|---|---|---|---|
| 25,000 | 21,000 | 0 | 1109,778 | 1130,779 | ( 1 1 1 ) | ( 0 0 0 ) |
| 50,000 | 40,000 | 0 | 1063,494 | 1103,494 | ( 1 3 1 ) | ( 0 0 0 ) |
| 100,000 | 59,000 | 0 | 988,397 | 1047,397 | ( 3 1 3 ) | ( 0 0 0 ) |
| 400,000 | 59,000 | 326,400 | 580,225 | 965,625 | ( 3 3 1 ) | ( 0 3 0 ) |
| 450,000 | 78,000 | 326,400 | 529,330 | 933,730 | ( 3 3 3 ) | ( 0 3 0 ) |
| 550,000 | 207,400 | 326,400 | 389,699 | 923,499 | ( 3 2 3 ) | ( 0 3 0 ) |
| 650,000 | 59,000 | 489,560 | 358,901 | 907,461 | ( 3 1 3 ) | ( 2 1 3 ) |
| 800,000 | 78,000 | 718,400 | 344,495 | 1140,896 | ( 3 3 3 ) | ( 3 3 3 ) |
| 860,000 | 207,400 | 643,640 | 268,814 | 1194,614 | ( 3 2 3 ) | ( 3 3 3 ) |
| 1184,600 | 466,200 | 718,400 | 144,139 | 1328,739 | ( 2 2 2 ) | ( 3 3 3 ) |

The expected damage cost as a function of the defence budget (*i.e*, budget for direct protection and extra-capacity deployment) is presented in Figure 3.5. Also, the defender's expected utility as a function of the defence budget is presented in Figure 3.6. These curves are drawn by evaluating the optimal protection and extra-capacity strategy for each budget, considering that the attacker chooses the harmful strategy. These curves show graphically the relationship between the investment sizes and the effect on facilities protection. From these curves, one can see that the budget greater than $650,000 makes no sense for the

given set of available protections, since additional investment cannot reduce the expected utility. We can distinguish between three regions in Figs. 3.5 and 3.6:

- In region 1 (budgets less than $550,000), the damage reduction is higher than in regions 2 and 3 (see Fig. 3.5). The contribution (in reducing the damage) of the budget increase is in fact higher for these lower budgets. The expected utility is also reduced by additional defence investment. This means that the additional defence investment is worthwhile since it is compensated for by the expected damage reduction.
- For budgets higher than $800,000 (region 3), a damage reduction is observed again but a magnitude that is lower than in region 1. However, the expected utility increases as the budget increases. This is explained by the fact that even if there is a reduction in the expected damage, the additional defence investment is too high (since the overall utility is the sum of the damage and the defence investment).
- When the budget is between $550,000 and $800,000 (region 2), the expected damage remains nearly constant (Fig. 3.5). The optimal defender utility is situated in region 2 (Fig. 3.6) with a budget of $650,000. After this point, the contribution of the additional defence investment in reducing the damage is less than the cost incurred by this investment. Consequently, the additional defence investment is not worthwhile since it is compensated for by the expected damage reduction.

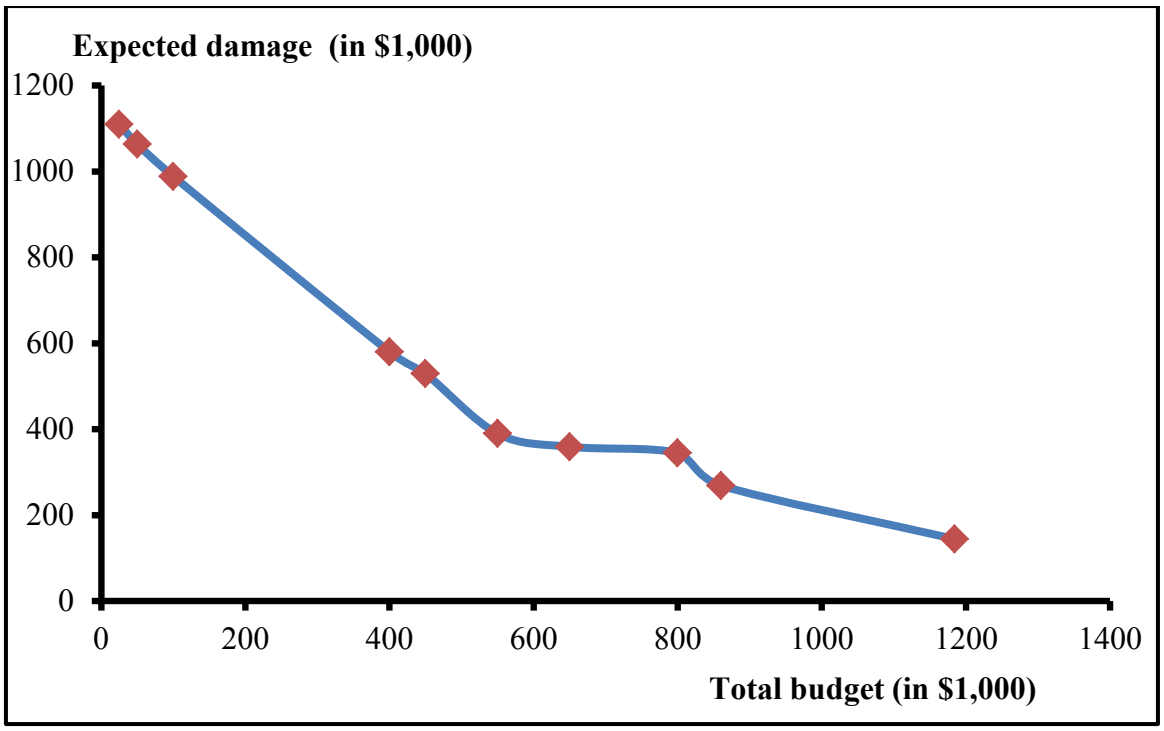


**Fig. 3.5-** Expected damage cost as a function of the defence budget ($\varepsilon_j = 1$).

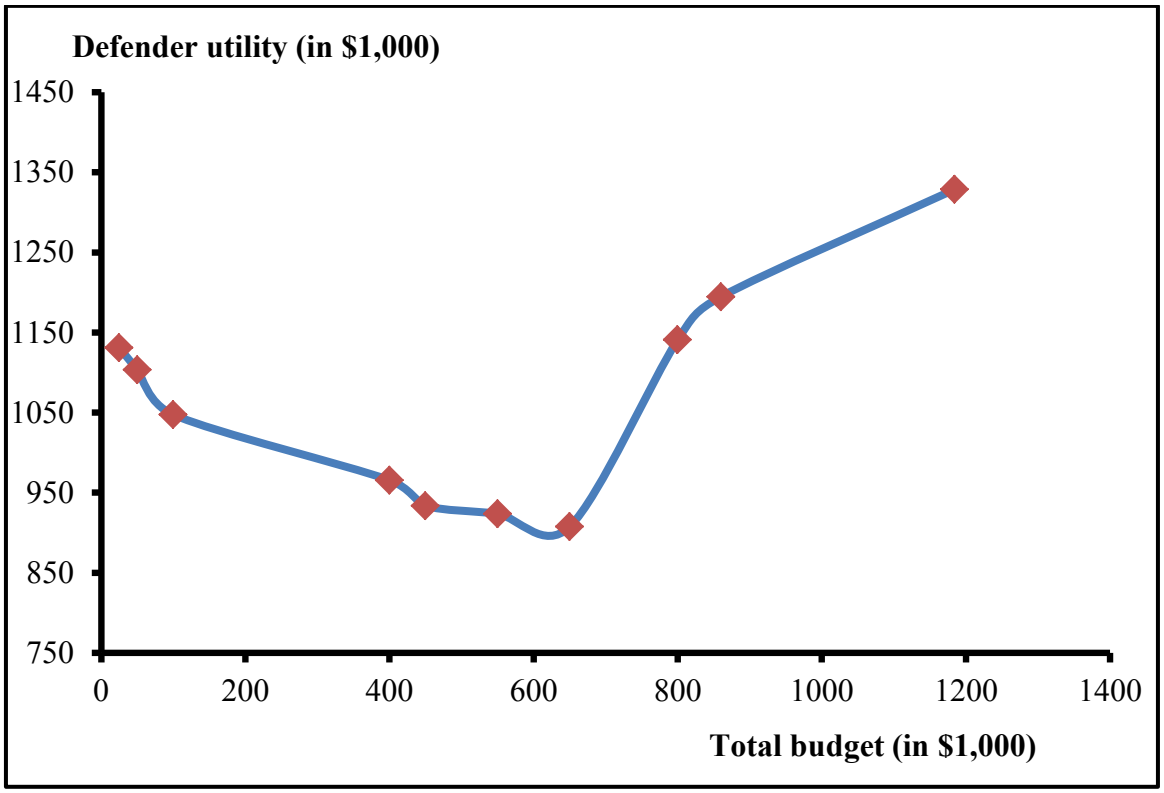


**Fig. 3.6-** Defender expected utility as a function of the defence budget ($\varepsilon_j = 1$).

## 3.8 Conclusion

This article deals with the protection of supply network in the context of the *capacitated* fixed-charge location and capacity acquisition problem. Facility location and capacity acquisition are of vital importance for supply chain management. We consider that not only a set of investment alternatives are available for direct protection of facilities, but also extra-capacities of neighbouring functional facilities can be used after attacks for indirect protection. The strategic decision dealt with is how to allocate optimally the protective resources and the extra-capacity among the facilities, knowing that these facilities are exposed to external intentional attacks. The idea of using extra-capacity to indirectly protect supply networks against intentional attack is then used to develop a game-theoretic model, with the objective of finding the best trade-off between direct investments in protection and indirect protection by extra-capacities deployment. In this model, a non-cooperative two-period game is analysed. The attacker tries to maximise, in the second period, his utility function by maximising the expected damage with several alternatives of attack. On the other hand, the defender attempts to minimise, in the first period, the expected damage caused by attacks with several alternatives of facilities protection and extra-capacity options and consequently to maximise his utility function, where resources for direct protection and extra-capacities are limited. A method is developed to evaluate the utilities of the players. The expected costs evaluated by our method include the cost incurred because of the change in transportation cost after attacks, the cost necessary to restore disabled facilities and the backorder cost. An algorithm is presented for determining the equilibrium solution and the optimal defender strategy. The defence strategy obtained by our model is compared to six strategies, and the obtained results indicate clearly the superiority of our model in finding the best trade-off between direct protection investment and extra-capacity deployment. The developed approach gives important managerial insights for the protection of located facilities under capacity constraints, while using extra-capacity options for protection purposes.

Facility location decisions are long-term strategic decisions that are usually fixed and hard to change even in the intermediate term. Inefficient locations will result in excess costs

being incurred throughout the lifetime of these facilities. Protection decisions are also long-term strategic decisions that are usually fixed. However, they can be revised more frequently than location decisions. Because of this, we did not merge facility location decisions with facility protection decisions in the same model. The defender may rather locate the facilities; then, she (he) protects these facilities against anticipated threats using the game-theoretic model developed in this paper. The result is that our model advantageously covers the case of already existing facilities that may need to be protected or fortified. However, this model cannot deal with the situation where the designer needs to take into account the protection requirements when locating the facilities (*i.e.*, to make location and protection decisions simultaneously. We are currently working on the general problem of optimal facility location (including extra capacity) and protection minimising the total expected cost. We are also working on the modelling and analysis of interdependencies between facilities while considering multi-echelon supply chain networks.

**References**


[1] Hausken K. Strategic Defence and Attack of Complex Networks. International Journal of Performability Engineering 2009;5(1):13–30.

[2] Levitin G, Gertsbakh I, Shpungin Y. Evaluating the damage associated with intentional supply deprivation in multi-commodity network. Reliability Engineering and System Safety 2013; 119:11–17.

[3] Albert R, Barabasi AL. Statistical Mechanics of Complex Networks, Reviews of Modern Physics 2002;74:47–97.

[4] Patterson SA, Apostolakis GE. Identification of Critical Locations Across Multiple Infrastructures for Terrorist Actions. Reliability Engineering and System Safety 2007;92 (9):1183–1203.

[5] Colbourn CJ. The Combinatorics of Network Reliability. New York: Oxford University Press; 1987.

[6] Bricha N, Nourelfath M. Critical supply networks protection against intentional attacks: a game-theoretical model. Reliability Engineering and System Safety 2013;119:1–10.

[7] Rajagopalan S, Andreas CS. Capacity Acquisition and Disposal with Discrete Facility Sizes. Management Science 1994;40(7):903–917.

[8] Verter V, Dincer C. An Integrated Evaluation of Facility Location, Capacity Acquisition and Technology Selection for Designing Global Manufacturing Strategies. European Journal of Operational Research 1992;60(1):1–18.

[9] Verter V, Dincer C. Facility location and capacity acquisition: an integrated approach. Nav Res Logist 1995;42:1141–1160.

[10] Dasci A, Laporte G. An Analytical Approach to the Facility Location and Capacity Acquisition Problem under Demand Uncertainty. Journal of the Operational Research Society 2005;56: 397–405.

[11] Li S, Tirupati D. Dynamic capacity expansion problem with multiple products: Techology selection and timing of capacity expansion. Operations Research 1994;42(5):958–976.

[12] Shulman A. An Algorithm for Solving Dynamic Capacitated Plant Location Problems with Discrete Expansion Sizes. Operations Research 1991;39:423–436.

[13] Venables H, Moscardini A. Ant Based Heuristics for the Capacitated Fixed Charge Location Problem. Ant Colony Optimization and Swarm Intelligence, lecture Notes in Computer Science 2008;5217: 235–242.

[14] Chan F, Wang Z, Zhang J. A two-level hedging point policy for controlling a manufacturing system with time-delay, demand uncertainty and extra capacity. European Journal of Operational Research 2007;176(3):1528–1558.

[15] David SW, Erkoc M, Karabuk S. Managing capacity in the high-tech industry: a review of literature. The engineering economist, Institute of Industrial Engineers 2005;50:125–158.

[16] Garey M, Johnson D. Computers and Intractability. A Guide to the Theory of NP-Completeness. Freemann, San Francisco; 1979.

[17] Hausken K. Production and Conflict Models versus Rent-Seeking Models, Public Choice, Springer 2005;123(1):59–93.

[18] Hausken K, Levitin G. Minmax defence strategy for complex multi-state systems. Reliability Engineering and System Safety 2009;94(2):577–587.

[19] Nitzan S. Modelling rent-seeking contests. European Journal of Political Economy 1994;10(1):41–60.

[20] Tullock G. Efficient rent seeking. In: Buchanan JM, Tollison RD, Tullock G, editors. Toward a theory of the rent-seeking society. College Station, TX: Texas A & M University Press; 1980. p. 97–112.

[21] Levitin G, Hausken K. Redundancy vs. Protection vs. False Targets for Systems under Attack. IEEE Transactions on Reliability 2009;58(1):58–68.

[22] Skaperdas S. Contest success functions. Econ Theory 1996;7(2):283–290.

[23] Hausken K. Protecting complex infrastructures against multiple strategic attackers. International Journal of Systems Science 2011;42(1):11–29.

[24] Bier VM, Hausken K. Defending and attacking a network of two arcs subject to traffic congestion. Reliability Engineering and System Safety 2013;112: 214-224.

[25] Azaiez N, Bier VM. Optimal resource allocation for security in reliability systems. European Journal of Operational Research 2007;181:773–86.

[26] Levitin G, Hausken K. Redundancy vs. protection in defending parallel systems against unintentional and intentional impacts. IEEE Transactions on Reliability 2009;58(4):679–690.

[27] Ramirez-Marquez JE, Rocco CM, Levitin G. Optimal network protection against diverse interdictor strategies. Reliability Engineering and System Safety 2011;96:374-382.

[28] Rocco CM, Ramirez-Marquez JE. Identification of top contributors to system vulnerability via an ordinal optimization based method. Reliability Engineering and System Safety 2013;114: 92-98.

[29] Scaparra M, Church R. A bilevel mixed-integer program for critical infrastructure protection planning. Computers and Operations Research 2008;35(6): 1905–23.

[30] Snyder LV. Facility location under uncertainty: a review. IIE Transactions 2006;38(7):547–64.

[31] Levitin G, Hausken K. Protection vs. redundancy in homogeneous parallel systems. Reliability Engineering and System Safety 2008;93(10):1444–1451.

# Chapitre 4

# Protection of warehouses and plants under capacity constraint

L'article intitulé «**Protection of warehouses and plants under capacity constraint**» est inséré dans ce chapitre. Il a été acceptée (avec modifications mineures) pour publication dans le journal « *Reliability Engineering and System Safety* ». Il a été révisé suite aux recommandations des évaluateurs et il est présentement soumis pour approbation finale. La version présentée dans cette thèse est identique à la dernière version révisée et resoumise.

# Résumé

Les entrepôts permettent de réduire les coûts de transport, la distance et le temps de réponse aux clients. L'efficacité d'un réseau d'approvisionnement est déterminée par le bon fonctionnement des entrepôts. Malgré le rôle important de ces entrepôts, on ne donne pas beaucoup d'importance à leurs protections. Leurs indisponibilités peuvent avoir un impact considérable sur la performance du réseau d'approvisionnement. Pour cela, les entrepôts doivent être protégés de la même manière que les usines contre les menaces telles que les attaques intentionnelles. Cet article présente une méthode de protection des usines et des entrepôts contre les attaques intentionnelles dans le contexte de localisation d'usines et d'entrepôts à capacités limitées. Un jeu non coopératif à deux périodes entre le défenseur et l'attaquant est développé pour trouver la solution d'équilibre et la stratégie optimale de défense sous contraintes de la capacité. Le défendeur investit à la première période afin de minimiser les dégâts attendus que l'attaquant pourrait causer à la seconde période. La capacité supplémentaire des usines et des entrepôts en fonctionnement est utilisée après les attaques, afin de satisfaire toutes les demandes des clients et d'éviter les pénalités de retard. La fonction de succès de compétition est utilisée pour évaluer la probabilité de succès d'attaque des usines et des entrepôts. Un exemple numérique est présenté pour illustrer l'application du modèle. La stratégie optimale de défense obtenue par notre modèle est comparée à d'autres cas où les entrepôts sont moins protégés que les usines. Cette comparaison nous permet de mesurer, à quel point notre méthode est meilleure, et illustre l'effet d'investissements directs dans la protection et indirects par la capacité supplémentaire des entrepôts pour réduire le dommage encouru.

## 4.1 Abstract

Warehouses allow transportation costs reduction, distances reduction and response time reduction to clients. The efficiency and effectiveness in any supply network is largely determined by the good operation of the warehouses. While warehouses may be less properly protected, their unavailability may have substantial impact on the supply chain performance. For this, the warehouses must be protected in the same way as plants against threats such as intentional attacks. This paper presents a method for protection of plants and

warehouses against intentional attacks in the context of the capacitated plant and warehouses location and capacity acquisition problem. A non-cooperative two-period game between the defender and the attacker is developed to find the equilibrium solution and the optimal defender strategy under capacity constraints. The defender invests in the first period to minimize the expected damage and the attacker moves in the second period to maximize the expected damage. Extra-capacity of neighboring functional plants and warehouses is used after attacks, in order to satisfy all customers demand and to avoid the backorders. The contest success function is used to evaluate success probability of an attack of plants and warehouses. A numerical example is presented to illustrate an application of the model. The defender strategy obtained by our model is compared to the case where warehouses are subjected to less protection effort than the plants. This comparison allows us to measure, how much our method is better, and illustrates the effect of direct investments in protection and indirect protection by warehouse extra-capacities to reduce the expected damage.
*Key words:* Protection, Warehouse, Game theory, Capacity, Attack, Damage, Defense.

**Nomenclature**

| | |
|---|---|
| $n_p$ | number of plants in the system |
| $n_w$ | number of warehouses in the system |
| $n_k$ | number of customers in the system |
| $\beta$ | index that refers to plant or warehouse, $\beta = 1, 2, \ldots, n_p+n_w$ |
| $i$ | $i$th potential plant location, $i = 1, 2,\ldots, n_p$ |
| $j$ | $j$th potential warehouse location, $j = n_p+1, n_p+2,\ldots, n_p+n_w$ |
| $k$ | $j$th demand location, $k=1,2,..., n_k$ |
| $I$ | the set of candidate plant locations, indexed by $i$ |
| $J$ | the set of candidate warehouse locations, indexed by $j$ |
| $K$ | the set of customer locations, indexed by $k$ |
| $D_k$ | the demand at customer location $k \in K$ |
| $h_i$ | the total capacity acquisition cost function at plant $i \in I$ |
| $g_j$ | the total capacity acquisition cost function at warehouse $j \in J$ |
| $CP_i$ | the fixed cost of locating a plant at candidate site $i \in I$ |

| | |
|---|---|
| $CW_j$ | the fixed cost of locating a warehouse at candidate site $j \in J$ |
| $CAP_i$ | the maximum capacity that can be built-in at plant at candidate site $i \in I$ |
| $CAP_j$ | the maximum capacity that can be built-in at warehouse at candidate site $j \in J$ |
| $Uc_{ij}$ | the cost of producing and shipping one unit from candidate plant site $i \in I$, to candidate warehouse site $j \in J$ |
| $Uc_{jk}$ | the cost of shipping one unit from candidate warehouse site $j \in J$ to customer location $k \in K$ |
| $X_i$ | 1 if a plant is to be located at candidate site *i,* and 0 otherwise |
| $Y_j$ | 1 if a warehouse is to be located at candidate site *j*, and 0 otherwise |
| $\psi_{ij}$ | the quantity shipped from candidate plant site $i \in I$, to candidate warehouse site $j \in J$ |
| $Z_{jk}$ | the quantity shipped from candidate warehouse site $j \in J$ to customer location $k \in K$ |
| $\delta_\beta$ | number of protection types for facility $\beta$ |
| $p$ | index of protection type, $p = 1, 2, \ldots, \delta_\beta$ |
| $F_p$ | investment effort to protect a facility located at site $\beta$ using protection type $p$ |
| $f_{ip}$ | unit cost of effort to protect a facility located at site $\beta$ using protection type $p$ |
| $\overline{F_{ip}}$ | investment expenditure to protect a facility located at site $\beta$ using protection type $p$ |
| $\pi_\beta$ | value from $p = 1, 2, \ldots, \delta_\beta$ |
| $\pi_\beta^{opt}$ | optimal defence strategy value from $p = 1, 2, \ldots, \delta_\beta$ |
| **P** | vector of protection strategy, $\mathbf{P}=\left(\pi_\beta\right)$ |
| $\mathbf{P}_{\text{opt}}$ | vector of the optimal protection strategy, $\mathbf{P}_{\text{opt}} = \left(\pi_\beta^{opt}\right)$ |
| **F** | vector of investments to protection strategy **P,** $\mathbf{F}= \left(F_{\beta\pi_\beta}\right)$ |
| $\mathbf{F}_{\text{opt}}$ | vector of investments to protection strategy $\mathbf{P}_{\text{opt}}$, $\mathbf{F}_{\text{opt}} = \left( F_{\beta\pi_\beta^{opt}} \right)$ |

| | |
|---|---|
| $F_{\beta\pi_\beta}$ | element of investments vector **F** |
| $F_{\beta\pi_\beta^{opt}}$ | element of investments vector $\mathbf{F}_{\text{opt}}$ |
| $\lambda_{\beta p}$ | binary variable which is equal to 1 if a protection of type $p$ is used for facility $\beta$ |
| $\boldsymbol{\lambda}$ | matrix, $\boldsymbol{\lambda} = (\lambda_{\beta p})$ |
| $\rho_\beta$ | number of extra-capacity options for each facility $\beta$ |
| $e$ | index of extra-capacity options, $e = 1, 2, \ldots, \rho_\beta$ |
| $\tau_{\beta e}$ | proportion of the acquired capacity associated with the facility located at site $i$ using extra- capacity option $e$ |
| $C_\beta^*$ | capacity acquired associated with the facility located at site $\beta$ |
| $Ac_\beta$ | capacity acquisition cost at facility location $\beta$ per unit |
| $CE_{\beta e}$ | investment of extra-capacity associated with the facility located at site $\beta$ using extra-capacity option $e$, $CE_{\beta e} = Ac_\beta \tau_{\beta e} C_\beta^*$ |
| **E** | vector of extra-capacity strategy, $\mathbf{E} = \left(\theta_\beta\right)$ |
| $\theta_\beta$ | values from $e = 0, 1, \ldots, \rho_\beta$ |
| **T** | vector of investments to each extra-capacity strategy **E**, $\mathbf{T} = \left(\tau_{\beta\theta_\beta}\right)$ |
| $\xi_{\beta e}$ | binary variable which is equal to 1 if an extra-capacity option $e$ is selected for facility $\beta$ |
| $\alpha_i$ | number of attack types against any facility $\beta$ |
| $g$ | index of attack type ($g = 0, 1, 2, \ldots, \alpha_\beta$) |
| $Q_{ig}$ | attack effort to attack facility located at site $i$ using attack action $g$ |
| $q_{ig}$ | unit cost to attack facility located at site $i$ using attack action $g$ |
| $\overline{Q_{\beta g}}$ | investment expenditure to attack facility located at site $\beta$ using attack action $g$ |
| $\omega_\beta$ | value from $g = 1, 2, \ldots, \alpha_\beta$ |

| | |
|---|---|
| $\omega_\beta^{opt}$ | value from $g$ of the optimal attack strategy |
| $\mu_{\beta g}$ | binary variable which is equal to 1 if a type $g$ attack is used for facility $\beta$ |
| $\boldsymbol{\mu}$ | matrix, $\boldsymbol{\mu} = \left(\mu_{\beta g}\right)$ |
| $\boldsymbol{\mu}_{\text{opt}}$ | matrix, $\boldsymbol{\mu}_{\text{opt}} = \left(\mu_{\beta g}\right)$ |
| $f_1$ | the defender production function, $f_1\left(\overline{F_{\beta p}}\right) = F_{\beta p} = \frac{1}{f_{\beta p}}\overline{F_{\beta p}}$ |
| $f_2$ | the attacker production function, $f_2\left(\overline{Q_{\beta g}}\right) = Q_{\beta p} = \frac{1}{q_{\beta p}}\overline{Q_{\beta g}}$ |
| $D_B$ | defender budget |
| $AT_B$ | attacker budget |
| $\mathbf{G}$ | vector of attack strategy, $\mathbf{G}=\left(\omega_\beta\right)$ |
| $\mathbf{G}_{\text{opt}}$ | vector of the optimal attack strategy, $\mathbf{G}_{\text{opt}}= \left(\omega_\beta^{opt}\right)$ |
| $\mathbf{Q}_{\text{opt}}$ | vector of attack effort of the optimal attack strategy, $\mathbf{Q}_{\text{opt}} = \left( Q_{\beta\omega_\beta^{opt}} \right)$ |
| $Q_{\beta\omega_\beta^{opt}}$ | element of attack effort vector $\mathbf{Q}_{\text{opt}}$ |
| $\nu_{pg}(\beta)$ | destruction probability of a facility $\beta$ |
| $\nu_{p\omega_\beta^{opt}}(\beta)$ | destruction probability of a facility $\beta$ for the optimal defence strategy |
| $\boldsymbol{\nu}(\mathbf{P},\mathbf{G})$ | matrix, $\boldsymbol{\nu}(\mathbf{P},\mathbf{G}) = \left(\nu_{pg}(\beta)\right)$ |
| $\boldsymbol{\nu}(\mathbf{P},\mathbf{G}_{\text{opt}})$ | matrix, $\boldsymbol{\nu}(\mathbf{P},\mathbf{G}_{\text{opt}}) = \left( \nu_{p\omega_\beta^{opt}}(\beta) \right)$ |
| $\varepsilon_\beta$ | parameter that expresses the intensity of the contest concerning facility $\beta$ |
| $R_\beta$ | the cost required to restore the attacked facility $\beta$ and the loss of damaged items |
| $C_R(\mathbf{P},\mathbf{G})$ | expected cost necessary to restore the attacked facilities and the loss of damaged items depends on **P** and **G** |

| | |
|---|---|
| $C_R(\mathbf{P},\mathbf{G}_{opt})$ | expected cost required to restore the attacked facilities and the loss of damaged items depends on **P** and |
| $c$ | combinations index, ($c = 0,\ldots, 2^{n_p+n_w}-1$) |
| $S_c$ | combinations of disabled and functional facilities for the facilities |
| S | set of combinations of disabled and functional facilities, S = $\{S_c\}$ |
| $Ct_c(E)$ | cost incurred because of the change in transportation cost when the combination is $S_c$ which Depends on the vector **E** |
| $\overline{Ac}$ | average of the capacity acquisition costs per unit |
| $B_{img}$ | brand image of the company |
| $YD_c(E)$ | annual unmet demand when the combination is $S_c$ |
| $B_c(E)$ | backorder cost when the combination is $S_c$ which depends on the vector **E** |
| $\Delta C_{pg\mathrm{E}}(c)$ | attack outcomes of combination $c$ which depend on $p$, g and **E** |
| $T_c(\mathbf{E})$ | cost associated with the transportation cost change and the backorder cost which depends on the Vector **E** |
| $TB(\mathbf{P},\mathbf{G},\mathbf{E})$ | expected cost associated with the transportation cost change and the backorder cost which depends on **P, G** and **E** |
| $D(\mathbf{P},\mathbf{G},\mathbf{E})$ | expected damage which depends on **P, G** and **E** |
| $U_d(\mathbf{P},\mathbf{G},\mathbf{E})$ | defender expected utility which depends on **P, G** and **E** |
| $U_d(\mathbf{P},\mathbf{G}_{opt},\mathbf{E})$ | defender expected utility which depends on **P,** $\mathbf{G}_{opt}$ and **E** |
| $U_a(\mathbf{P},\mathbf{G},\mathbf{E})$ | attacker expected utility which depends on **P, G** and **E** |
| $U_{\min}$ | defender minimal utility |
| $U_{\max}$ | attacker maximal utility |

## 4.2 Introduction

### 4.2.1 Importance of warehouses

Warehouses are commonly used by manufacturers for conservation of stocks for production or distribution. It is widely recognized that the efficiency and effectiveness in any distribution network is largely determined by the good operation of warehouses. They are

fundamental elements in the supply network and they play a vital role in the success or failure of businesses today [13], and in determining a company's competitiveness. There are in fact many situations where it is not suitable to supply directly to customers. For example, some customers require to be served from warehouses rather than from plants because the supplier lead times cannot be reduced cost effectively to the short lead times required by customers [14]. Warehouses offer a same-day or next-day lead-time to customers from inventory [15], and they need to reach this objective reliably within high tolerances of speed, precision and safety. They must be able to properly receive the goods and ship them back to areas of applications as efficiently as possible, respecting the promised delivery dates to customers who are increasingly demanding [12]. Warehouses have a critical impact not only on customer service levels, but also on logistics costs [11,16-17].

### 4.2.2 Protection of warehouses

In a supply network, if one or many warehouses are unavailable, substantial losses may be incurred. Therefore, it is imperative to the success of businesses that warehouses are designed and protected so that they function reliably and cost effectively. In this paper, we consider warehouses as critical facilities that need to be protected against malevolent acts. Considering the plant and warehouse location problem [33], the objective is to define how to allocate optimally the protective resources among the plants and the warehouses, knowing that they are both exposed to external attacks.

The total procurement cost of warehouses is generally less expensive than the costs of plants. One reason is that a plant often requires much more technological production equipment and machines. It results that the protection of warehouses may receive less attention than plants by the designer, and much more protection effort is ‘naturally’ put on the plants. However, the impact of losing the functionality of warehouses may cause substantial damage. Knowing that an intelligent adversary may choose to attack the most vulnerable element (weak point) of the supply network in order to paralyze this network and to cause maximum damage, warehouse protection becomes essential when considering the attacker as a fully strategic optimizing agent.

In this article, the attacker is considered as an intelligent adversary player who chooses optimally how fiercely to attack and to attain the supply chain performance by disabling warehouses and/or plants. We develop a game-theoretical model where the defender and the attacker are considered as two strategic players. The proposed model takes into account the strategic behavior of the attacker in making decisions about defensive investments on warehouses and plants, both considered as critical facilities.

### 4.2.3 Some related work

A vast infrastructure of roads, transport, power grids and computer networks joins plants and warehouses and amalgamates them into a complex system with interdependent and critical facilities. Increasing interconnectivities among such critical facilities have made them more vulnerable than before [1,2]. The security of interdependent systems have been analyzed by many authors, see for example [3-5, 54-56]. The kind of interdependent systems dealt with in this paper is related to production-distribution systems encountered in supply chain networks; plants and warehouse being parts of this system. There exist a large literature on the classical production-distribution system design problem (*e.g.*, [6-10]), and on warehouse design (*e.g.*, [11]). There is also a mature literature on facility design with probabilistic failure of components [21]. A broad range of models for designing supply chains that are resilient to disruptions is presented in [23], which reviews more than one hundred papers on the subject. The multi-level optimization model presented in [22] aims at identifying the optimal allocation of limited protective resources across facilities by considering the event of a worst-case loss of a number of facilities. The possibility of intentional strikes or attacks is not normally taken into account by such a design. Except [18,24], previous papers on facility location and supply chain design models under uncertainty have missed taking into account the attacker as a fully strategic optimizing agent. In [24], a game-theoretical model was developed to deal with the protection of facilities against intentional attacks in the context of the incapacitated fixed-charge location problem. This work has been extended in [18] to the capacitated facility location problem, while using the extra-capacity concept for indirect protection of supply network facilities. While our previous papers [18,24] have focused on protecting plants, the present contribution deals also warehouse protection when designing supply networks.

The proposed approach is based on game theory. This theory studies of the interaction between rational decision-makers [36]. Each player has a number of strategies, which determine the outcome of the game and the pay-off to each player. The use of game theory to protect infrastructures against intentional attacks has become more prominent in recent research in the domain of reliability theory, *e.g.*, [37-40,46,47,53]. Based on these developments in reliability design, we present a game-theoretic model for the protection of warehouses and plants in the context of supply chain design. Given a set of investment alternatives for protecting the plants and the warehouses against identified threats, the objective is to select the optimal defense strategy. The attacker is considered as a player who tries to maximize the expected damage while weighing against the attacks expenditures. A method is developed to evaluate the utilities of the players (*i.e.*, the defender and the attacker). The model considers a non-cooperative two-period game between the players, and an algorithm is presented to determine the equilibrium solution and the optimal defense strategy.

The proposed approach is based on game theory. This theory studies of the interaction between rational decision-makers [36]. Each player has a number of strategies, which determine the outcome of the game and the pay-off to each player. The use of game theory to protect infrastructures against intentional attacks has become more prominent in recent research in the domain of reliability theory, *e.g.*, [37-40,46,47]. Based on these developments in reliability design, we present a game-theoretic model for the protection of warehouses and plants in the context of supply chain design. Given a set of investment alternatives for protecting the plants and the warehouses against identified threats, the objective is to select the optimal defense strategy. The attacker is considered as a player who tries to maximize the expected damage while weighing against the attacks expenditures. A method is developed to evaluate the utilities of the players (*i.e.*, the defender and the attacker). The model considers a non-cooperative two-period game between the players, and an algorithm is presented to determine the equilibrium solution and the optimal defense strategy.

### 4.2.4 Features of the proposed model

The proposed model is used to protect both warehouses and plants that are interdependent elements of the supply network. Following loss of any single element of the supply network, this network is considered to be "survivable" if all others elements are functional. Multiple simultaneous failures are usually treated as negligibly rare events. Of course, this can change radically when the failures are intelligently planned and synchronized instead of happening at random and they become a threat. For that reason, facilities of supply network must be protected against such events. Plant and warehouses of the supply network are critical interdependent elements which can be victim of these threats in the case of intentional attacks. By considering scenarios of simultaneous attacks of warehouses and plants, our model is able to hedge against multiple attacks that are intelligently planned and synchronized.

The second important feature of our model lies in the fact that two different protection strategies are employed: (1) a set of investment alternatives are available for "direct" protection of plants and warehouses; (2) extra-capacities of neighboring functional plants and warehouses can be used after attacks for "indirect" protection. Extra-capacity of plants can be used, after a capacity shock, to quickly bring back the production on schedule and to avoid the backlog of demands [19]. In the case of demand growth, plants and warehouses of supply network might hold extra-capacity against demand variability [20]. In our case, extra-capacity of neighboring functional plants and warehouses can be used after attacks, in order to satisfy all customers demand and to avoid the backorders. The idea of deploying extra-capacities to indirectly protect facilities is similar in spirit to the use of redundant system elements in the defence literature [40].

Third, the proposed model takes into account the discrete nature of protection and attack alternatives. Given a set of investments choices for protecting the plants and warehouses and a set of extra capacities, the strategic decision dealt with here is how to allocate optimally the direct protective resources and the indirect protection resources by extra capacity among the plants and warehouses, knowing that these facilities are exposed to external intentional attacks and taking into account that both the defender and the attacker are fully optimizing agents.

Another characteristic that makes the proposed model unique is that it deals with the protection of network logistic facilities in the context of the capacitated plant and warehouse location and capacity acquisition problem. Plant and warehouse location and capacity acquisition are of vital importance to supply chain management [25-28]. In this context, the objective of the game-theoretic model developed is to find the best trade-off between direct investments in protection and indirect protection by extra-capacities deployment.

### 4.2.5 Paper outline

The remainder of the paper is organized as follows. Section 2 details the proposed method. Section 3 presents the numerical results, and Section 4 concludes the paper.

## 4.3 Proposed method

### 4.3.1 The game

Our model considers two players: the defender and the attacker. The defender has a set of resource (*i.e*, investment alternatives) and he (she) will distribute it resource between deploying extra-capacity and protecting the plants and warehouses from outside attacks. We want to determine how to allocate optimally these resources among the plants and warehouses taking into account the attacker strategy. We analyze a two period game between the defender and the attacker. The defender moves in the first period by determining its free choice variables simultaneously in order to minimize the expected damage [37-40, 53]. Consequently he (she) maximizes his utility. The attacker moves in the second period by determining its free choice variables simultaneously and independently in order to maximize the expected damage. Consequently he (she) also maximizes his utility.

In our model, the vulnerability of a facility is defined by its destruction probability and there is a conflict over this vulnerability between the defender and the attacker. This conflict can be characterized as a contest game. The vulnerabilities of facilities are evaluated as functions of the attacker's and the defender's efforts. Thus both agents can estimate the expected damage caused by the attack for any possible distribution of these

efforts. After evaluating the utility of each player, the game is solved with backward induction, in which the second period is solved first.

### 4.3.2 Steps of the method

The method is based on the following steps:

(i) Defining the logistic network;

(ii) Finding the optimal location of plants and warehouses;

(iii) Identifying the protections and the anticipated attacks;

(iv) Characterizing the contest game;

(v) Evaluating the utilities of the players;

(vi) Solving the game.

In what follows each of these steps is detailed.

#### 4.3.2.1 Defining the logistic network

The objective of this step is to define the characteristics of plants and warehouses, their potential locations, and the suppliers demand characteristics. As indicated before, we consider in this work the capacitated plant and warehouse location and capacity acquisition problem. The aim in this problem is to decide concurrently on the optimal location and capacity size of each new plant and each new warehouse to be established [29-31].

The plant and warehouse location problem [32-34] considers the problem of locating plants and warehouses to minimize the sum of the plants and warehouses location costs, the costs of capacity acquisition associated with the size of open plants and open warehouses, and the shipping costs from open plants to open warehouses and from there to customers. This is subjected to the following constraints: all demands must be served; plants and warehouses capacities must not be exceeded; warehouses can only be served from open plants; and customers can only be served from open warehouses. The plant and warehouse location problem is known to be NP-hard [35].

Figure 4.1 sketches an example of designed logistic network. Such design requires the definition of many input data to be used in the optimization model.

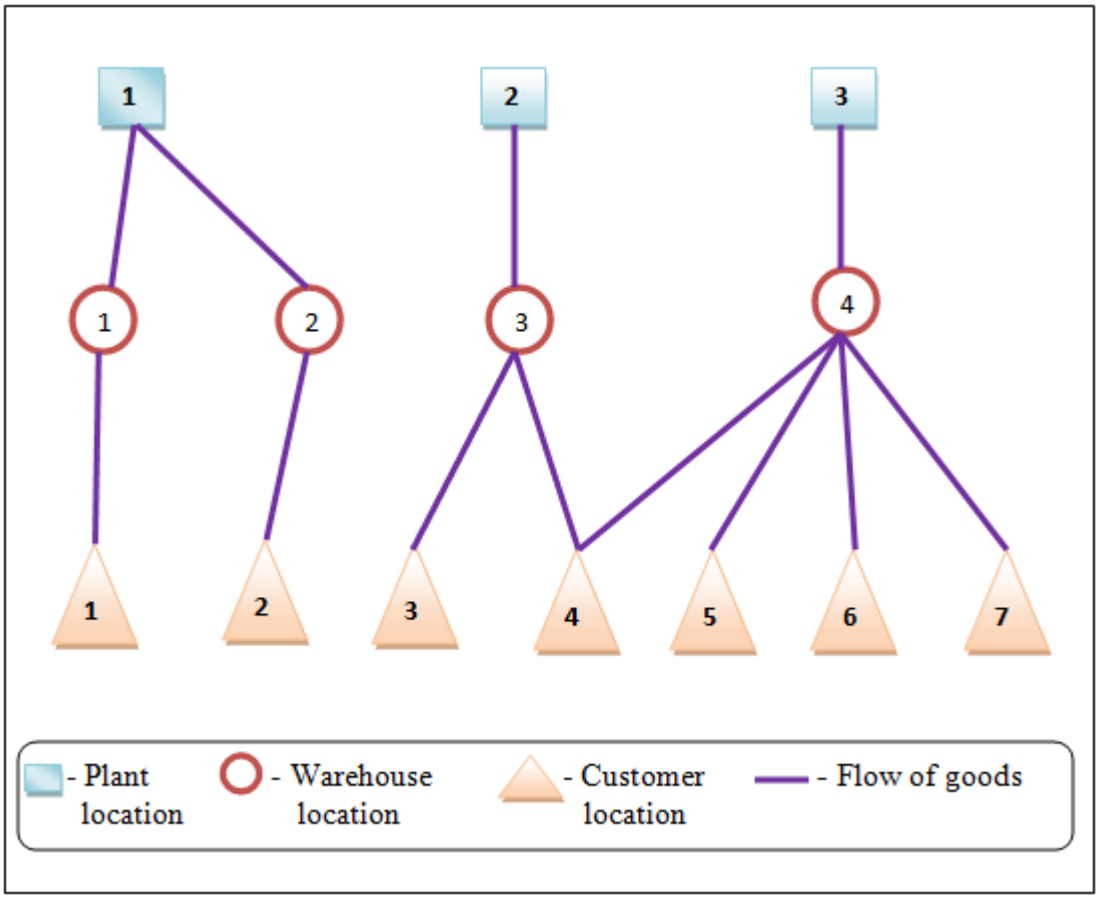


**Fig. 4.1-** An example of designed logistic network.

To select the best locations, potential (candidate) locations and maximum capacities of plants and warehouses are initially specified by the designer. The demand can be defined for each customer location by aggregation. It is also usually considered that a demand at customer location is proportional to the population. The cost parameters can be estimated in different ways. For example, the transportation costs depend on distances that can be measured in many ways including rectilinear distance, straight-line distance, and actual distance. In this work, we assume that all input parameters are known values.

#### 4.3.2.2 Finding the optimal location of plants and warehouses

The decision variables are related, respectively, to the locations of the facilities, and the shipment pattern between the facilities and the customers.

The capacitated plant and warehouse location and capacity acquisition problem is mathematically expressed in the following way:

$$\text{Minimize} \quad \sum_{i\in I} CP_i X_i + \sum_{j\in J} CW_j Y_j + \sum_{i\in I}\sum_{j\in J} Uc_{ij} Z_{ij} + \sum_{j\in J}\sum_{k\in K} Uc_{jk} Z_{jk} + \sum_{i\in I} f_i \left( \sum_{j\in J} Z_{ij} \right) + \sum_{j\in J} g_j \left( \sum_{k\in K} Z_{jk} \right) \tag{4.1}$$

$$\text{Subject to} \quad \sum_{j\in J} Z_{ij} \le CAP_i X_i \quad \forall i \in I \tag{4.2}$$

$$\sum_{i\in I} Z_{ij} - \sum_{k\in K} Z_{jk} \ge 0 \quad \forall j \in J \tag{4.3}$$

$$\sum_{k\in K} Z_{jk} \le CAP_j Y_j \quad \forall j \in J \tag{4.4}$$

$$\sum_{j\in J} Z_{jk} = D_k \quad \forall k \in K \tag{4.5}$$

$$X_i \in \{0,1\} \quad \forall i \in I \tag{4.6}$$

$$Y_j \in \{0,1\} \quad \forall j \in J \tag{4.7}$$

$$Z_{ij},\ Z_{jk} \ge 0 \quad \forall i \in I; \forall j \in J; \forall k \in K \tag{4.8}$$

The objective function (4.1) minimizes the sum of the fixed plant location costs, the fixed warehouse location costs, and the variable costs. The variable costs include production costs at plant *i*, transportation costs from plant *i* to warehouse *j*, and transportation costs from warehouse *j* to customer *k*. Capacity constraint (4.2) ensures that an open plant *i* does not supply more than its capacity. Constraint (4.3) specifies that the amount shipped out of a warehouse *j* cannot exceed the quantity received from the plant *i*. Capacity constraint (4.4) ensures that the amount shipped through a warehouse cannot exceed its capacity. Constraint (4.5) guarantees that each customer's demand will be fully satisfied. Constraints (4.6) and (4.7) require the location variables to be binary, and constraint (4.8) is a non-negativity constraint.

Facility location decisions are long term strategic decisions that are usually fixed and hard to change even in the intermediate term. Inefficient locations for plants and warehouses will result in excess costs being incurred throughout the lifetime of these facilities.

Protection decisions are also long term strategic decisions that are usually fixed. However, they could be revised more frequently than location decisions. Because of this, we are not merging in the same model facility location decisions with facility protection decisions. The defender may rather locate the plants and the warehouses; then, she (he) protects these facilities against anticipated threats using the game-theoretic model developed in this paper. It results that our model is advantageously covering also the case of already existing facilities that may need to be protected or fortified.

#### 4.3.2.3 Identifying the protections and the anticipated attacks

During the last years, the number of companies offering security solutions for facilities has grown significantly. The protection types depend on the supply chain in which the plants and the warehouses are used. They may vary from basic and simple inexpensive investments to advanced and sophisticated expensive investments. In practice, security experts propose many protection types and/or different technologies. Examples of such protection investments include safeguarding the facility with human inspection, development of procedures, technology investments, hiring security experts, installing

firewalls, applying encryption techniques, using access control mechanisms, and developing intrusion detection systems [38].

On the other hand, as our methodology requires attacks to be anticipated, we need to identify the attack types also. Example of anticipated attacks are given in [38]; and they include destruction, theft, and interfering with human inspection, avoidance of surveillance, covert action to avoid detection, manipulation of information, breaking through the security defense, circumventing the work of the security experts, penetrating the firewalls, deciphering the encryption, and bypassing the access control mechanisms and intrusion detection systems. Thus when designing plants and warehouses, security experts and companies offer many alternatives for protection to hedge against anticipated attacks.

Consider a system containing $n_p \geq 1$ plants and $n_w \geq 1$ warehouses subjected to intentional attacks. Considering that these ($n_p$ + $n_w$) facilities have been designed using the optimization model (4.1)-(4.8), we define the following notations for the attacks and the protection types.

Let $\beta$ ($\beta$ = 1, 2, …, $n_p$+$n_w$) be an index that refers to plant $i$ ($i$ = 1, 2,…, $n_p$) and to warehouse $j$ ($j = n_p+1, n_p+2,\ldots, n_p+n_w$). We denote by $\delta_\beta$ the number of available protection types against the identified threat for plants and warehouses. Let $p$ be an index that indicate each protection type, $p$ = 1, 2, …, $\delta_\beta$. Let $\overline{F_{\beta p}}$ be the defender investment expenditure in dollar terms.

We consider a vector **P** = $\left(\pi_\beta\right)$ which represents a protection strategy of the $n_p$ plants and $n_w$ warehouses such as $\pi_\beta$ takes values from $p$ = 1, 2, …, $\delta_\beta$. For example we have 3 plants and 4 warehouses and **P** = $\begin{pmatrix}2 & 1 & 3 & 1 & 1 & 3 & 2\end{pmatrix}$ means that we have plant 1 is protected using type 2 protection, plant 2 is protected using type 1 protection, plant 3 is protected using type 3 protection, warehouses 4 and 5 are protected using type 1 protections, warehouse 6 is protected using type 3 protection and warehouse 7 is protected using type 2 protection.

To each protection strategy **P**, corresponds a vector of investments **F** = $\left(F_{\beta\pi_\beta}\right)$. For example, when **P** = $\begin{pmatrix}2 & 1 & 3 & 1 & 1 & 3 & 2\end{pmatrix}$, we have **F** = $\begin{pmatrix}F_{12} & F_{21} & F_{33} & F_{41} & F_{51} & F_{63} & F_{72}\end{pmatrix}$.

Let $\lambda_{\beta p}$ be a binary variable which is equal to 1 if a protection of type $p$ is selected for facility $\beta$, and 0 otherwise. We assume that only one type of protection of facility $\beta$ is used:

$$\sum_{p=1}^{\delta_\beta} \lambda_{\beta p} = 1, \ \forall \beta. \tag{4.9}$$

Extra-capacities of neighboring functional facilities can be used after attacks for "indirect" protection. Let $\rho_\beta$ be the number of available extra-capacity options for each facility $\beta$. Let $e$ ($e$ = 1, 2, …, $\rho_\beta$) be an index that indicates each extra-capacity option. The defender incurs an investment of proportion of the capacity acquired $\tau_{\beta e}$ associated of the facility located at site $\beta$ using extra-capacity option $e$. Let $C_\beta^*$ denote the capacity acquired. We assume that the capacity acquisition cost at facility location is a linear function. We then consider that the investment of extra-capacity $CE_{\beta e}$ associated of the facility located at site $\beta$ using extra-capacity option $e$, measured in dollar terms, is given by $CE_{\beta e} = Ac_\beta \tau_{\beta e} C_\beta^*$, where $Ac_\beta$ is the capacity acquisition cost at facility location $\beta$ per unit.

We represent an extra-capacity strategy of the $\beta$ facilities by a vector **E** = $\left(\theta_\beta\right)$, $\theta_\beta$ takes values from $e$ = 0, 1, …, $\rho_\beta$. For example, **E** = $\begin{pmatrix}2 & 1 & 2 & 3 & 2 & 3 & 3\end{pmatrix}$ means that extra-capacity option 2 is selected for plant 1, plant 3 and warehouse 5, extra-capacity option 1 is selected for plant 2, extra-capacity option 3 is selected for warehouses 4, 6 and 7.

To each extra-capacity strategy **E**, corresponds a vector of extra capacity indices **T** = $\left(\tau_{\beta\theta_\beta}\right)$. For example, when **E** = $\begin{pmatrix}2 & 1 & 2 & 3 & 2 & 3 & 3\end{pmatrix}$, we have **T**= $\left\{\tau_{12},\ \tau_{21},\ \tau_{32},\ \tau_{43},\ \tau_{52},\ \tau_{63},\ \tau_{73}\right\}$.

Let us introduce a binary variable $\xi_{\beta e}$ which is equal to 1 if an extra-capacity option $e$ is selected for facility $\beta$. Assuming that one extra-capacity option is used, we have:

$$\sum_{e=0}^{\rho_\beta} \xi_{\beta e} = 1, \ \forall \beta. \tag{4.10}$$

The attacker seeks how fiercely to attack the system and to attain the $n_p$ plants and $n_w$ warehouses performance with a set of $\alpha_\beta$ available attack actions. Let $g$ ($g$ = 0, 1, 2, …, $\alpha_\beta$) be an index that indicate each attack type. $g$ = 0 indicates the absence of an attack. The attacker investment expenditure in dollar terms is denoted by $\overline{Q_{\beta g}}$.

An attack strategy against $n_p$ plants and $n_w$ warehouses is denoted by a vector **G** = $\left(\omega_\beta\right)$ such as $\omega_\beta$ takes values from $g$ = 1, 2, …, $\alpha_\beta$. For example, **G** = $\left(3 \quad 1 \quad 3 \quad 2 \quad 1 \quad 3 \quad 2\right)$ means that we have 2 plants that can be attacked using attacks of type 3, plant 2 that can be attacked using attack of type 1, 2 warehouses that can be attacked using attacks of type 2, warehouse 5 that can be attacked using attack of type 1 and warehouse 6 that can be attacked using attack of type 3.

We consider a binary variable $\mu_{\beta g}$ which is equal to 1 if an attack of type $g$ is used for facility $\beta$ (and equal to 0 otherwise). We assume that any facility $\beta$ is attacked by only one type of attack:

$$\sum_{g=1}^{\alpha_\beta} \mu_{\beta g} = 1, \ \forall \beta. \tag{4.11}$$

#### 4.3.2.4 Characterizing the contest game

The defender-attacker interaction is characterized by a contest game, in which each player exerts effort in order to increase his or her winning probability. Contests have been applied in many areas of economics and other social sciences. An excellent introduction to the basic theory and applications can be found in [50]. They include advertising by rival firms, tournaments or influence-activities within organizations, patent and other technology races, lobbying and rent-seeking, litigation, wars, political campaigns, as well as sports.

A critical component of a contest game is how combinations of efforts by the players participating in a contest translate into probabilities of wins and losses [51]. The functions that describe these probabilities as functions of efforts are often called contest functions. The outputs of contest functions are probabilities of wins and losses, while their inputs are the efforts of the participating players. Such efforts are combined so that a player's probability of winning is increasing in her or his effort but is decreasing in the efforts of all the adversaries. Furthermore, the calculation of the efforts depends on the context in which the contest is meant to apply. In some cases, the efforts are denominated in labor time expended. In other situations, the cost of effort is typically represented by monetary expenditures but the effort itself can be the output of an ordinary production function that is a function of a one or several inputs (purchased with money).

As indicated before, the defender incurs a monetary expenditure $\overline{F_{\beta p}}$ to protect a facility $\beta$ (plant or warehouse) using protection type $p$. The output of the defender production function is given by the effort $F_{\beta p}$ as a function of the input expenditure $\overline{F_{\beta p}}$. This function (denoted by $f_1$) can take many different forms. In this paper, we assume that $\overline{F_{\beta p}} = f_{\beta p} F_{\beta p}$, where $f_{\beta p}$ is a unit cost ( $f_{\beta p} > 0$) to protect a facility located at site $\beta$ using protection type $p$. This means that:

$$f_1\left(\overline{F_{\beta p}}\right) = F_{\beta p} = \frac{1}{f_{\beta p}} \overline{F_{\beta p}}. \tag{4.12}$$

Lower $f_{\beta p}$ means greater defense efficiency: $\frac{1}{f_{\beta p}}$ is the efficiency of the defense investment, and $f_{\beta p}$ is the inefficiency.

The defender incurs a budget expenditure $D_B$ such as $\sum_{\beta=1}^{m} \sum_{p=1}^{\delta_\beta} \lambda_{\beta p} \overline{F_{\beta p}} + \sum_{\beta=1}^{m} \sum_{e=0}^{\rho_\beta} \xi_{\beta e} CE_{\beta e} \leq D_B$

Analogously, the attacker investment expenditure in dollar terms is denoted by $\overline{Q_{\beta g}}$ such as $\overline{Q_{\beta g}} = q_{\beta g} Q_{\beta g}$, where $Q_{\beta g}$ is an investment effort incurred by the attacker at unit cost $q_{\beta g}$ (

$q_{\beta g} > 0$) to attack a facility located at site $\beta$ using attack action $g$. That is, the attacker production function (denoted by $f_2$) is given by:

$$f_2\left(\overline{Q_{\beta g}}\right) = Q_{\beta p} = \frac{1}{q_{\beta p}}\overline{Q_{\beta g}}. \tag{4.13}$$

From the attacker viewpoint, the inefficiency of investment is $q_{\beta g}$, and $\frac{1}{q_{\beta p}}$ is the efficiency.

The attacker incurs a budget expenditure $AT_B$ such as $\sum_{\beta=1}^{m}\sum_{g=0}^{\alpha_\beta}\mu_{\beta g}\overline{Q_{\beta g}} \le AT_B$

The contest function $f_3$ determines the probability of winning and losing as a function of the defender and the attacker efforts. It defines the probability of a successful attack on facility, which decreases in the defensive investment, and increases in the offensive investment. That is,

$$\nu_{pg}(\beta) = f_3\left(Q_{\beta g}, F_{\beta p}\right),\ \frac{\partial f_3}{\partial Q_{\beta g}} > 0,\ \frac{\partial f_3}{\partial F_{\beta p}} < 0. \tag{4.14}$$

The vulnerability of a facility $\beta$ is defined by its destruction probability $\nu_{pg}(\beta)$. There is a conflict over this vulnerability between the defender and the attacker. The vulnerability of plants and warehouses can depend on the players' efforts in many forms. We use the ratio form which is commonly used in the rent seeking literature [41-45] as follows:

$$\nu_{pg}(\beta) = \frac{\left(Q_{\beta g}\right)^{\varepsilon_\beta}}{\left(F_{\beta p}\right)^{\varepsilon_\beta} + \left(Q_{\beta g}\right)^{\varepsilon_\beta}},\ \text{where } \varepsilon_\beta \ge 0 \text{ is the intensity of the contest.} \tag{4.15}$$

As pointed out in [52], the probability of winning in this case depends on the ratio of efforts, $\frac{Q_{\beta g}}{F_{\beta p}}$, of the two parties. When $\varepsilon_\beta = 1$, the efforts have proportional impact on the vulnerability. It is assumed that $\varepsilon_\beta$ does not depend on $p$ and $g$.

#### 4.3.2.5 Evaluating the utilities of the players

In general a target may have economic value, human value, and/or symbolic value [38]. Although supply chain facilities may have symbolic and human values, we consider only the economic value of the plants and the warehouses. The defender expected utility can be then formulated a function of the economic damage and the protection expenditure. More precisely, we have:

*Defender Utility = – Damage – Protection Expenditure*. (4.16)

Also, the attacker utility depends on the economic damage and on the attack expenditure:

*Attacker Utility = Damage – Attack Expenditure*. (4.17)

We assume that attacks against different facilities succeed or fail independently. We also assume that the attacker can attack each facility only once, and that many facilities can be attacked at the same time.

To illustrate the damage evaluation, let us consider the example of Figure 4.1 and answer the following typical question: If a Plant or a warehouse is disabled, what is the resulting monetary loss?

First, there is a cost that will be incurred to restore the disabled facility, *i.e.*, to make it functional. Second the loss of damaged items. Such the restoration cost and the loss of damaged items depend on the attack and protection types.

The cost required to restore the attacked facility $\beta$, depends on the time required to restore the attacked facility $\beta$ and repair costs of damaged items. If $R_\beta$ is the cost required to restore the attacked facility $\beta$ and the loss of damaged items, the expected cost $C_R$ necessary to restore the disabled and the loss of damaged items is given by:

$$C_R(\mathbf{P},\mathbf{G}) = \sum_{\beta=1}^{m} \sum_{g=0}^{\alpha_\beta} \sum_{p=1}^{\delta_\beta} \lambda_{\beta p} \mu_{\beta g} \nu_{pg}(\beta) R_\beta . \quad (4.18)$$

Third, there is a cost incurred because of the backorder and the change in transportation cost after attacks. In fact, a backorder cost is incurred when the demands cannot be

satisfied. This will happen either when the entire system is disabled, or when even the available extra-capacities are not enough to fulfil the demands. Note here that in general the backorder cost is relatively high. There is also a change in transportation cost after attacks. When one or several facilities are unavailable, to avoid the backlog of demands and backorders, available extra-capacities of neighboring functional facilities are used. Adding the available extra-capacity to initial capacity, customers could be served and may receive shipments from these facilities, which can sometimes be farther away (subject to constraints that their total capacity must not be exceeded). As a matter of fact, the transportation cost will change as customers are reassigned.

Each facility $\beta$ can be either Disabled or Functional. Let S = $\{S_c\}$ be a set of possible combinations when considering all facilities. Since the term facility refers to a plant or a warehouse, we have ($n_p$+$n_w$) facilities and $2^{n_p+n_w}$ possible combinations.

Let us denote by $Ct_c$ the cost incurred because of the change in transportation cost, *i.e.* the cost under combination $S_c$ minus the cost in a normal situation. We also denote by $B_c$ the backorder cost when the combination is $S_c$. As $Ct_c$ and $B_c$ depend on the vector **E** of extra-capacity strategy, they are rather written $Ct_c$(**E**) and $B_c$(**E**). Let us denote by $T_c$(**E**) the sum of the backorder cost and the cost incurred because of the change in transportation cost when the combination is $S_c$. That is,

$$T_c(\mathbf{E}) = Ct_c(\mathbf{E}) + B_c(\mathbf{E}). \qquad (4.19)$$

Two important points must be noted. First, the capacity of each functional facility is equal to the capacity acquired according to the optimal solution of model (4.1)-( 4.8), plus the extra-capacity deployed according to the vector strategy **E**. Secondly, a backorder cost must be taken into account whenever the total demand is higher than the total quantity shipped. Note that in the context of supply networks, the backorder cost is relatively high, Let us denote by $B_{img}$ the brand image of the company, $YD_c$ the annual unmet demand, and $\overline{Ac}$ the average of the capacity acquisition costs per unit. Consider here that the backorder is computed per year, based on 20% of the average of the capacity acquisition costs, when the total demand is higher than the total quantity shipped, we have

$$B_c(\mathbf{E}) = \begin{cases} B_{img} + 0.2 \times \overline{Ac} \times YD_c(E) & \text{if } YD_c(E) > 0 \\ 0 \end{cases} \quad (4.20)$$

To evaluate $Ct_c(\mathbf{E})$ and $B_c(\mathbf{E})$, the objective function and the constraints are rewritten, to take into account the remarks mentioned above, $(2^{(n_p+n_w)} - 2)$ optimization models have to be solved. In fact, this should be done for all combinations $c$, except when all facilities are functional or disabled. Each solution of the optimization model corresponds to a combination $S_c$. Note that $Ct_c(\mathbf{E})$ can be negative; but as the backorder costs are relatively high, there is always a damage $T_c(\mathbf{E})$.

The backorder costs and the changes of the transportation costs are related to all the possible outcomes. Each attack outcome $T_c(\mathbf{E})$ is multiplied by the probability of the corresponding combination to calculate $\Delta C_{pg\mathbf{E}}(c)$, with $p$, $g$ and $\mathbf{E}$ given and $c$ varying from 0 to $2^{(n_p+n_w)} - 1$. Considering that each facility can be either attacked or not, there are also $2^{(n_p+n_w)}$ possibilities of attacks for all the facilities ($n_p$ plants and $n_w$ warehouses), for given strategies **P** and **G**.

The expected value of the cost incurred because of the backorder and the change in transportation cost is given by:

$$TB(\mathbf{P},\mathbf{G},\mathbf{E}) = \sum_{c=1}^{2^{(n_p+n_w)}-1} \Delta C_{pg\mathbf{E}}(c). \quad (4.21)$$

The expected damage is then:

$$D(\mathbf{P},\mathbf{G},\mathbf{E}) = \sum_{\beta=1}^{m} \sum_{g=0}^{\alpha_\beta} \sum_{p=1}^{\delta_\beta} \lambda_{\beta p} \mu_{\beta g} \nu_{pg}(\beta) R_\beta + \sum_{c=1}^{2^{(n_p+n_w)}-1} \Delta C_{pg\mathbf{E}}(c). \quad (4.22)$$

The defender expected utility is:

$$U_d(\mathbf{P},\mathbf{G},\mathbf{E}) = -D(\mathbf{P},\mathbf{G},\mathbf{E}) - \sum_{\beta=1}^{m}\sum_{p=1}^{\delta_\beta}\lambda_{\beta p}\overline{B_{\beta p}} - \sum_{\beta=1}^{m}\sum_{e=0}^{\rho_\beta}\xi_{\beta e}CE_{\beta e}\,,$$

$$= -\sum_{\beta=1}^{m}\sum_{g=0}^{\alpha_\beta}\sum_{p=1}^{\delta_\beta}\lambda_{\beta p}\mu_{\beta g}\nu_{pg}(\beta)R_\beta + \sum_{c=1}^{2^{(n_p+n_w)}-1}\Delta C_{pg\mathbf{E}}(c) - \sum_{\beta=1}^{m}\sum_{p=1}^{\delta_\beta}\lambda_{\beta p}\overline{B_{\beta p}} - \sum_{\beta=1}^{m}\sum_{e=0}^{\rho_\beta}\xi_{\beta e}CE_{\beta e}\,. \tag{4.23}$$

The attacker expected utility is:

$$U_a(\mathbf{P},\mathbf{G},\mathbf{E}) = D(\mathbf{P},\mathbf{G},\mathbf{E}) - \sum_{\beta=1}^{m}\sum_{g=0}^{\alpha_\beta}\mu_{\beta g}\overline{Q_{\beta g}}\,,$$

$$= \sum_{\beta=1}^{m}\sum_{g=0}^{\alpha_\beta}\sum_{p=1}^{\delta_\beta}\lambda_{\beta p}\mu_{\beta g}\nu_{pg}(\beta)R_\beta + \sum_{c=1}^{2^{(n_p+n_w)}-1}\Delta C_{pg\mathbf{E}}(c) - \sum_{\beta=1}^{m}\sum_{g=0}^{\alpha_\beta}\mu_{\beta g}\overline{Q_{\beta g}}\,. \tag{4.24}$$

#### 4.3.2.6 Solving the game

This is a two-period game where the defender moves in the first period, and the attacker moves in the second period. This means that the defender selects a strategy in the first period that minimizes his utility, considering that the attacker will maximize his utility in the second period. To find the equilibrium solution, the game is solved with backward induction in which the second period is solved first. For this, we use the following algorithm which is an adaptation of the algorithm in [24] to take into account the warehouses and the extra-capacity options:

**1) Inputs:**

- A system of $n_p$ plants and $n_w$ warehouses located by solving the optimization model (1)-(8).
- A set of $\delta_\beta$ protection types for each facility $\beta$ ($p$ = 1, 2, …, $\delta_\beta$); the term facility refers to plants and warehouses ($\beta$ = 1, 2, …, $n_p$+$n_w$).
- A set of $\alpha_\beta$ attack types per facility $\beta$ ($g$ = 0, 1, …, $\alpha_\beta$).
- A set of $\rho_\beta$ extra-capacity options per facility $\beta$ ($e$ = 0, 1, 2, …, $\rho_\beta$).
- *Parameters*:

- Protection investment efforts $F_{\beta p}$;
- Unit costs of protection efforts $f_{\beta p}$;
- Attack investment efforts $Q_{\beta g}$;
- Unit costs of attack efforts $q_{\beta g}$;
- Capacity acquired $C_\beta^*$;
- Capacity acquisition cost per unit $Ac_\beta$;
- Proportion of the capacity acquired $\tau_{\beta e}$;
- Contest intensities $\varepsilon_\beta$;
- Restoration costs and loss of damaged items $R_\beta$
- Brand image cost of the company $B_{img}$.
- defender budget $D_B$; and
- attacker budget $AT_B$

**2) Initialization**

Assign $U_{\min} = \infty$ ($U_{\min}$ is the defender's minimal utility);

Assign $U_{\max} = 0$ ($U_{\max}$ is the attacker's maximal utility).

**3) Determination of the strategy that maximizes the attacker's utility**

For each defender budget $D_B$

**3.1.** For each protection strategy **P** = $\left(\pi_\beta\right)$

**3.1.1.** For each attacker budget $AT_B$

**3.1.1.1.** For each attack strategy **G** = $\left(\omega_\beta\right)$

**3.1.1.1.1.** If $\sum_{\beta=1}^{m}\sum_{g=0}^{\alpha_\beta}\mu_{\beta g}\overline{Q_{\beta g}} \le AT_B$

**3.1.1.1.1.1.** Construct a matrix $\boldsymbol{\lambda} = \left(\lambda_{\beta p}\right)$ such as

$$\lambda_{\beta p} = \begin{cases} 1 & if \ \ \pi_\beta = p \\ 0 & otherwise \end{cases}, \text{ and } \sum_{p=1}^{\delta_\beta}\lambda_{\beta p} = 1, \ \forall\beta;$$

**3.1.1.1.1.2.** Construct a matrix $\boldsymbol{\mu} = \left(\mu_{\beta g}\right)$ such as

$$\mu_{\beta g} = \begin{cases} 1 & if \ \ \omega_\beta = g \\ 0 & otherwise \end{cases}, \text{ and } \sum_{g=0}^{\alpha_\beta} \mu_{\beta g} = 1, \ \forall \beta;$$

**3.1.1.1.1.3.** Determine the matrix $\boldsymbol{\nu}(\mathbf{P},\mathbf{G}) = \left(\nu_{pg}(\beta)\right)$;

**3.1.1.1.1.4.** Calculate the costs $C_R(\mathbf{P},\mathbf{G})$;

**3.1.1.1.1.5.** For each extra-capacity strategy $\mathbf{E} = \left(\theta_\beta\right)$

**3.1.1.1.1.5.1.** If $\sum_{\beta=1}^{m}\sum_{p=1}^{\delta_\beta} \lambda_{\beta p}\overline{F_{\beta p}} + \sum_{\beta=1}^{m}\sum_{e=0}^{\rho_\beta} \xi_{\beta e} CE_{\beta e} \le D_B$

**3.1.1.1.1.5.1.1.** For each combination $c = 1, 2, \ldots, 2^{(n_p+n_w)} - 1$

**3.1.1.1.1.5.1.1.1.** Determine the cost $T_c(\mathbf{E})$;

**3.1.1.1.1.5.1.2.** Calculate the expected cost $TB(\mathbf{P},\mathbf{G},\mathbf{E})$;

**3.1.1.1.1.5.1.3.** Calculate the attacker's utility $U_a(\mathbf{P},\mathbf{G},\mathbf{E})$;

**3.1.1.1.1.5.1.3.1.** If $U_a(\mathbf{P},\mathbf{G},\mathbf{E}) > U_{max}$ assign $U_{max} = U_a(\mathbf{P},\mathbf{G},\mathbf{E})$, $\mathbf{G}_{\text{opt}} = \mathbf{G} = \left(\omega_\beta^{opt}\right)$, $\mathbf{Q}_{\text{opt}} = \left(Q_{\beta\omega_\beta^{opt}}\right)$;

**4) Determination of the optimal defense strategy** (*i.e.*, maximizing the defender's utility)

For each defender budget $D_B$

**4.1.** For each protection strategy $\mathbf{P} = \left(\pi_\beta\right)$

**4.1.1.** Assign $\boldsymbol{\mu}_{\text{opt}} = \left(\mu_{\beta g}\right)$ such as

$$\mu_{\beta g} = \begin{cases} 1 & if \ \ \omega_\beta^{opt} = g \\ 0 & otherwise \end{cases};$$

**4.1.2.** Determine the matrix $\boldsymbol{\nu}(\mathbf{P},\mathbf{G}_{\text{opt}}) = \left(\nu_{p\omega_\beta^{opt}}(\beta)\right)$ such as

$$\nu_{p\omega_\beta^{opt}}(\beta) = \frac{\left(Q_{\beta\omega_\beta^{opt}}\right)^{\varepsilon_\beta}}{\left(F_{\beta p}\right)^{\varepsilon_\beta} + \left(Q_{\beta\omega_\beta^{opt}}\right)^{\varepsilon_\beta}};$$

**4.1.3.** Calculate the cost $C_R(\mathbf{P},\mathbf{G}_{\text{opt}})$;

**4.1.4.** For each extra-capacity strategy $\mathbf{E} = \left(\theta_\beta\right)$

**4.1.4.1.** If $\sum_{\beta=1}^{m}\sum_{p=1}^{\delta_\beta}\lambda_{\beta p}\overline{F_{\beta p}} + \sum_{\beta=1}^{m}\sum_{e=0}^{\rho_\beta}\xi_{\beta e}CE_{\beta e} \le D_B$

**4.1.4.1.1.** For each combination $c = 1, 2, \ldots, 2^{(n_p+n_w)}-1$

**4.1.4.1.1.1.** Determine the cost $T_c(\mathbf{E})$;

**4.1.4.1.2.** Calculate the expected cost $TB(\mathbf{P},\mathbf{G}_{\text{opt}},\mathbf{E})$;

**4.1.4.1.3.** Calculate the defender's utility $U_d(\mathbf{P},\mathbf{G}_{\text{opt}},\mathbf{E})$;

**4.1.4.1.4.** If $-U_d(\mathbf{P},\mathbf{G}_{\text{opt}},\mathbf{E}) < U_{min}$ assign $U_{min} = -U_d(\mathbf{P},\mathbf{G}_{\text{opt}},\mathbf{E})$,

$\mathbf{P}_{\text{opt}} = \mathbf{P} = \left(\pi_\beta^{opt}\right)$, $\mathbf{F}_{\text{opt}} = \left(F_{\beta\pi_\beta^{opt}}\right)$, $\mathbf{E}_{\text{opt}} = \mathbf{E} = \left(\theta_\beta{}^{opt}\right)$,

$\mathbf{T_{opt}} = \mathbf{T} = \left(\tau_{\beta\theta_\beta}{}^{opt}\right)$.

## 4.4 Numerical results

In this section, we consider an example to illustrate the algorithm above. Then, the defense strategy obtained is compared to the case where warehouses are subjected to less protection effort than the plants. We assume that the numerical results are presented for unlimited budgets except in section 3.3, the defense and the attack budgets are both limited.

### 4.4.1 Input data

Let us consider three plants, four warehouses and seven demand nodes. Tables 4.1 and 4.2 provide the fixed costs of locating plants and warehouses, respectively. Table 4.3 gives the yearly demand. Table 4.4 presents the unit costs of producing and shipping from plant site *i* to warehouse site *j*. Table 4.5 presents the unit costs of shipping from warehouse site *j* to customer location *k*.

We assume that the total capacity acquisition costs at plant and warehouse locations are linear functions. Tables 4.6 and 4.7 give these capacities acquisition costs per unit for

plants and warehouses, respectively. We assume that the cost of the brand image of the company ($B_{img}$) is \$200,000.

**Table 4.1-** Fixed cost of locating a plant at site *i*.

| Plant site *i* | Fixed cost (in \$) |
|---|---|
| 1 | 7,000,000 |
| 2 | 6,800,000 |
| 3 | 9,100,000 |

**Table 4.2-** Fixed cost of locating a warehouse at site *j*.

| Warehouse site *j* | Fixed cost (in \$) |
|---|---|
| 1 | 1,500,000 |
| 2 | 1,100,000 |
| 3 | 1,700,000 |
| 4 | 2,400,000 |

**Table 4.3-** Demand per year at customer location.

| Customer location *k* | Demand |
|---|---|
| 1 | 18,000 |
| 2 | 10,000 |
| 3 | 16,000 |
| 4 | 18,000 |
| 5 | 22,500 |
| 6 | 21,000 |
| 7 | 19,000 |

**Table 4.4-** Unit cost (in \$) of producing and shipping from plant site *i* to warehouse site *j*.

| Plant site *i* | Warehouse site *j* | Unit cost (in \$) |
|---|---|---|
| 1 | 1 | 26 |
| 1 | 2 | 27 |
| 1 | 3 | 31 |
| 1 | 4 | 31 |
| 2 | 1 | 29 |
| 2 | 2 | 28.5 |
| 2 | 3 | 26 |
| 2 | 4 | 29 |

| | | |
|---|---|---|
| 3 | 1 | 32 |
| 3 | 2 | 30 |
| 3 | 3 | 28 |
| 3 | 4 | 25 |

**Table 4.5-** Unit cost (in $) of shipping from warehouse site *j* to customer location *k*.

| Warehouse site *j* | Customer location *k* | Unit cost (in $) |
|---|---|---|
| 1 | 1 | 13 |
| 1 | 2 | 14.25 |
| 1 | 3 | 16.5 |
| 1 | 4 | 15.75 |
| 1 | 5 | 17.5 |
| 1 | 6 | 17.25 |
| 1 | 7 | 17.5 |
| | | |
| 2 | 1 | 14.5 |
| 2 | 2 | 12.75 |
| 2 | 3 | 14.5 |
| 2 | 4 | 14.75 |
| 2 | 5 | 16 |
| 2 | 6 | 15.75 |
| 2 | 7 | 16.75 |
| | | |
| 3 | 1 | 16 |
| 3 | 2 | 14.5 |
| 3 | 3 | 13.5 |
| 3 | 4 | 12.75 |
| 3 | 5 | 14.5 |
| 3 | 6 | 14.75 |
| 3 | 7 | 15 |
| | | |
| 4 | 1 | 17.5 |
| 4 | 2 | 16.25 |
| 4 | 3 | 16 |
| 4 | 4 | 15 |
| 4 | 5 | 13 |
| 4 | 6 | 13.25 |
| 4 | 7 | 14 |

**Table 4.6-** Capacity acquisition cost at plant location per unit.

| Plant site *i* | Cost per unit (in $) |
|---|---|
| 1 | 11 |
| 2 | 10 |
| 3 | 12 |

**Table 4.7-** Capacity acquisition cost at warehouse location per unit.

| Warehouse site *j* | Cost per unit (in $) |
|---|---|
| 1 | 5 |
| 2 | 4 |
| 3 | 6 |
| 4 | 7 |

In a normal situation (*i.e.*, when there is no attack), the optimal solution obtained by the model (4.1)-( 4.8) corresponds to the supply network pictured in Figure 4.1. Table 4.8 gives the optimal quantities to be shipped from plants to warehouses, and Table 4.9 presents the optimal quantities to be shipped from warehouses to customers. Tables 4.10 and 4.11 give the optimal capacities to acquire for plants and warehouses, respectively. This optimal solution entails a fixed cost of $29,600,000, and the following yearly costs: a transportation cost of $4,818,250; a capacity acquisition cost in plants of $1,406,400; and a capacity acquisition cost in warehouses of $775,200. We consider one option of extra capacity equal to 30% of the acquired capacity.

The cost $Ct_c(E)$ incurred because of the change in transportation cost when the combination is $S_c$ is calculated by the cost under combination $S_c$ minus the cost in a normal situation. Since the restoration time is one week, each cost $Ct_c(E)$ is evaluated as the change in transportation cost during this week. For example, when the vector of extra-capacity strategy E= (1 0 1 0 0 0 0) and the combination *S2* when plant 2 is disabled, the cost $Ct_2(E)$ is given by the cost under combination $S_2$ minus the cost in a normal situation during one week. That is, $Ct_2(E)$ is equal to (5,205,512 - 4,818,250)/52 = $7,448. Here, 52 is the number of weeks during 1 year. The backorder cost $B_c(E)$ is equal to 0 because $YD_c(E)$ =0. Then, the cost $T_c(\mathbf{E})$ is equal to $7,448.

**Table 4.8-** Optimal quantities to be shipped from plants to warehouses.

| Site $i$ | Site $j$ | Quantity shipped from site $i$ to site $j$ |
|---|---|---|
| 1 | 1 | 18,000 |
| 1 | 2 | 10,000 |
| 2 | 3 | 26,800 |
| 3 | 4 | 69,200 |

**Table 4.9-** Optimal quantities to be shipped from warehouses to customers.

| Site $j$ | Customer location $k$ | Quantity shipped from site $j$ to Customer $k$ |
|---|---|---|
| 1 | 1 | 18,000 |
| 2 | 2 | 10,000 |
| 3 | 3 | 16,000 |
| 3 | 4 | 10,800 |
| 4 | 4 | 7,200 |
| 4 | 5 | 22,000 |
| 4 | 6 | 21,000 |
| 4 | 7 | 19,000 |

**Table 4.10-** Optimal capacities to acquire for plants.

| Plant site $i$ | $Cap_i^*$ |
|---|---|
| 1 | 28,000 |
| 2 | 26,800 |
| 3 | 69,200 |

**Table 4.11-** Optimal capacities to acquire for warehouses.

| Warehouse site $j$ | $Cap_j^*$ |
|---|---|
| 1 | 18,000 |
| 2 | 10,000 |
| 3 | 26,800 |
| 4 | 69,200 |

Table 4.12 gives the protection investment efforts $B_{\beta p}$ to protect a facility (plant and warehouse) located at site $\beta$ using protection type $p$, and the unit costs of protection efforts $b_{\beta p}$. Analogously, Table 4.13 presents the attack investment efforts $Q_{\beta m}$ (to attack facility at

site $\beta$ using attack action $m$), and the unit costs of attack efforts $q_{\beta m}$. We consider one option of extra capacity equal to 30% of the acquired capacity. The restoration costs of disabled plants and warehouses are given in Tables 4.14 and 4.15, respectively. We consider that all contest intensities are equal to 1, which means that the efforts have proportional impact on the vulnerability.

**Table 4.12-** Defense parameters.

| Protection types $p$ | Unit costs $b_{\beta p}$ | Protection efforts $B_{\beta p}$ |
|---|---|---|
| 1 | 70 | 100 |
| 2 | 200 | 130 |
| 3 | 555 | 280 |

**Table 4.13-** Attack parameters.

| Attack types $m$ | Unit costs $q_{\beta m}$ | Attack efforts $Q_{\beta m}$ |
|---|---|---|
| 1 | 220 | 30 |
| 2 | 350 | 54 |
| 3 | 150 | 25 |

**Table 4.14-** The restoration costs of disabled plants and the loss of damaged items (in $).

| Disabled plant $i$ | $R_i$ |
|---|---|
| 1 | 16,000 |
| 2 | 18,000 |
| 3 | 11,000 |

**Table 4.15-** The restoration costs of disabled warehouses and the loss of damaged items (in $).

| Disabled warehouse $j$ | $R_j$ |
|---|---|
| 1 | 7,000 |
| 2 | 6,000 |
| 3 | 8,000 |
| 4 | 9,500 |

### 4.4.2 Determination of the optimal defense strategy

After evaluating the costs $Ct_c(\mathbf{E})$ and $B_c(\mathbf{E})$ for all combinations of disabled plants and warehouses, the algorithm first determines the optimal attack strategy, *i.e.*, the strategy that maximizes the attacker utility. The most harmful attack corresponds to the following strategy:

$\mathbf{G}_{opt}$ = (2 2 2 1 1 1 2).

This means that plants 1, 2 and 3 are disabled using type 2 attacks; warehouses 1, 2 and 3 are disabled using type 1 attacks; and warehouse 4 is disabled using a type 2 attack. The maximum loss is \$29,302,749 and the corresponding attacker utility is $U_{max}$ = \$29,226,429.

To find the equilibrium solution (the optimal defense and extra-capacity strategy), taking into account the attack strategy above (where the attacker maximises his utility), the first period of the game is solved in order to maximize the defender utility, and consequently to allocate optimally the protective resources and extra-capacity among the facilities. The optimal defense and extra-capacity strategy obtained is as follows:

- $\mathbf{P}_{opt}$ = (3 3 3 1 1 3 3): this means that plants 1, 2 and 3 are protected using type 3 protections; warehouses 1 and 2 are protected using type 1 protections; and warehouses 3 and 4 are protected using type 3 protections.
- $\mathbf{E}_{opt}$ = (1 1 1 1 1 1 1): this means that extra-capacities for plants and warehouses are of 30%. The total cost of extra-capacity is \$654,480.

The loss is \$12,482,612 and the corresponding defender utility is $U_{min}$ = \$13,928,092.

### 4.4.3 Limited defense and attack budgets

Figs. 4.2 and 4.3 present the optimal strategies of the defender and the attacker as functions of the contest intensity, when the defense and the attack budgets are both limited. Two pairs of defense and attack budgets are considered. We remark that when the attacker's budget is relatively low (Fig. 4.2), the defender benefits from the greatest contest intensity. However, when the attacker's budget is high (Fig. 4.3), the defender benefits instead from the lowest contest intensity. These results show that larger contest intensities are preferred by the most resourceful player, which is coherent with the intuition and the existing defense literature.

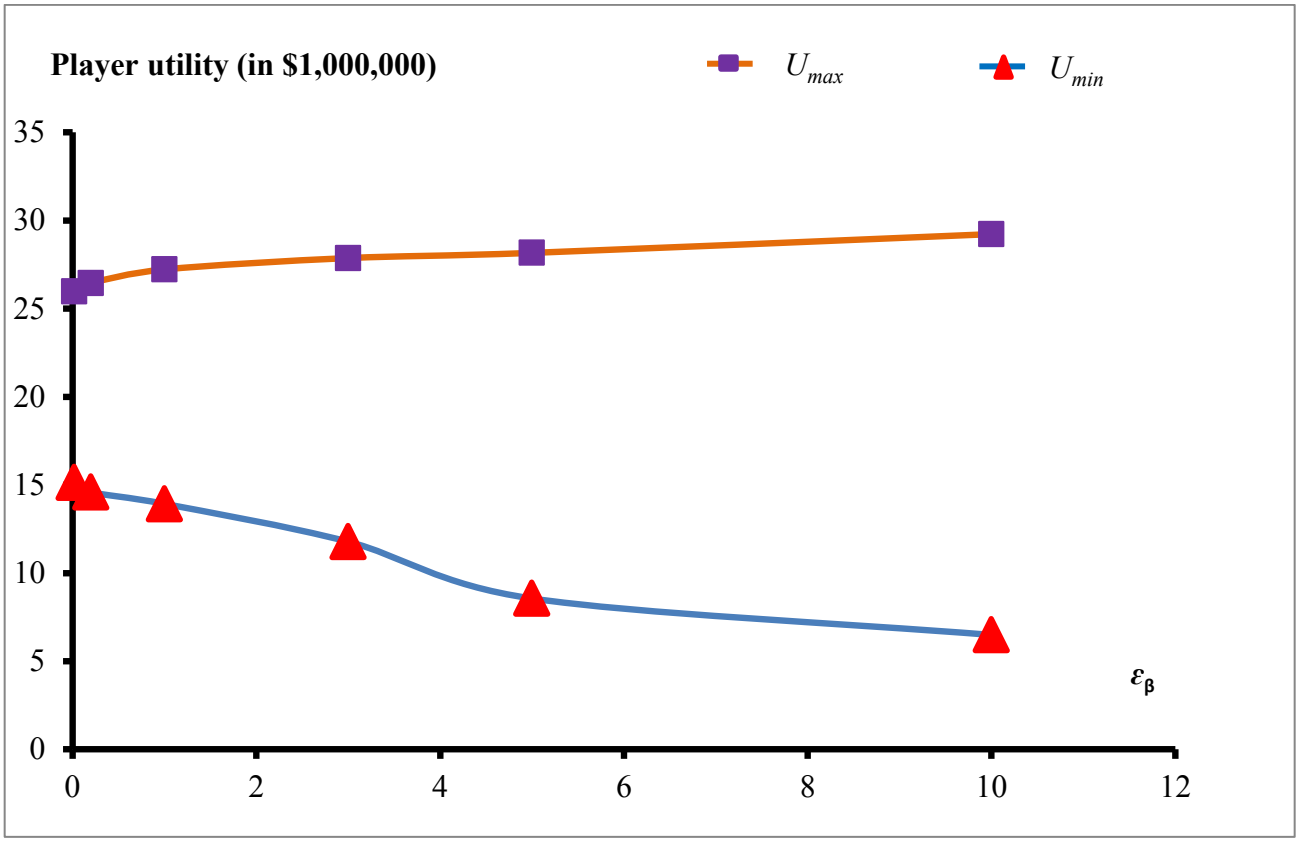


**Fig. 4.2-** Player utility as a function of the contest intensity, when the defense budget is $1,445,480 and the attack budget is $26,250.

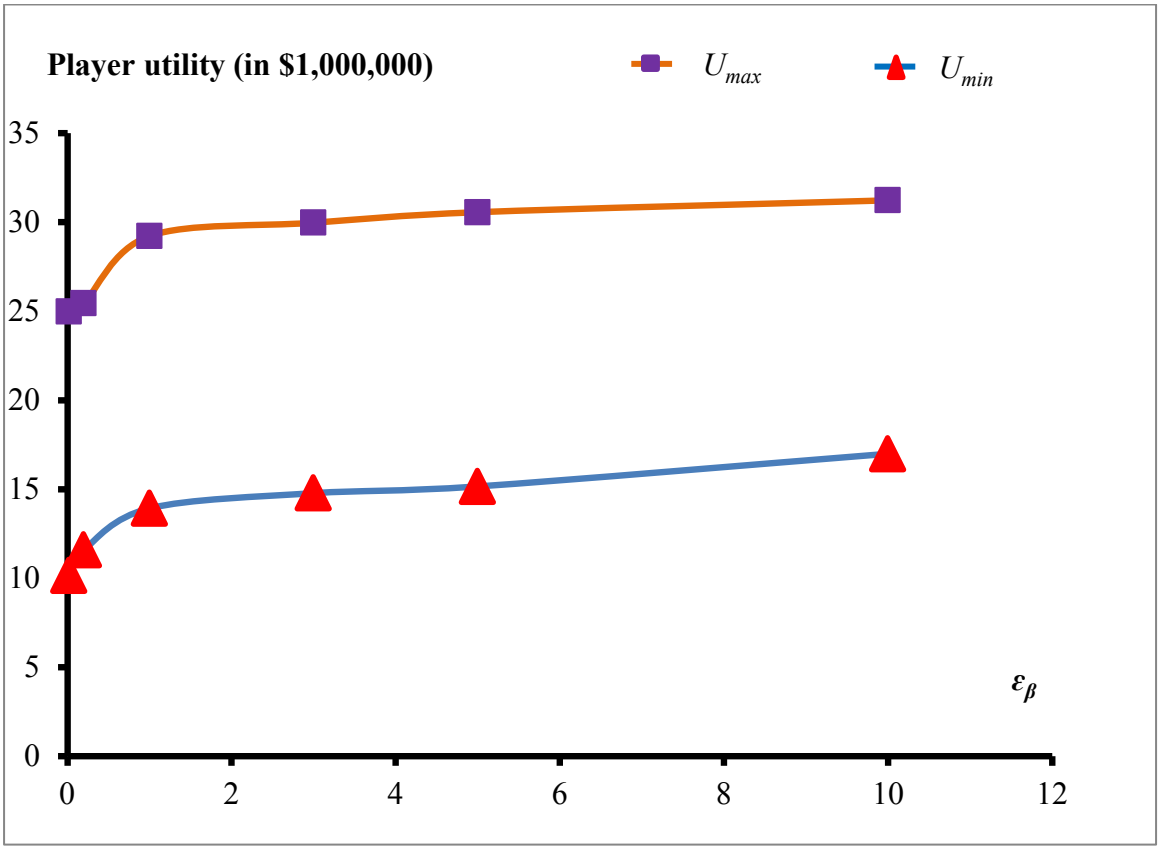


**Fig. 4.3**- Player utility as a function of the contest intensity, when the defense budget is $1,445,480 and the attack budget is 10m.

### 4.4.4 Comparison

Even if warehouses have a critical impact on customer service levels and on logistics costs, their total procurement cost is lower than the costs of plants. Consequently, the protection of warehouses may receive less attention than plants, and more protection effort is generally put on the plants. Here, the objective is to compare the proposed protection strategy to the strategy where warehouses are subjected to less protection effort than the plants. We consider the case where the warehouses are protected by cheaper protection types, and the plants by more expensive protection types. In our example, this means that all plants are protected using type 3 protections and all warehouses are protected using type 1 protections. That is, the protection strategy corresponds to **P** = (3 3 3 1 1 1

1); and the extra-capacity strategy corresponds to **E** = (1 1 1 1 1 1 1). The corresponding defender utility is $U_{min}$ =$17,241,373.

The results above indicate that the defender strategy obtained by our model is 31% better (than the strategy under which the warehouses are protected by cheaper protection types and the plants by more expensive protection types). Our model takes into account the strategic behavior of the attacker in making decisions about defensive investments on warehouses and plants, both considered as critical facilities. In fact, while warehouses may be subjected to less protection effort, their unavailability may have substantial impact on the supply chain performance. Instead of minimally protecting these warehouses, our approach takes into account the impact of their unavailability in finding the best trade-off between protection investments and extra-capacity deployment for plants and warehouses.

## 4.5 Conclusion

Warehouses are fundamental components in the supply network and they play a vital role in the success or failure of businesses today. Therefore, it is extremely important to deploy efficient strategies and measures to protect them in the same way as plants against intentional attacks. This paper considers the protection of plants and warehouses against intentional attacks. It presents a method to find the best trade-off between direct investments in protection and indirect protection by extra-capacities of plants and warehouses, based on a non-cooperative two-period contest game between the defender and the attacker. Extra-capacity of neighboring functional plants or warehouses is used to satisfy the customer demand after attacks when one or several plants or warehouses are unavailable. The method developed evaluates the utilities of the players. The expected costs evaluated include the cost incurred because of the change in transportation cost after attacks, the cost necessary to restore disabled facilities, the loss of damaged items and the backorder cost. An algorithm is developed to determine the equilibrium solution and the optimal defender strategy under capacity constraints. The defender strategy obtained by our model was compared to the case where warehouses are subjected to less protection effort than the plants. This comparison allowed us to measure, how much our method is better, and illustrated the effect of direct investments in protection and indirect protection by warehouse extra-capacities to reduce the expected damage.

Solving these problems should help bridge the gap between our game-theoretical model analysis, and the application in real-life supply chains.

Even if the computation time required to solve the game for the example problem did not exceed 45 minutes, it remains that the proposed method will be time-consuming if larger problems are considered. It is necessary to solve exponentially large numbers of NP-hard problems; and all of them for every instance of the problem. One way to reduce the computation time to solve larger problems is to use meta-heuristics to reduce the number of NP-hard problems that need to be run to solve the game.

We are currently working on the modeling and analysis of interdependent security (contagion) between critical facilities (*i.e*, milk supply chain) [48]. This work includes consideration of all means by which an attacker might deliberately contaminate food (agro-terrorism) [49], including local acts of sabotage.

**References**


[1] O'Rourke TD. Critical Infrastructure, Interdependencies, and Resilience. Bridge, National Academy of Engineering 2007;37(1):22–29.

[2] Pederson P, Dudenhoeffer D, Hartley S, Permann M. Critical Infrastructure Interdependency Modeling: A Survey of Critical Infrastructure Interdependency Modeling, Idaho National Laboratory, United-States of America 2006.

[3] Kunreuther H, Heal G. Interdependent Security. Journal of Risk and Uncertainty, Special Issue on Terrorist Risks 2003; 26: 231-249.

[4] Zhuang J, Bier V, Gupta A. Subsidies in interdependent security with heterogeneous discount rates. The Engineering Economist 2007; 52(1):1–19.

[5] Hausken K. Income, interdependence, and substitution effects affecting incentives for security investment. Journal of Accounting and Public Policy 2006; 25(6):629-665.

[6] Vidal CJ, Goetschalckx M. Startegic production distribution models: A critical review with emphasis on global supply chain models. European Journal of Operational Research 1997; 98 1–18.

[7] Beamon BM. Supply chain design and analysis: Models and methods. International Journal of Production Economics 1998; 55:281–294.

[8] Erenguc SS, Simpson NC, Vakharia AJ. Integrated production/distribution planning in supply chains: An invited review. European Journal of Operational Research 1999;115:219–236.

[9] Sarmiento AM, Nagi R. A review of integrated analysis of production-distribution systems. IIE Trans 1999; 31:1061–1074.

[10] Verter V, Dasci A, Bulgak MA. The production-distribution system design problem. C. Floudas, P. Pardalos, eds. Encyclopedia of Optimization. Kluwer Academic Publishers, Boston, MA 2001.

[11] Baker P, Canessa M. Warehouse design : A structured approach. European Journal of Operational Research 2009;193(2):425–436.

[12] Frazelle E. World-class Warehousing and Material Handling. McGraw-Hill, New York 2002.

[13] Frazelle E. Supply Chain Strategy: The Logistics of Supply Chain Management. McGraw-Hill, New York 2002.

[14] Harrison A, Van Hoek R. Logistics Management and Strategy, second ed. Pearson, Harlow 2005.

[15] Baker P. Aligning distribution center operations to supply chain strategy. International Journal of Logistics Management 2004;15 (1), 111–123.

[16] Establish Inc./Herbert W. Davis & Co. Logistic Cost and Service 2005. In: Presented at Council of Supply Chain Managers Conference 2005.

[17] ELA European Logistics Association/AT Kearney Management Consultants. Differentiation for Performance, Deutscher Verkehrs-Verlag GmbH, Hamburg 2004.

[18] Bricha N, Nourelfath M. Supply network protection under capacity constraint. CIRRET-2014-06 Report, 2014.

[19] Chan F, Wang Z, Zhang J. A two-level hedging point policy for controlling a manufacturing system with time-delay, demand uncertainty and extra capacity. European Journal of Operational Research 2007;176(3):1528–1558.

[20] David SW, Erkoc M, Karabuk S. Managing capacity in the high-tech industry: a review of literature. The engineering economist, Institute of Industrial Engineers 2005;50:125–158.

[21] Colbourn CJ. The Combinatorics of Network Reliability. New York: Oxford University Press 1987.

[22] Scaparra M, Church R. A bilevel mixed-integer program for critical infrastructure protection planning. Computers and Operations Research 2008;35(6): 1905–23.

[23] Snyder LV. Facility location under uncertainty: a review. IIE Transactions 2006;38(7):547–64.

[24] Bricha N, Nourelfath M. Critical supply networks protection against intentional attacks: a game-theoretical model. Reliability Engineering and System Safety 2013;119:1–10.

[25] Rajagopalan S, Andreas CS. Capacity Acquisition and Disposal with Discrete Facility Sizes. Management Science 1994;40(7):903–917.

[26] Verter V, Dincer C. An Integrated Evaluation of Facility Location, Capacity Acquisition and Technology Selection for Designing Global Manufacturing Strategies. European Journal of Operational Research 1992;60(1):1–18.

[27] Verter V, Dincer C. Facility location and capacity acquisition: an integrated approach. Nav Res Logist 1995;42:1141–1160.

[28] Dasci A, Laporte G. An Analytical Approach to the Facility Location and Capacity Acquisition Problem under Demand Uncertainty. Journal of the Operational Research Society 2005;56: 397–405.

[29] Li S, Tirupati D. Dynamic capacity expansion problem with multiple products: Techology selection and timing of capacity expansion. Operations Research 1994;42(5):958–976.

[30] Shulman A. An Algorithm for Solving Dynamic Capacitated Plant Location Problems with Discrete Expansion Sizes. Operations Research 1991;39:423–436.

[31] Venables H, Moscardini A. Ant Based Heuristics for the Capacitated Fixed Charge Location Problem. Ant Colony Optimization and Swarm Intelligence, lecture Notes in Computer Science 2008;5217: 235–242.

[32] Geoffrion AM, Graves GW. Multicommodity Distribution System Design by Benders Decomposition. Management Science 1974;20(5):822–844.

[33] Kaufman L, Eede MV, Hansen P. A plant and warehouse location problem. Oper Res Quart 1977;28:547–554.

[34] Daskin MS. Network and Discrete Location: Models, Algorithms and Applications , John Wiley and Sons, Inc., New York 1995.

[35] Garey M, Johnson D. Computers and Intractability. A Guide to the Theory of NP-Completeness. Freemann, San Francisco 1979.

[36] Martin JO. An Introduction to Game Theory . The MIT Press 2003.

[37] Hausken K, Levitin G. Minmax defence strategy for complex multi-state systems. Reliability Engineering and System Safety 2009;94(2):577–587.

[38] Hausken K. Protecting complex infrastructures against multiple strategic attackers. International Journal of Systems Science 2011;42(1):11–29.

[39] Levitin G, Hausken K. Redundancy vs. Protection vs. False Targets for Systems under Attack. IEEE Transactions on Reliability 2009;58(1):58–68.

[40] Levitin G, Hausken K. Redundancy vs. protection in defending parallel systems against unintentional and intentional impacts. IEEE Transactions on Reliability 2009;58(4):679–690.

[41] Tullock G. Efficient rent seeking. In: Buchanan JM, Tollison RD, Tullock G, editors. Toward a theory of the rent-seeking society. College Station, TX: Texas A & M University Press; 1980:97–112.

[42] Nitzan S. Modelling rent-seeking contests. European Journal of Political Economy 1994;10(1):41–60.

[43] Hirshleifer J. Conflict and rent-seeking success functions: Ratio vs. difference models of relative success. Public Choice 1989; 63:101–112.

[44] Skaperdas S. Contest success functions. Econ Theory 1996;7(2):283–290.

[45] Hausken K. Production and Conflict Models versus Rent-Seeking Models, Public Choice, Springer 2005;123(1):59–93.

[46] Hausken K. Strategic Defence and Attack of Complex Networks. International Journal of Performability Engineering 2009;5(1):13–30.

[47] Levitin G, Gertsbakh I, Shpungin Y. Evaluating the damage associated with intentional supply deprivation in multi-commodity network. Reliability Engineering and System Safety 2013; 119:11–17.

[48] Nganje W, Bier V, Han H, Zack L. Models of interdependent Security along the Milk Supply Chain. Proceeding Issue, American Journal of Agricultural Economic 2008;90:1265–1271.

[49] Wein LM, Liu Y. Analyzing a bioterror attack on the food supply: The case of botulinum toxin in milk. Proceedings of the National Academy of Sciences 2005;102(12): 9984–9989.

[50] Konrad KA. Strategy and dynamics in contests: London School of Economics Perspectives in Economic Analysis. Oxford University Press 2009.

[51] Jia H, Skaperdas S, Samarth V. Contest functions: Theoretical foundations and issues in estimation. International Journal of Industrial Organization 2013; 31(3):211-222.

[52] Hirshleifer J. Conflict and rent-seeking success functions: Ratio vs. difference models of relative success. Public Choice 1989; 63:101–112.

[53] Hausken K, Levitin G. Review of systems defense and attack models. International Journal of Performability Engineering (2012); 8(4):355-366.

[54] Ramirez-Marquez JE, Rocco CM, Levitin G. Optimal network protection against diverse interdictor strategies. Reliability Engineering and System Safety 2011; 96(3):374-382.

[55] Network Protection Against Diverse Attacks- A Multi-objective Perspective, PSAM 11/ESREL 2012, Helsinki, June 2012.

[56] Ramirez-Marquez JE, Rocco CM. Vulnerability based robust protection strategy selection in service networks. Computers & Industrial Engineering 2012; 63(1) 235-242

# Chapitre 5

# Conclusion Générale

Le travail présenté dans cette thèse montre l'importance de la défense des réseaux logistiques. Nous avons proposé une méthode basée sur la théorie des jeux dans le cadre de la problématique générale de conception robuste des réseaux logistiques. Cette méthode permet le calcul des dégâts, l'évaluation de la valeur d'une entité ciblée et la répartition optimale des ressources limitées de défense en tenant compte de la stratégie de l'attaquant. Trois coûts ont été évalués par cette méthode : le coût nécessaire à la restauration des entêtés endommagées, les coûts encourus en raison du changement des coûts de transport suite à des attaques intentionnelles et le coût dû à une rupture de stock. Plusieurs algorithmes ont été développés afin de déterminer la solution d'équilibre et la stratégie de défense optimale dans le cas de plusieurs configurations de réseaux logistiques rencontrées en pratique.

Dans ce qui suit, nous présentons un résumé des trois contributions de la thèse :

- La contribution du premier article vise le développement d'un modèle sous forme d'un jeu non coopératif à deux périodes entre le défendeur et l'attaquant permettant la protection optimale des installations d'un réseau logistique contre les attaques intentionnelles dans le contexte de localisation d'installations à capacité illimitée. Le but est de sélectionner la stratégie de défense optimale en tenant compte de la stratégie de l'attaquant, étant donné un ensemble d'alternatives d'investissement pour protéger les installations contre les attaques intentionnelles.

La contribution du second article repose sur le développement d'un modèle qui consiste à étudier l'impact de la capacité supplémentaire sur la réduction du dommage. Nous avons considéré non seulement un ensemble d'alternatives d'investissement pour la protection « directe » des installations contre les attaques intentionnelles, mais aussi la capacité supplémentaire des installations voisines en fonctionnement pour la protection « indirecte » des installations. La capacité supplémentaire est utilisée après les attaques, pour faire face au risque de la capacité réduite à cause des attaques, continuer à servir les clients dont les commandes sont en cours, rattraper le retard au niveau de la production dans les délais et éviter ainsi les pénalités de retard. Le modèle développé dans cette contribution prend la forme d'un jeu non coopératif à deux périodes entre le défendeur et l'attaquant. Ce modèle vise la sélection de la stratégie de défense optimale (choix d'une capacité supplémentaire et d'un moyen de protection à partir d'un ensemble d'alternatives d'investissement pour

défendre les installations contre les menaces), et ce, dans le contexte de localisation d'installations à capacité limitée.

- La contribution du troisième article est une extension de nos travaux dans le contexte de localisation d'usines et d'entrepôts à capacités limitées. Cette contribution réside dans le développement d'un modèle qui consiste à étudier l'importance des entrepôts dans un réseau logistique. Les entrepôts sont au cœur de l'organisation des flux de l'entreprise et ils jouent un rôle stratégique de régulateur d'un réseau logistique. Si un ou plusieurs entrepôts d'un réseau logistique ne sont pas disponibles suite à des attaques, les pertes peuvent être importantes. Il en résulte que pour le succès des entreprises et pour un fonctionnent fiable, les entrepôts doivent être protégés de la même façon que les usines. Le modèle développé dans cette contribution, est sous forme d'un jeu non coopératif à deux périodes entre le défendeur et l'attaquant, qui vise la sélection de la stratégie optimale de défense pour l'usine et l'entrepôt (choix d'un moyen de protection et d'une capacité supplémentaire) et ce dans le contexte de localisation d'usines et d'entrepôts à capacités limitées.

La méthode développée dans le cadre de cette thèse permet l'allocation optimale des ressources de défense des entités des réseaux logistiques contre les attaques intentionnelles en tenant compte de la stratégie de l'attaquant, dans le contexte de l'optimisation de la localisation des installations. Deux de ces contributions originales sont publiées dans des une revue internationale de renom, tandis que la troisième a été soumise au moment de la rédaction de ce texte. Nos travaux ont également fait l'objet de communications dans diverses conférences internationales et publiées dans les actes de ces conférences.

# Perspectives

Les travaux réalisés dans cette thèse ouvrent différentes perspectives importantes et permettent l'extension des modèles proposés à l'étude de :

- L'information incomplète sur les installations du réseau logistique et sur les stratégies de l'attaquant : il a été supposé dans ce travail que les joueurs ont des connaissances complètes sur les paramètres de la partie. Comme dans la pratique, cette information peut être *incertaine*, il serait important de caractériser la distribution de probabilité de chaque paramètre. Les modèles développés dans cette thèse constituent la pierre angulaire en vue d'une telle extension.
- La possibilité de multiples attaques par plusieurs agresseurs contre les installations du réseau logistique : ceci consistera à étendre notre modèle de protection des réseaux logistique au cas où plusieurs attaquants effectuent de nombreuses attaques consécutives contre différentes installations. Dans ce cas, les attaquants et le défendeur peuvent adapter leurs stratégies sur la base des résultats de précédentes attaques. La question sera alors de trouver la stratégie *dynamique* optimale pour la défense des installations du réseau logistique.
- La modélisation et l'analyse de la sécurité des infrastructures interdépendantes : un exemple bien commenté dans la littérature de la défense est le cas de la contagion dans un réseau d'approvisionnement du lait.