Cybersecurity Investments with Nonlinear Budget Constraints: Analysis of the Marginal Expected Utilities

Patrizia Daniele
Department of Mathematics and Computer Science
University of Catania, Italy
Antonino Maugeri
Department of Mathematics and Computer Science
University of Catania, Italy
and
Anna Nagurney
Isenberg School of Management
University of Massachusetts, Amherst, Massachusetts 01003

In *Operations Research, Engineering, and Cyber Security: Trends in Applied Mathematics and Technology*, N.J. Daras and T.M. Rassias, Editors, Springer International Publishing Switzerland, 2017, pp. 117-134.

Abstract: In this paper, we consider a recently introduced cybersecurity investment supply chain game theory model consisting of retailers and consumers at demand markets with the retailers being faced with nonlinear budget constraints on their cybersecurity investments. We construct a novel reformulation of the derived variational inequality formulation of the governing Nash equilibrium conditions. The reformulation then allows us to exploit and analyze the Lagrange multipliers associated with the bounds on the product transactions and the cybersecurity levels associated with the retailers to gain insights into the economic market forces. We provide an analysis of the marginal expected transaction utilities and of the marginal expected cybersecurity investment utilities. We then establish some stability results for the financial damages associated with a cyberattack faced by the retailers. The theoretical framework is subsequently applied to numerical examples to illustrate its applicability.

Key words: cybersecurity, investments, supply chains, game theory, Nash equilibrium, variational inequalities, Lagrange multipliers, stability

1 Introduction

Cybercrime is a major global issue with cyberattacks adversely affecting firms, governments, other organizations, and consumers ([15]). For example, it has been estimated that cyberattacks cost firms $400 billion annually ([22]). In a recent study ([19]) that surveyed 959 top executives in such industries as banking, insurance, energy, retail, pharmaceuticals, healthcare, and automotive, it was found that 63% reported that their companies experienced significant attacks daily or weekly. Cyberattacks can result not only in direct financial losses and/or the loss of data, but also in an organization's highly valued asset - its reputation. It is quite understandable, hence, that world-wide spending on cybersecurity was approximately $75 billion in 2015, with the expectation that, by 2020, companies around the globe will be spending around $170 billion annually (see [12]).

Organizations, as noted by ([19]), are part of ecosystems and the decisions that they make individually, including those in terms of cyberinvestments, may affect other organizations. Indeed, as discussed in [16], who developed a supply chain game theory model for cybersecurity investments, the level of a cybersecurity investment of a retailer may affect not only his vulnerability to cyberattacks but also that of the network of the supply chain consisting of retailers and consumers who engage in electronic transactions. Effective modeling of the complexity of cyberattacks and cybersecurity investments using operations research techniques, including game theory, can assist in the analysis of complex behaviors and provide, ultimately, tools and insights for policymakers.

For example, [13] developed a multiproduct network economic model of cybercrime with a focus on financial services, since that industrial sector is a major target of cyberattacks. The model captured the perishability of the value of financial products to cybercriminals in terms of the depreciation in prices that the hacked products command over time in the black market. [15], subsequently, constructed a supply chain game theory model in which sellers maximize their expected profits while determining both their product transactions with consumers as well as their cybersecurity investments. However, network vulnerability was not captured. [16] then showed how the model in [15] could be extended to quantify and compute network vulnerability. The studies [15] and [16] were inspired, in part, by the contributions in [20]. The supply chain game theory network framework of [15] and [16] is, nevertheless, more general than that of [20] since the firms, which are retailers, are not assumed to be identical, and the demand side for products of the supply chain network is also captured. In addition, the firms can have distinct cybersecurity investment cost functions and are faced with distinct damages, if attacked. Such features provide greater modeling flexibility as well as realism.

More recently, [14], building on the prior supply chain network cybersecurity investment modeling and analysis work noted above, introduced a novel game theory model in which the budget constraints for cybersecurity investments of retailers, which are nonlinear, are explicitly included, and conducted a spectrum of sensitivity analysis exercises. Consumers reflect their preferences for the product through the demand price functions, which depend on the product demands and on the average security of the network.

The methodology utilized for the formulation, analysis, and solution of the game theory models in [13], [15], [16], and [14] was that of the theory of variational inequalities. We refer the reader to [11] for a survey of game theory, as applied to network security and privacy, and to [9] for some background on optimization models for cybersecurity investments. For a collection of papers on cryptography and network security, see the edited volume [6].

In this paper, we return to the cybersecurity investment supply chain game theory model with nonlinear budget constraints of [14]. We provide an alternative formulation of the variational inequality derived therein in order to provide a deeper qualitative and economic analysis with a focus on the Lagrange multipliers associated with the constraints. The constraints in the model in [14] include not only the nonlinear budget constraints but also lower and upper bounds on the cybersecurity levels as well as on the product transactions.

It is worth mentioning that a wide spectrum of papers has been devoted to the analysis of the behavior of the solutions to a variational inequality which models equilibrium problems by means of the Lagrange multipliers. For instance, we cite the papers [1], [3], [5] for the financial equilibrium problem, the paper [2] for the random traffic equilibrium problem, the papers [7], [8] for the elastic-plastic torsion problem, and the paper [4] for the unilateral problems. This paper is the first to analyze a cybersecurity investment supply chain game theory model with nonlinear budget constraints by means of Lagrange multipliers.

This paper is organized as follows. In Section 2, we briefly recall, for completeness and easy reference, the supply chain network game theory model for cybersecurity investments with nonlinear budget constraints developed in [14] and provide the variational inequality formulation of the Nash equilibrium conditions. The model consists of retailers and consumers at demand markets with the former competing on their product transactions as well as their cybersecurity levels. In Section 3, we construct an alternative formulation of that variational inequality. We then provide an analysis of the marginal expected transaction utilities and of the marginal expected cybersecurity investment utilities. In addition, we present some stability results for the marginal expected cybersecurity investment utilities with respect to changes in the financial damages sustained in a cyberattack. Section 4 illustrates how the framework developed in Section 3 can be applied in the context of numerical examples. We summarize our results and present our conclusions in Section 5.

2 The Model

We now recall the supply chain game theory model of cybersecurity investments with nonlinear budget constraints introduced in [14] (see also [21] for other equilibrium models with nonlinear constraints). The supply chain network, consisting of retailers and consumers at demand markets, is depicted in Figure 1. Each retailer i; $i = 1, \ldots, m$, can transact with demand market j; $j = 1, \ldots, n$, with Q_{ij} denoting the product transaction from i to j. Also, each retailer i; $i = 1, \ldots, m$, determines his cybersecurity or, simply, security, level s_i; $i = 1, \ldots, m$. We group the product transactions for retailer i; $i = 1, \ldots, m$, into the n-dimensional vector Q_i and then we group all such retailer transaction vectors into the mn-dimensional vector Q. The security levels of the retailers are grouped into the m-dimensional vector s.

The cybersecurity level in the supply chain network is the average security and is denoted by $\bar{s}$, where $\bar{s} = \sum_{i=1}^{m} \frac{s_i}{m}$.

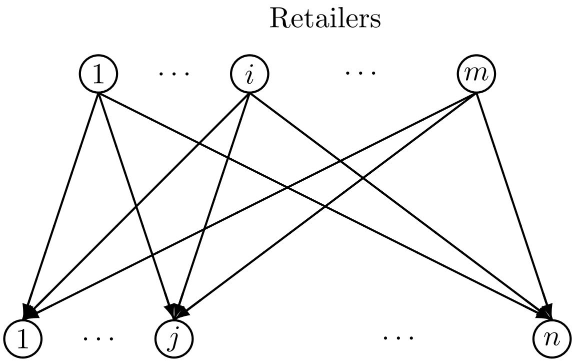

Figure 1: The Bipartite Structure of the Supply Chain Network Game Theory Model

The retailers seek to maximize their individual expected utilities, consisting of expected profits, and compete in a noncooperative game in terms of strategies consisting of their respective product transactions and security levels. The governing equilibrium concept is that of Nash equilibrium ([17], [18]).

The demand at each demand market j, d_j, must satisfy:

$$d_j = \sum_{i=1}^{m} Q_{ij}, \quad j = 1, \ldots, n. \tag{1}$$

We group the demands at the demand markets into the n-dimensional vector d.

The product transactions are subject to upper bounds and must be nonnegative so that we have the following constraints:

$$0 \leq Q_{ij} \leq \bar{Q}_{ij}, \quad i = 1, \ldots, m; j = 1, \ldots, n. \tag{2}$$

The cybersecurity level of each retailer i must satisfy the following constraint:

$$0 \leq s_i \leq u_{s_i}, \quad i = 1, \ldots, m, \tag{3}$$

where $u_{s_i} < 1$ for all i; $i = 1, \ldots, m$. The larger the value of s_i, the higher the security level, with perfect security reflected in a value of 1. However, since, as noted in [14], we do not expect perfect security to be attainable, we have $u_{s_i} < 1$; $i = 1, \ldots, m$. If $s_i = 0$ this means that retailer i has no security.

The demand price of the product at demand market j, $\rho_j(d, \bar{s})$; $j = 1, \ldots, n$, is a function of the vector of demands and the network security. We can expect consumers to be willing to pay more for higher network security. In view of the conservation of flow equations above, we can define $\hat{\rho}_j(Q, \bar{s}) \equiv \rho_j(d, \bar{s})$; $j = 1, \ldots, n$. We assume that the demand price functions are continuously differentiable.

There is an investment cost function h_i; $i = 1, \ldots, m$, associated with achieving a security level s_i with the function assumed to be increasing, continuously differentiable and convex. For a given retailer i, $h_i(0) = 0$ denotes an entirely insecure retailer and $h_i(1) = \infty$ is the investment cost associated with complete security for the retailer. An example of an $h_i(s_i)$ function that satisfies these properties and that is utilized here (see also [14]) is

$$h_i(s_i) = \alpha_i \left(\frac{1}{\sqrt{(1 - s_i)}} - 1 \right) \text{ with } \alpha_i > 0.$$

The term α_i enables distinct retailers to have different investment cost functions based on their size and needs. Such functions have been introduced by [20] and also utilized by [16]. However, in those models, there are no cybersecurity budget constraints and the cybersecurity investment cost functions only appear in the objective functions of the decision-makers.

In the model with nonlinear budget constraints as in [14] each retailer is faced with a limited budget for cybersecurity investment. Hence, the following nonlinear budget constraints must be satisfied:

$$\alpha_i \left(\frac{1}{\sqrt{(1 - s_i)}} - 1 \right) \leq B_i; \quad i = 1, \ldots, m, \tag{4}$$

that is, each retailer can't exceed his allocated cybersecurity budget.

The profit f_i of retailer i; $i = 1, \ldots, m$ (in the absence of a cyberattack and cybersecurity investment), is the difference between his revenue $\sum_{j=1}^{n} \hat{\rho}_j(Q, s) Q_{ij}$ and his costs associated, respectively, with production and transportation: $c_i \sum_{j=1}^{n} Q_{ij} - \sum_{j=1}^{n} c_{ij}(Q_{ij})$, that is,

$$f_i(Q,s) = \sum_{j=1}^{n} \hat{\rho}_j(Q,s) Q_{ij} - c_i \sum_{j=1}^{n} Q_{ij} - \sum_{j=1}^{n} c_{ij}(Q_{ij}). \tag{5}$$

If there is a successful cyberattack on a retailer i; $i = 1, \ldots, m$, retailer i incurs an expected financial damage given by

$$D_i p_i,$$

where D_i, the damage incurred by retailer i, takes on a positive value, and p_i is the probability of a successful cyberattack on retailer i, where:

$$p_i = (1 - s_i)(1 - \bar{s}), \quad i = 1, \ldots, m, \tag{6}$$

with the term $(1-\bar{s})$ denoting the probability of a cyberattack on the supply chain network and the term $(1 - s_i)$ denoting the probability of success of such an attack on retailer i.

Each retailer i; $i = 1, \ldots, m$, hence, seeks to maximize his expected utility, $E(U_i)$, corresponding to his expected profit given by:

$$E(U_i) = (1-p_i) f_i(Q,s) + p_i(f_i(Q,s) - D_i) - h_i(s_i) = f_i(Q,s) - p_i D_i - h_i(s_i). \tag{7}$$

Let $\mathbb{K}^i$ denote the feasible set corresponding to retailer i, where $\mathbb{K}^i \equiv \{(Q_i, s_i) | 0 \leq Q_{ij} \leq \bar{Q}_{ij}, \forall j,\ 0 \leq s_i \leq u_{s_i}$ and the budget constraint holds for $i\}$ and define $\mathbb{K} \equiv \prod_{i=1}^{m} \mathbb{K}^i$.

We now recall the following definition from [14]:

Definition 2.1 (A Supply Chain Nash Equilibrium in Product Transactions and Security Levels) *A product transaction and security level pattern $(Q^*, s^*) \in \mathbb{K}$ is said to constitute a supply chain Nash equilibrium if for each retailer $i; i = 1, \ldots, m$,*

$$E(U_i(Q_i^*, s_i^*, \hat{Q}_i^*, \hat{s}_i^*)) \geq E(U_i(Q_i, s_i, \hat{Q}_i^*, \hat{s}_i^*)), \quad \forall (Q_i, s_i) \in \mathbb{K}^i, \tag{8}$$

where

$$\hat{Q_i^*} \equiv (Q_1^*, \ldots, Q_{i-1}^*, Q_{i+1}^*, \ldots, Q_m^*); \quad \textit{and} \quad \hat{s_i^*} \equiv (s_1^*, \ldots, s_{i-1}^*, s_{i+1}^*, \ldots, s_m^*).$$

Hence, according to (8), a supply chain Nash equilibrium is established if no retailer can unilaterally improve upon his expected utility (expected profit) by choosing an alternative vector of product transactions and security level.

The following theorem was established in [14]:

Theorem 2.1 (Variational Inequality Formulation) *Assume that, for each retailer i; $i = 1, \dots, m$, the expected profit function $E(U_i(Q,s))$ is concave with respect to the variables $\{Q_{i1}, \dots, Q_{in}\}$, and s_i, and is continuously differentiable. Then $(Q^*, s^*) \in \mathbb{K}$ is a supply chain Nash equilibrium according to Definition 1 if and only if it satisfies the variational inequality*

$$-\sum_{i=1}^{m}\sum_{j=1}^{n} \frac{\partial E(U_i(Q^*, s^*))}{\partial Q_{ij}} \times \left(Q_{ij} - Q^*_{ij}\right) - \sum_{i=1}^{m} \frac{\partial E(U_i(Q^*, s^*))}{\partial s_i} \times (s_i - s^*_i) \geq 0, \qquad \forall (Q,s) \in \mathbb{K} \tag{9}$$

or, equivalently, $(Q^*, s^*) \in \mathbb{K}$ is a supply chain Nash equilibrium product transaction and security level pattern if and only if it satisfies the variational inequality

$$\sum_{i=1}^{m}\sum_{j=1}^{n}\left[c_i + \frac{\partial c_{ij}(Q^*_{ij})}{\partial Q_{ij}} - \hat{\rho}_j(Q^*, s^*) - \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial Q_{ij}} \times Q^*_{ik}\right] \times (Q_{ij} - Q^*_{ij})$$
$$+\sum_{i=1}^{m}\left[\frac{\partial h_i(s^*_i)}{\partial s_i} - \left(1 - \sum_{k=1}^{m}\frac{s^*_k}{m} + \frac{1 - s^*_i}{m}\right) D_i - \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial s_i} \times Q^*_{ik}\right]$$
$$\times (s_i - s^*_i) \geq 0, \quad \forall (Q,s) \in \mathbb{K}. \tag{10}$$

3 Equivalent Formulation of the Variational Inequality

The aim of this section is to find an alternative formulation of the variational inequality (9) governing the Nash equilibrium for the cybersecurity supply chain game theory model with nonlinear budget constraints by means of the Lagrange multipliers associated with the constraints defining the feasible set $\mathbb{K}$. To this end, we remark that $\mathbb{K}$ can be rewritten in the following way:

$$\mathbb{K} = \Big\{(Q,s) \in \mathbb{R}^{mn+n} : -Q_{ij} \leq 0,\ Q_{ij} - \overline{Q}_{ij} \leq 0,\ -s_i \leq 0,\ s_i - u_{s_i} \leq 0,$$
$$h_i(s_i) - B_i \leq 0,\ i = 1, \dots, m,\ j = 1, \dots, n\Big\}, \tag{11}$$

and that variational inequality (9) can be equivalently rewritten as a minimization problem. Indeed, by setting:

$$V(Q,s) = -\sum_{i=1}^{m}\sum_{j=1}^{n} \frac{\partial E(U_i(Q^*, s^*))}{\partial Q_{ij}} \left(Q_{ij} - Q^*_{ij}\right) - \sum_{i=1}^{m} \frac{\partial E(U_i(Q^*, s^*))}{\partial s_i} \left(s_i - s^*_i\right),$$

we have:

$$V(Q,s) \geq 0 \text{ in } \mathbb{K} \text{ and } \min_{\mathbb{K}} V(Q,s) = V(Q^*, s^*) = 0. \tag{12}$$

Then, we can consider the following Lagrange function:

$$
\begin{aligned}
\mathcal{L}(Q, s, \lambda^1, \lambda^2, \mu^1, \mu^2, \lambda) &= -\sum_{i=1}^{m}\sum_{j=1}^{n} \frac{\partial E(U_i(Q^*, s^*))}{\partial Q_{ij}} \left(Q_{ij} - Q^*_{ij}\right) \\
&- \sum_{i=1}^{m} \frac{\partial E(U_i(Q^*, s^*))}{\partial s_i} \left(s_i - s^*_i\right) \\
&+ \sum_{i=1}^{m}\sum_{j=1}^{n} \lambda^1_{ij}(-Q_{ij}) \\
&+ \sum_{i=1}^{m}\sum_{j=1}^{n} \lambda^2_{ij}(Q_{ij} - \overline{Q}_{ij}) + \sum_{i=1}^{m} \mu^1_i(-s_i) \\
&+ \sum_{i=1}^{m} \mu^2_i(s_i - u_{s_i}) + \sum_{i=1}^{m} \lambda_i(h_i(s_i) - B_i), \quad (13)
\end{aligned}
$$

where $(Q, s) \in \mathbb{R}^{mn+n}$, λ^1, $\lambda^2 \in \mathbb{R}^{mn}_+$, $\mu^1, \mu^2 \in \mathbb{R}^m_+$, $\lambda \in \mathbb{R}^m_+$. Since for the convex set $\mathbb{K}$ the Slater condition is verified and (Q^*, s^*) is a minimal solution to problem (12), by virtue of well-known theorems (see [10]), there exist $\overline{\lambda}^1$, $\overline{\lambda}^2 \in \mathbb{R}^{mn}_+$, $\overline{\mu}^1$, $\overline{\mu}^2$, $\overline{\lambda} \in \mathbb{R}^m_+$ such that the vector $(Q^*, s^*, \overline{\lambda}^1, \overline{\lambda}^2, \overline{\mu}^1, \overline{\mu}^2, \overline{\lambda})$ is a saddle point of the Lagrange function (13); namely,

$$
\begin{aligned}
\mathcal{L}(Q^*, s^*, \lambda^1, \lambda^2, \mu^1, \mu^2, \lambda) &\leq \mathcal{L}(Q^*, s^*, \overline{\lambda}^1, \overline{\lambda}^2, \overline{\mu}^1, \overline{\mu}^2, \overline{\lambda}) \\
&\leq \mathcal{L}(Q, s, \overline{\lambda}^1, \overline{\lambda}^2, \overline{\mu}^1, \overline{\mu}^2, \overline{\lambda}) \qquad (14)
\end{aligned}
$$

$\forall (Q, s) \in \mathbb{K}$, $\forall \lambda^1, \lambda^2 \in \mathbb{R}^{mn}_+$, $\forall \mu^1, \mu^2, \lambda \in \mathbb{R}^m_+$ and

$$
\begin{aligned}
&\overline{\lambda}^1_{ij}(-Q^*_{ij}) = 0, \quad \overline{\lambda}^2_{ij}(Q^*_{ij} - \overline{Q}_{ij}) = 0, \quad i = 1, \dots, m,\ j = 1, \dots, n, \\
&\hfill (15) \\
&\overline{\mu}^1_i(-s^*_i) = 0, \quad \overline{\mu}^2_i(s^*_i - u_{s_i}) = 0, \quad \overline{\lambda}_i(h_i(s^*_i) - B_i) = 0, \quad i = 1, \dots, m.
\end{aligned}
$$

From the right-hand side of (14) it follows that $(Q^*, s^*) \in \mathbb{R}^{mn+n}_+$ is a minimal point of $\mathcal{L}(Q, s, \overline{\lambda}^1, \overline{\lambda}^2, \overline{\mu}^1, \overline{\mu}^2, \overline{\lambda})$ in the whole space $\mathbb{R}^{mn+n}$ and, hence, for all $i = 1, \dots, m$, and $j = 1, \dots, n$, we get:

$$
\frac{\partial \mathcal{L}(Q^*, s^*, \overline{\lambda}^1, \overline{\lambda}^2, \overline{\mu}^1, \overline{\mu}^2, \overline{\lambda})}{\partial Q_{ij}} = -\frac{\partial E(U_i(Q^*, s^*))}{\partial Q_{ij}} - \overline{\lambda}^1_{ij} + \overline{\lambda}^2_{ij} = 0 \quad (16)
$$

$$
\begin{aligned}
\frac{\partial \mathcal{L}(Q^*, s^*, \overline{\lambda}^1, \overline{\lambda}^2, \overline{\mu}^1, \overline{\mu}^2, \overline{\lambda})}{\partial s_i} &= -\frac{\partial E(U_i(Q^*, s^*))}{\partial s_i} \\
&\quad -\overline{\mu}^1_i + \overline{\mu}^2_i + \overline{\lambda}_i \frac{\partial h_i(s^*_i)}{\partial s_i} = 0 \qquad (17)
\end{aligned}
$$

together with conditions (15).

Conditions (15)–(17) represent an equivalent formulation of variational inequality (9).
It is easy to see that from (16) and (17) the variational inequality (9) follows. Indeed, multiplying (16) by $(Q_{ij} - Q^*_{ij})$ we obtain:

$$-\frac{\partial E(U_i(Q^*, s^*))}{\partial Q_{ij}}(Q_{ij} - Q^*_{ij}) - \overline{\lambda}^1_{ij}(Q_{ij} - Q^*_{ij}) + \overline{\lambda}^2_{ij}(Q_{ij} - Q^*_{ij}) = 0$$

and, taking into account (15), we have:

$$-\frac{\partial E(U_i(Q^*, s^*))}{\partial Q_{ij}}(Q_{ij} - Q^*_{ij}) = \overline{\lambda}^1_{ij} Q_{ij} - \overline{\lambda}^2_{ij}(Q_{ij} - \overline{Q}_{ij}) \geq 0.$$

Analogously, multiplying (17) by $(s_i - s^*_i)$, we get:

$$-\frac{\partial E(U_i(Q^*, s^*))}{\partial s_i}(s_i - s^*_i) - \overline{\mu}^1_i(s_i - s^*_i) + \overline{\mu}^2_i(s_i - s^*_i) + \overline{\lambda}_i \frac{\partial h_i(s^*_i)}{\partial s_i}(s_i - s^*_i) = 0.$$

From (15), we have:

$$\overline{\mu}^1_i(-s^*_i) = 0, \quad \overline{\mu}^2_i s^*_i = \overline{\mu}^2_i u_{s_i}.$$

Moreover, if $\overline{\lambda}_i > 0$, then $h_i(s^*_i) = B_i = \max h_i(s_i)$, but $h_i(s_i)$ is a nondecreasing function; hence, it attains its maximum value at $s^*_i = u_{s_i}$. Therefore, we get:

$$-\frac{\partial E(U_i(Q^*, s^*))}{\partial s_i}(s_i - s^*_i) = \overline{\mu}^1_i s_i - \overline{\mu}^2_i(s_i - u_{s_i}) - \overline{\lambda}_i \frac{\partial h_i(s^*_i)}{\partial s_i}(s_i - u_{s_i}) \geq 0$$

because $h_i(s_i)$ is a nonnegative convex function such that $h_i(0) = 0$. Then $h_i(s_i)$ attains the minimum value at 0. Hence, $\dfrac{\partial h_i(0)}{\partial s_i} \geq 0$ and, since $\dfrac{\partial h_i(s_i)}{\partial s_i}$ is increasing, it results in:

$$0 \leq \frac{\partial h_i(0)}{\partial s_i} \leq \frac{\partial h_i(s_i)}{\partial s_i}, \quad \forall 0 \leq s_i \leq u_{s_i}.$$

The term $\dfrac{\partial E(U_i(Q^*, s^*))}{\partial Q_{ij}}$ is called the *marginal expected transaction utility*, $i = 1, \ldots, m$, $j = 1, \ldots, n$, and the term $\dfrac{\partial E(U_i(Q^*, s^*))}{\partial s_i}$ is called the *marginal expected cybersecurity investment utility*, $i = 1, \ldots, m$. Our aim is to study such marginal expected utilities by means of (15)–(17).

3.1 Analysis of Marginal Expected Transaction Utilities

From (16) we get

$$-\frac{\partial E(U_i(Q^*,s^*))}{\partial Q_{ij}} - \overline{\lambda}^1_{ij} + \overline{\lambda}^2_{ij} = 0, \quad i=1,\ldots,m,\ j=1,\ldots,n.$$

So, if $0 < Q^*_{ij} < \overline{Q}_{ij}$, then we get (see also (10))

$$-\frac{\partial E(U_i(Q^*,s^*))}{\partial Q_{ij}} = c_i + \frac{\partial c_{ij}(Q^*_{ij})}{\partial Q_{ij}} - \hat{\rho}_j(Q^*,s^*) - \sum_{k=1}^{m} \frac{\partial \hat{\rho}_k}{\partial Q_{ij}} \times Q^*_{ik} = 0, \quad (18)$$

$$i=1,\ldots,m,\ j=1,\ldots,n,$$

whereas if $\overline{\lambda}^1_{ij} > 0$, and, hence, $Q^*_{ij} = 0$, and $\overline{\lambda}^2_{ij} = 0$, we get

$$-\frac{\partial E(U_i(Q^*,s^*))}{\partial Q_{ij}} = c_i + \frac{\partial c_{ij}(Q^*_{ij})}{\partial Q_{ij}} - \hat{\rho}_j(Q^*,s^*) - \sum_{\substack{k=1\\k\neq i}}^{m} \frac{\partial \hat{\rho}_k}{\partial Q_{ij}} \times Q^*_{ik} = \overline{\lambda}^1_{ij}, \quad (19)$$

$$i=1,\ldots,m,\ j=1,\ldots,n,$$

and if $\overline{\lambda}^2_{ij} > 0$, and, hence, $Q^*_{ij} = \overline{Q}_{ij}$, and $\overline{\lambda}^1_{ij} = 0$, we have

$$-\frac{\partial E(U_i(Q^*,s^*))}{\partial Q_{ij}} = c_i + \frac{\partial c_{ij}(Q^*_{ij})}{\partial Q_{ij}} - \hat{\rho}_j(Q^*,s^*) - \sum_{\substack{k=1\\k\neq i}}^{m} \frac{\partial \hat{\rho}_k}{\partial Q_{ij}} \times Q^*_{ik} = -\overline{\lambda}^2_{ij}, \quad (20)$$

$$i=1,\ldots,m,\ j=1,\ldots,n.$$

Now let us analyze the meaning of equalities (18)–(20). From equality (18), which holds when $0 < Q^*_{ij} < \overline{Q}_{ij}$, we see that for retailer i, who transfers the product Q^*_{ij} to the demand market j, the marginal expected transaction utility is zero; namely, the marginal expected transaction cost $c_i + \frac{\partial c_{ij}(Q^*_{ij})}{\partial Q_{ij}}$ is equal to the marginal expected transaction revenue $\hat{\rho}_j(Q^*,s^*) + \sum_{\substack{k=1\\k\neq i}}^{m} \frac{\partial \hat{\rho}_k}{\partial Q_{ij}} \times Q^*_{ik}$.

In equality (19), minus the marginal expected transaction utility is equal to $\overline{\lambda}^1_{ij}$; namely, the marginal expected transaction cost is greater than the marginal expected transaction revenue. Retailer j has a marginal loss given by $\overline{\lambda}^1_{ij}$.

In contrast, in case (20), in which $Q_{ij} = \overline{Q}_{ij}$ and $\overline{\lambda}^2_{ij} > 0$, minus the marginal expected transaction utility is equal to $-\overline{\lambda}^2_{ij}$; namely, the marginal expected revenue is greater than the expected transaction cost. Retailer j has a marginal gain given by $\overline{\lambda}^2_{ij}$.

In conclusion, we remark that the Lagrange variables $\overline{\lambda}^1_{ij}$, $\overline{\lambda}^2_{ij}$ give a precise evaluation of the behavior of the market with respect to the supply chain product transactions.

3.2 Analysis of Marginal Expected Cybersecurity Investment Utilities

From (17) we have:

$$-\frac{\partial E(U_i(Q^*, s^*))}{\partial s_i} - \overline{\mu}^1_i + \overline{\mu}^2_i + \overline{\lambda}_i \frac{\partial h_i(s^*)}{\partial s_i} = 0, \quad i = 1, \ldots, m. \tag{21}$$

If $0 < s^*_i < u_{s_i}$, then $\overline{\mu}^1_i = \overline{\mu}^2_i = 0$ and we have (see also (10))

$$\begin{aligned} &\frac{\partial h_i(s^*_i)}{\partial s_i} + \overline{\lambda}_i \frac{\partial h_i(s^*_i)}{\partial s_i} \\ &= \left(1 - \sum_{k=1}^{m} \frac{s^*_k}{m} + \frac{1 - s^*_i}{m}\right) D_i + \sum_{k=1}^{m} \frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial s_i} \times Q^*_{ik}. \end{aligned} \tag{22}$$

Since $0 < s^*_i < u_{s_i}$, $h(s^*_i)$ cannot be the upper bound B_i; hence, $\overline{\lambda}_i$ is zero and (22) becomes:

$$\frac{\partial h_i(s^*_i)}{\partial s_i} = \left(1 - \sum_{k=1}^{m} \frac{s^*_k}{m} + \frac{1 - s^*_i}{m}\right) D_i + \sum_{k=1}^{m} \frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial s_i} \times Q^*_{ik}. \tag{23}$$

Equality (23) shows that the marginal expected cybersecurity cost is equal to the marginal expected cybersecurity investment revenue plus the term $\left(1 - \sum_{k=1}^{m} \frac{s^*_k}{m} + \frac{1 - s^*_i}{m}\right) D_i$; namely, the marginal expected cybersecurity investment revenue is equal to $\frac{\partial h_i(s^*_i)}{\partial s_i} - \left(1 - \sum_{k=1}^{m} \frac{s^*_k}{m} + \frac{1 - s^*_i}{m}\right) D_i$. This is reasonable because $\left(1 - \sum_{k=1}^{m} \frac{s^*_k}{m} + \frac{1 - s^*_i}{m}\right) D_i$ is the marginal expected damage expense.

If $\overline{\mu}^1_i > 0$ and, hence, $s^*_i = 0$, and $\overline{\mu}^2_i = 0$, we get:

$$\begin{aligned} &-\frac{\partial E(U_i(Q^*, s^*))}{\partial s_i} \\ &= \frac{\partial h_i(0)}{\partial s_i} - \left(1 - \sum_{\substack{k=1 \\ k \neq i}}^{m} \frac{s^*_k}{m} + \frac{1 - s^*_i}{m}\right) D_i - \sum_{k=1}^{m} \frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial s_i} Q^*_{ik} = \overline{\mu}^1_i. \end{aligned} \tag{24}$$

In (24) minus the marginal expected cybersecurity investment utility is equal to $\overline{\mu}^1_i$; hence, the marginal expected cybersecurity cost is greater than the

marginal expected cybersecurity investment revenue plus the marginal damage expense. Then the marginal expected cybersecurity investment revenue is less than the marginal expected cybersecurity cost minus the marginal damage expense. We note that case (24) can occur if $\frac{\partial h_i(0)}{\partial s_i}$ is strictly positive.
In contrast, if $\overline{\mu}_i^2 > 0$ and, hence, $s_i^* = u_{s_i}$, retailer j has a marginal gain given by $\overline{\mu}_i^2$, because

$$\begin{aligned}
-\frac{\partial E(U_i(Q^*, u_{s_i}))}{\partial s_i} &= -\left(1 - \sum_{\substack{k=1\\k\neq i}}^{m} \frac{u_{s_k}}{m} + \frac{1-u_{s_i}}{m}\right) D_i \\
&- \sum_{k=1}^{m} \frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial s_i} \times Q_{ik}^* \\
&+ \frac{\partial h_i(u_{s_i})}{\partial s_i} + \overline{\lambda}_i \frac{\partial h_i(u_{s_i})}{\partial s_i} = -\overline{\mu}_i^2. \qquad (25)
\end{aligned}$$

We note that $\overline{\lambda}_i$ could also be positive, since, with $s_i^* = u_{s_i}$, $h_i(s_i)$ could reach the upper bound B_i. In (25) minus the marginal expected cybersecurity investment utility is equal to $-\overline{\mu}_i^2$. Hence, the marginal expected cybersecurity cost is less than the marginal expected cybersecurity investment revenue plus the marginal damage expense. Then the marginal expected cybersecurity investment revenue is greater than the marginal expected cybersecurity cost minus the marginal damage expense.
From (25) we see the importance of the Lagrange variables $\overline{\mu}_i^1$, $\overline{\mu}_i^2$ which describe the effects of the marginal expected cybersecurity investment utilities.

3.3 Remarks on the Stability of the Marginal Expected Cybersecurity Investment Utilities

Let us consider the three cases related to the marginal expected cybersecurity investment utilities studied in Subsection 3.2. Each of these cases holds for certain values of the damage D_i. Let us consider the value D_i for which the first case (23) occurs. We see that in this case there is a unique value of D_i for which (23) holds and if we vary such a value, also the value s_i^* in (23) varies. Now let us consider the value D_i for which (24) holds and let us call D_i^* the value of D_i for which we have

$$\begin{aligned}
&-\frac{\partial E(U_i(Q^*, s^*))}{\partial s_i} \\
&= \frac{\partial h_i(0)}{\partial s_i} - \left(1 - \sum_{\substack{k=1\\k\neq i}}^{m} \frac{s_k^*}{m} + \frac{1-s_i^*}{m}\right) D_i^* - \sum_{k=1}^{m} \frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial s_i} Q_{ik}^* = 0.
\end{aligned}$$

Then for $0 < D_i < D_i^*$ the solution (Q^*, s^*) to variational inequality (9) remains unchanged because (24) still holds for these new values of D_i and the marginal expected cybersecurity investment utility remains negative, but it is increasing with respect to D_i. Analogously, if we consider the value D_i for which (25) holds and call D_i^* the value such that

$$\begin{aligned}-\frac{\partial E(U_i(Q^*, u_{s_i}))}{\partial s_i} = & - \left(1 - \sum_{\substack{k=1\\k\neq i}}^{m} \frac{u_{s_k}}{m} + \frac{1-u_{s_i}}{m}\right) D_i^* \\ & - \sum_{k=1}^{m} \frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial s_i} \times Q_{ik}^* \\ & + \frac{\partial h_i(u_{s_i})}{\partial s_i} + \overline{\lambda}_i \frac{\partial h_i(u_{s_i})}{\partial s_i} = 0,\end{aligned}$$

we see that for $D_i > D_i^*$ the solution (Q^*, s^*) to (9) remains unchanged because (25) still holds and the marginal expected cybersecurity investment utility remains positive and is increasing with respect to D_i.

4 A Numerical Example

The first example consists of two retailers and two demand markets as depicted in Fig. 2.

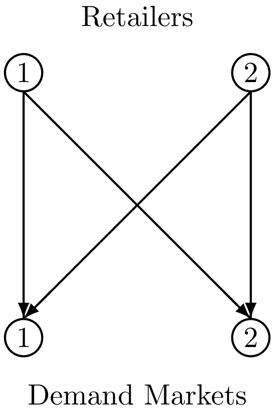

Figure 2: Network Topology for Example 1

It is inspired by related examples as in [14]. So, the cost function data are:

$$\begin{aligned} c_1 &= 5, & c_2 &= 10, \\ c_{11}(Q_{11}) &= .5Q_{11}^2 + Q_{11}, & c_{12}(Q_{12}) &= .25Q_{12}^2 + Q_{12}, \\ c_{21}(Q_{21}) &= .5Q_{21}^2 + Q_{21}, & c_{22}(Q_{22}) &= .25Q_{22}^2 + Q_{22}. \end{aligned}$$

The demand price functions are:

$$\rho_1(d, \overline{s}) = -d_1 + .1\frac{s_1 + s_2}{2} + 100, \quad \rho_2(d, \overline{s}) = -.5d_2 + .2\frac{s_1 + s_2}{2} + 200.$$

The damage parameters are: $D_1 = 200$ and $D_2 = 210$ with the investment functions taking the form:

$$h_1(s_1) = \frac{1}{\sqrt{1-s_1}} - 1, \quad h_2(s_2) = \frac{1}{\sqrt{1-s_2}} - 1.$$

The damage parameters are in millions of \$US, the expected profits (and revenues) and the costs are also in millions of \$US. The prices are in thousands of dollars and the product transactions are in thousands. The budgets for the two retailers are identical with $B_1 = B_2 = 2.5$ (in millions of \$US). In this case the bounds on the security levels are $u_{s_1} = u_{s_2} = .91$ and the capacities $\overline{Q}_{ij}$ are set to 100 for all i, j.
For $i = 1$, 2 we obtain:

$$\begin{aligned}
-\frac{\partial E(U_i(Q,s))}{\partial Q_{i1}} &= 2Q_{i1} + Q_{11} + Q_{21} - .1\frac{s_1+s_2}{2} + c_i - 99,\\
-\frac{\partial E(U_i(Q,s))}{\partial Q_{i2}} &= Q_{i2} + .5Q_{12} + .5Q_{22} - .2\frac{s_1+s_2}{2} + c_i - 199,\\
-\frac{\partial E(U_i(Q,s))}{\partial s_i} &= -\frac{1}{20}Q_{i1} - \frac{1}{10}Q_{i2} - \left(1 - \frac{s_1+s_2}{2} + \frac{1-s_i}{2}\right) D_i\\
&\quad + \frac{1}{2\sqrt{(1-s_i)^3}}.
\end{aligned}$$

Now, we want to find the equilibrium solution, taking into account the different values assumed by λ^1, λ^2, μ^1, μ^2 and λ, and searching, among them, the feasible ones. After some algebraic calculations, we realize that for $i = 1, 2$ and $j = 1, 2$ we get the solution when $\overline{\lambda}^1_{ij} = \overline{\lambda}^2_{ij} = \overline{\mu}^1_i = \overline{\lambda}_i = 0$, and $\overline{\mu}^2_i > 0$. Hence, $s^*_1 = s^*_2 = 0.91$ (which is the maximum value). In this case, the marginal expected transaction utilities are zero, whereas the marginal expected cybersecurity investment utilities are positive; namely, there is a marginal gain, given by $\overline{\mu}^2_i$, $i = 1, 2$. Solving the system:

$$\left\{\begin{array}{lll}
\dfrac{\partial \mathcal{L}(Q^*, s^*, \overline{\lambda}^1, \overline{\lambda}^2, \overline{\mu}^1, \overline{\mu}^2, \overline{\lambda})}{\partial Q_{i1}} & = & 0\\[2ex]
\dfrac{\partial \mathcal{L}(Q^*, s^*, \overline{\lambda}^1, \overline{\lambda}^2, \overline{\mu}^1, \overline{\mu}^2, \overline{\lambda})}{\partial Q_{i2}} & = & 0 \qquad i = 1, 2,\\[2ex]
\dfrac{\partial \mathcal{L}(Q^*, s^*, \overline{\lambda}^1, \overline{\lambda}^2, \overline{\mu}^1, \overline{\mu}^2, \overline{\lambda})}{\partial s_i} & = & 0
\end{array}\right.$$

namely:

$$\left\{\begin{array}{lcl}
3Q^*_{11} + Q^*_{21} - 0.1\dfrac{s^*_1 + s^*_2}{2} + c_1 - 99 - \overline{\lambda}^1_{11} + \overline{\lambda}^2_{11} & = & 0 \\[2ex]
Q^*_{11} + 3Q^*_{21} - 0.1\dfrac{s^*_1 + s^*_2}{2} + c_2 - 99 - \overline{\lambda}^1_{21} + \overline{\lambda}^2_{21} & = & 0 \\[2ex]
1.5Q^*_{12} + .5Q^*_{22} - 0.2\dfrac{s^*_1 + s^*_2}{2} + c_1 - 199 - \overline{\lambda}^1_{12} + \overline{\lambda}^2_{12} & = & 0 \\
.5Q^*_{12} + 1.5Q^*_{22} - 0.2\dfrac{s^*_1 + s^*_2}{2} + c_2 - 199 - \overline{\lambda}^1_{22} + \overline{\lambda}^2_{22} & = & 0 \\[2ex]
-\dfrac{1}{20}Q^*_{11} - \dfrac{1}{10}Q^*_{12} - \dfrac{3 - 2s^*_1 - s^*_2}{2}D_1 + \dfrac{1 + \overline{\lambda}_1}{2\sqrt{(1 - s^*_1)^3}} - \overline{\mu}^1_1 + \overline{\mu}^2_1 & = & 0 \\[2ex]
-\dfrac{1}{20}Q^*_{21} - \dfrac{1}{10}Q^*_{22} - \dfrac{3 - s^*_1 - 2s^*_2}{2}D_2 + \dfrac{1 + \overline{\lambda}_2}{2\sqrt{(1 - s^*_2)^3}} - \overline{\mu}^1_2 + \overline{\mu}^2_2 & = & 0,
\end{array}\right.$$

and therefore, assuming for $i = 1, 2$, $j = 1, 2$, $\overline{\lambda}^1_{ij} = \overline{\lambda}^2_{ij} = \overline{\mu}^1_i = \overline{\lambda}_i = 0$, and $\overline{\mu}^2_i > 0$, hence $s^*_1 = s^*_2 = 0.91$, and $D_1 = 200$ and $D_2 = 210$, we have:

$$\left\{\begin{array}{lcl}
3Q^*_{11} + Q^*_{21} & = & 94.091 \\[1ex]
Q^*_{11} + 3Q^*_{21} & = & 89.091 \\[1ex]
1.5Q^*_{12} + .5Q^*_{22} & = & 195.82 \\[1ex]
.5Q^*_{12} + 1.5Q^*_{22} & = & 190.82 \\[1ex]
\overline{\mu}^2_1 & = & \dfrac{1}{20}Q^*_{11} + \dfrac{1}{10}Q^*_{12} - \dfrac{3 - 3 \times .91}{2}200 - \dfrac{1}{2\sqrt{(1 - .91)^3}} \\[2ex]
\overline{\mu}^2_2 & = & \dfrac{1}{20}Q^*_{21} + \dfrac{1}{10}Q^*_{12} - \dfrac{3 - 3 \times .91}{2}210 - \dfrac{1}{2\sqrt{(1 - .91)^3}}.
\end{array}\right.$$

The solution to the previous system is:

$$Q^*_{11} = 24.148, \quad Q^*_{21} = 21.586, \quad Q^*_{12} = 99.16, \quad Q^*_{22} = 94.16,$$

$$\overline{\mu}^2_1 = 19.6055, \quad \overline{\mu}^2_2 = 20.3273,$$

where $\overline{\mu}^2_1$ and μ^2_2 are the positive marginal expected gains.
For this example the stability results of Subsection 3.3 hold. We are in the third case and if we double the value of the damage for the first retailer and assume now $D_1 = 400$, then the new value of the Lagrange multiplier is $\overline{\mu}^2_1 = 46.6055$.

5 Conclusions

Cyberattacks are negatively globally impacting numerous sectors of economies as well as governments and even citizens, and resulting in financial damages, disruptions, loss of services, etc. Hence, organizations, including companies from financial service firms to retailers, as well as utilities, are investing in cybersecurity. In this paper, we revisit a recently introduced cybersecurity investment supply chain game theory model described in [14] consisting of retailers and consumers at demand markets in which nonlinear budget constraints of the retailers associated with cybersecurity investments are explicitly included. The retailers compete in both product transactions and cybersecurity levels seeking to maximize their expected utilities, that is, expected profits, which capture both the expected revenues and the expected damages in the case of a cyberattack, which can differ from retailer to retailer. The consumers display their preferences through the demand price functions which are functions of the market demands for the product as well as the average security level of the network, which depends on all the retailers' investment levels. The governing equilibrium concept in this model of noncooperative behavior is that of Nash equilibrium.

In this paper, we provide a novel alternative formulation of the variational inequality formulation derived in [14]. The alternative formulation enables a deep analysis of the Lagrange multipliers associated with both the bounds on the product transactions between retailers and demand markets and the security levels of the retailers, with accompanying insights into the economic market forces. Specifically, we provide an analysis of both the marginal expected transaction utilities and the marginal expected cybersecurity investment utilities of the retailers. We also obtain stability results for the marginal expected cybersecurity investment utilities with respect to changes in the values of the retailers' financial damages.

The novel theoretical framework is then further illustrated through a numerical example for which the equilibrium product transaction and cybersecurity investment patterns are computed, along with the Lagrange multipliers. In addition, stability results are also given for the case where the first retailer's damage due to a cyberattack doubles.

The results in this paper add to the growing literature of operations research and game theory techniques for cybersecurity modeling and analysis.

Acknowledgments The research of the first author was partially supported by Istituto Nazionale di Alta Matematica Francesco Severi (Progetto di Ricerca GNAMPA 2015: *Nuove frontiere dei problemi di equlibrio su rete: dallo sviluppo sostenibile alla dinamica dei disastri ambientali ai crimini informatici*). The research of the third author was supported, in part, by the National Science Foundation under Grant No. 1551444. This support is gratefully acknowledged.

References

[1] A. Barbagallo, P. Daniele, S. Giuffré, A. Maugeri, Variational Approach for a General Financial Equilibrium Problem: The Deficit Formula, the Balance Law and the Liability Formula. A Path to the Economy Recovery, *European Journal of Operational Research*, 237(1), (2014), 231-244.

[2] P. Daniele, S. Giuffré, Random Variational Inequalities and the Random Traffic Equilibrium Problem, *J. Optim. Theory Appl.*, 167(1), (2015), 363-381.

[3] P. Daniele, S. Giuffré, M. Lorino, Functional Inequalities, Regularity and Computation of the Deficit and Surplus Variables in the Financial Equilibrium Problem, *Journal of Global Optimization*, DOI 10.1007/s10898-015-0382-4.

[4] P. Daniele, S. Giuffré, A. Maugeri, F. Raciti, Duality Theory and Applications to Unilateral Problems, *J. Optim. Theory Appl.*, 162, (2014), 718-734.

[5] P. Daniele, S. Giuffré, M. Lorino, A. Maugeri, C. Mirabella, Functional Inequalities and Analysis of Contagion in the Financial Networks, in **Handbook of Functional Equations**, Springer Optim. Appl., 95, Springer, New York, (2014), 129-146.

[6] N.J. Daras, M.T. Rassias, (Eds.), **Computation, Cryptography, and Network Security**, Springer International Publishing Switzerland (2015).

[7] S. Giuffré, A. Maugeri, D. Puglisi, Lagrange Multipliers in Elastic-Plastic Torsion Problem for Nonlinear Monotone Operators, *J. Differential Equations*, 259(3), (2015), 817-837.

[8] S. Giuffré, A. Maugeri, A Measure-Type Lagrange Multiplier for the Elastic-Plastic Torsion, *Nonlinear Anal.*, 102, (2014), 23-29.

[9] L.A. Gordon, M.P. Loeb, M.P., W. Lucyshyn, L. Zhou, Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model, *Journal of Information Security*, 6, (2015), 24-30.

[10] J. Jahn, **Introduction to the Theory of Nonlinear Optimization**, Berlin, Springer-Verlag (1994).

[11] M.H. Manshaei, T. Alpcan, T. Basar, J.-P. Hubaux, Game Theory Meets Network Security and Privacy, *ACM Computing Surveys*, (2013), June, 45(3), Article No, 25.

[12] S. Morgan, Cybersecurity Market Reaches $75 Billon in 2015; Expected to Reach $170 Billion by 2020, *Forbes*, December 20 (2015).

[13] A. Nagurney, A Multiproduct Network Economic Model of Cybercrime in Financial Services, *Service Science*, 7(1), (2015), 70-81.

[14] A. Nagurney, P. Daniele, S. Shukla, A Supply Chain Network Game Theory Model of Cybersecurity Investments with Nonlinear Budget Constraints, *Annals of Operations Research*, 248(1), (2017), 405-427.

[15] A. Nagurney and L.S. Nagurney, A Game Theory Model of Cybersecurity Investments with Information Asymmetry, *Netnomics*, 16(1-2), (2015), 127-148.

[16] A. Nagurney, L.S. Nagurney,a and S. Shukla, A Supply Chain Game Theory Framework for Cybersecurity Investments Under Network Vulnerability, in **Computation, Cryptography, and Network Security**, N.J. Daras and M.T. Rassias, Editors, Springer International Publishing Switzerland (2015), 381-398.

[17] J.F. Nash, Equilibrium Points in n-Person Games, *Proceedings of the National Academy of Sciences, USA*, 36, (1950), 48-49.

[18] J.F. Nash, Noncooperative Games. *Annals of Mathematics*, 54, (1951), 286-298.

[19] R. Ostvold and B. Walker, Business Resilience in the Face of Cyber Risk, Accenture (2015).

[20] N. Shetty, G. Schwartz, M. Felegehazy, J. Walrand, Competitive Cyber-Insurance and Internet Security. *Proceedings of the Eighth Workshop on the Economics of Information Security (WEIS 2009)*, University College London, England, June 24-25 (2009).

[21] F. Toyasaki, P. Daniele, T. Wakolbinger, A Variational Inequality Formulation of Equilibrium Models for End-of-Life Products with Nonlinear Constraints, *European J. Oper. Res.*, 236(1), (2014), 340-350.

[22] W. Yakowicz, Companies Lose $400 Billion to Hackers Each Year, *Inc.*, September 8 (2015).