A PROJECTED DYNAMIC SYSTEM ASSOCIATED WITH A CYBERSECURITY INVESTMENT MODEL WITH BUDGET CONSTRAINTS AND FIXED DEMANDS

GABRIELLA COLAJANNI, PATRIZIA DANIELE*, DANIELE SCIACCA

Department of Mathematics, University of Catania, Catania, Italy

Abstract. In this paper, we present a cybersecurity investment supply chain model with nonlinear budget constraints and fixed demands, which gives a generalized Nash equilibrium model. We define the related variational equilibrium and study the associated projected dynamic system (PDS), establishing the relationship between the solutions to the variational inequality and the stationary points of the PDS. Then, we propose a computational procedure to find such stationary points and, finally, some numerical examples illustrate the obtained results.

Keywords. Expected utility; Supply chains; Variational inequalities; Projected Dynamic Systems.

1. INTRODUCTION

Cybersecurity consists in safeguarding the confidentiality, integrity and availability of information managed by an organization. A safeguard not only from direct attacks, but also, for example, from phenomena such as natural disasters or from accidental problems. More specifically, IT security is a subset of information security and can be defined as the set of products, services, organizational rules and individual behaviors that protect computer systems of a company.

In general, cybersecurity actually involves many distinct activities: security at the application level, data level, at the network level (when you exchange data over the Internet, network security must be guaranteed, so that these are not intercepted) and so on. According to a Gartner analysis, in 2018 around 114 billion dollars in computer security have been spent globally and network protection accounts for almost 12.5 billion. Investments in Identity and Access management, also crucial in the corporate sphere, went from a value of 8.8 billion in 2017 to 9.7 billion in 2018, which will become 10.6 in 2019. According to a report from the Information Security and Privacy Observatory of the Polytechnic of Milan, also in Italy there is a development trend: in 2017 the market for information security solutions reached a value of 1.09 billion euros, in growth of 12% compared to 2016. A step forward clearly higher than that observed in previous years, when the domestic market was at about 4-6%. The need to be compliant with the new European privacy law, the GDPR, which alone accounts for about half

of the expenditure increase identified by the research, pushes large companies more than the great attacks mentioned above. It is worth mentioning that cybersecurity has a thirty-year history: the first computer virus in history, Brain A, arrived in 1986 directly from Pakistan. Later it was the turn of AIDS in 1989, a malware that presented very strong analogies with the current ransomware. From then on, every year there were particular viruses: in 1992 Michelangelo arrived, in 1995 Concept, while the millennium ended with Happy 99. The new millennium opened with Melissa and Loveletter, while 2003 was the year both of the first successful attack against a critical infrastructure, the US transport company CSX, and of the first mobile virus in history. Going forward over the years we get to more recent names like Zeus and Stuxnet. The most attacked system is Android, in particular due to the lack of protection provided by users, although iOS can certainly not be considered immune from the risk. The costs of all these activities are considerable: in 2017 cybercrime alone caused damages for 500 billion dollars. Scams, extortion, money and personal data theft hit almost a billion people in the world, causing only an estimated loss of 180 billion dollars to private citizens. According to a recent Kaspersky Lab and B2B International survey, the lack of IT security awareness is still alarming in companies all around the world. The study, which involved 7,993 employees, showed that only 12% of employees is fully aware of the IT security policies and rules established by the company they work for and 24% of people believe that their company has not established any policy. However, it is interesting to note that ignorance of the rules is not considered an excuse: almost half of respondents (49%) think, in fact, that all employees - themselves included - should take responsibility for protecting corporate IT resources from threats computer. Given these premises, employees not only risk to become the victims of cyber criminals, but they also risk to make their company victims of cyber threats. The priority of organizations should therefore be to engage in staff education. As we mentioned earlier, in recent years many secure corporate investments have been driven by the entry into force of the GDPR. Despite the greater overall attention regarding the issue of cyber security, the attacks of cybercrime show no sign of abating, on the contrary. This is highlighted by a study released by Clusit, which refers to the first half of 2018: in this period, 730 serious attacks were recorded globally, which correspond to a 31% growth compared to the previous semester. Numbers that make the first half of 2018 the worst ever: in particular, during this period there was an average of 122 serious attacks per month (compared to an average of 94 per month in 2017). At the global level in 2018, 1,552 serious attacks were registered, with an average of 129 episodes per month, which is almost 37.7% more than in 2017. As for the targets, health was certainly in the sights, so that they suffered the greatest increase in actions, even 99% compared to 2017. One of the hottest areas of computer security is undoubtedly the one related to Cyberwar: groups of hackers, specially backed and financed by sovereign states, that carry out attacks with the aim of stealing data or damaging the functioning of organizations (public or private) of powers considered rivals. Russia has often been accused of pushing such practices, but in July 2019 Moscow was the victim of a cyberwar attack. In particular SyTech, provider of the FSB secret service (Federal Security Service of the Russian Federation), was the victim of a cyber attack: the cyber criminals would have stolen - according to what reconstructed by the BBC - about 7.5 terabytes of confidential information. Subsequently the cyber criminals shared the information stolen from the collective hacker Digital Revolution, which sent it to some newspapers. In the literature cybersecurity models have been studied both in the case of elastic (see [2] and [12]) and fixed demands (see

[1]). Further, an analysis of the dual problem and its associated Lagrange multipliers has been performed, together with the study of the marginal expected transaction utility for each retailer. Other cybersecurity models have been introduced by Daras and Rassias in [3], by Nagurney A., Nagurney L.S., Alvarez Flores and Shukla in [10, 11, 13, 14, 15] and by Shetty, Schwartz, Felegehazy, and Walrand in [17].

In this paper we start from the model in [1] and characterize the solutions of the deriving variational inequality through the critical points of a suitable projected dynamic system. The paper is organized as follows. In Section 2, we present the model as a bipartite supply chain network with retailers and consumers at demand markets in the presence of budget constraints and with a mean value of the security levels which also depends on the flows of product. Then, we give the variational equilibrium definition of the generalized Nash equilibrium. In Section 3, we characterize the solutions to the variational inequality as the stationary points of an associated projected dynamic system and find uniqueness results. In Section 4, we give a computational procedure based on the Euler method to find the solutions to the variational inequality. Finally, in Section 5, we provide some illustrative numerical examples and in Section 6, we present the conclusions.

2. THE MODEL

As in [12], we consider a supply chain network consisting of retailers and consumers at demand markets, as depicted in Figure 1. Each retailer i can transact with each demand market j and Q_{ij} denotes the product transaction from i to j, $i = 1, \ldots, m$, and $j = 1, \ldots, n$. We associate with each retailer i a cybersecurity level $s \in [0, 1[$, $i = 1, \ldots, m$. We group the product transactions for each retailer i into the vector $Q_i \in \mathbb{R}^n$ and then we group all such retailer transaction vectors into the vector $Q \in \mathbb{R}^{mn}$. Analogously, the security levels of the retailers are grouped into the vector $s \in \mathbb{R}^m$.

Unlike [12], where the arithmetic mean of all the security levels is chosen as the average value, here we assume that the mean value depends also on the quantity of product. Hence, we choose the following weighted average as the cybersecurity level in the entire supply chain network:

$$\bar{s} = \frac{\displaystyle\sum_{i=1}^{m} s_i \sum_{j=1}^{n} Q_{ij}}{\displaystyle\sum_{i=1}^{m} \sum_{j=1}^{n} Q_{ij}},$$

where we assume that $\displaystyle\sum_{i=1}^{m} \sum_{j=1}^{n} Q_{ij} > 0$, namely there exists some $Q_{ij} > 0$.

Also, as in [14], we introduce a retailer's vulnerability $v_i = 1 - s_i$, $i = 1, \ldots, m$, and the network vulnerability $\bar{v} = 1 - \bar{s}$.

As in [1], the demand at each demand market j, d_j, is assumed to be fixed and known and such that it satisfies the following conservation law:

$$d_j = \sum_{i=1}^{m} Q_{ij}, \quad j = 1, \ldots, n. \tag{2.1}$$

We group the demands at the demand markets into the vector $d \in \mathbb{R}^n$.
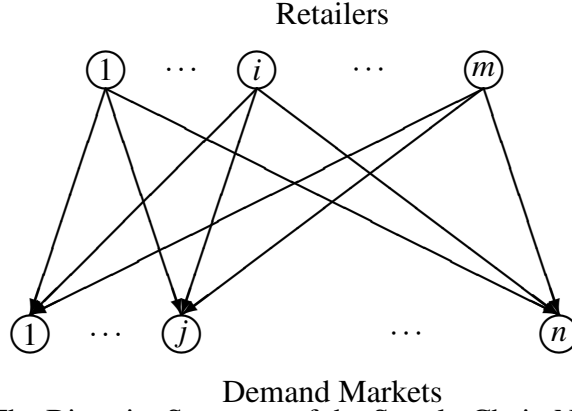
Retailers

Demand Markets
FIGURE 1. The Bipartite Structure of the Supply Chain Network Model

We denote by $\bar{Q}_{ij}$ an upper bound of the product transactions, which have also to be nonnegative, so that the following conditions have to be satisfied:

$$0 \le Q_{ij} \le \bar{Q}_{ij}, \text{ with } \sum_{i=1}^{m} \overline{Q}_{ij} > d_j \quad i = 1, \dots, m; j = 1, \dots, n. \tag{2.2}$$

We denote by u_{s_i} the upper bound of the cybersecurity level of each retailer i, $i = 1, \dots, m$, with $u_{s_i} < 1$, since perfect security cannot be guaranteed:

$$0 \le s_i \le u_{s_i}, \quad i = 1, \dots, m, \tag{2.3}$$

As in [1], we assume that the demand price functions are continuously differentiable and are given by $\hat{\rho}_j(Q, s) \equiv \rho_j(d, s)$, $j = 1, \dots, n$.

As in [17], in [14] and in [1], we choose as an investment cost function h_i, $i = 1, \dots, m$, the following function:

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

where the presence of the coefficient α_i allows distinct retailers to have different investment cost functions based on their size and needs.

Assuming, as in [12] and in [1], that there is a limited budget for cybersecurity investments, we have that the following nonlinear budget constraints must be satisfied:

$$\alpha_i \left(\frac{1}{\sqrt{(1 - s_i)}} - 1 \right) \le B_i, \quad i = 1, \dots, m. \tag{2.4}$$

Denoting by $E(U_i)$ the expected utility of each retailer i, $i = 1, \dots, m$, his aim is to maximize such a profit given by:

$$E(U_i) = \sum_{j=1}^{n} \hat{\rho}_j(Q, s) Q_{ij} - c_i \sum_{j=1}^{n} Q_{ij} - \sum_{j=1}^{n} c_{ij}(Q_{ij}) - p_i D_i - h_i(s_i), \tag{2.5}$$

where the first term represents his revenue, the second term represents the production costs, the third term represents the transportation costs, $p_i D_i$ is the expected financial damage in the case of a successful cyberattack with $p_i = (1 - s_i)(1 - \bar{s})$, $i = 1, \dots, m$, and the fourth term represents the investment cost function.

We define the feasible set:

$$\mathbb{K} \equiv \Big\{ (Q,s) \in \mathbb{R}^{mn+m} : -Q_{ij} \leq 0,\ Q_{ij} - \overline{Q}_{ij} \leq 0,\ -s_i \leq 0,$$

$$s_i - u_{s_i} \leq 0,\ h(s_i) - B_i \leq 0,\ i = 1,\ldots,m,\ j = 1,\ldots,n \Big\},$$

and we add the set of shared constraints $\mathscr{S}$ as follows:

$$\mathscr{S} \equiv \{Q|(1)\,\text{holds}\}.$$

As in [1], we can state the following Generalized Nash Equilibrium (GNE) definition (see also [6] and [18]).

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

$$E(U_i(Q_i^*, s_i^*, \hat{Q}_i^*, \hat{s}_i^*)) \geq E(U_i(Q_i, s_i, \hat{Q}_i^*, \hat{s}_i^*)), \quad \forall (Q_i, s_i) \in \mathbb{K}^i, \forall Q \in \mathscr{S}, \qquad (2.6)$$

where

$$\hat{Q}_i^* \equiv (Q_1^*, \ldots, Q_{i-1}^*, Q_{i+1}^*, \ldots, Q_m^*),$$

$$\hat{s}_i^* \equiv (s_1^*, \ldots, s_{i-1}^*, s_{i+1}^*, \ldots, s_m^*)$$

and

$$\mathbb{K}^i \equiv \Big\{ (Q_i, s_i) : 0 \leq Q_{ij} \leq \overline{Q}_{ij},\ \forall j; 0 \leq s_i \leq u_{s_i},\ h(s_i) - B_i \leq 0 \Big\}.$$

Hence, we can determine the equilibrium solution via a variational inequality, rather than a quasi-variational inequality, through a variational equilibrium ([7] and [8]), which is different that the one in [1], since we have used a different mean value.

Definition 2.2. (Variational Equilibrium) A product transaction and security level pattern (Q^*, s^*) is said to be a variational equilibrium of the above Generalized Nash equilibrium if $(Q^*, s^*) \in \mathbb{K}$, $Q^* \in \mathscr{S}$, is a solution of the variational inequality

$$-\sum_{i=1}^{m} \sum_{j=1}^{n} \frac{\partial E(U_i(Q^*, s^*))}{\partial Q_{ij}} \times (Q_{ij} - Q_{ij}^*) - \sum_{i=1}^{m} \frac{\partial E(U_i(Q^*, s^*))}{\partial s_i} \times (s_i - s_i^*) \geq 0,$$

$$\forall (Q, s) \in \mathbb{K}, \forall Q \in \mathscr{S}; \qquad (2.7)$$

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

$$\sum_{i=1}^{m} \sum_{j=1}^{n} \left[c_i + \frac{\partial c_{ij}(Q_{ij}^*)}{\partial Q_{ij}} - \hat{\rho}_j(Q^*, s^*) - \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial Q_{ij}} \cdot Q_{ik}^* \right.$$
$$\left. + (1 - s_i^*) \frac{-s_i^* \sum\limits_{h=1}^{m} \sum\limits_{k=1}^{n} Q_{hk}^* + \sum\limits_{h=1}^{m} s_h^* \left(\sum\limits_{k=1}^{n} Q_{hk}^* \right)}{\left(\sum\limits_{h=1}^{m} \sum\limits_{k=1}^{n} Q_{hk}^* \right)^2} \cdot D_i \right] \times (Q_{ij} - Q_{ij}^*)$$

$$+ \sum_{i=1}^{m} \left[-\sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial s_i} \cdot Q_{ik}^* + \frac{\alpha_i}{2} \frac{1}{\sqrt{(1 - s_i^*)^3}} \right. \tag{2.8}$$
$$\left. + \left(1 - \frac{\sum\limits_{h=1}^{m} s_h^* \left(\sum\limits_{k=1}^{n} Q_{hk}^* \right)}{\sum\limits_{h=1}^{m} \sum\limits_{k=1}^{n} Q_{hk}^*} + (1 - s_i) \frac{\sum\limits_{k=1}^{n} Q_{hk}^*}{\sum\limits_{h=1}^{m} \sum\limits_{k=1}^{n} Q_{hk}^*} \right) \cdot D_i \right] \times (s_i - s_i^*) \geq 0,$$

$$\forall (Q, s) \in \mathbb{K}, \forall Q \in \mathscr{S}.$$

Also in this case, problem (2.8) admits a solution since the classical existence theorem, which requires that the set $\mathscr{K} \equiv \mathbb{K} \cap \mathscr{S}$ is closed, convex, and bounded and the function entering the variational inequality is continuous, is satisfied (see also [9]).

We now put variational inequality (2.8) into standard form, that is: determine $X^* \in \mathscr{K} \subset \mathbb{R}^N$ such that

$$\langle F(X^*), X - X^* \rangle \geq 0, \quad \forall X \in \mathscr{K}, \tag{2.9}$$

where F is a given function from $\mathscr{K}$ to $\mathbb{R}^N$ and $\mathscr{K}$ is a closed and convex set. We define the $(mn + m)$-dimensional column vector $X = (Q, s)$ and the $(mn + m)$-dimensional column vector $F(X) \equiv (F^1(X), F^2(X))$, where the (i, j)-th component, F_{ij}^1, of $F^1(X)$ is given by

$$F_{ij}^1(X) \equiv -\frac{\partial E(U_i(Q, s))}{\partial Q_{ij}}, \tag{2.10}$$

and the i-th component, F_i^2, of $F^2(X)$ is given by

$$F_i^2(X) \equiv -\frac{\partial E(U_i(Q, s))}{\partial s_i}, \tag{2.11}$$

and the feasible set $\mathscr{K}$ is defined as above. Clearly, variational inequality (2.8) can be rewritten as (2.9).

Now, we want to build the projected dynamic system associated with our Nash's game model for the network of cybersecurity investments, which has not been studied yet.

3. The associated projected dynamic system

First, we propose a dynamic adaptation process that will be subsequently formulated in terms of a projected dynamic system (see also [16]). Then, we show that the set of stationary points

of the projected dynamic system coincides with the set of solutions to variational inequality (2.8). As we know, in the feasible set $\mathcal{K}$ there are nonlinear budget constraints (2.4) and it would not be a convex polyhedron. This could have some critical issues in the description of the dynamic adjustment processes, according to which the variables of the problem vary over time, and in the construction of the associated dynamic system to these processes. To overcome these computational difficulties, constraints (2.4) can be relaxed by resorting to an alternative variational formulation of the problem that incorporates the constraints in the objective function, making use of the associated Lagrange function.

However, it is possible to realize a linearization of the feasible set $\mathcal{K}$, by taking into account the upper bounds on the levels of cybersecurity and the constraints (2.4). Observe, in fact, that the quantities α_i, B_i and u_{s_i}, $i = 1, \ldots, m$, are fixed and not negative, so we can say that the nonlinear budget constraints are met if and only if

$$\alpha_i \left(\frac{1}{\sqrt{(1-s_i)}} - 1 \right) \leq B_i \Leftrightarrow \frac{1}{\sqrt{(1-s_i)}} - 1 \leq \frac{B_i}{\alpha_i}$$

$$\Leftrightarrow \left(\frac{B_i}{\alpha_i} + 1 \right) \sqrt{1-s_i} \geq 1 \Leftrightarrow s_i \leq 1 - \left(\frac{\alpha_i}{B_i + \alpha_i} \right)^2.$$

Observe that $\left(\frac{\alpha_i}{B_i + \alpha_i} \right)^2$ has no dimension and $\left(\frac{\alpha_i}{B_i + \alpha_i} \right)^2 < 1$, for every $i = 1, \ldots, m$. As a consequence, it follows:

$$1 - \left(\frac{\alpha_i}{B_i + \alpha_i} \right)^2 < 1.$$

So, if we denote by

$$\hat{s}_i = \min \left\{ u_{s_i}, 1 - \left(\frac{\alpha_i}{B_i + \alpha_i} \right)^2 \right\},$$

then the feasible set for each retailer can be written as:

$$\tilde{\mathbb{K}}^i = \left\{ (Q_i, s_i) : 0 \leq Q_{ij} \leq \bar{Q}_{ij}, \ i = 1, \ldots 0 \leq s_i \leq \hat{s}_i, j = 1, \ldots, n \right\},$$

and $\tilde{\mathbb{K}} = \prod_{i=1}^m \tilde{\mathbb{K}}^i$. Now, if we add the set of sharer constraints $\mathscr{S}$, the feasible set of problem (2.8) becomes $\tilde{\mathcal{K}} = \tilde{\mathbb{K}} \cap \mathscr{S}$, which is a convex, closed, non empty and bounded polyhedron.

Moreover, $\tilde{\mathcal{K}}$ can be rewritten as $\tilde{\mathcal{K}} = \tilde{\mathcal{K}}_1 \times \tilde{\mathcal{K}}_2$, where

$$\tilde{\mathcal{K}}_1 = \left\{ Q \in \mathbb{R}^{mn} | 0 \leq Q_{ij} \leq \bar{Q}_{ij}, \ i = 1, \ldots, m, j = 1, \ldots, n, \sum_{i=1}^m Q_{ij} = d_j, \ j = 1, \ldots, n \right\}, \quad (3.1)$$

$$\tilde{\mathcal{K}}_2 = \left\{ s \in \mathbb{R}^m | 0 \leq s_i \leq \hat{s}_i, i = 1, \ldots, m \right\}. \quad (3.2)$$

We first present the dynamics that describe at each time the behavior of the manufacturers as a function of the product flows with the demand markets. Let us suppose that the product flows between retailers and demand markets vary with a rate which is proportional to the marginal profits with respect to the flows, i.e.

$$-F_{ij}^1(Q, s) \equiv \frac{\partial E(U_i(Q, s))}{\partial Q_{ij}}, \quad \forall i = 1, \ldots, m, \ j = 1, \ldots, n. \quad (3.3)$$

Hence, retailers continuously adapt the quantities Q_{ij} with the intention of maximizing their profits. However, the flows have to satisfy the capacity constraints and the conservation law, which requires that the sum of the quantities sold by each retailer to a fixed market demand is equal to the demand quantity, d_j, which is fixed and known. Therefore, for each market of demand, retailers adapt the quantities to be shipped with the aim of maximizing their own expected profit. Therefore, the incentive of each retailer to avoid less advantageous flows will adapt dynamically to the quantity of product that other retailers send to each demand market, so that the sum of the flows is equal to the demand in each market of question. As a consequence, the model suggests that product flows vary in relation to a rate that is equal to the projection of the profit of each retailer within the feasible set $\tilde{\mathcal{K}}_1$, namely,

$$\Pi_{\tilde{\mathcal{K}}_1}(Q, -F^1(Q, s)), \tag{3.4}$$

where, for every given $x \in K$, $\mathbb{K} \subset \mathbb{R}^m$, and $v \in \mathbb{R}^n$, $\Pi_K : \Omega \times \mathbb{R}^n \to \mathbb{R}^n$ is the projection of vector v at x with respect to K defined by

$$\Pi_K(x, v) = \lim_{\delta \to 0} \frac{(P_K(x + \delta v) - x)}{\delta}, \tag{3.5}$$

and $P_K : \mathbb{R}^n \to K$ is the projection operator, where, for any $v \in \mathbb{R}^n$, $P_K(v)$ is such that

$$\|P_K(z) - z\| = \inf_{y \in K} \|y - z\|. \tag{3.6}$$

Indeed, it represents the best direction along which it is possible to relocate the product flows in order to increase the profit of the retailers (see [16]).

Now, we describe the dynamics of the cybersecurity levels of each retailer i. In this case, the feasible set, $\tilde{\mathcal{K}}_2$, is defined only by box constraints and so it is possible to have a closed form of the equations that regulate the dynamic adjustment processes. We assume that the rate of change of the security levels s_i, denoted by $\dot{s}_i$, is equal to the difference between the following two quantities:

- the expected marginal revenues related to cybersecurity investments, namely,

$$\sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q, s)}{\partial s_i} Q_{ik};$$

- the difference between expected marginal costs related to cybersecurity investments, namely, $\dfrac{\partial h_i(s_i)}{\partial s_i}$, and the marginal expenses related to expected damages (see [1]), that is,

$$\left(1 - \frac{\sum\limits_{h=1}^{m} s_h \left(\sum\limits_{k=1}^{n} Q_{ik} \right)}{\sum\limits_{h=1}^{m} \sum\limits_{k=1}^{n} Q_{hk}} + (1 - s_i) \frac{\sum\limits_{k=1}^{n} Q_{ik}}{\sum\limits_{h=1}^{m} \sum\limits_{k=1}^{n} Q_{hk}} \right) D_i.$$

Therefore, as long as the security levels s_i are $0 < s_i < \hat{s}_i$, it is reasonable to assume that the rate of change of cybersecurity levels of a retailer i is proportional to $-F_i^2(X)$. So, if the marginal revenues related to the sale to all the demand markets exceed the difference between the expected marginal costs related to the cybersecurity investments and the marginal expenses

related to the expected damages, then the level of cybersecurity of the retailer i increases, otherwise it decreases. Therefore, if $0 < s_i < \hat{s}_i$, then we have the following dynamics:

$$
\dot{s}_i = \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q,s)}{\partial s_i} Q_{ik} - \left[\frac{\partial h_i(s_i)}{\partial s_i} - \left(1 - \frac{\sum_{h=1}^{m} s_h \left(\sum_{k=1}^{n} Q_{ik} \right)}{\sum_{h=1}^{m} \sum_{k=1}^{n} Q_{hk}} + \frac{(1-s_i) \sum_{k=1}^{n} Q_{ik}}{\sum_{h=1}^{m} \sum_{k=1}^{n} Q_{hk}} \right) D_i \right]. \quad (3.7)
$$

On the other hand, when $s_i = 0$, the non-negativity of security levels in (2.3) guarantees that the information security level remains at zero if $F_i^2(X) \geq 0$. So, in this case, only an increase in the cybersecurity level for the retailer i is possible and this happens only when the marginal revenues related to the sale to all the demand markets exceed the difference between the expected marginal costs related to security investments and the marginal expenses related to expected damages. Therefore, when $s_i = 0$, then we have the following dynamics:

$$
\dot{s}_i = \max \left\{ 0, \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q,s)}{\partial s_i} Q_{ik} - \left[\frac{\partial h_i(s_i)}{\partial s_i} - \left(1 - \frac{\sum_{h=1}^{m} s_h \left(\sum_{k=1}^{n} Q_{ik} \right)}{\sum_{h=1}^{m} \sum_{k=1}^{n} Q_{hk}} \right. \right. \right.
$$
$$
\left. \left. \left. + (1-s_i) \frac{\sum_{k=1}^{n} Q_{ik}}{\sum_{h=1}^{m} \sum_{k=1}^{n} Q_{hk}} \right) D_i \right] \right\}. \quad (3.8)
$$

Finally, when $s_i = \hat{s}_i$, the new upper limit of security levels establishes that the cybersecurity level remains at the limit value u_{s_i} when $F_i^2(X) \leq 0$. Therefore, in this case, only a decrease in the cybersecurity level is possible and this happens only when the marginal revenues related to the sale to all the demand markets do not exceed the difference between the expected marginal costs related to the investments in cybersecurity and the marginal expenses related to the expected damages. Therefore, when $s_i = \hat{s}_i$, we have the following dynamics:

$$
\dot{s}_i = \min \left\{ 0, \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q,s)}{\partial s_i} Q_{ik} - \left[\frac{\partial h_i(s_i)}{\partial s_i} - \left(1 - \frac{\sum_{h=1}^{m} s_h \left(\sum_{k=1}^{n} Q_{ik} \right)}{\sum_{h=1}^{m} \sum_{k=1}^{n} Q_{hk}} \right. \right. \right.
$$
$$
\left. \left. \left. + (1-s_i) \frac{\sum_{k=1}^{n} Q_{ik}}{\sum_{h=1}^{m} \sum_{k=1}^{n} Q_{hk}} \right) D_i \right] \right\}. \quad (3.9)
$$

Ultimately, the dynamics of the cybersecurity levels can be expressed as:

$$
\dot{s}_i = \begin{cases}
\max\left\{0, \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q,s)}{\partial s_i} Q_{ik} - \left[\frac{\partial h_i(s_i)}{\partial s_i} - \left(1 - \frac{\sum_{h=1}^{m} s_h \left(\sum_{k=1}^{n} Q_{ik}\right)}{\sum_{h=1}^{m} \sum_{k=1}^{n} Q_{hk}}\right.\right.\right. \\
\qquad\qquad \left.\left.\left. + (1 - s_i) \frac{\sum_{k=1}^{n} Q_{ik}}{\sum_{h=1}^{m} \sum_{k=1}^{n} Q_{hk}}\right) D_i\right]\right\}, \\
\quad \text{if } s_i = 0 \\[2ex]
\sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q,s)}{\partial s_i} Q_{ik} - \left[\frac{\partial h_i(s_i)}{\partial s_i} - \left(1 - \frac{\sum_{h=1}^{m} s_h \left(\sum_{k=1}^{n} Q_{ik}\right)}{\sum_{h=1}^{m} \sum_{k=1}^{n} Q_{hk}} + (1 - s_i) \frac{\sum_{k=1}^{n} Q_{ik}}{\sum_{h=1}^{m} \sum_{k=1}^{n} Q_{hk}}\right) D_i\right], \\
\quad \text{if } 0 < s_i < \hat{s}_i \\[2ex]
\min\left\{0, \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q,s)}{\partial s_i} Q_{ik} - \left[\frac{\partial h_i(s_i)}{\partial s_i} - \left(1 - \frac{\sum_{h=1}^{m} s_h \left(\sum_{k=1}^{n} Q_{ik}\right)}{\sum_{h=1}^{m} \sum_{k=1}^{n} Q_{hk}}\right.\right.\right. \\
\qquad\qquad \left.\left.\left. + (1 - s_i) \frac{\sum_{k=1}^{n} Q_{ik}}{\sum_{h=1}^{m} \sum_{k=1}^{n} Q_{hk}}\right) D_i\right]\right\}, \\
\quad \text{if } s_i = \hat{s}_i.
\end{cases}
\tag{3.10}
$$

In a more compact form, the previous estimates can be rewritten as:

$$
\dot{s} = \Pi_{\tilde{\mathcal{K}}_2}(s, -F^2(Q,s)).
\tag{3.11}
$$

Since the projection operator Π_K can be splitted with respect to the Cartesian product (see [4]), that is, $\tilde{\mathcal{K}} = \tilde{\mathcal{K}}_1 \times \tilde{\mathcal{K}}_2$, we have $\Pi_{\tilde{\mathcal{K}}} = (\Pi_{\tilde{\mathcal{K}}_1}, \Pi_{\tilde{\mathcal{K}}_2})$, and the previous dynamic adaptation process can be expressed by the following dynamic projected system on the whole space $\tilde{\mathcal{K}}$

$$
\dot{X} = \Pi_{\tilde{\mathcal{K}}}(X, -F(X)), \quad X(0) = X^0,
\tag{3.12}
$$

where F is defined as in the previous section, $X = (Q,s) \in \mathbb{R}^{mn+m}$, $\tilde{\mathcal{K}} = \tilde{\mathcal{K}}_1 \times \tilde{\mathcal{K}}_2$ and $X^0 = (Q^0, S^0)$ is a generic point of the border of $\tilde{\mathcal{K}}$ corresponding to the initial product transaction between all retailers and all demand markets and to the initial security levels in each retailer.

The next theorem establishes that the projected dynamic system evolves until it reaches a stationary point, that is, until $\dot{X} = 0$, when there is no transaction variation of products and cybersecurity levels and that the stationary points of the PDS (3.12) coincide with the equilibrium points of the network, according to Definition 2.2.

Theorem 3.1. *A vector* $(Q^*, s^*) \in \tilde{\mathscr{K}}$ *is a stationary point of the projected dynamic system* (3.12) *if and only if* (Q^*, s^*) *is an equilibrium point according to Definition* 2.2.

Proof. Following [16], X^* is a stationary point of the projected dynamic system (3.12) if and only if X^* is a solution to the variational inequality

$$\langle F(X^*), X - X^* \rangle \geq 0, \quad \forall X \in \tilde{\mathscr{K}}. \tag{3.13}$$

Explicitly, (3.13) gives:

$$\sum_{i=1}^{m} \sum_{j=1}^{n} \left[c_i + \frac{\partial c_{ij}(Q_{ij}^*)}{\partial Q_{ij}} - \hat{\rho}_j(Q^*, s^*) - \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial Q_{ij}} \cdot Q_{ik}^* \right.$$

$$\left. + (1 - s_i^*) \frac{-s_i^* \sum_{h=1}^{m} \sum_{k=1}^{n} Q_{hk}^* + \sum_{h=1}^{m} s_h^* \left(\sum_{k=1}^{n} Q_{hk}^* \right)}{\left(\sum_{h=1}^{m} \sum_{k=1}^{n} Q_{hk}^* \right)^2} \cdot D_i \right] \times (Q_{ij} - Q_{ij}^*)$$

$$+ \sum_{i=1}^{m} \left[\frac{\partial h_i(s_i^*)}{\partial s_i} + \left(1 - \frac{\sum_{h=1}^{m} s_h^* \left(\sum_{k=1}^{n} Q_{ik}^* \right)}{\sum_{h=1}^{m} \sum_{k=1}^{n} Q_{hk}^*} + (1 - s_i^*) \frac{\sum_{k=1}^{n} Q_{ik}^*}{\sum_{h=1}^{m} \sum_{k=1}^{n} Q_{hk}^*} \right) D_i \right.$$

$$\left. - \sum_{k=1}^{n} \frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial s_i} \cdot Q_{ik}^* \right] \times (s_i - s_i^*) \geq 0, \quad \forall (Q, s) \in \tilde{\mathscr{K}}, \tag{3.14}$$

and (3.14) coincides with variational inequality (2.8). Hence, every stationary point (Q^*, s^*) of the projected dynamic system (3.12) is a solution to the variational inequality (2.8) and, hence, a Nash equilibrium, according to Definition 2.2. $\square$

Theorem 3.2. *Function F (or, equivalently, $-F$) is Lipschitz continuous if the utility function of each retailer* i, $i = 1, \ldots, m$, *is continuously differentiable with respect to the variables* $Q_{i1}, \ldots, Q_{in}$ *and* s_i.

Proof. We remark that the following generalization of the Lagrange theorem holds true: let F be a real differentiable function on an open set $U \subseteq \mathbb{R}^n \to \mathbb{R}^m$, which contains the segment $[X, Y]$; then:

$$\|F(X) - F(Y))\| \leq \sup_{\xi \in \mathscr{K}} \|J_F(\xi)\| \|X - Y\|, \tag{3.15}$$

where $J_F(\cdot)$ denotes the Jacobian matrix of F.

F and $\tilde{\mathscr{K}}$ satisfy all the assumptions of such a theorem, hence (3.15) holds. Moreover, since

$\tilde{\mathcal{K}}$ is a bounded set, then the derivatives of F with respect to the variables $Q_{i1}, \ldots, Q_{in}$ and s_i are bounded in such a set. As a consequence, we obtain:

$$\sup_{\xi \in \tilde{\mathcal{K}}} \|J_F(\xi)\| = L < \infty.$$

If we choose as the Lipschitz constant for F exactly L, then we get the assertion immediately.
□

The following corollary is a consequence of the previous theorem.

Corollary 3.1. *If the utility function of each retailer i, $i = 1, \ldots, m$, is continuously differentiable with respect to the variables $Q_{i1}, \ldots, Q_{in}$ and s_i, then, for every $X^0 \in \tilde{\mathcal{K}}$, there exists a unique solution $X_0(\tau)$ to the problem* (3.12).

Further, the following theorem holds (see [16]).

Theorem 3.3. *The following conditions hold:*
- *(1) if F is monotone and $(Q^*, s^*) \in \tilde{\mathcal{K}}$ is a solution to variational inequality* (2.8)*, then (Q^*, s^*) is a global monotone attractor;*
- *(2) if F is strictly monotone, then the unique solution $(Q^*, s^*) \in \tilde{\mathcal{K}}$ to variational inequality* (2.8) *is a global strictly monotone attractor;*
- *(3) if F is strongly monotone, then the unique solution $(Q^*, s^*) \in \tilde{\mathcal{K}}$ to variational inequality* (2.8) *is globally exponentially stable;*
- *(4) if F is strongly monotone with degree $\alpha < 2$, then the unique solution $(Q^*, s^*) \in \tilde{\mathcal{K}}$ to variational inequality* (2.8) *is a finite-time attractor.*

4. COMPUTATIONAL PROCEDURE

In this section we, will present a computational procedure for the resolution of the projected dynamic system (3.12) in order to find its stationary points. We can solve variational inequality (2.8) using the Euler method presented in [16]. The general iterative scheme to obtain a solution to the projected dynamic system (3.12) at iteration τ takes the form:

$$X_{\tau+1} = P_{\tilde{\mathcal{K}}}(X_\tau - a_\tau F(X_\tau)), \tag{4.1}$$

where $P_{\tilde{\mathcal{K}}}$ is the ortogonal projection (on the feasible set $\tilde{\mathcal{K}}$) defined in (3.6). As in [5], in order to get the convergence of the method, the sequence a_τ has to satisfy the following conditions: $\sum_{\tau=0}^{\infty} a_\tau = \infty$, $a_\tau > 0$, $a_\tau \to 0$, when $\tau \to \infty$.

As in the case of the traffic model with fixed demand (see [16]), the presence of a fixed demand does not allow us to calculate the projection operator in a closed form, but, rather, as the solution to a quadratic optimization problem. However, using a special structure of the deriving subproblems, each of these projections can be computed using an exact balancing algorithm. Nevertheless, these considerations refers only to the flow variables Q_i, $i = 1, \ldots, m$, since, as we shall see, for the security variables it is possible to write closed formulas deriving from the processes of dynamic adjustment (3.10). Specifically, at each iteration τ of the Euler method, formula (4.1), restricted to the variables Q, has the following form:

$$Q^{\tau+1} = \min_{Q \in \tilde{\mathcal{K}}_1} \frac{1}{2} Q^T \cdot Q - (Q^T - a_\tau F^1(Q^\tau, s^\tau))^T \cdot Q, \tag{4.2}$$

where, at each iteration τ, $s^{\tau+1}$ is the m-dimensional vector, whose components are:

$$
s_i^{\tau+1} = \max \left\{ 0, \min \left\{ u_{s_i}, s_i^\tau + a_\tau \left[\sum_{k=1}^n \frac{\partial \hat{\rho}_k(Q^\tau, s^\tau)}{\partial s_i} \cdot Q_{ik}^\tau - \left(1 - \frac{\sum_{h=1}^m s_h^\tau \left(\sum_{k=1}^n Q_{ik}^\tau \right)}{\sum_{h=1}^m \sum_{k=1}^n Q_{hk}^\tau} \right. \right. \right. \right.
$$
$$
\left. \left. \left. \left. + (1 - s_i^\tau) \frac{\sum_{k=1}^n Q_{ik}^\tau}{\sum_{h=1}^m \sum_{k=1}^n Q_{hk}^\tau} \right) D_i \right] \right\} \right\}. \tag{4.3}
$$

Given the structure of the feasible set $\tilde{\mathcal{K}}_1$, each subproblem (4.2), in turn, can be decomposed into mn subproblems, one for each retailer/demand market pair, each of which is a quadratic optimization problem with a special structure that can be solved in closed form using an exact balancing. In particular, subproblem (4.2) is equivalent to the solution of the following mn subproblems: for each retailer/demand market pair, calculate

$$
\min \frac{1}{2} \sum_{i=1}^m \sum_{j=1}^n Q_{ij}^2 + \sum_{i=1}^m \sum_{j=1}^n h_{ij}^\tau Q_{ij} \tag{4.4}
$$

under the constraints

$$
\sum_{j=1}^n Q_{ij} = d_j, \quad \forall j = 1, \dots, n, \tag{4.5}
$$

and

$$
0 \le Q_{ij} \le \bar{Q}_{ij}, \quad \forall i = 1, \dots, m, \ j = 1, \dots, n, \tag{4.6}
$$

where

$$
h_{ij}^\tau = a_\tau F^1(Q^\tau) - Q^\tau. \tag{4.7}
$$

5. NUMERICAL EXAMPLES

In this section, we apply the model to some numerical examples that consist of a network with two retailers and two demand markets, as depicted in Figure 2. Since we want to report all the
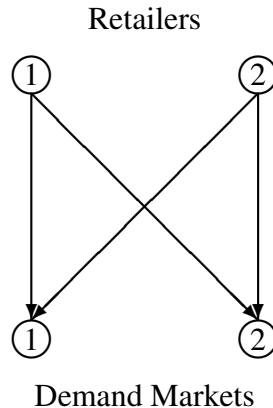
Retailers

Demand Markets
FIGURE 2. Network Topology for the Numerical Examples

results for transparency purposes, we select the size of the problem as reported. The numerical

data are inspired by realistic values and are constructed for easy interpretation purposes. These examples are inspired by related examples as in [1]. We assume the following cost function data are given:

$$
\begin{array}{rclrcl}
c_1 & = & 5, & c_2 & = & 10, \\
c_{11}(Q_{11}) & = & 0.5Q_{11}^2 + Q_{11}, & c_{12}(Q_{12}) & = & 0.25Q_{12}^2 + Q_{12}, \\
c_{21}(Q_{21}) & = & 0.5Q_{21}^2 + Q_{21}, & c_{22}(Q_{22}) & = & 0.25Q_{22}^2 + Q_{22}.
\end{array}
$$

The demand price functions are:

$$
\rho_1(d,\bar{s}) = -d_1 + 0.1\bar{s} + 100, \quad \rho_2(d,\bar{s}) = -0.5d_2 + 0.2\bar{s} + 200.
$$

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

$$
h_1(s_1) = \frac{\alpha_1}{\sqrt{1-s_1}} - 1, \quad h_2(s_2) = \frac{\alpha_2}{\sqrt{1-s_2}} - 1,
$$

where $\alpha_1 = \alpha_2 = 1$.

The maximum budget, the upper bounds of the cybersecurity level and of the product transactions are respectively:

$$
B_1 = B_2 = 2.5, \quad u_{s_1} = u_{s_2} = 0.91, \quad \overline{Q}_{ij} = 100, \forall i,j = 1,2.
$$

The demand at the demand markets, for each example respectively, are expressed in Table 1.

Example	$d_1 = Q_{11} + Q_{21}$	$d_2 = Q_{12} + Q_{22}$
Example1	20	80
Example2	40	190
Example3	60	200
Example4	80	380

TABLE 1. Demand at the demand markets

To solve the examples we used Matlab on a laptop with an HP 255.5 computer, compute cores 2C+3G, 2.60 GHz, RAM: 8 GB. For the convergence of the method a tolerance $\varepsilon = 10^{-4}$ was fixed; that is, the Euler method was considered to have converged if the absolute value of the difference between the variables in two successive iterations differed by no more than ε. Specifically, the method has been implemented with a constant step $\alpha = 0.1$. Furthermore, we initialized the algorithm by setting each variable equal to 0.

The optimal variables and the elapsed time are shown in the following Table 2.

Example	Q_{11}^*	Q_{12}^*	Q_{21}^*	Q_{22}^*	s_1^*	s_2^*	**Elapsed time**
Example1	10.10	40.19	9.90	39.81	0.91	0.91	18.24 s
Example2	20.26	95.27	19.74	94.73	0.91	0.91	1.31 s
Example3	30.26	100.00	29.74	100	0.9092	0.9092	9.65 s
Example4	40.25	190.26	39.75	189.74	0.9099	0.9099	7.52 s

TABLE 2. Optimal variables and elapsed time

Therefore, following a percentage change of d_1 and d_2, as shown in Table 3, $Q_{11}^*, Q_{12}^*, Q_{21}^*$ and Q_{22}^* in turn undergo a percentage variation as shown in Table 4.

	Example 1-2	Example 2-3	Example 3-4	Example 1-4
d_1	1	0.50	0.33	3
d_2	1.38	0.05	0.90	3.75

TABLE 3. Percentage variation of d_1, d_2 in %

	Example 1-2	Example 2-3	Example 3-4	Example 1-4
Q_{11}^*	1	0.49	0.33	2.99
Q_{12}^*	1.37	0.05	0.90	3.73
Q_{21}^*	0.99	0.51	0.34	3.01
Q_{12}^*	1.38	0.06	0.90	3.77

TABLE 4. Percentage variation of $Q_{11}^*, Q_{12}^*, Q_{21}^*$ and Q_{22}^* (%)

We also calculate the marginal profits with respect to the flows, namely, the marginal expected transaction utilities, and the marginal expected cybersecurity investment utilities and reported them in Table 5.

	Example 1	Example 2	Example 3	Example 4
$\dfrac{\partial E(U_1(Q,s))}{\partial Q_{11}}$	-2538.7	-8258.0	-10599	-25228
$\dfrac{\partial E(U_1(Q,s))}{\partial Q_{12}}$	-2618.7	-8310.8	-10649	-25233
$\dfrac{\partial E(U_2(Q,s))}{\partial Q_{21}}$	-2606.5	-8408.1	-10876	-25536
$\dfrac{\partial E(U_2(Q,s))}{\partial Q_{22}}$	-2686.7	-8460.6	-10926	-25541
$\dfrac{\partial E(U_1(Q,s))}{\partial s_1}$	41.0205	34.9708	35.6513	24.4532
$\dfrac{\partial E(U_2(Q,s))}{\partial s_2}$	42.3637	36.4137	37.3172	25.9325

TABLE 5. Marginal profits

Table 5 clearly shows that the marginal expected transaction utilities are always negative and decreasing, whereas marginal expected cybersecurity investment utilities always have positive values.

In Figure 3, we report the changes of the optimal solutions Q_{ij}^* in each situation, when d_1 and d_2 vary.

6. CONCLUSIONS

In this paper, we proposed a cybersecurity investment model based on networks with nonlinear budget constraints and fixed demands. We used as the average value of the security levels for the entire supply chain network a weighted average which depends also on the flow of commodities. We obtained a GNE and the related variational equilibrium. Furthermore, we studied
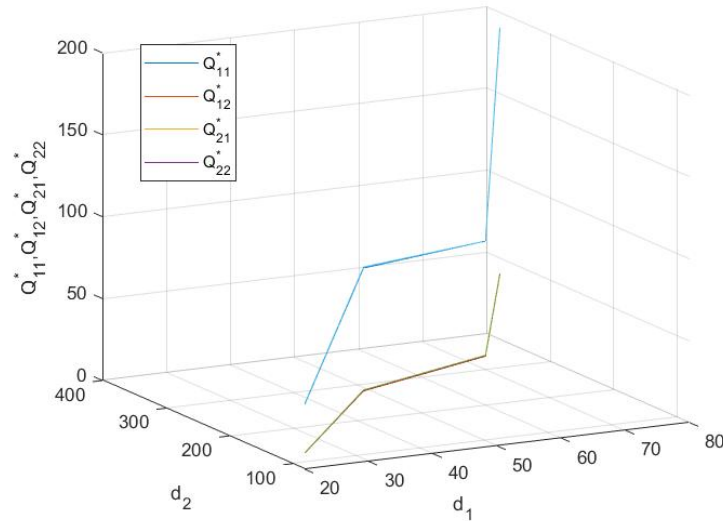
FIGURE 3. Sensitivity analysis

the associated projected dynamic system and characterized the solutions to the variational inequality with the stationary points of the PDS. Also, we presented a computational procedure, based on the Euler method, to find the optimal distribution of commodities. The results in this paper add to the growing literature of operations research for cybersecurity modeling and analysis.

Acknowledgements

REFERENCES

[1] G. Colajanni, P. Daniele, S. Giuffrè, A. Nagurney, Cybersecurity investments with nonlinear budget constraints and conservation laws: variational equilibrium, marginal expected utilities, and Lagrange multipliers, Int. Trans. in Oper. Res. 25 (2018), 1443–1464.

[2] P. Daniele, A. Maugeri, A. Nagurney , Cybersecurity Investments with Nonlinear Budget Constraints: Analysis of the Marginal Expected Utilities, in Operations Research, Engineering, and Cyber Security: Trends in Applied Mathematics and Technology, Eds. Daras NJ, Rassias MT, Springer Optim. Appl. vol. 113, pp. 117-134, Springer, 2017.

[3] N.J. Daras, M.T. Rassias, Computation, Cryptography, and Network Security, Springer, Switzerland, 2015.

[4] J. Dong, A. Nagurney, D. Zhang, A projected dynamical system model of general financial equilibrium with stability analysis, Mathl. Comput. Modelling, 24 (1996), 35-44.

[5] P. Dupuis, H. Ishii, On Lipschitz continuity of the solution mapping to the Skorokhod problem, with applications, Stochastics and Stochastic Reports 35 (1991), 31-62.

[6] A. Fischer, M. Herrich, K. Schonefeld , Generalized Nash equilibrium problems - Recent advances and challenges, Pesquisa Operacional, 34 (2014), 521-558.

[7] A.A. Kulkarni, U.V. Shanbhag, On the variational equilibrium as a refinement of the generalized Nash equilibrium, Automatica, 48 (2012), 45-55.

[8] J.P. Luna, Decomposition and Approximation Methods for Variational Inequalities, with Applications to Deterministic and Stochastic Energy Markets, PhD Thesis, Instituto Nacional de Matematica Pura e Aplicada, Rio de Janeiro, Brazil, 2013.

[9] A. Maugeri, F. Raciti, On existence theorems for monotone and nonmonotone variational inequalities, J. Convex Anal. 16 (2009), 899-911.

[10] A. Nagurney, A multiproduct network economic model of cybercrime in financial services, Service Sci. 7 (2015), 70-81.

[11] A. Nagurney, E. Alvarez Flores, C. Soylu, A generalized Nash equilibrium network model for post-disaster humanitarian relief, Trans. Res. E 95 (2016), 1-18.

[12] A. Nagurney, P. Daniele, S. Shukla, A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints, Ann. Oper. Res. 248 (1), 2017, 405-427.

[13] A. Nagurney, L.S. Nagurney, A game theory model of cybersecurity investments with information asymmetry, Netnomics 16 (2015), 127-148.

[14] A. Nagurney, L.S. Nagurney, S. Shukla, A Supply Chain Game Theory Framework for Cybersecurity Investments Under Network Vulnerability, In: N.J. Daras, M.T. Rassias (ed.) Computation, Cryptography, and Network Security, pp. 381-398, Springer, Switzerland, 2015.

[15] A. Nagurney, S. Shukla, Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability, Eur. J. Oper. Res. 260 (2017), 599-600.

[16] A. Nagurney, D. Zhang, Projected Dynamical Systems and Variational Inequalities with Applications, Kluwer Academic Publischers, Boston, Massachusetts, 1996.

[17] 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.

[18] A. von Heusinger, Numerical Methods for the Solution of the Generalized Nash Equilibrium Problem, PhD Dissertation, University of Wurtburg, Germany, 2009.