KEDGE BUSINESS SCHOOL
ILS2016
Information Systems Logistics and Supply Chain
6th International Conference
université de BORDEAUX

Paper Title: ABM-Based Supply Chain Risk Analysis and Modelling

Luca Urciuoli[1]

[1] MIT International Logistics Programme, Zaragoza, Spain
{lurciuoli@zlc.edu.es}

Abstract. Understanding the impact of risks and related countermeasures in a supply chain is a challenging task. Especially, security risks, i.e. intentional and unauthorized acts against a supply chain, are considered emerging and important risks calling for heightened attention from managers as well as governmental actors. This paper aims to apply Agent Based Modelling to facilitate the quantification of the impacts of security risks and related countermeasures. Hence, the methodology is explained and a numerical case, based on postal operations in the region of Aragon, Spain, is provided. Results show that the methodology may provide very interesting insights in terms of reduction of security threats, potential to jam postal systems and ultimately experienced delays by customers.

Keywords: supply chain security, postal security, resilience, security measures, supply chain security impacts.

1 Introduction

The ability of identify and systematically explain how risks and their related countermeasures impact the performance of a supply chain is a challenge for most practitioners and researchers. Especially security risks, i.e. intentional and unauthorized acts perpetrated against a supply chain, are considered particularly challenging since they are characterized by a significantly high degree of uncertainty [1-3]. Supply chain risk management is suggested as a systematic approach to identify and address diverse types of risks, including e.g. natural catastrophes, equipment failure, and demand risks [1, 4-7]. In a risk management approach, particular attention should be given to the type of response to risks; e.g. new routines or technologies in order to 1) minimize the likelihood of an event or 2) reduce the potential consequences. However, often it is very uncertain how to measure the impacts of these measures: how will security be improved and what would be the related monetary benefits of improved security? Will it be necessary to trade-off supply chain performance? Understanding these impacts is a known dilemma of any supply chain risks and security managers. The ability to quantify and communicate these impacts would mean the possibility to develop convincing arguments for securing necessary investment budgets and running consistent business re-engineering processes. In addition, security managers might be able to smartly and optimally allocate their budgets by trading-off security improvements, collateral benefits against performance losses.

Previous research has develop tools and mathematical techniques, including qualitatively and quantitatively methods, to approach this problem [3, 8]. The common understanding of these tools is that security safeguards should not be merely assessed upon their potential to reduce threats. Costs like monetary investments, maintenance, personnel, and operational bottlenecks etc. should be considered as well. In addition, the collateral benefits of security, brand image, process efficiency, damage and quality etc. are relevant in order to build robust business cases for security measures [9]. However, previous approaches lack the ability to fairly reproduce and model complex systems like supply chains and related risks. In particular, none of the previous work uses Agent Based Modelling (ABM), which is known technique allowing analysts to model fairly complex systems where decisions are made in a decentralized manner.

Hence, the aim of this paper is to apply ABM to model and simulate security risks in postal supply chains. The ultimate goal is to show how ABM can be used for multiple purposes, including enhanced understanding of the monetary impacts of security threats and related countermeasure. In the next section, a methodology to apply ABM techniques is proposed and thereby explained how it has been applied to model postal security risks. Next, the outcome of the methodology is evaluated with a numerical case applied to postal operations run in a consolidation center run by the postal operator CORREOS in the region of Aragon, Spain. Finally, the paper concludes by summarizing the results and discussing the practical and scientific contributions.

2 Approach

The methodology proposed in this study is composed by the following main parts (Figure 1):

- **Scenario identification and structuring**. The scenario identification and structuring aims to outline the context or system to be considered in the analysis. Particular focus should be given to describe and include relevant risks to be modelled (e.g. security risks), the operations performed in the supply chain to be included in the analysis, the geographic environment where the model will run, and finally, the measures that analysts want to test in the model.
- **Scenario quantification**. As part of the quantification, analysts are requested to identify impacts on threats, benefits and costs of security measures. In particular, the following indicators have to be identified and quantified:
    - *Loss reductions.* Reduction of threats will induce a fractional reduction of losses. This reduction will result into savings for companies.
    - *Cost factors*. Both variable and fixed costs for implementing a security measure needs to be identified and collected.
    - *Operational and strategic benefits*. Benefits can be identified as monetary or intangible benefits (i.e. not monetary).
    - *Identification and quantification of impacts on security threats.* Assessing how security measures impacts security threats.
- **Collection of body of evidence**. The collection of body of evidence needs to classify data used in the model into different variables. Variables to be used can be discrete or stochastic:
    - Discrete variables. As per definition, these variables can only take a finite number of values.
    - Stochastic variables. These variables are necessary in order to model uncertainty. They are continuous and therefore can take infinite number of values. For instance, threats against postal supply chains are uncertain and for that reasons will be modelled by using stochastic variables.

  At the same time, different approaches could be used to gather or exploit data that cannot be collected:
    - Panels of experts. Whenever data is missing, which is a typical situation when modelling security risks and/or assessing impacts of security measures, panels of experts may be used.
    - Bayes' Theorem. The Bayes theorem may be applied in order to gather and re-use statistical data from different contexts/cases.
    - Experimental measures. This technique could be applied to prototypes or new routines to be implemented in the supply chain. Analysts will need first to deduct how the technique is expected to perform and thereafter define Key Performance Indicators. The KPIs will be measured through testing in a laboratory or close-to-real environment.
- The last steps of the methodology consist of running the simulation, evaluating of outputs and reporting.

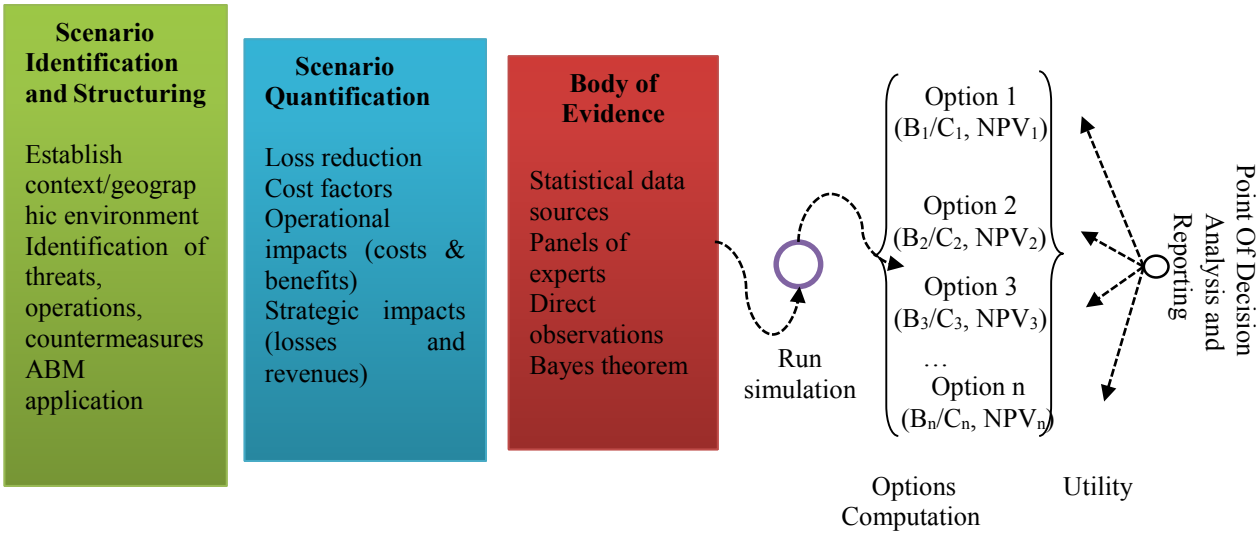

Figure 1: The analytical model (adapted from [10]).

2.1 Scenario Identification and Structuring

Main steps that are performed in this first phase of the model are: definition of geographic environment, scenarios construction and formalization, application of Agent Based Modelling (ABM).
Definition of geographic environment. Establishing a simulation environment consists of identifying the relevant geographic areas that will be studied in the simulation model. GIS-based software (Geographic Information Systems) allows positioning main supply chain facilities in a map, by simply geocoding geographic positions (i.e. latitude and longitude) and storing them into a repository file (a database or a shapefile). Using GIS allows analysts to run and simulate routes travelled by trucks in a real geographic environment. Similarly driving times or delivery lead-times between origins and destination facilities can be computed by using existing shortest path algorithms.
In GIS, a transport system can be represented by three layers of data: land use, flows and transport. The land use layer could be represented by political or economic boundaries in which facilities could be placed and supply chain operations will run (countries, regions, provinces etc.). Supply chain facilities are represented by nodes in the "flows layer", while cargo movement happens on multiple edges and links belonging to the transport network. Each of the three layers is normally stored in independent databases and has its own set of features and additional data [11].

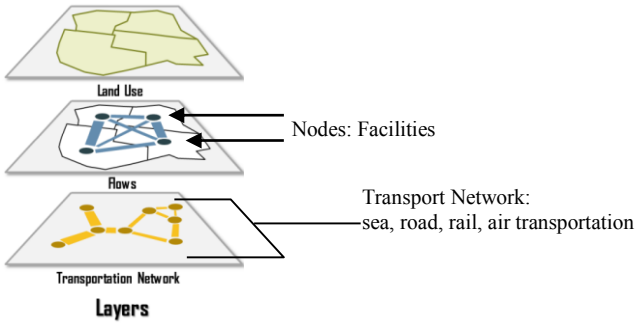

Figure 2: schematic representation of supply chain/transport networks [11].

In post operations, the "flows" layer will include the following nodes:

- **Mailboxes.** Used for posting letters and placed in diverse points in cities in order to facilitate access to citizens.
- **Post offices.** Consumers/clients consign their postal packages in local post offices. In these offices the packages are labelled, temporary stored and thereby shipped to a consolidation centre.
- **Clients' facilities.** Some business clients may have a special deal with the postal operator and thereby send parcels directly from their premises.
- **Consolidation centres.** Some consolidation centres may provide access to road and air transportation (used for international post shipments). The consolidation centres are equipped with modern machines for automatically sorting and consolidating packages according to their final destination. The consolidation or sorting centres have inbound and outbound flows. Inbound flows can be of two types:
    - Flows of packages/letters incoming from a local region and to be delivered to another national consolidation centre.
    - Flows of packages/letters incoming from another consolidation center/sorting center and to be distributed to the local region assigned to the consolidation center receiving the package.

The transport layer will instead include:

- **Transport Network.** A network composed by nodes and edges representing transport movements by road, rail, sea or air.
- **Vessels moving parcels/letters**. Trucks moving the parcels need to be assigned to the road **transport** network and thereby O/D distance or lead time matrices computed. Truck typologies can be the following
    - *Urban/regional delivery.* Short distances covered from the post offices to the regional consolidation centre. Normally capacity of these trucks is smaller.
    - *Interregional transport.* Semi-trailers are normally used to move a higher amount of parcels between the consolidation centres.

Identification of risks, operations and countermeasures. The identified risks, operations and countermeasures will be used to construct different sets of scenarios. Previous research suggests that such a set of scenarios should be complete, finite and disjoint [12, 13]. Hence, the analyst should start from an initial scenario S_0, corresponding to the scenario in which operations are run as expected or corresponding to normal conditions. At some point in the initial scenario, deviations may take place. If one thinks of the initial scenario as a trajectory in the state space of the system, the deviations will correspond to a certain set of cascading events starting with an Initial Event (IE) and leading to End-States (ES) that are different from the one identified in S_0. The identification and description of these different set of events will constitute sets of different scenarios S_i. Research suggests two approaches to perform this step, the first is to identify the possible IEs from the trajectory and draw the outgoing trees. The second is instead to take the opposite way and find out the possible ESs and the related incoming trees [12].

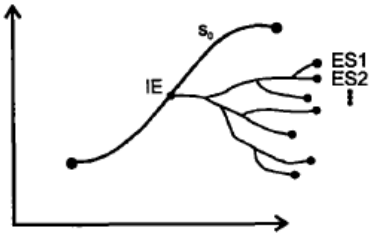

Figure 3: identification of Initial Events (IE) and End States (ES) from the trajectory [3, 12].

An important part of the identification of scenarios consists of identifying security risks or threats that trigger the Initial Event (IE). Specifically in supply chain or transport operations, a threat could be described as prohibited items smuggled into a container, or a pallet or package stolen and therefore removed from the transport chain, or a package containing a biological viruses or bomb is introduced into the supply chain. These threats can be mathematically formalized into a vector $\overline{\mu} = \{\mu_1, \mu_2, \mu_3, \dots, \mu_i, \}$ where μ_i is the generic *modus operandi* in the set of potential supply chain attacks M ($\mu_n \in \mathrm{M}$).

A security measure can be a routine, i.e. a sequence of processes or instructions to be followed by an operator or a manager applying the security measure. The mathematical formalization of this set will be $\overline{\varphi}^r = \{\varphi_1^r,\ \varphi_2^r, \varphi_3^r, \dots, \varphi_j^r\}$, where $\overline{\varphi}^r \in \Phi^r$, set of security routines. Similarly, a technical device, i.e. an

apparatus or system to be installed at the companies' premises or in the vehicles of the postal operator, can be indicated $\overline{\varphi}^t = \{\varphi_1^t,\ \varphi_2^t, \varphi_3^t, \dots, \varphi_k^t\}$, where $\overline{\varphi}^t \in \Phi^t$, set of security technologies. Security measures and devices can be combined into policies, certifications or strategies and can be indicated with: $P_l(\Phi^r, \Phi^t)$. Finally, operations can be formalized with a vector in each of the facilities *f* considered in the model, $\overline{OP}_o^f = \{OP_1^f, OP_2^f, OP_3^f, \dots, OP_o^f\}$, where $\overline{OP}_o^f \in O^f$, set of considered operations in facility *f*.
A scenario, originating from a given IE, depends on the specific interaction between the threats and the security measures or policies applied (i.e. single or combined application of routines and technical devices). Hence, scenarios can be formalized as $S_n(\mu_i, \overline{\varphi}^r, \overline{\varphi}^t, \overline{OP}_o^f)$, or likewise $S_n(\mu_i, P_l, \overline{OP}_o^f)$.
Similarly, to understand the performance impacts of security measures it is necessary to understand and formalize the interaction between the security measures and the logistics system used by the company. The mathematical formalization of this interaction is described in the Scenario Quantification section.
Agent Based Modelling. A possible approach to interactively reproduce all possible outcomes coming from the interaction between security measures, operations and threats is to use Agent Based Modelling (ABM). Contrarily to system approaches, ABM is decentralized and individual-centric, which implies that main objects to be modelled are represented as agents whose behaviors are defined by the analyst (e.g. drivers, reactions, memory, states etc.). It is believed that this approach may fit very well the problem of simulating the behavior of supply chain security attacks, that are typically performed by rational individuals with own goals and rules [14]. For instance, in postal operations, agents could be:

- **Criminals**, deciding where in the postal chain to attack and how.
- **Parcels**. Parcels cannot have any behavioural characteristics. Yet, they may contain a threat and need to be followed in the postal supply chain in order to measure whether threats can be detected by the security measures or not.
- **Security measures.** Security measures can behave in two ways: prevent, detect or recovery. In particular, measures aiming to detect can potentially fail and thereby produce false positives/negatives or true positives/negatives.
- **Delivery trucks.** They can behave differently depending on traffic conditions, travelled routes distances or travelling times, drivers' choices and even insiders actions.
- **Postal facilities, e.g. mailboxes, postal offices, consolidation centres.** The behaviour of postal facilities is very much dependent on the behaviour of parcels, operators working in them, arrival time o trucks etc.

2.5 Scenario Quantification

The quantification of the identified threat scenarios S_n is probably the most difficult and relevant part of the model. Each of the identified scenarios can be quantified with his own Net Benefit, NB, as defined below:

$$NB_{S_n} = \delta L_{S_n} - TC_{S_n} + CB_{S_n} \qquad 1$$

Where

NB = Net Benefit for each scenario $S_n(\mu_n, \overline{\varphi}^r, \overline{\varphi}^t, \overline{OP}_o^f)$, if combining with security technologies or routines or $S_n(\mu_n,\ P_l, \overline{OP}_o^f)$, where $P_l(\Phi^r, \Phi^t)$ is a policy or security certification obtained as a combination of sets of technologies and routines.

δL_{S_n} = losses reduced after introducing a set of security measures.
TC_{S_n} = Total Costs of the introduced set of security measures.
CB_{S_n} = Collateral benefits of hardened security. In this context collateral benefits can be considered as the sum of operational and strategic benefits. Hence, given by $CB_{S_n} = OB_{S_n} + SB_{S_n}$.

The loss reduction can be defined as the fractional reduction in frequency of occurrence of threat μ_i in correspondence of the application of security measure $\overline{\varphi}^r, \overline{\varphi}^t$, or a combination of both in a policy $P_l(\Phi^r, \Phi^t)$.
Costs can be mathematically formalized in a total cost vector $\overline{TC}_P = \{TC_{P_1}, TC_{P_2}, TC_{P_3}, \dots, TC_{P_l}\}$, where the generic element is given by the sum $TC_{P_l} = FC_{P_l} + VC_{P_l} + OC_{P_l}, \forall\ P_l \in P,\ P \subseteq (\Phi^r \cup \Phi^t)$, and FC_{P_l} and VC_{P_l} are respectively the fixed and monthly variable costs of a generic policy, certification or security

strategy established by a company/postal operator, P_l. OC_{P_l} represents the costs related to potential losses of performance. These costs come as a consequence of the interaction between the security measure $\overline{\varphi}^{\mathrm{r}}, \overline{\varphi}^{\mathrm{t}}$, or a combination of both in a policies $\mathrm{P_l}(\Phi^{\mathrm{r}}, \Phi^{\mathrm{t}})$, and the operations run in the facilities considered, $\overline{OP}_o^f \in \mathrm{O}^f$, set of considered operations in facility *f*. Finally, collateral benefits (CB) are considered to be any potential improvement brought by the security measures. From a mathematical viewpoint, these can be modelled as the sum of operational and strategic benefits:

$$\mathrm{CB}_{S_n} = OB_{S_n} + \mathrm{SB}_{S_n} \qquad 2$$

Where:

CB_{S_n} = Collateral benefits identified for single security routines or devices, combination of them (e.g. policies, certifications, security strategies etc.), in relation to a specific scenario originated by the interaction of the security measures or policies with threats, i.e. $S_n(\mu_n, \overline{\varphi}^r, \overline{\varphi}^t, \overline{OP}_o^f)$ or $S_n(\mu_n,\ P_l, \overline{OP}_o^f)$
OB_{S_n} = Monetary benefits associated to operational improvements brought by single security routines, devices or any possible combination (e.g. policies, certifications, security strategies etc.).
SB_{S_n} = Strategic Benefits associated to single security routines, devices, or any possible combination (e.g. policies, certifications, security strategies etc.). this variable can be difficult to quantify and therefore it is recommended to use panels of experts from the company.
$S_n(\mu_n, \overline{\varphi}^r, \overline{\varphi}^t, \overline{OP}_o^f)$ or $S_n(\mu_n, P_l, \overline{OP}_o^f)$ = scenarios generated as interaction threats with security routines and technologies or interaction of threats with policies/certifications (combination of routines and policies).

3 A Numerical Case

As part of the scenario identification, Open Street Maps[1] have been used as the GIS environment of the model. The area of interested and routes of moving objects were constructed around the geographical area of Zaragoza, including 10 post offices and 1 consolidation center (located in San Gregorio, north of Zaragoza). All facilities were geocoded in the GIS map and thereby programmed as agents to be used in the simulation model.
The security threat considered into this narrow implementation example consist of smuggling a prohibited item in parcels, e.g. antiques in madeira wood, protected animal species, fake drugs, cocaine etc. This threat is generated directly at the post offices, where perpetrators send the corrupted parcel from a post office to an agreed destination (in Spain or abroad). The operations consist of temporarily storing the parcels in the post offices, collecting with trucks and delivery to the consolidation center. A total of 10 trucks, one for each post office, have been added to the model as agents. At the consolidation center the parcels are simply sorted and wait for the next truck moving them to the next destination, i.e. another consolidation center in Spain. The security measures consist of the following scanning technologies;

- **X-Ray.** X-ray images to detect illicit items hidden in the packages.
- **Cameras.** The cameras may detect tampering or any involuntary damage associated to a modified shape of the package. Detection happens on all sides of the parcel except one (the side lying on the conveyor belt).
- **D-Tube.** It is based on electronic sensors that can "sniff" the substances on the shell of the parcel. This technology is coupled with a curtain that hit the moving parcels in order to lift up the substances. The substances are channelled by means of tubes to the sensors.

The flow of parcels through the scanning technologies is modelled by using discrete event simulation. Once the parcels enter the consolidation center they go first through an x-Ray machine, then the cameras and finally the d-Tube. After each machine a decision point, based on whether the parcel contains illicit items or not, can compute the probability for triggering an inspection or for letting the parcel go to the next technology. If the parcel is selected for inspection, it is sent to a pool of 10 customs officers that will proceed with a more detailed inspection. If the parcel originally contains illicit items and is selected for inspection, then the parcel is removed from the queue and labelled as a *true positive*. If the parcel does not contain illicit items, yet it is selected for inspection, it will be put back in the exit node and labelled as a *false positive*. If a parcel, containing illicit items, is not selected for inspection by any of the security technologies,

[1] https://www.openstreetmap.org/

then it will be labelled as a *false negative*; or on the contrary if the parcel does not contain any threats as a *true negative*.
Loss reductions are measured as changes into the amount of packages containing threats reaching the exit node of the consolidation center. Hence, the loss reduction can be quantified in terms of the frequency reduction of the threat by the monetary losses related to that specific event. The cost factors include the following: fixed costs for installing the security technologies (x-Ray, cameras, and d-Tube) [€] and 2) variable costs **n**ecessary maintenance and repair for the machines on annual basis [€/Year]. The operational benefits are associated to congestions created in the consolidation center or delays of parcels, but also the positive performance of the security technologies. Hence, the following KPIs will be measured:

- **Police officers working time.** Inspections of parcels will increase customs officers working time [time unit e.g. hours].
- **Police officers' costs (personnel costs).** The increased inspection rates will increase customs officers working time and consequently overall personnel costs [€ x time unit].

Each of the three technologies was tested independently and in dual combinations in further simulation runs. According to the results, the system will evolve into a congestion state in only two configurations, i.e. when using the three technologies simultaneously or when using the x-ray in combination with the d-tube. In these particular situations, it was possible to observe a homogenous and constantly increasing congestion that the system was never able to dispose during 1 year time (Figure 4). The situation is different for the other systems where instead oscillating congestion flows are observed (Figure 4). In this situation, the police officers experience a high level of congestion, yet it is able to perform all inspections during the daily working shift and thereby dispose the waiting packages. This capability directly affects the waiting time of parcels that needs to be inspected and by that the overall final time delays. The lowest oscillating peaks were observed when using merely the cameras technologies.

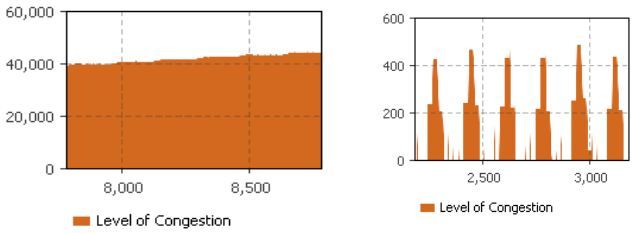

Figure 4: increasing congestion level (left diagram) and oscillating (right diagram).

The potential net benefits for the different scenarios, where different combinations of security measures are used, are given in Table 1. The comparison of net-benefits allows the selection of the optimal combination of security measures to be installed in the consolidation center (in this example x-ray and cameras).

Table 1: comparison of different combination of security measures.

	Security Measures	Congestion Level in Terminal	Parcels delays (not inspected)	Parcels delays (inspected)	Hit Rate	Secure Rate	Net Benefit
S1	X-Ray – Cameras-D-Tube	congestion with > 40000 parcels	< 1 hour	< 1000 hours	0.002	1	588,625
S2	X-Ray	cycles disposed (peaks 400)	< 1 hour	< 20 hours	0.004	0.99	1,264,093
S3	Cameras	cycles disposed (peaks 40)	1 minute	15 hours	0.04	0.99	78,663
S4	D-tube	cycles disposed (peaks 400)	< 1 hour	18 hours	0.003	0.94	1,251,259
S5	x-ray and cameras	cycles disposed (peaks 400)	< 1 hour	19 hours	0.04	1	1,331,916
S6	Cameras and d-tube	cycles disposed (peaks < 600)	< 1 hour	19 hours	0.004	1	1,255,115
S7	x-ray and d-tube	congestion with > 30000 parcels	about 1 hour	about 1000 hours	0.002	1	1,094,671

4 Conclusion

This report expounds a methodology using Agent Based Modelling for measuring the impact of security technologies in postal operations. Technologies have proven to reliably detect theft or smuggling, however it is still unknown if the performance of postal chains may be put at stake. Introducing a scanning technology in a supply chain often means delaying operations or adding additional complexity that may jeopardize performance. Hence, it remains to understand what level of security is acceptable and whether that level will justify the investments and any potential loss of performance. The application to the case study focusing on CORREOS postal operations in the region of Aragon, Spain shows that results might contain very interesting insights that could be difficult to discover and evaluate otherwise. First of all, the methodology supports the brainstorming about the real impact of technology on security threats and the related savings of their impacts. In addition, it allows the computation of average time delays' of parcels flows going through a consolidation center. In particular, the methodology highlights that parcels not selected for inspection are merely subject to delays caused by the security measures screening processes added in the consolidation facility. Other parcels, false positives (safe packages selected for inspection), will instead be strongly delayed by the true positives (unsafe packages), the number of unsafe parcels entering the system. Finally, the methodology shows that by quantifying costs associated to delays or unsatisfied customers it may be possible to quantify net benefits and thereby assess and select most cost effective security measures. Future research, will focus on the gathering of additional data for expanding the analysis to two additional cases: the first considering several consolidation centers in Spain. The second case will consider an international parcel shipment between South America and Spain.

References

1. Manuj, I. and J.T. Mentzer, *Global supply chain risk management strategies.* International Journal of Physical Distribution & Logistics Management, 2008. **38**(3): p. 192-223.
2. Sheffi, Y., *Supply chain management under the threat of international terrorism.* The International Journal of Logistics Management, 2001. **12**(2): p. 1-11.
3. Urciuoli, L., *Supply chain security—mitigation measures and a logistics multi-layered framework.* Journal of transportation security, 2010. **3**(1): p. 1-28.
4. Asbjørnslett, B.E., *Assessing the vulnerability of supply chains*, in *Supply Chain Risk*. 2009, Springer. p. 15-33.
5. Finch, P., *Supply chain risk management.* Supply Chain Management: An International Journal, 2004. **9**(2): p. 183-196.
6. Franck, C. *Framework for supply chain risk management*. in *Supply Chain Forum: An International Journal*. 2007. KEDGE Business School.
7. Zsidisin, G.A., A. Panelli, and R. Upton, *Purchasing organization involvement in risk assessments, contingency plans, and risk management: an exploratory study.* Supply Chain Management: An International Journal, 2000. **5**(4): p. 187-198.
8. Lee, H.L. and S. Whang, *Higher supply chain security with lower costs: lessons from total quality management.* International Journal of Production Economics, 2005. **96**(3): p. 289-300.
9. Rice Jr, J.B. and P.W. Spayd, *Investing in supply chain security.* Border Management in the New Century, 2005: p. 75.
10. Urciuoli, L., *Investing in transport security solutions: using the quantitative risk assessment (QRA) approach.* International Journal of Risk Assessment and Management, 2011. **15**(4): p. 275-298.
11. Rodrigue, J.-P., C. Comtois, and B. Slack, *The geography of transport systems*. 2013: Routledge.
12. Kaplan, S., *The Words of Risk Analysis.* Risk Analysis, 1997. **17**(4).
13. Haimes, Y.Y., *Risk Modeling, Assessment, and Management*. 1998: John Wiley & Sons.
14. Helbing, D. and S. Balietti, *How to do agent-based simulations in the future: From modeling social mechanisms to emergent phenomena and interactive systems design.* Chapter" Agent-Based Modeling" of the book" Social Self-Organization" by Dirk Helbing (Springer, Berlin, 2012), 2013: p. 25-70.