CHAPTER 20

Supporting Decision-Making Through Methodological Scenario Refinement: The PREVENT Project

Maria Kampa, George Kampas, Ilias Gkotsis, Youssef Bouali, Anabel Peiró Baquedano, and Rami Iguerwane

20.1 Introduction

Safety and security are of primary concerns for any transport system. This issue concerns both transportation nodes and terminals that can become a potential target for terrorism acts. Without a doubt, the establishment of a safe and secure transport environment is essential for citizens and transport operators across Europe.

M. Kampa (✉) · G. Kampas
Center for Security Studies, Athens, Greece
e-mail: m.kampa@kemea-research.gr; g.kampas@kemea-research.gr

I. Gkotsis
KEMEA – Center for Security Studies, Athens, Greece
e-mail: i.gkotsis@kemea-research.gr

B. Akhgar et al. (eds.), *Technology Development for Security Practitioners*, Security Informatics and Law Enforcement,
https://doi.org/10.1007/978-3-030-69460-9_20

Transport security can cover multiple dimensions of different threats and vulnerabilities from terrorist attacks to prevention of vandalism. Mass transportation systems hold a unique position as possible targets for attacks. They are built up as networks and feature a large concentration of people as well as a fundamental economic role. Moreover, increased security levels in air transport caused attackers to refocus on surface transport terrorism, including public transport. The threats of the entire transport supply chain and/or infrastructure also recognize many other forms like crimes committed on the terminals. It is a common understanding that emerging technologies can assist in creating a security transport ecosystem while reducing the duration and intensity of security checks and enhancing the capabilities of the transport operators in identifying and stopping potential attacks. In this regard the definition of future end users' requirements that allow an adaptation of the security system through a subsequent joint procurement is mandatory.

PREVENT project aims to map, through an iterative approach, the gaps and the needs of the transport operators around Europe in relation to security and propose the most promising one. These needs were identified in the format of an initial set of 12 scenarios, which were sequentially filtered to 6 by taking into account legal, procurement, and operational obstacles and constraints, as well as the economic component. Given the above, the end users group consisting of more than 30 public transport managers, operators, and security/police agencies from various EU Member States or others affiliated with the EU countries concluded in a shared challenge. Following this extensive analysis, the buyers involved in the project also decided as a next step that the purchasing activities of the desired solution shall be dealt with using a Pre-Commercial Procurement, meaning the purchase of R&D services from the industry.

Y. Bouali
Engineering Ingegneria Informatica Spa, Rome, Italy
e-mail: Youssef.Bouali@eng.it

A. P. Baquedano
Corvers Procurement Services BV, 's-Hertogenbosch, The Netherlands
e-mail: a.baquedano@corvers.com

R. Iguerwane
SNCF, Paris, France
e-mail: ext.rami.iguerwane@sncf.fr

The roadmap of actions, including the methodological approaches to verify the Common Challenge, is analyzed in the sections below. Section 20.2 will provide the outline of the methodology adopted. Section 20.3 will summarize the development of the security scenarios and the 12 to 8 scenarios' refinement; Sect. 20.4 highlights the refinement from 8 to the final 6 scenarios analyzing the different aspects that have been taken into account. Finally, Sect. 20.5 concludes with the main two results of the project, and Sect. 20.6 provides the conclusions of the aforementioned analysis.

20.2 PREVENT Methodological Framework

Scenario planning is a technique that can support decision-making by taking into account a number of uncertain and uncontrolled parameters that may have an impact on the implementation. The correlation between the scenario planning and decision-making has been established in several studies [6]. In this regard, this method was selected to help the practitioners select the most promising need after evaluating different aspects that could have an impact on their selection (Fig. 20.1).

As described in the image above, three progressive phases have been implemented:

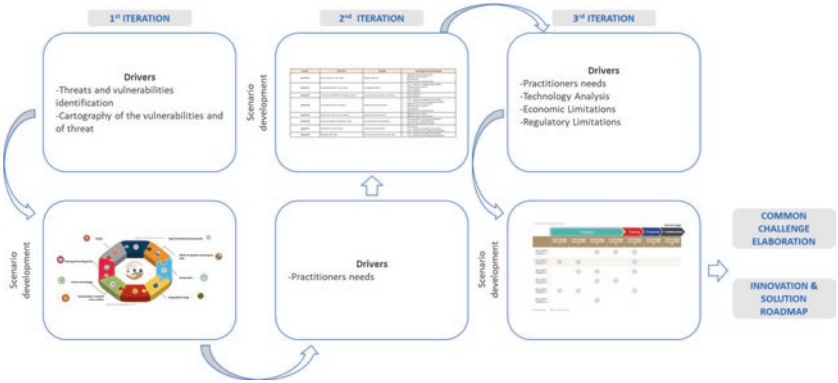

Fig. 20.1 PREVENT methodological framework

Iteration 1 12 security scenario definition. During this phase previously known and experienced, but also new and emerging threats are identified. The result of this phase is the definition of the initial set of the 12 scenarios.

Iteration 2 Refinement of security scenarios. Evaluation screening based on the practitioners' needs and second round of scenario screening (12 to 8). Final 8 scenarios were chosen through a voting-based refinement that involved all the project partners and external stakeholders.

Iteration 3 Final sorting of security scenarios. Evaluation screening through practitioners' needs, technological, economic, and regulatory criteria. Third round of scenario screening (8 to 6). Final 6 scenarios selection.

Project Outcome Common Challenge Elaboration. Based on the final set of scenarios, the end users via discussions session concluded to the most promising scenario, taking into account all parameters.

20.3 Security Scenarios Definition and First Refinement

The ultimate goal of building scenarios is to assess outcomes from alternative future trajectories, through model analysis and planning with stakeholders, to inform decision-making. In this regard, the elaboration of common security scenarios in the context of PREVENT was divided into the following logical steps.

As an initial step for the scenario development, PREVENT project focused on involving a substantial amount of stakeholders through the development of a group entitled "User Observatory Group" (UOG) which included practitioners from public transport operators (PTO) and law enforcement agencies (LEA), who have committed to take part in PREVENT's activities alongside with the Consortium partners. The active involvement of the UOG members and the Consortium partners to the project activities was ensured in order to create economies of scale and better analysis, to manage and spread the risks, and to foster the widest possible and collaborative uptake of the shared approach to security challenges in public transport in relation with terrorism.

The second step toward a concrete scenario development involves the identification of threats and vulnerabilities that the public transport operators face, through a security processes and practices analysis. In addition, PREVENT took into account other aspects like terrorists' attack patterns, the current European Transportation system – which facilitates the "free movement" between EU MS – and the security checks operations.

The aforementioned parameters allowed the preparation of an initial framework detailing a scenario attack through the elaboration of a certain storyline.

In this context, each PREVENT PTO and LEA has been invited to detail three attack events of high risk (Risk = Impact × Probability): one that occurred in the past, a realistic probable attack, and a complex high impact attack (Fig. 20.2).

Thus, based on the aforementioned attack events and the collaborative work, the first 12 scenarios have been developed including various aspects of an attack ranging from the threat, weapon type, the attack target, the location, and the rest factors as included in the image below. In this regard, the 12 scenarios defined were the following:

Scenario 1. An identified terrorist is crossing different European countries
Scenario 2. Stabbing attack in a PTO station
Scenario 3. CBRN attack in station with drones carrying the weapon
Scenario 4. Bomb attack in an underground station
Scenario 5. Hijacking of a train by a terrorist
Scenario 6. Several terrorists with weapons are using different kind of transportation
Scenario 7. Cyberattack on a PTO train dispatching, presumed isolated
Scenario 8. Bomb attack in a bus

Fig. 20.2 Types of terrorist events considered in PREVENT

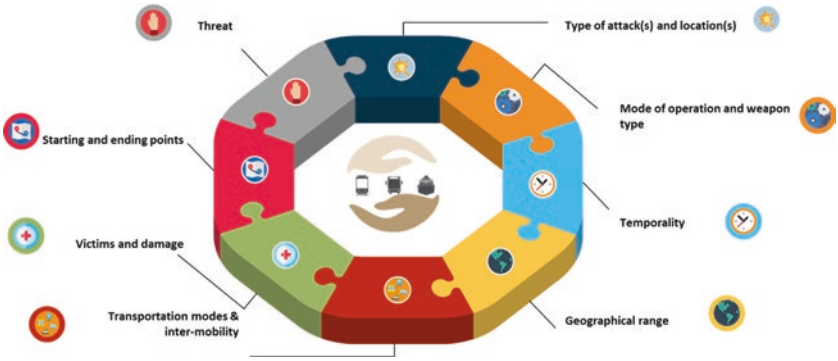

Fig. 20.3 Aspects of an attack analyzed within scenarios

Scenario 9. Left objects/baggage with explosive
Scenario 10. Vehicle crash in a crowd
Scenario 11. Sabotage: block fixed on rails to stop trains
Scenario 12. Massive shooting with rifles in a PTO station (Fig. 20.3)

Moreover, the scenarios included various gaps that need to be addressed in the European PTO environment. The total of 16 gaps have been identified and grouped into 4 distinct categories:

- Detection
- Tracking
- Protection
- Collaboration

allowing the elaboration of a scenarios and gaps matrix, where each scenario was associated with one or more primary and/or secondary gaps (Fig. 20.4).

For the refinement of this first set of scenarios, the methodology followed was quite simple, as the goal was the prioritization of the most crucial scenarios depending on the needs of PTOs and other practitioners. Thus, PREVENT initiated vote sessions and needs related discussions during project meetings where the PREVENT partners and the UOG members were invited to express their individual needs and capabilities into the scope of concluding eventually to the following eight security scenarios:

Fig. 20.4 Scenario gap matrix

Scenario 1. Mass shooting in a train station
Scenario 2. Unattended item(s) in a train station
Scenario 3. Terrorist crossing different European countries
Scenario 4. Reconnaissance before an attack
Scenario 5. Attack with a suicide vest in a subway
Scenario 6. Laying of an explosive material by a drone
Scenario 7. Bomb alert in a metro station
Scenario 8. Sabotage of the tracks

20.4 8 TO 6 SECURITY SCENARIOS

Besides the need's dimension, PREVENT partners decided to include for the second iteration of the scenario's refinement also three other dimensions that could potentially have an impact in the scenarios or even serve as a blocking point.

In this context, the next step included their progressive refinement leading to the selection of the six more promising ones by taking into account the four following essential components as analyzed in the proceeding:

- *Need:* Public transport operators' and security services' needs and expectations in the field of preempting terrorist attacks were evaluated.

- *Technology:* Technological readiness and innovation level of the identified available solutions (bearing in mind the definition of the state of the art of COTS technologies, related suppliers, patents and IPRs, as well as interoperability needs, benefits, and risks).
- *Regulatory:* Different aspects of the procurement legal background and GDPR aspects were analyzed.
- *Economic:* The procurement economic capabilities of the end users and the economic assessment of the eight scenarios were elaborated.

20.4.1 Technological Analysis

The initial step of the technological analysis was the definition of the available technologies for each gap identified in the scenario's definition phase, as included in the Scenarios and Gaps matrix presented in Sect. 20.3. In this regard, a list of technologies was provided, and the end users were called to evaluate and challenge the level of maturity of these technologies based on a benchmark methodology. For the benchmark, the partners adapted the Technology Readiness Level (TRL) scale [10] to the European PTO environment and to PREVENT's needs. Indeed, a technology such as facial recognition is technologically very advanced and even sometimes deployed in countries such as China,[1] so its TRL would be 9. But, principally due to regulatory obstacles, facial recognition is not so advanced in the European PTO environment, so its maturity would be probably 3 on a TRL scale adapted to it[2,3] Based on the results of the adjusted TRL maturity of the long list of technologies and the places of the PTO environment that each technology could be deployed, the ten most relevant technologies were finally selected according to the desire to implement them and the needs of the end users (Fig. 20.5).

Definition of the State-of-the-Art and IPR Search

Following the technologies identification, a state-of-the-art (SOTA) analysis was deemed necessary in order to plan accurately for a procurement. In particular, at that stage, such analysis is required to study the technologies that can best meet the Consortium's needs and their stage of

[1] https://www.businessinsider.com/chinese-company-claims-its-facial-recognition-95-accurate-masks-2020-3

[2] Article 10 Regulation (EU) 2018/1725.

[3] Article 9 GDPR, Article 10 Law Enforcement Directive.

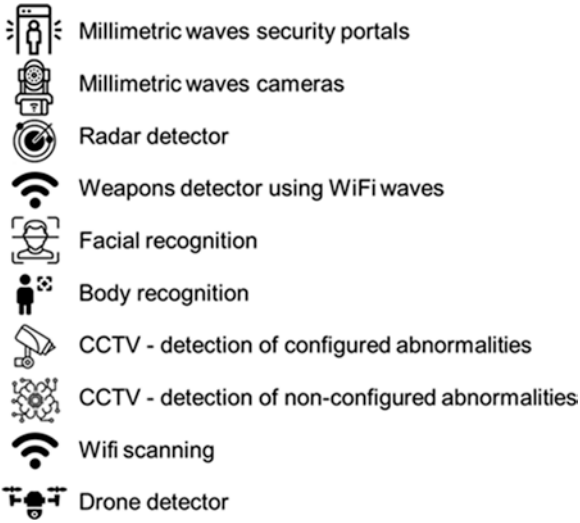

Fig. 20.5 Ten selected technologies

development. It reveals whether a specific technology which could meet these needs is already available on the market or whether some degree of R&D is needed in order to further develop potential solutions. It informs the purchasing strategy toward either a procurement of R&D toward a desired solution (i.e., a Pre-Commercial Procurement, PCP), the modification or adaptation of existing solutions (i.e., a Public Procurement of Innovative Solutions, PPI), or the procurement of an identified Commercial Off-The-Shelf (COTS) solution.

In the PREVENT context, the state-of-the-art (SOTA) analysis included two activities:

(a) An evaluation of the available Commercial Off-The-Shelf (COTS) products which can satisfy the identified gaps and where relevant the integration effort required to reach the desired functionalities and interoperability. Consequently, the Consortium concluded to a list of products, equipment, and technical solutions available on the market that can be purchased, but do not fully cover the needs of the end users.

(b) A macro analysis of the total stock of relevant patents, standards, and literature to obtain information on their type, scope, breadth, content, radicalness, and technical relevance, as well as the associated institutions and related suppliers owning intellectual property rights (IPRs).

This second activity was performed by capitalizing in the iPlytics platform[4] and a keyword search that the applications provide. Therefore, a wide range of results of the world's state of knowledge in the field of the technologies analyzed under the PREVENT project was revealed. Out of this initial long list, the most relevant documents were identified on the basis of their degree of technical relevance and legal relevance.

The partners selected those patents that may be key to technological recommendations from the PREVENT project. So, an in-depth technical examination of the most relevant documents was performed by a technical expert partner, and the initial results were shortlisted. In addition, the most important intellectual property has been chosen, which in the context of the project may contribute to solving the problems defined in the security scenarios and meet needs articulated by PTOs and practitioners. Links between owners of key patents (or the most active patents in each topic) and manufacturers of solutions available on the market (described in the COTS analysis) were also compared.

The outcome of the analysis included the number of patents, the top 10 applicants, and the geographical location, among other important analytics deemed relevant for the scope of the project. Moreover, it should be emphasized that no close relations were identified between the manufacturers of technical solutions from the COTS analysis and global leaders in the field of their patents on individual topics. As a result, it was concluded that manufacturers rely on their knowledge or patent specific technical solutions that they can use in all their market products. A final recommendation was that it is worth following the global tycoons who are leading the world in CCTV technologies or radar technologies, because they can be potential contractors for future technologies.

Interoperability Needs

In order to define the interoperability needs and viable adoption models for PREVENT proposed technologies, the eight scenarios have been

[4] https://www.iplytics.com/

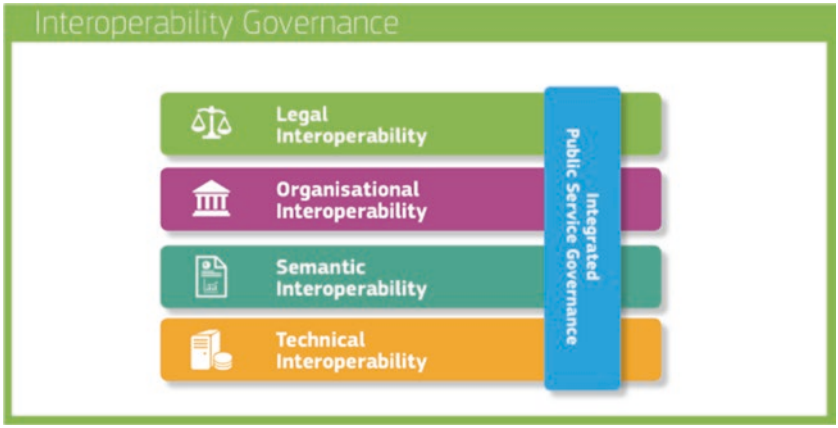

Fig. 20.6 Layers of interoperability of the EIF

analyzed and structured based on the European Interoperability Framework (EIF) of the ISA program. The EIF is "a commonly agreed approach to the delivery of European public services in an interoperable manner. It defines basic interoperability guidelines in the form of common principles, models and recommendations." This framework describes different layers of interoperability as shown in Fig. 20.6:

- Four layers of interoperability: legal, organizational, semantic, and technical
- A cross-cutting component of the four layers: integrated public service governance
- A background layer: interoperability governance

In the framework of PREVENT, these interoperability layers cover different aspects of interoperability and technology adoption requirements as described in Table 20.1.

20.4.1.1 EIF-Based Questionnaires

In PREVENT, practitioners played an important role in conducting key activities and providing domain know-how and expertise necessary to achieve planned goals. In this regard, both public transport operators (PTOs) partners of the project and members of the User Observatory

Table 20.1 PREVENT interoperability layers

Interoperability levels	*Contextualization to PREVENT*
Interoperability governance	PREVENT proposed technologies shall take into consideration existing regulations and policies on interoperability frameworks and propose recommendations in case there are gaps or constraints due to as-is situation
Integrated public service governance	PREVENT shall take into consideration the involvement of all potential users at national and European levels and describe different coordination and governance mechanisms among them
Legal and ethical interoperability	PREVENT shall take into consideration existing legal and ethical policies and strategies when framing interoperability and technology adoption requirements and propose recommendations of putting in place new legislation in case there are gaps or constraints
Organizational interoperability	PREVENT shall propose different interoperability configurations for potential users in different scenarios, both at MS and European levels
Semantic interoperability	All aspects of data and information exchange with regard to the adoption of proposed technologies will be addressed
Technical interoperability	PREVENT proposed technologies shall support service-oriented architecture (SOA) design paradigm using open and internationally accepted standards, a solution that makes PTOs independent of vendors, products, and technologies which offers great advantages and flexibility in shaping the adoption models' scenarios

Group have been involved in order to evaluate and define the interoperability and technology adoption requirements related to the proposed technologies. Two dedicated questionnaires have been prepared based on the EIF framework in order to collect the different aspects of interoperability: legal, organizational, semantic, and technological. The involved practitioners ensure a wide coverage of different public transport categories (train, metro, security forces in public transport), as well as different European countries (France, Portugal, Italy, Greece, Poland, and Switzerland). The abovementioned questionnaires have been submitted under two dimensions:

1. Coordination dimension: respondents were asked to provide their evaluations with regards interoperability requirements related to coordination/cooperation features of proposed technologies between different public transport organizations and and/or

authorities. Two levels of coordination were proposed: national level (within the same Member State borders and jurisdictions) and EU level (between organizations belonging to two or more different European countries).
2. Technology-based dimension: respondents were asked to provide their evaluations with regard interoperability requirements related to the proposed ten technologies as described in Sect. 20.4.1.

The results of the collected answers are briefly summarized in the below points:

- Interoperability requirements are very heterogenous among different organizations and through different Member States.
- In addition to EU regulations, each Member State has its own/specific laws and regulations which in many cases differ from other countries.
- For organizational interoperability, two major types of governance were considered depending on the level of autonomy the PTOs have or in the case they depend on national authority.
- Concerning the semantic interoperability, many data models exist throughout Europe, and there is a clear need for data model standardization in the domain of public transport.
- Data management is under the responsibility of the PTOs, who express major concerns on access rights when exchanging data with other organizations.
- With regard to technical interoperability, any new technology adoption will require consequent adjustment (in terms of hardware and software) of existing systems.
- Any new technology requires also coordination with other authorities and service providers.
- New technology requires setup of new security policy, specifying minimal security requirements that all users and entities must respect.

20.4.2 Regulatory Aspects

The regulatory environment was analyzed in order to identify the aspects that may have an impact on pursuing any of the scenarios as presented in Sect. 20.3. The major criteria to block and exclude one or more of the initial use case scenarios were based on the avoidance of conflicts among

national regulatory frameworks. Particular attention was also paid to the impact of the GDPR on handling of information within and between practitioners, requesting support from the GDPR and Security Advisors working on the project.

The analysis was based on the input provided by the public buyers involved in the PREVENT project as partners or members of the User Observatory Group (UOG) regarding potential legislative obstacles to the implementation of any of the scenarios. The work focused on the regulatory aspects across the MS of the public buyers, to evolve from the different contexts and practices toward a single regulatory component that can be shared across public buyers for the deployment of the future procurement. The outcomes of the research were further analyzed in order to elaborate a conclusion on the most flexible and adequate legal framework.

The flexibility to deploy an R&D procurement procedure outside the scope of the defense and security procurement legislation (when costs and benefits are shared), the flexibility to conduct ad hoc joint cross-border procurement and to conduct market consultations, and the availability of fast court proceedings were the criteria selected to identify the most suitable public procurement legislation. Additional criteria, such as the willingness to act as lead procurers and the previous experience with the deployment of PCP, are also important to choose the applicable public procurement legislation.

Regarding the impact of the privacy regulation on the selected scenarios in the analyzed countries, it is important to underline that in the regulatory framework, the principle of accountability triggered a double obligation on the part of the data controller: to ensure the respect of the principles relating to the processing of personal data and, more in general, of the data protection law and to demonstrate and fully document such respect.

Therefore, with regard to the scenarios, there weren't absolute limitations or serious impediments on the privacy law side, but rather requirements that must be met in order to ensure compliance with the regulatory sources analyzed. However, particular attention must be paid to scenarios that involve the use of biometric systems, such as facial recognition where particular technical and organizational measures should be taken.

20.4.3 Economic Aspects

An economic assessment of the scenarios of the PREVENT project was performed. The goal was to identify the ones that are the most economically advantageous and to provide recommendations for the refinement of the scenarios. Following an extensive literature review, in order to identify the economic aspects of a scenario, the MCDA analysis [2–4] on the gaps addressed by the scenarios was considered the most suitable method (Fig. 20.7).

In this regard, seven criteria were selected in mutual agreement with the stakeholders, aiming at "measuring" the pros and cons of each gap:

1. The expected improvement of the services quality
2. The Gap Security Value, calculated based on the level of importance of each gap and its contribution to each scenario
3. The current disturbance in the activities of the PTOs deriving from this gap
4. The percentage of occurrence of each gap
5. The current cost of the currently used equipment
6. An approximate estimation of the current financial loses deriving from each gap
7. An estimation of the current price of the technologies available addressing the gaps

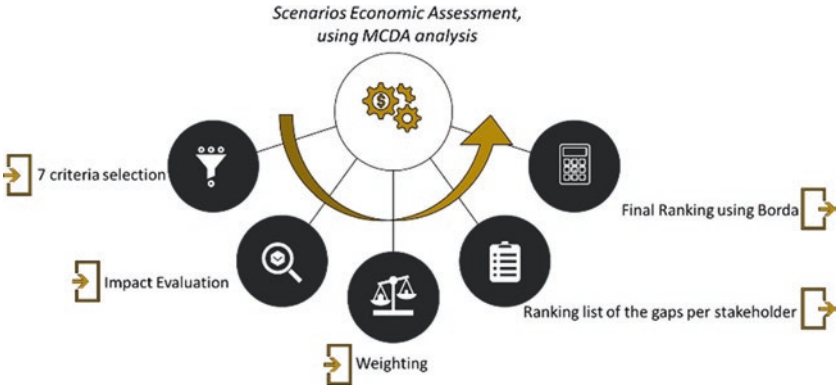

Fig. 20.7 Scenarios economic assessment using MCDA

Following the criteria selection, the proposed methodology involved two phases:

- Impact Evaluation. Impact evaluation is the phase where end users assigned a score s_i, to each gap and criteria C. All these values were normalized at the end, so that the best values became 1 and the worst values became 0.
- Weighting. Weighting indicates the importance of a criterion C in comparison with the other criteria. This was the outcome of the analysis made by requesting the end user to fill in a resistance to change grid.

After collecting the information requested above and making the necessary calculations, the evaluation matrix per end user was prepared. The overall preference score for each gap per end user was simply the weighted average of its scores on all the criteria. Letting the preference score for gap "i" on criterion C be represented by s_{ij} and the weight for each criterion by w_j, then n criteria the overall score for each gap, S_i, was given by:

$$S_i = w_1 s_{i1} + w_2 s_{i2} + w_n s_{in} = \sum_{j=1}^{n} w_j s_{ij} \tag{20.1}$$

Based on the weighted score above, the ranking list of the gaps per stakeholder was produced. The next step of this methodology is to merge the different lists ranking the gaps (one list for every participant) into a unique list.

The weighted scores, calculated earlier, reveal the most-preferred and the least-preferred solutions for a given participant. Of course, the most and the least-preferred gap vary greatly from one participant to another. In that context, it is of utmost importance to compute a unique list, which should somehow take into account the individual preferences of the participants, as expressed in their individual lists. For this purpose, the Borda method [9] was used: for a given solution, instead of computing the average of the scores from the individual lists, the respective "high-ranking score" (HRS) was calculated. Namely, the calculation made includes the number of times that this solution appeared in the top six of an individual's list, and this value was the HRS. Based on the HRS, the ranking of the gaps was calculated. This gap ranking was finally transformed in Scenario Value through the usage of the scenario gap matrix.

20.4.4 Security Scenarios Definition

To achieve a general overview of the aforementioned components, a table summarizing all the needs, technological and limitations analysis was used so as to facilitate the selection of the final set of scenarios (Table 20.2).

On the basis of this exhaustive analytical work and with the continuous engagement of the practitioners, the initial scenarios were refined and adapted into six final scenarios:

Scenario 1: Unattended item(s) in a train station
Scenario 2: Reconnaissance before an attack
Scenario 3: Mass shooting in a train station
Scenario 4: Sabotage of the tracks
Scenario 5: Terrorist crossing different European countries
Scenario 6: Attack with a suicide vest in a subway

Each addressed shared technological anti-terrorist needs in public transport operators' environment, providing different target audiences with information about how the operational and technical challenges of the common security scenarios can be addressed from a technological point of view, taking into account the regulatory and economic capabilities.

20.5 Project Outcomes

20.5.1 Common Challenge Elaboration

As subsequent step and based on the six scenarios, the PREVENT project partners identified the Common Challenge as described below:

Enhancing security situational awareness through:

- *Timely automatic detection of unattended items in public transport infrastructure and in public areas in the vicinity*
- *Identification and tracking of perpetrators*
- *Advanced crisis management system*

This represented the most viable – in many terms – shared need among the different stakeholders. The exploitation of the vulnerabilities in relation to this need has a massive economic cost, which can be measured in

Table 20.2 Example table used for the final scenario's selection

Scenarios	*Technology 1*	*Technology 2*	*Technology 3*	*Technology 4*	*Technology 5*	*Technology 6*	*Technology 7*	*Technology 8*	*Technology 9*	*Technology 10*	*Economical analysis (scenario scoring)*
Scenario #1											
Scenario #1											
Scenario #1											
Scenario #1											
Scenario #1											
Scenario #1											
Scenario #1											
Scenario #1											
Technological analysis	■ *TRL =* ■ *X patents*										
Legal analysis	*GDPR complient …*										

terms of indicators ranging from the cash value to financial losses, business interruption, and damage to property or in worst cases passenger losses. In this context, earlier detection of terrorists and potentially dangerous objects, tracking of detected individuals or situations and coordination of security forces' response, are critical actions that will mitigate the terrorism-related risks.

It is important to mention that this Common Challenge will serve as the basis for the subsequent procurement that will be undertaken on the form of a Pre-Commercial Procurement (PCP) since the need identified will be satisfied through the R&D services provided by the industry's side.

20.5.2 Innovations and Solutions Roadmap

One other important outcome of the aforementioned work was also the development of an innovations and solutions roadmap. This roadmap focuses on providing the PREVENT's consortium partners, as well as the largest European audience, with a consolidated overall picture of the main results obtained under the core activities of the project into a roadmap of solutions and innovations. Such a roadmap is meant to be a multidimensional and interactive map of innovations and solutions providing different target audiences with information about how the operational and technical challenges of the common security scenarios can be addressed from a technological point of view, taking into account the regulatory and economic capabilities.

In Fig. 20.8, the data structure of the aforementioned tool is presented. In particular, the five layers of the innovation roadmap and the rational and relationship between one layer another are analyzed:

Layer 1 – Security Threats Represents the list of identified threats and gaps related to security in public transport. Such threats have different security levels and may target people, infrastructure, transportation means, and/or related public spaces.

Layer 2 – Security Threats' Categorization:

- Detection: focuses on technology gaps that allow the detection of a potential threat in a PTO environment – abandoned items detection, weapons detection, explosive material detection, etc. They are in the scope of this benchmark.

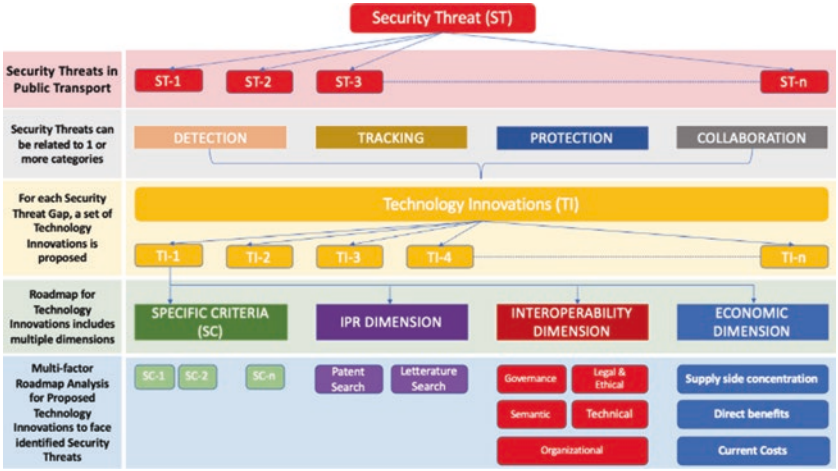

Fig. 20.8 Technology Innovations overall roadmap structure

- Tracking: focuses on technology gaps that allow the tracking of a person responsible for a threat or an attack that has occurred.
- Protection: focuses on technology gaps that allow a protection of strategic places in PTO areas.
- Collaboration: focuses on technology gaps that allow a better collaboration between PTOs and LEAs.

Layer 3 – Proposed Technology Innovations For each security threat/gap, a list of technologies and/or low TRL innovations is proposed.

Layer 4 – Roadmap Analysis Dimensions Each proposed technology innovation will be characterized under four dimensions – technology-specific criteria, IPR dimension, interoperability dimension, and economic dimension.

Layer 5 – Multi-Factor Roadmap Picture The four characterization dimensions are further detailed according to information collected from different sources under work packages 3, 4, and 5.

20.6 Conclusions

Given the increased complexity of the PTO security environment, this chapter contributes to a framework of decision-making based on scenario planning that stresses greater emphasis on the needs of the end users as well as other parameters that could potentially have an impact on the final selection. From the work undertaken by the Consortium, it is evident that technology, regulatory, and economic-related factors are vital data that end users should possess in order to bypass the uncertainties of any decision.

In this regard, PREVENT focused on satisfying the security needs and wants of a variety of end user by designing 12 scenarios and developing a rich methodology in order to refine them and to ensure that the final selection made will represent a viable in many terms need. The Consortium tackled several limitations on the decision-making mechanism ranging from the involvement of the end users and the efficient expression of their needs up to providing sufficient data for the definition of the Common Challenge of a future procurement, not only in security or transport field but also in every field that an innovative procurement is suitable to be conducted.

Acknowledgments

PREVENT project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement no. 833444. The content of this chapter reflects only the author's view, and the European Union is not responsible for any use that might be made of such content.

Bibliography

1. PREVENT – PRocurEments of innoVativE, advaNced systems to support security in public Transport, Grant Agreem. No 833444 Horizon 2020 Eur. Union. (2019).
2. *Multi-criteria analysis: A manual.* (2009, January). London: Department for Communities and Local Government, ISBN: 978-1-4098-1023-0.
3. Noleppa, S. (2013, December). *Economic approaches for assessing climate change adaptation options under uncertainty: Excel tools for Cost-Benefit and Multi-Criteria Analysis.* Eschborn: Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH.

4. Ribeiro, F., Ferreira, P., & Araújo, M. *Evaluating future scenarios for the power generation sector using a Multi-Criteria Decision Analysis (MCDA) tool: The Portuguese case*. https://repositorium.sdum.uminho.pt/bitstream/1822/26142/1/Ribeiro%202013.pdf. Last accessed 2020/07/20.
5. Hedel, R., et al. (2018). Assessment of the European Programme for Critical Infrastructure Protection in the surface transport sector. *International Journal of Critical Infrastructures, 14*(4), 311–335.
6. Chermack, T. J. (2004, April). Improving decision-making with scenario planning. *Futures, 36*(3), 295–309.
7. European Interoperability Framework (EIF) of the ISA programme. https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf. Last accessed 2020/07/20.
8. Organisation for Economic Co-operation and Development. Methodology for Assessment of National Procurement Systems (Version 4). 2006. Available at: http://www.oecd.org/dataoecd/1/36/37390076.pdf. The User's Guide (Section 1) of the document provides very helpful guidance on conducting procurement assessments. Last accessed 2020/07/20.
9. Saari, D. G. (1985, February). The optimal ranking method in the Borda count. IIASA Collaborative Paper. https://core.ac.uk/download/pdf/52944585.pdf. Last accessed 2020/07/20.
10. Technology Readiness Levels (TRL), EC. https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf . Last accessed 2020/07/22.