ISSN 2421-4442

SICUREZZA TERRORISMO SOCIETÀ

Security Terrorism Society

INTERNATIONAL JOURNAL - Italian Team for Security, Terroristic Issues & Managing Emergencies

3
2016

EDUCatt

SICUREZZA, TERRORISMO E SOCIETÀ

INTERNATIONAL JOURNAL
Italian Team for Security,
Terroristic Issues & Managing Emergencies

3

ISSUE 1/2016

Milano 2016

EDUCATT - UNIVERSITÀ CATTOLICA DEL SACRO CUORE

SICUREZZA, TERRORISMO E SOCIETÀ
INTERNATIONAL JOURNAL – Italian Team for Security, Terroristic Issues & Managing Emergencies

ISSUE I – 3/2016

EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.7234.22.35 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione); librario.dsu@educatt.it (distribuzione)
web: www.educatt.it/libri
Associato all'AIE – Associazione Italiana Editori
ISBN: 978-88-9335-048-8

copertina: progetto grafico Studio Editoriale EDUCatt

Table of contents

Planning Security Measures for Major Sport Events' Transport System: a Practical Risk-Based Methodology

Giovanni Pisapia[1]

Executive

Human life in urban areas depends greatly on the services of urban transport. However, we face difficult and complicated problems of safety and security relating to urban transport in normal cases as well as in disaster situations. Understanding the problems, finding approaches and solutions, implementing them, and evaluating results are essential for creating safer transport system (Taniguchi, Fwa and Thompson, 2014).
Recent terrorist incidents – Madrid 2004 (Burridge, 2014), London 2005 (Cowell, 2005), Mombai 2006 (Najar and Kumar, 2015) and Moscow 2010 (Barry, 2010) for example – highlight the risks of urban transport systems. These are exacerbated during major sport events, when the risks of criminal and terrorist activities is particularly high (Richards at all, 2011) and where different transport modes (e.g. air, train, buses, subways) and operators, both private and public, are utilized to move the Games' clients.
Within this context, this article details a practical approach to plan security measures for major sport events' transport system: it describes the main components of the Games' Transport Security Project (TSP) and illustrates the different steps of the methodology to select and implement proportionate and effective security measures. The article will initially provide an overview of the importance of transport security and its challenges, before focusing on the transport security project's requirements and the related methodology.

Recenti attacchi terroristici, ad esempio Madrid 2004, Londra 2005, Mombai 2006, Mosca 2010 e Bruxelles 2016, sottolineano i rischi del sistema del trasporto urbano. I terroristi scelgono spesse volte il trasporto pubblico di superficie per i loro attentati in quanto, con attacchi di questo tipo, si causano rilevanti ripercussioni economiche alla città aggredita, dato che questo settore è di vitale importanza per la vita dei cittadini in generale.
Questa situazione è aggravata quando si svolgono grandi eventi sportivi, dal momento che questi aumentano il volume dei passeggeri nella città ospitante, in particolare vicino ai punti di interesse dell'evento, incrementano la presenza di persone di alto profilo alle manifestazioni, e forniscono un punto di richiamo per l'attenzione dei media, sia locali che internazionali.

[1] Member of the Italian Team for Security, Terroristic Issues & Managing Emergencies (ITSTIME - Italian Team for Security, Terroristic Issues & Managing Emergencies), Department of Sociology, Università Cattolica del Sacro Cuore - Milano, Largo Gemelli 1, 20123, Milan, Italy. E-mail: giovannipisapia@gmail.com.

Il trasporto è un elemento importante per organizzare un grande evento sportivo. Il sistema deve essere allo stesso tempo efficiente, per consentire i movimenti in libertà dei vari clienti (ad esempio atleti e media) ed efficace, nel proteggere i passeggeri e le infrastrutture. All'interno di questo quadro, dato l'elevato rischio relativo alla sicurezza del sistema, c'è la necessità di mettere a punto elementi di sicurezza adeguati per la protezione dei passeggeri, del personale e delle infrastrutture.
La sicurezza, intesa come difesa da atti criminali anche di natura terroristica, insieme alla sicurezza su lavoro (safety) e la gestione delle emergenze, costituiscono un continuum volto a mantenere il sistema dei trasporti, durante grandi eventi sportivi, funzionale, sicuro e protetto.
In pratica, questi principi devono essere concretizzati in elementi pratici per creare un sistema atto a proteggere l'incolumità dei passeggeri e del personale e la protezione delle infrastrutture.
Il sistema di trasporti durante grandi eventi sportivi è complesso, per le diverse tipologie (ad esempio aerei, treni, autobus, metropolitane) ed i vari operatori, sia pubblici che privati, utilizzati per movimentare clienti sul territorio.
In questo contesto, questo articolo descrive un approccio pratico per pianificare misure di sicurezza adeguate per il sistema dei trasporti per grandi eventi sportivi, con un'analisi degli elementi principali del progetto e delle diverse fasi (dieci in tutto) per selezionare misure di sicurezza efficaci e proporzionali al rischio stimato.
L'articolo vuole innanzitutto dare una panoramica dell'importanza e della complessità nell'istituire misure di sicurezza per i trasporti urbani di superficie, prima di concentrarsi sui requisiti utili, e la relativa metodologia, per pianificare misure di sicurezza adeguate.
L'obiettivo è quello di descrivere gli elementi principali di una metodologia atta a mettere in sicurezza (intesa come difesa da atti criminali, anche di natura terroristica) il sistema dei trasporti durante un grande evento sportivo.
Al fine di mantenere l'efficacia e l'accessibilità del trasporto per i vari clienti durante grandi eventi sportivi, adeguate misure di sicurezza devono, allo stesso tempo, non interferire con le operazioni di trasporto e fornire un ragionevole raggiungimento degli obiettivi di sicurezza in termini di deterrenza, rilevamento, e mitigazione del rischio.

Keywords

security, detect, deter, deny, mitigate, threat analysis, improvised explosive device, terrorism, risk assessment, transport system, traffic management

1. Introduction

Between 1st January 1970 and the 31st December 2015, there has been a total of 4690 terrorist and serious criminal assaults on all public surface transportation targets worldwide. If attention is confined to attacks on buses, passenger trains and ferries, the total is 3409. The countries of South Asia, especially India and Pakistan, account for 1274 or 37,4% of these attacks. The Middle East follows with 810 attacks, or 23,8% of the total, and Southeast Asia with 319, or 9.4% of the total. Another 48 attacks (1.4%) occurred in the countries of Eastern Europe, bringing the European total to 361 (10.6% of

the total). This figure includes the Baltic States, but not Russia or the other countries of the former Soviet Union. With regards to lethality, attacks in South Asia, for example, killed an average of 3.6 people per attack, while in Western and Eastern Europe, the rations were significantly less: 1.4 and 0.7 respectively (Jenkins and Butterworth, 2016).

There are reasons why terrorists so often choose a transportation setting for their attacks: with such an attack, it is possible to disrupt the economy of a city, region and nation in general, as this sector is vital for business and individuals alike. Damage to this sector has widespread economic effects. This situation is exacerbated when major sport events (MSE) take place, as these increase the passengers' volumes in the host city, drawing large crowds around site precincts and transport hubs, raise the presence of high-profile individuals and provide a focus for media attention (Tarlow, 2002).

Transportation is an important element to organize a successful major event, as it is concerned with the efficient movements of people during the Games. The system is required to be as open and efficient as possible to allow personal freedom of movements for the Games' clients (e.g. athletes, media and press). The system, at the same time, has to protect the clients while being transported throughout the Games' theatre. Within this setting, there is a trade-off between these requirements and the implementation of security elements to ensure passengers and infrastructure are safe and secure.

It is important that Games' host cities, organizing committees (OC) and government departments, when planning transport operations for a major sport event, take note of safety and security considerations at the outset of the project. It is also an interest of the Games' transport managers to ensure the Games' transport system is secure. Current man-made threats, including an attack through destructive devices, require the adoption of effective security measures – which include physical, technology, and security processes – to secure passengers and transport assets.

It is practically impossible to achieve a one hundred percent security protection for such a complex system as the transport operations during major sport events. However, probabilities of an adverse incident occurring could be lowered by applying knowledge and expertise in implementing safety and security measures. In addition, as Games' continue to attract increasing national and international media attention, and as competing needs for resources and attention to manage such events are brought to the fore, it is important to highlight the challenges and possible methodological solutions to plan and operate an efficient and risk-proportionate transport security system.

Often security is an add-on rather than a principal component of a project. Security instead should be among the first considerations in the development of a design for a new transport hub or infrastructure. When security measures

are included in the design of a building, the costs are generally minimal. When retrofitting is required, it can be costly, unattractive and dysfunctional, as observed at many airports, where management is still grappling with finding space for the security apparatus that is integrated into passenger and luggage flow (Edwards and Goodrich, 2013).

This article describes the main elements of a major sport event's transport security project, from the outset to the decommissioning phase, and proposes a practical methodology for conceptualizing and designing proportionate and effective security measures. It focuses exclusively on the security requirements for major events' transport systems, leaving aside safety and emergency management considerations, which would need to be managed through different processes. The article stems from the author's practical experience in conceptualizing, managing, and implementing Games' transport security projects.

The article will initially define the terms security, safety and emergency management, often used interchangeably by operators. It will then focus on the challenges in implementing security elements for public transport systems. The article will then provide a brief summary of Games' transport system requirements and the elements necessary to establish a transport security project. It will then present a viable methodology, tested during previous Games, to design, plan, and implement security measures for major sport events' transport systems.

2. Security, Safety and Emergency Management for Transport Systems

Safety, security and emergency management are terms that are often used interchangeably. While closely related, each term represents distinct domain. At times, the purposes of these three areas of knowledge overlap, while, in other occasions, they find themselves at odds. It is thus important a clear understanding of each term, as the areas they represents are different.

Frances L. Edwards and Daniel C. Goodrich, in their seminal book on transport security, state that, in general, security can be defined as the effort to protect assets – physical, human or intellectual – from criminal interference, removal or destruction, whether by terrorists or domestic criminals, or incidental to technological failures or even natural hazards events. In particular, security defines the domain of protecting something valuable for any form of deliberate interference. It thus requires a physical response to an external conscious threat, normally meaning that this is a human versus human issue. In transportation, security involves both the items being transported (e.g.

goods, people) and the machinery used to transport the items. Instead, safety developed out of the need to prevent accidental deaths and injuries due to natural or inadvertent man-made activities. It is an effort to mitigate the damage inflicted by unconscious forces that humans encounter, that can usually be avoided by thinking through the environmental issues and creating barriers or procedures to help prevent unsafe events from occurring. Instead, emergency management becomes necessary when either safety or security fails (Edwards and Goodrich, 2013).

As detailed by Frances L. Edwards and Daniel C. Goodrich (2013), safety in surface transportation systems is characterized by compulsory regulations for the sector, which includes operators' safety on the job, as well as passenger safety while on the asset. For example, a driver's license is required to operate motorized transport to ensure that all drivers know the vehicle codes and roles of the road to avoid accidents. Different classes of licences are required for more complex transportation equipment. Mass transit work rules are focused on enhancing safety for crew and passengers, limiting the length of shifts worked and outlawing unsafe behaviours like texting while driving. Physical barriers are also used, such as divided highways, and traffic controls, like lights and signals, to enhance safety for passengers, for example while waiting to load onto a bus in a pickup/drop off area.

While safety standards are regulated, security is usually benchmarked against best practices rather than formal standards. Part of the reason is that specific sets of circumstances exist for each type of transport routeand asset, necessitating a separate security analysis for each to define appropriate solutions (Edwards and Goodrich, 2013). For example, in the UK, The Department for Transport (DfT) sets and enforces counter-terrorism security measures on a number of transport modes including aviation, the national rail network and the London Underground. However, it does not regulate the bus and coach sector, for which it provides exclusively guidance for the industry following requests for advice from some bus operators in the wake of the London bombings in July 2005 (UK Department for Transport, 2012).

3. Challenges in Implementing Security Measures for Surface Transport Systems

As stated by Frances L. Edwards and Daniel C. Goodrich (2013), surface transportation assets provide an attractive target to terrorists and criminals because of the value of their contents – both material and human – and the openness of the system. To be successful, security measures have to impact, for example, the adversary's view of a target's attractiveness while enhancing

the passenger's view of the asset's functionality. From a security perspective, the surface transport openness limits the measures available to transportation operators and owners to prevent security breaches that could cause damage to their systems and customers. Surface transportation, in order to be efficient and effective, must be open to potential users, be readily accessible and focused on timeliness in the delivery of service. These characteristics make it difficult to include a high level of security. Unlike air transport, where the use of air space is controlled by the government and there are controlled gateways and lead time before flights, surface transportation relies on enabling specific clients to make a travel decision at a moment's notice and on enabling carriers to change schedule, for example to enhance clients' satisfaction. While these factors work toward the success of the system, they unfortunately become difficult when implementing security. These challenges are exacerbated during major sport events, where an effective and efficient transportation system is vital in order to get people into the country, move them around the host city and transport them to and from the Games' venues. Any attack that shuts down the transport network has a direct impact on the Games and arguably is an attack on the Games' itself, regardless of whether the actual venues are targeted or not (Swain, 2011).

To keep transport systems accessible to the Games' client groups, security measures would have to be identified and applied in a careful way to ensure they do not interfere with the operation of systems and assets, while at the same time providing reasonable attainment of the security objectives of deterrence, detection, denial and mitigation.

How then to plan proportionate and effective security measures for the transport system during major sport events? This article will provide an answer by detailing the elements of a successful transport security project, focusing on the methodology developed to protect such system from terrorist attacks and crime incidents through proportionate and effective measures aimed at protecting the travellers and the transport assets.

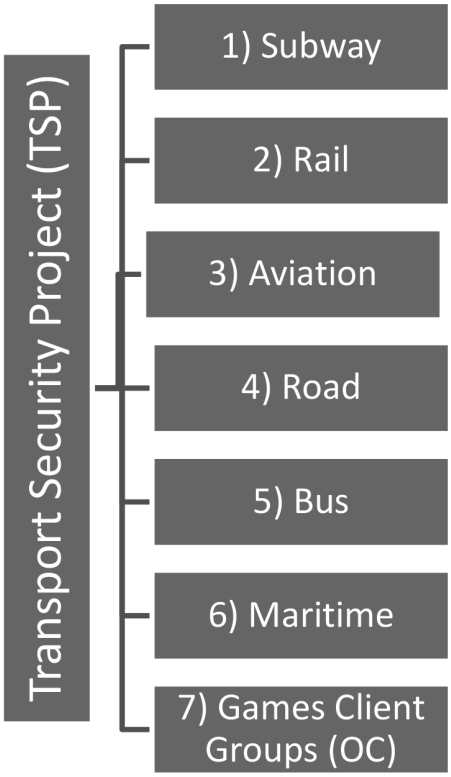
4. Major Sport Events' Transport Security Project (TSP)

Games' transport system consists in a complex and geographically dispersed operation, conducted over a substantial period of time, characterized by the movement of different Games' clients (e.g. spectators) to various official competition, non-competition and training venues. Within this background, planning transport security measures for major sport events presents significant challenges given the different partner agencies and regulations from across the public transport realm. It is therefore required the establish-

ment of a project to conceptualize, design and implement security elements for the Games' transport security. The following are the most prominent elements to build a successful transport security project (TSP):

- A complex regulatory environment characterizes the Games' transport system. Thus, the project requires the establishment of *clear roles, responsibilities and risk ownership* among different partner agencies.
- The project needs a *multi-agency approach* to develop an integrated security plan targeted at the risk of terrorism and general criminal activities against the travelling public, the Games' client groups and the transport infrastructure.
- The *project's objectives* need to be clearly articulated:
  - To conduct *security risk assessments* for all relevant transport hubs and routes, including public transport infrastructures.
  - To advise all transport system operators, including the organizing committee (OC) for the Games' clients groups, of suggested protective *transport security measures.*
  - To coordinate all *operational transport security plans* for the event, which will consist in different law enforcement and transport operators' security operational plans.
  - To support the OC and transport operators to ensure that transport routes and hubs operating plans comply with relevant *security regulations and guidance*.
  - To ensure the transport security operational plans are fully integrated with other *security operational plans* (e.g. venue and site; VIP; command, control and communication; crisis and emergency management).
- To organize systematically the activities among the different role-players, the project has to be divided into seven *modal groups* (Figure 1, below), which need to comprise all the transport modes that have to be assessed from a security perspective: train, subway, bus, air, roads network, maritime and the organizing committee Games' client groups transport system. The latter is usually composed of Games family clients and members who have access to on-demand pool cars and drivers, athletes and team officials dedicated bus service from/to the Village/s, media/press and technical official dedicated bus service, and spectator and workforce dedicated service.

Figure 1 - *Transport Security Project's Seven Modal Groups*



– The *Games' traffic management*, for which the local traffic authorities are responsible for in conjunction with the OC Transport Department, has to sit outside the project's remit.
– The project has to be coordinated through its *Working Group*, chaired by the project's manager, where representatives from each modal group (above) are present. Such Group is responsible for agreeing on the project's major milestones and deadlines, allocating associated tasks, agreeing on roles and responsibilities, co-ordinating planning activities and sharing information. The Group has to incorporate specialist advisers or regulatory bodies. At an operational level, actual planning takes place within the different modal groups, which are relatively small, less formally structured, and can be called on an ad-hoc basis, when required. From a reporting perspective, the modal groups report to the Working Group on a monthly basis. The project manager is in charge of compiling a highlight report to the security steering group, which has an oversight on the project's activities, after consultation with each modal group.

- The project has to be divided into *planning and operational phases*. During the former, the focus is on the seven modal groups' activities, which is concluded with the drafting of clear security operational plans for each operator within the different modes. Within this phase, training, tests and rehearsals are carried out to ensure all operators are ready to implement security solutions for the event. Also, alignment between the various partners in implementing the transport security requirements is paramount. The second phase consists in the implementation of the agreed transport security elements for the event. The transport security operations are managed through a central command centre, where communication and coordination of activities on the ground among operators takes place. Specific dates for such phases depend on the event's timelines, such as the arrival of the first athletes, the "soft" opening of the village and the first public event attended by spectators.
- From a resource perspective, a *project manager* is required to define and coordinate all activities, supported by specialist advisers, tasked to conduct risk assessments of the transport infrastructure, including hubs and routes servicing the Games. In addition, each "mode" need to have its *project lead*, and each transport operator need to have personnel responsible for the security planning for the event, capable of translating risk assessments recommendations into practical countermeasures to lower the measured crime and terrorist risks during the event.
- During the event, each transport operators and the law enforcement agencies require to *deploy personnel and implement the agreed security measures*. Such measures could consist in private security personnel patrols at transport hubs and enhanced CCTV surveillance system capabilities over the Games' routes. Law enforcement agencies are expected to work in conjunction with transport operators to define their policing plans to secure the event's transport system. During the event, the project manager and her specialist advisers are tasked to *monitor the implementation of the security plans* by the various role-players, providing assistance and managing the transport security desk in the command, control and communication (C3) room for the event.
- The *project's legacy* consists in an enhanced security setting for the host city's transport system operators. Heightened security measures implemented by the various operators (e.g. subway, buses) during the Games could stay on after the event, such as physical (e.g. hostile vehicle mitigation measures), operational (e.g. patrols) and procedural (e.g. command, control and communication) enhancements. In addition, the coordination of this multi-stakeholder project augments the cooperation between

the various operators and law enforcement agencies on crime prevention activities for the safety of passengers after the Games.

– Ideally, the project team should be based within the *OC premises* to be able to retrieve updated information from internal functional areas, *in primis* transport. Such information is necessary to conduct the security risk assessments of the transport system, which define the countermeasures to be implemented during the Games.
– Such a complex project is characterized by different *risks*, among which, the following should be taken into consideration during the planning phase:
  - As all security operations should be planned with a *specific risk level for the event*, the rise in the threat level during the planning might lead to inadequate transport security measures. In case the risk of the event increases, then additional resources would need to be implemented. It is thus important to take into consideration such eventuality when defining resource contingencies during the event.
  - Stemming from the project's multi-agency approach, a possible risk consists in having *confused roles and responsibilities* among role-players, leading to inadequate transport security due to the lack of clarity and detail. To overcome it, clear roles and responsibilities concerning transport security requirements among law enforcement agencies, transport operators and OC need to be defined early in the project's definition. An useful tool is drafting and agreeing on a RACI matrix[2] among all partners at the outset of the project.

The core of the project consists in the identification of effective security measures for Games' transport system. Such endeavour requires the adoption of a methodology to identify the most appropriate and proportionate security elements. The section below will detail the main elements of such methodology.

5. A Practical Methodology to Secure Games' Transport System

As detailed above, Games' transportation assets provide an attractive target to terrorists and criminals because of the value of their contents, both material and human, and its openness, in particular its surface section. This openness

[2] RACI stands for Responsible (who will be doing the task), Accountable (who has the authority to take decisions and who is ultimately accountable for the task), Consulted (anyone who might provide relevant information) and Informed (who has to be kept updated about the progress, anyone those work depends on this task).

further limits the measures available to transportation operators and owners to prevent security breaches that could cause damage to their systems and customers. It is thus important the setting up of an effective transport security project to be able supervise the planning and implementation of the security elements for the Games. Even more important is the implementation of a rational methodology to determine the security mitigation measures to be implemented by assessing a number of variables such as threat, vulnerabilities and consequences, which impact subsequently on the project's resources and funds.

Figure 2 - *Transport Security Project's Methodology (10 Steps)*

Such methodology has to assess both terrorism and crime-related risks, bearing in mind that security countermeasures implemented to mitigate against terrorist risks, such as policing patrols or CCTV surveillance systems, might also counter some other forms of crimes. The proposed methodology consists in the following ten steps (Figure 2, below):

– Identify relevant transport infrastructure.
– Retrieve background information.
– Conduct site visit.

– Carry-out risk assessment.
– Draft risk assessment report.
– Coordinate the transport security integration group.
– Finalize security risk management report.
– Approval by the security steering group.
– Draft the transport infrastructure's security plan.
– Implement security measures during the Games operational phase.

The *first step* consists in clarifying which transport infrastructure falls within the realm of the project. For this purpose, the starting point is to have a clear definition of the Games' transport infrastructure to inform which elements need to be secured. A workable definition is: parts of any type of the transport route or transport hub carrying Games' passengers or traffic to, and from, a competition or non-competition venue. Thus, transport routes and hubs that are the main points for loading and unloading Games' passengers, from which they may initiate or terminate their journeys, and their subsequent routes, even though these may not be in the Games' venue precincts, should be included within the project's scope.

However, additional attention should also be given to the entire public transport system within the host city, as this could be at a heighted risk from criminal activities because of an increase of media attention and passengers' volume during the event. TSP should be also responsible for the security of rivers and maritime in the venues' precincts, in addition to the air exclusion orders. Out of scope matters consist, for example, in logistics security measures, general safety issues or traffic management for the Games. All these elements need to be managed separately through different projects, which need to be integrated with the TSP to ensure a holistic coordinated approach to the event's operations.

The definition above guides in defining the transport infrastructure, including assets such as hubs, depots, routes, bus, railway stations and their immediate precincts, which need to be secured through the project's deliverables.

Security requirements for the "last mile", the spectators' route that starts from a transport hub (usually one per site) to the venue and vice-versa, are usually the responsibility of venue security planners, who are responsible for all security operations within the Games' sites, including their precincts. In this respect, it is important to ensure the integration between venue and transport security plans, from a spatial perspective, to avoid gaps between the two projects in the security overlay, ensuring an effective theatre wide security operation.

Once Games' transport infrastructure has been determined, the *second step* consists in retrieving all background information by the relevant opera-

tors. The *third step* consists in carrying out a site visit of the transport infrastructure by the Project's team, law enforcement personnel and the relevant transport operators. Such infrastructure could consist, among others, in a depot, route, hub or buses loading area. The task consists in gaining a visual appreciation of the site, analyse current security measures in place and ascertain possible vulnerabilities in terms of considered risks related to criminal activities and terrorism.

The first three steps are dependent on partners (e.g. host city, OC, transport operators) to provide necessary relevant information on all transport hubs, routes, drop-off and load zones for the Games' clients, including spectators and workforce. Such information should include sites and routes drawings and estimated numbers of people transported through the various modes. If such information is not confirmed, because of uncertainties related to the finalization of the transport operations, it is impossible to define necessary security elements for the Games and establish required financial resources. Thus, the risk of inadequate security due to the lack of confirmation of Games transport infrastructure highlights the need to develop, during the planning phase, effective information flows between the security and the transport structures to ensure planning can occur without delays. It is thus important that the transport and security project plans are aligned to ensure activities are coordinated.

The *fourth step* consists in drafting the transport infrastructure's security risk assessment. This constitutes the fulcrum of the entire methodology as all security measures need to be proportionate to the estimated terrorism/crime-related threats and informed by the risk assessment process. This step is required to recommend adequate and reasonable security measures that can effectively lower the determined risk of terrorism and crime against Games' transport infrastructure (Roper, 1999). Thus, only through a strong risk assessment process it is possible to avoid or over-protecting or failing to protect adequately an asset (Pisapia, 2008).

Usually, this is conducted by using a pre-determined and agreed methodology by all relevant partners, including the responsible law enforcement authorities, organizing committee, and transport operators. Various methodologies exist to draft risks assessments of critical infrastructure and key assets (American Petroleum Institute and the National Petrochemical & Refiners Associations, 2004; American Society for Industrial Security, 2003; American Society of Mechanical Engineers, 2006; Federal Emergency Management Agency, 2005; Matalucci, 2002). However, the important elements that such methodology needs to have are:

– An objective rationale.

– A consistent approach and evaluation of risk across transport infrastructure assets, including routes for example.
– A rationalized basis for security planning.
– Prioritization of resources and mitigation across transport assets through a comparative process.

Such methodology informs security planning through a numerically based assessment of the risks against transport infrastructure by the most likely terrorist attacks modus operandi (e.g. improvised explosive devices - IED) and crime incidents (e.g. theft, vandalisms). Safety risks (e.g. fire) need to be dealt with separately, through a different process. Such methodology takes into consideration the following elements: capability, intent, vulnerability, likelihood, impact, asset attractiveness and overall risk.

The scoring takes place immediately after stage three (site visit), ideally on the next day. To ensure consistency, so that similar assets with similar risk score are protected through similar security measures, the assessments need to be conducted by the project team as permanent members and, if required, with operators of the specific asset analysed included as temporary members. It is important that subject matter experts from law enforcement agencies and the private sector are present consistently when the scoring takes place. Whilst the scorings does not need to be a unanimous process between the members of the group, there must be agreed consensus of the outcome.

Once the risk assessment is conducted, the project team will draft the risk assessment report (*step five*). Such documentation includes: the outline of the transport infrastructure, how the risk assessment method was carried out, the risk-scoring matrix against each defined terrorist attack modus operandi/ crime incidents, the suggested countermeasures, and how those mitigations will improve the security of the infrastructure, highlighting the difference between the scores of the non-mitigated risks, the mitigated risks and the residual risks.

The countermeasures need to follow the general objectives of security, which the US Transportation Research Board has identified as: deter, detect, deny and mitigate. A security measure for the Games' transport system can thus be selected based on how well it contributes to one or more of the following security objectives (Transport Research Board, 2006):

– *Deter*: to cause an adversary to abandon consideration of targeting an asset during their planning stage due to the introduction of certain security measures. Deterrence is due to one or both of the following: the target was devalued or the probability of success was decreased. Deterrence measures implemented for the latter's objective include active surveillance of stations and platforms with staffed cameras that result in immediate response

to a perceived threat, or selective passenger screening using personnel and dogs for example. The goal is to make the adversary's surveillance and planning efforts fruitless or very difficult while posing little inconvenience to customers. The other deterrence strategy is devaluing the target by protecting the principal assets. This can be accomplished by fencing or walls, guarded entrances or alarms (Edwards and Goodrich, 2013).

– *Detect*: to discover the planning of a threatening event, such as may be indicated by extensive observation of operations or equipment, or the presence of a threat agent (e.g., weapon or explosive). Detection of planning for an attack on transportation infrastructure can be accomplished through intelligence gathering and analysis, or through observed behavior at stations and assets. For example, people taking photos of critical infrastructure elements that are not touristic attractions or inherently interesting may indicate target surveillance. Detection may also occur in the early stages of attack plan implementation. Monitored cameras may detect suspicious behavior on a platform or attempts to enter restricted spaces by unauthorized personnel. Passengers may report the presence of a suspicious package, or canines may sniff out an explosive device before it detonates (Edwards and Goodrich, 2013).
– *Deny*: to deny access to a target consists in measures such as barrier reinforcement, unexpected relocation of the target, and patterns that differ from those expected. Potential hiding places for explosive devices like refuse containers and vending machines can be redesigned or repositioned to impede their use.
– *Mitigate*: to reduce the effects of an event when it occurs by either reducing the magnitude of an event (e.g., reduced target size) or preventing the threat agent from being maximally effective (e.g., because of a sprinkler system or rapid identification of a released toxin).

Through the implementation of these four objectives, the security of transportation assets and infrastructure is greatly enhanced, although perfect security is impossible in an open environment. To keep surface transit accessible to the Games' client groups, these security measures would have to be applied in ways that do not interfere with the operation of systems and assets, while at the same time providing reasonable attainment of the objectives of deterrence, detection, denial and mitigation.

The recommended security elements need to be aligned with the agreed *standard security measures for the event*, which details the costs and modelling of each possible security option, agreed by all stakeholders before the start of the process. This will ensure a standardized approach, guaranteeing that similar transport infrastructures with similar estimated risks are protected through

similar agreed security measures. Such security standard elements refer to physical, technological and procedural elements, such as:

- Fencing: to ensure the integrity of sites after security measures are implemented.
- Vehicle search area: to screen all vehicles entering a Games' site and ensuring they are free of prohibited and illegal items.
- Pedestrian search area: to screen all persons entering the Games' site to ensure they are not in possession of prohibited or illegal item.
- Security technology equipment to deter and detect a possible adversary, namely CCTV surveillance system, pedestrian intrusion detection system (PIDS) and public lighting.
- Law enforcement personnel and private contract security staff deployment to deter, detect and respond to a criminal act.
- Vehicle dispatch center: area where all vehicles and materials are subjected to search before materials are delivered to a venue.
- Vendor secure certification scheme: suppliers allowed to pre-screen materials for direct delivery to venues.
- Accreditation and access control: to manage, monitor and allow accredited persons access to the venue or controlled area.
- Security awareness training for operators (e.g. drivers, loading personnel): see something/say something policy.
- Security elements related to vehicle access to venues: road closures[3], parking restrictions, hostile vehicle mitigation (HVM) measures and automatic number plate recognition (ANPR) cameras for the protection from an unauthorized vehicle entry to Games' site[4].

Because prefect security is impossible for all transport nodes, the risk assessment will determine which elements must be implemented. For example, access points to a transport hub with poor lighting and little activity are usually hardened, made more resistant to intrusion. However, it is impossible to protect 100 % the transport system's assets: there are never enough resources to accomplish that goal. The cost in personnel and constant of such security upgrades would be detrimental to the operations. Therefore, the risk assessment process assists with maximizing the security resources available to protect the most relevant assets (Edwards and Goodrich, 2013) in a proportionate and reasonable way.

[3] Defined in the UK as Traffic Regulation Orders (TROs) and Anti-Terrorist Traffic Regulation Orders (ATTROs)

[4] Two possible terrorist attacks methods to limit with such measures are suicide vehicle borne improvise explosive device (SVBIED) or a vehicle borne improvise explosive device (VBIED) against protected assets.

Once the risk assessment document is drafted, with all security countermeasures to lower the estimated risks, it is tabled at the transport security integration project group (*step six*), where the transport operator and all relevant role-players comment, discuss and finally agree on the recommended security requirements spelled out in the report. Such forum allows non-security partners to elaborate on the possible impacts and feasibility of suggested security elements on the transport operations. The discussion focuses on the implementation of the suggested security measures in line with the transport operations.

Once the transport security integration group has validated the security elements, *step seven* consists in drafting the final risk management report, complete with agreed security countermeasures, which need to establish an integrated security system for the transport asst. When designing the security system, three intertwined aspects need to be taken into consideration: physical, technological and process-related.

The *physical element* of security establishes and maintains barriers to create a protective perimeter to the transport assets. It is designed to slow down an intruder, or make the intrusion more obvious, or to allow for a timely response and interdiction. Such barriers may include fences, locks, doors and windows. Physical security has to appear robust, even if there are unavoidable vulnerabilities. The key to successful physical deterrence is to create the image of consistent resistance to an asset. In addition to physical security, *technologies* are the second element of a security system: cameras, motion detectors, automatic vehicle locating (AVL) systems and electronic alarm devices. The operation of these systems determines whether they are actually a deterrent or just a means of prosecuting criminals after the fact. In addition to the physical and technological security layers, the third element of an integrated security system consists in *policies, procedures and contingency plans*: while physical security is transparent, the policies and procedures are less apparent. They complement the physical and technological security elements by ensuring these are employed appropriately and that, when compromise of security occurs, it is met with a proper response (Edwards and Goodrich, 2013).

One policy, which has proved to be successful, is the "*see something/say something*" approach. As riders have a vested interest in the safe operation of a transit system, it is a matter of informing the system users of ways that can become part of the organization's security solution. One method is to create a communication conduit into the security apparatus for passengers with knowledge about threats to the system to share. This policy drastically increase the size and scope of the security apparatus because of the number of eyes and ears helping the security system to identify and engage potential

threats. The same concept is applied to transport staff members who do not have a direct security role: they need to be reminded that they are an integral part of the security apparatus: their actions or failures to act or report an issue can have a significant impact on their organization's security (Edwards and Goodrich, 2013).

The report is then forwarded to the security steering group (*step eight*), which consists of a wider audience of security professionals from the relevant agencies, including the OC and the law enforcement. The steering group meets monthly and notes of decisions are recorded and distributed among all members. The report will be then analysed and a decision taken on the recommendations proposed. The objective of the group is to validate, by senior security role-players, the proposed appropriate security measures to reduce the ascertained risk to an acceptable level. An interesting aspect of such task is to acknowledge the difference in appetite for risk and budget considerations by the different role-players, such as the OC and the law enforcement agencies. This forum will thus be able to track the overall costs of the project, by recording the security costs for each transport infrastructure. Considerations need to be given about the responsibilities for the implementation of such security measures, as some will fall under the transport operators, while others under the law enforcement agencies and the host city.

Once the steering group approves the security elements, it is possible to draft of the transport infrastructure's security plans (*step nine*) by the transport operators, the OC and the law enforcement agencies. The latter includes the drafting of police operational orders for each transport hub and route. The *final tenth step* consists in the actual implementation of the security measures during the event, and the monitoring of what is implemented against what was agreed during the planning phases.

The successful implementation of this ten steps' methodology depends on the effective and prompt exchange of information between transport operators, including the OC transport functional area, law enforcement agencies, the host cities and the project team to ensure risks are assessed correctly, countermeasures are identified, and security measures are implemented against the Games' transport system.

To ensure the implementation of the methodology with the time and resource constraints of the project, a *project plan* needs to be drafted with all relevant actives and deadlines. The most important milestones of the TSP consist in: draft all project documentation, schedule all transport infrastructures' risk assessments, establish and convene the Transport Security Project's Working Group (where the modal groups leads meet to report on their activities), ensure all operational plans by partners are fully aligned, and draft the testing and exercising drills for the event.

From a governance perspective, the project need to be overseen by the responsible law enforcement agency for the event's security. Following the implementation of the stipulated security measures during the Games, the project manager will be in charge of drafting a debriefing report to summarize all the security measures implemented and highlights challenges and best practices.

6. Conclusions

This article's objective was to describe the main elements of the transport security project for a major sport event and provide a viable methodology to conceptualize, design and implement security measures for Games' transport system. The project acknowledged that transport infrastructure cannot be fully protected against criminal and terroristic attacks: for example, roads and rails lines cover so many miles that the systems' lengths preclude any complete system-wide security. Thus, bearing in mind economic and feasibility issues, the methodology proposed assisted to set priorities to protect passengers and critical assets.

Through the implementation of the methodology described in this article, the security of transportation infrastructures for major sport events can be greatly enhanced, although perfect security is impossible in an open environment. To keep surface transit accessible to the Games' client groups, these measures have to be applied in ways that do not interfere with the transport operations, while at the same time providing reasonable attainment of the security objectives of deterrence, detection, denial and mitigation.

However, security is just one of the elements that, with safety and emergency management, constitute a broader continuum aimed at keeping Games' transport system functional, safe and secure (Edwards and Goodrich, 2013). In practical terms, all these principles need to be implemented to create a holistic safe and secure system. For example, a transport bus depot has surveillance system and controlled entry points to protect the site from illegal intrusions and related system disruptions. At the same time, bus drivers are trained in safe practices and it is ensured proper licenses are enforced. However, inevitably, an event occurs that interferes with the operations, which need to be dealt with promptly to ensure the safety of passengers and employees until the disruption is over. It is thus important for emergency management, safety and security functions to be embedded into the Games' transport system to establish a holistic system with the focus on human life preservation and property protection.

Annex: List of Acronyms

Full Name	*Acronym*
Anti-Terrorism Traffic Regulation Orders	ATTROs
Automatic Number Plate Recognition	ANPR
Automatic Vehicle Locating System	AVL
Command, Control and Communications	C3
Department for Transport	DfT
Geographic Information System	GIS
Hostile Vehicle Mitigation	HVM
Italian Team for Security, Terroristic Issues & Managing Emergencies	ITSTIME
Major Sport Events	MSE
Organizing Committee	OC
Pedestrian Intrusion Detection System	PIDS
Pedestrian Screening Areas	PSA
Residents Access Parking and Permit	RAPP
Suicide Vehicle Borne Improvise Explosive Device	SVBIED
Temporary Traffic Regulation Orders	TTROs
Transport Security Project	TSP
United Kingdom	UK
Vehicle Borne Improvise Explosive Device	VBIED
Vehicle Permit Checkpoint	VPC
Vehicle Screening Areas	VSA

References

American Petroleum Institute (API), National Petrochemical & Refiners Associations (NPRA) (2004), *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries*, Second Edition, October 2004.

American Society for Industrial Security (ASIS) International (2003), *The General Security Risk Assessment Guideline*, Alexandria, Virginia.

American Society of Mechanical Engineers (ASME) (2006), *RAMPCP: the Framework*, ASME Innovative Technologies Institute LLC (ASME-ITI), Washington D.C.

Barry E. (2010), *Chechen Rebel Says He Planned Attacks*, 31 March 2010. Accessed on 2016-02-12 at: http://www.nytimes.com/2010/04/01/world/europe/01dagestan.html?fta=y.

Burridge T. (2014), *Spain remembers Madrid train bombings 10 years on*, BBC News, 11 March 2014, Madrid. Accessed on 2016-02-12 at: http://www.bbc.com/news/world-europe-26526704.

Cowell A. (2005), *Subway and Bus Blasts in London Kill at Least 37*, 8 July 2005. Accessed on 2016-02-12 at: http://www.nytimes.com/2005/07/08/world/europe/subway-and-bus-blasts-in-london-kill-at-least-37.html?_r=0.

Edwards F.L., Goodrich D.C. (2013), *Introduction to Transportation Security*, CRC Press by Taylor & Francis Group, LLC.

Federal Emergency Management Agency (FEMA) (2005), *Risk Assessment, a How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*, Risk Management Series, FEMA 452, January 2005.

Jenkins B.M., Butterworth B.R. (2016), *Long-Term Trends in Attacks on Public Surface Transportation in Europe and North America*, Mineta Transport Institute (MTI), 25 January 2016.

Matalucci R.V. (2002), *Risk Assessment Methodology for Dams (RAM-D)*, from proceedings of the 6th International Conference on Probabilistic Safety Assessment and Management (PSAM6), 23-28 June 2002, San Juan, Puerto Rico, USA.

Najar N., Kumar H. (2015), *Indian Court Convicts 12 in 2006 Bombings of Mumbai Trains*, 11 September 2015. Accessed on 2016-02-12 at http://www.nytimes.com/2015/09/12/world/asia/indian-court-convicts-12-in-2006-bombings-of-mumbai-trains.html.

Pisapia G. (2008), *The Development of a Terrorism Risk Management Framework (TRMF) for the Protection of Critical Infrastructure Facilities from Terrorist Physical Attacks*, unpublished Ph.D. thesis, Universita' Cattolica del Sacro Cuore, Milano, 2008.

Richards A., Fussey P., Silke A. (2011), *Terrorism and the Olympics, Major Event Security and Lessons for the Future*, Routledge, Taylor and Francis Group.

Roper C.A. (1999), *Risk Management for Security Professionals*, Butterworth-Heinemann, Boston.

Swain S. (2011), *Securing the Transport System*, in Richards Anthony, Fussey Pete and Silke Andrew (2011) *Terrorism and the Olympics, Major Event Security and Lessons for the Future*, Routledge, Taylor and Francis Group.

Taniguchi E., Fwa T.F., Thompson R.G. (2014), *Urban Transportation and Logistics. Health, Safety, and Security Concerns*, CRC Press Taylor & Francis Group.

Tarlow, P.E. (2002), *Event risk management and safety*, New York: Wiley.

Transportation Research Board (2006), *Report 86 Volume 11: Security Measures for Ferry Systems*. Accessed on 2016-02-12 at: http://www.nap.edu/catalog.php?record_id=13927).

UK Department for Transport (2012) *Bus and Coach Security Recommended Best Practice*, Second edition, July 2012.

La Rivista semestrale *Sicurezza, Terrorismo e Società* intende la *Sicurezza* come una condizione che risulta dallo stabilizzarsi e dal mantenersi di misure proattive capaci di promuovere il benessere e la qualità della vita dei cittadini e la vitalità democratica delle istituzioni; affronta il fenomeno del *Terrorismo* come un processo complesso, di lungo periodo, che affonda le sue radici nelle dimensioni culturale, religiosa, politica ed economica che caratterizzano i sistemi sociali; propone alla *Società* – quella degli studiosi e degli operatori e quella ampia di cittadini e istituzioni – strumenti di comprensione, analisi e scenari di tali fenomeni e indirizzi di gestione delle crisi.

Sicurezza, Terrorismo e Società si avvale dei contributi di studiosi, policy maker, analisti, operatori della sicurezza e dei media interessati all'ambito della sicurezza, del terrorismo e del crisis management. Essa si rivolge a tutti coloro che operano in tali settori, volendo rappresentare un momento di confronto partecipativo e aperto al dibattito.

La rivista ospita contributi in più lingue, preferendo l'italiano e l'inglese, per ciascuno dei quali è pubblicato un Executive Summary in entrambe le lingue. La redazione sollecita particolarmente contributi interdisciplinari, commenti, analisi e ricerche attenti alle principali tendenze provenienti dal mondo delle pratiche.

Sicurezza, Terrorismo e Società è un semestrale che pubblica 2 numeri all'anno. Oltre ai due numeri programmati possono essere previsti e pubblicati numeri speciali.

EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.72342235 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione) - librario.dsu@educatt.it (distribuzione)
redazione: redazione@itstime.it
web: www.sicurezzaterrorismosocieta.it
ISBN: 978-88-9335-048-8

Euro 20,00