Globalization, the State and the Individual, No 2(14)/2017, s. 249–256

Mileva Galina Velikova

PhD, assoc. Professor, Varna Free University "Chernorizets Hrabar", Faculty of Law, Department "Security and Safety", Varna, Bulgaria

Risk mapping system of threats to human security and critical infrastructure during mass events and its application in big municipalities

Summary

The article offers a system for monitoring and early warning of threats to human security and critical infrastructure in big municipalities during mass events. The main outcome of the EU project SMART CIBER, where Varna Municipality is in partnership, is to create a model of a digital map revealing the level of "Risk" and its location through the intersection of several pre-defined risk-indicators.

Keywords: terrorism threat, critical infrastructure, mass event, risk assessment, digital map, clusters of information, indexes and indicators

As noted in the Handbook for police and security authorities concerning cooperation at major events with an international dimension, III.2.3 Terrorist Threats, due to the fact that the European Union and some of its Member States are important players in international politics, the European Union and its Member States are likely to be targets of politically or religiously motivated international terrorists. [1, p. 10] In the document is presupposed that apart from international terrorists attacking the European Union or its Member States at major events there is a possibility of attacks by terrorist groups or organizations located within the European Union or its Member States. The aims of such terrorist attacks could be the event itself, VIPs, politicians of the European Union, national delegations of Member States or the public taking part in the event.

The presence of the international media is an important point from the perpetrators' perspective, since this offers a platform for the presentation of the group's or organisation's ideology. For the prevention of terrorist attacks information and intelligence about terrorist groups and organisations is essential and ought to be available at all times. Therefore, it is important for the organising Member State and its law enforcement agencies to share information and intelligence in general and as appropriate to the event. The law enforcement agencies should decide which terrorist groups and organisations – and individual persons – could be relevant, and check their own data base according to the event. In addition, all other Member States should independently contribute relevant information with respect to those persons, groups and organisations. The selection of suitable, necessary and appropriate security measures should be based on threat assessment and risk analysis.

In the annual report, Europol's Director notices that "… the threat [of al-Qaeda – inspired terrorism] has evolved and lone actors or small EU-based groups are becoming increasingly prominent, as is the Internet as a key facilitator for terrorism-related activities" [2, p. 7]. It is concluded that 2011 presented a highly diverse terrorism picture which would probably be mirrored in 2012, with a possible increase in lone and solo actor plots [2, p. 8]. "…the incidents in Norway in July 2011 prove that attacks performed by individually-operating actors are not a practice limited to al-Qaeda inspired terrorism" [2, p. 11].

Some key judgments in the paper are made. Firstly, numbers of terrorist incidents and arrests continue to fall, but overall activity relating to terrorism and violent extremism still represents a significant threat to EU Member States. Secondly, "…The different modi operandi used in the violent extremist incidents in Norway in July 2011 … has demonstrated the devastating effect of firearms. Since the Mumbai attacks of 2008, the potential impact of a successful firearms assault has been obvious and may be chosen by future attackers" [2, p. 34].

The picture of terrorism threat in Europe described above requires increased joint efforts of Member States to gather preliminary information to prevent and

protect people and critical infrastructure, especially in large municipalities in conducting mass events. Evaluating the security-related risks and risks of terrorism assaults and their assessment is an indispensable tool for reaching the goal successfully.

The project **SMART CIBER** (System of Maps Assessing Risk of Terrorism against Critical Infrastructures in Big Events Rallies) is directly financed by "The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks" (CIPS) programme under the European Commission General Department of Home Affairs. The programme is designed to protect citizens and critical infrastructures from terrorist attacks and other security incidents. It does this by fostering prevention and preparedness, particularly by improving the protection of critical infrastructures. At the same time, projects address consequence management – a key component for the smooth coordination of crisis management and security actions, in particular following terrorist attacks.

Over 140 million euro for the period 2007–2013 has allocated by the European Union for operational cooperation and coordination actions (strengthening networking, mutual confidence and understanding, developing contingency plans, exchanging and disseminating information, experiences and best practices). [3]

The project SMART CIBER is carried out by the Municipality of Milan along with Università Cattolica del Sacro Cuore, Municipality of Varna (Bulgaria), Municipality of Budapest (Hungary), Safety Region of Rotterdam (the Netherlands), Region Lombardia (Italy) and the United Nations Interregional Crime and Justice Research Institute (UNICRI). It aims at improving the assessment of the risk of terrorism against critical infrastructures at EU level (public transport, electricity, water, gas, etc) in metropolitan areas, with a special focus on big events. Starting from the experiences of four European countries (Italy, the Netherlands, Hungary and Bulgaria), the project wants to develop an "Integrated Risk-Map Against Terrorism Issue", informatics map revealing the level of "Risk" and its location through the intersection of several pre-defined risk-indicators.

The project objectives can be summarized as follows: 1) to create, promote and support the development of a model for the protection of critical infrastructure, with particular emphasis on to the methodologies for risk assessment; 2) to improve the information management about critical infrastructures; 3) to achieve the integration of all risk maps belonging to subjects involved in the prevention of terrorist attacks; 4) to establish specific indicators helpful to report on the map the risks of terrorist attacks against critical infrastructure providing a regular update of such a mapping; 5) to use a private network that includes the whole partnership, so that everyone has a standard diagnostic framework and constantly updated list of potential risks.

Specific tasks and actions arising from these objectives are: 1) Defining indicators. The aim is to identify empirical and objective indicators which can be shared

by all partners in order to measure terrorism risk; 2) Comparative analysis and experience sharing. This task requires drawing a comprehensive picture of system and methodologies in place in the EU regarding risk assessment in order to share best practices; 3) Model of integrated mapping of terrorism risks. This means to elaborate a mapping model based on terrorism risk indicators integrating critical areas for big events; 4) Organizational and technological aspects. This task is connected with defining the conditions to make the mapping model useable in all partner countries; 5) Tests in Milan, Rotterdam, Budapest, Varna. The task is focused on validating the model in each city; 6) Final elaboration of methodological tool. It is based on tests, to develop the operational guidelines for mapping risks and replicate the model in other contexts as well as use it as a tool for risk assessment at EU level; 7) Dissemination of the results. The aim is to familiarize stakeholders with risk assessment mapping system in view of its wide application and further development.[4]

Project SMART CIBER target groups in Bulgaria

The first project SMART CIBER target group is Varna Municipality, Directorate "Security Management and Public Order Control'**.** It has the following departments: 1) Defensive and Mobilization Preparation; 2) Civil Protection Operations; 3) Classified Information and Video Surveillance; 4) Public Order Protection with its subdepartments Public Order sector and Environmental Control sector; 5) Construction Control and Supervision and 6) Commercial Activity and Tourism Control with its subdepartments Commercial Activity Control sector and Tourism Control sector. Most of the rights and responsibilities of these municipal structures are focused towards strategic planning, coordination and information management, policy making and management of the risk maps, rather than law and security enforcement itself.

Nevertheless, there is a functioning structure – registered as a separate legal entity with a 100% ownership of the Municipality – which is entrusted particularly with the security, prevention and protection of certain public infrastructural facilities: the Municipal Security Company or as it is also known, the Municipal Police.

Facilities, guarded by the Municipal Security company ("Municipal Police") are: "Prostor" Sports complex, "Primorski" swimming complex, "Chaika" tennis court complex, "Vinitsa" equestrian facilities, "Lokomotiv" Sports complex, "Delfini" swimming pool, "Vladislavovo" Stadium, Municipal Sports Complex, "Asparuhovo" rowing facilities, "Mladost" and "Primorski park" sports complexes, "Youth Centre" Municipal facilities. In addition to all these sports infrastructures the Municipal police has the responsibility to ensure the security of the Port Warehouse facilities; the Open-Air Amphitheatre and both large city parks – Pri-

morski and Asparuhovo – are patrolled by their vehicles, as are all city pedestrian underpasses. Their furthermost responsibility is the Aladzha Monastery complex on the outskirts of the City.

As it is evident, most of these structures are largely recreational. For all other critical infrastructures (CI) the responsibility of providing for their security lies completely with the private or public operators and infrastructure owners. Should they be of public interest, they are also within the competence of various public order and law enforcement organizations – the second project SMART CIBER target group. With all of the below-listed organizations the Municipality and its "Security Management and Public Order Control" Directorate has daily working relationships and frequent collaborations:

1. Ministry of Interior:
   a. Represented locally by the Provincial Police Directorate of the MI and its five District Police Precincts, based on the City territory.
   b. The other separate enforcement subdivisions of the MI are:
      i. National Police Service – incl. Specialized Police Forces and National Gendarmerie Service – deployed specifically to secure important facilities and buildings, to respond to riots and counter militant threats – an intermediate form between Police and Army forces.
      ii. Border Police Service (with applicability in Varna as well)
   c. Fire Safety and Civil Protection Chief Directorate has taken over the functions of the recently closed national "Civil Protection" service, which aims to prevent and act in cases of natural disasters, accidents, terrorist threat and military preparations.
2. National Security State Agency has counterespionage duties. It also includes Organized Crime Service with special and ad hoc duties.
3. Ministry of Defense
4. Private security contractors, which obtain permits with the MI structures.

The main aim is all local and regional law enforcement organizations to be directly involved in implementing "the risk maps" by sharing information and contributing constantly to their continuous elaboration.

The third project SMART CIBER target group is the largest and it comprises of CI stakeholders – public or private. These can include infrastructure managing agencies, municipal, national or private event organizers, 'crisis scenario' teams, researchers, inter-institutional task forces, etc.

The transportation services in Varna are both public and private. The Municipality aims to implement a new and general reorganization of its integrated services; but about 40% of the city's public transportation means would remain private, although tied to the general administrative city planning, mapping and systematic approach. Energy supply services are all private. Water Supply and

Sanitation services are all public, with 51% belonging to the Ministry of Regional Development and 49% to the Municipality. Local roads, bridges etc. are owned by the Municipality. The Port is State-owned. Almost all other culturally and socially significant buildings are privately owned.

The perceived fragmentation of ownership and responsibility consequently transfers into various databases, monitoring systems, control and enforcement procedures. However, all critical infrastructure planning and permit issuing is done (or at least coordinated) at a centralized local and national level. Information Security departments are maintained at the different levels by the City and Regional administrations, as well as the Ministries of Internal Affairs and of Defense.

Project SMART CIBER beneficiaries in Bulgaria are: 1) The Ministry of Interior – maintaining and coordinating public security forces; observing laws and procedures adopted to prevent and combat instances of terrorism; adopting and implementing the law enforcement to create the adequate procedures to prevent and repress 'risk scenarios' about the terrorism threat; 2) Public security forces at all levels – Regional Police Directorate, Specialized Terrorism Combat Forces, National Services for Combat against Organized Crime, etc.; 3) The 'Capital of Culture 2019' initiative committee, to be transformed into an organizing body, with the model for prevention against terrorist risks; 4) Civil Society, all inhabitants and guests of the City of Varna, receiving actual and potential protection as European citizens – if and when under threat benefiting from the policies and forces in place to combat such risks.

As it was mentioned above, the main project outcome is to create a model of integrated mapping of terrorism risks on the basis of identification of empirical and objective indicators and critical analysis on the interconnections between them. The system of indices and indicators for the model can be reached through at least three different perspectives (approaches).

The first approach is based on structural data (demographic indicators), which have been adopted from the city map of Turin (Italy) and can be adapted, according to the requirements of the project SMART CIBER. It has already been tested as a system through specific software. [5]

As an optional approach for selecting data, it can be used the EVIL DONE model. [6, 7] The EVIL DONE model is based on the theories of situational criminology applied to terrorism and acts as a tool that, although still in the process of development, has already been tested by the police in various countries especially to assess the attractiveness and exposure to risk of potential targets of terrorism. For the SMART CIBER project this is very interesting because, firstly, the model is set in the perspective of "Big Events" and "Critical Infrastructure", which are by definition "attractive" targets; and secondly, it can provide operational guidance with respect to the evolution of risk scenarios, indicating the criticality of specific

areas of the city. EVIL DONE is an acronym in which each letter represents a characteristic of the object analyzed (area, place, CI, etc.).

In the final part of the article would be present a detailed model of a digital map which can be tailored by project partners according to their legal, cultural and social framework in order to make it operational within their specific contexts and to identify who can provide relevant information (e.g. structural data), as well as to develop future cooperation with the Critical Infrastructures, classified as highly potential targets of terrorism according to the EU Council Decision n° 2007/124/EC about a Program of Prevention, Preparedness and Consequence Management of Terrorism and Security related Risks [8] and the specific Action Plan on Critical Information Infrastructures Protection (CIIP) – COM (2009) 149. [9]

In order to construct an integrated digital risk map from methodological point of view there have to be defined clusters of information, indexes and indicators. Clusters of information are the perspectives of the observation ("what we look at"). The index is a theoretical category that serves to guide the observation ("the focus of the observation"). Indicators are empirical facts/data that serve to measure the extent of a phenomenon ("what we collect"). Namely, a phenomenon is looked at through a specific focus of observation (clusters + indexes) in order to collect relevant and measurable empirical data (indicators).

In the course of the project at least 3 clusters are selected: 2 concern the risk map while the last deals with further developments on the basis of some limits.

1. Cluster 0: set of data focused on specific structural data (geo-location).
2. Cluster 0.0: set of "sensitive targets" belonging to the Critical Infrastructures (CI) & the Big City (BC) contexts (geo-location).
3. Cluster 0.1: indicators of social uneasiness drawing on the cluster 0 (geo-location).
4. Cluster 1: critical infrastructures, namely relevant indicators focused on critical infrastructures related to early warnings (EWs) and red flags (RFs) (geo-location).
5. Cluster 2: big cities, namely relevant indicators within the urban context related to early warnings (EWs) and red flags (RFs) (geo-location).
6. Cluster 3: resilience opportunities (further developments).

Indexes are used in order to measure risk alerts. Early Warnings (EWs) are weak signs that should raise risk alerts, especially if matched with other data. On the map EWs have to be represented with a light red color (static). Red Flags (RF) measure medium or high risk. On the map, RFs have to be represented with a dark red color (dynamic). EWs turn into RFs on the basis of: 1) Repetitions (% of a single indicator; % interaction among indicators that is data matching); 2) Spatial proximity (two or more than two indicators in the same area).

The limits of this approach can be summarized as follows: 1) The observers are mainly the local police, therefore there is a lack of other crucial data collected

by, for instance, the state police; 2) Selective attention with the consequent risk of ignoring important EWs; 3) The training which needs to be homogenous and focused on "what to look at"; 4) Technological differences among the partners; 5) Technological determinism: risk of relying exclusively on technology without taking into account a more socio-technical approach to security devices; 6) This model is not sufficiently predictive and literature has highlighted the impossibility of predicting through indicators only.

Some recommendations have to be implemented in order the outcome of the project – the digital risk map to become a useful tool for local risks of terrorism and other related risks to be predicted.

- At utmost importance is to develop training activities (theory & practice) specifically addressed to local police agents & critical infrastructures employees;
- It is crucial to develop a network of info-sharing among the involved institutions and stakeholders (CI and Municipality of Milan) through an "official agreement";
- It is also crucial to define the responsibility-sharing (who is responsible for what) through an "official agreement";

The institutions and stakeholders involved in should define a specific protocol about "mass-media communication and approach" in case of emergency events (safety/security: ex. terrorist attack).

References:

Council Recommendation of 6 December 2007 concerning a Handbook for police and security authorities concerning cooperation at major events with an international dimension, Journal of the European Union, (2007/C 314/02), p. 10.

TE-SAT 2012: European Union Terrorism Situation and Trend Report, Europol, https://www.europol.europa.eu/sites/default/files/publications/europoltsat.pdf.

http://ec.europa.eu/dgs/home-affairs/financing/fundings/security-and-safeguarding-liberties/terrorism-and-other-risks/index_en.htm.

http://smartciber.eu/index.php/en/.

Lombardi, M., A. Ceresa, C. Fonio, System of indices and indicators for the model, SMART CIBER project, 2013, p. 2–5.

Clarke, R. V., G. R. Newman, Outsmarting the Terrorists, 2006.

Özer M., H. Akbaş, The Application of Situational Crime Prevention to Terrorism, Turkish Journal of Police Studies Vol: 13 (2), p. 179–194.

European Official Journal, L58 of 24.02.2007.

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDFz.