Transilvania University of Brasov,
Romania

13th INTERNATIONAL CONFERENCE
"STANDARDIZATION, PROTYPES AND QUALITY:
A MEANS OF BALKAN COUNTRIES' COLLABORATION"

Brasov, Romania, November 3 - 4, 2016

European Security Standardisation: An Overview of EC 487 Mandate

Dr. POUSTOURLI Aikaterini
Technological Educational Institute of Central Macedonia, Serres – Greece, pkate@teiser.gr

Abstract
Due to the luck of European security standards and mainly under the global need for common efforts in order to strengthen the European societies from natural and manmade risks, threats and disasters, EU issued several Mandates like M/487. The specific Mandate concerns the analysis of the current security standards landscape in Europe taking account of the legislative background and having an exclusively civil application focus. Is completed in two phases until nowadays. The first phase achieved the Analysis of the Current Security Landscape (2012) and the second one phase completed the documentation of the proposed standardization work programmes and road maps execution (2013). The execution of the Mandate was undertaken in close cooperation with the widest possible range of interested groups and particularly the Joint Research Centre of the European Commission (JRC), the European Standardisation Organisations (ESOs), the European Network of Law Enforcement Technology Services (ENLETS), European Network of Forensic Science Institutes (ENFSI), Security industry organisations like European Organisation for Security (EOS), European Research Institutes and Agencies as well as those of National Agencies and European Technology Platforms with a relevant interest in this domain. International cooperation was ensured, in particular with IEC, ISO and ITU. In the begging of 2016 and after the events of November in Paris and of Match in Brussels is highly topical a review of their results and the possible transition to the next third phase.

Keywords
standardisation, security, mandates, European Commission, CBRNE

1. Introduction

The Commission programming mandate addressed to CEN, CENELEC and ETSI to establish security standards (Mandate M/487 of 17 February 2011) concerns the development of a work programme for the definition of European Standards and other standardization deliverables in the area of security. The Mandate has an exclusively civil application and focuses on assisting the EU to ensure that security is better and consistently addressed in different security landscapes. The main objective of the Mandate is to increase the harmonisation of the European security market and reduce fragmentation with the establishment of a set of comprehensive European standards.

The Mandate highlights the importance of involving different stakeholders and operators, particularly end-users of security systems and SMEs. It emphasizes the need to take into account security measures in line with the security levels determined by public authorities and their underlying risk assessments, identifying security needs and secure interoperability schemes between the various nodes and centres for civil security in Europe dealing with law enforcement and crisis management. Similar needs from private perspectives should also be included. As to the specific role of the standardisation activities related to security, the Mandate refers to the following sources:

- the ESRIF Report and its highlighted importance of an integrated approach to security;
- the Commission's Communication on reaction to ESRIF pointing out the need for a prompt investing in an ambitious industrial policy for the security sector;
- the ECORYS Study on Competitiveness of the EU Security Industry recommending the development of new European and common international standards for security as a mean to reduce the security market fragmentation, which is leading to a lack of competitiveness of the Security European Industry;
- the Commission's Communication Towards an increased contribution from standardisation to innovation in Europe underlining the contribution that standards could and should make to

innovation (policy) and the Stockholm Programme inviting the Council and Commission to develop internal security strategy tailored to the real needs of users and focused on improving interoperability.

The Mandate strongly emphasizes the need to take into account the human factor issues, privacy concerns and identification of operator requirements for enhancing systems effectiveness. These should duly be taken into account, not forgetting transversal areas either.

European Standardisation bodies are directly invited to ensure that the deliverables developed meet European legislative and other requirements, in particular as regards privacy and Intellectual Property Rights (IPR). Until now, two official issues of the Mandate 487 were realised: the phase 1 of "Analysis of the current security landscape" and the phase 2 of "Proposed standardization work programmes and road maps". In the following chapters we will summarise the main scope and the main results of them.

2. Mandate 487

2.1. Mandate 487 phase 1, Analysis of the current security landscape (2012)

The final report of Mandate 487 phase 1 entitled "Analysis of the Current Security Landscape" issued in May 2011 by European Commission in order to establish Security Standards. This mandate requested a study to analyse the current standardisation 'landscape' in the field of security standards and subsequently, the development of a proposed work programme. The mandate is horizontal, potentially covering all subjects related to civil security. The mandate has been accepted by the European Standards Organisations (ESOs), being CEN, CENELEC and ETSI. The work has been allocated to CEN/TC 391 'Societal and Citizen Security' whose secretariat is provided by the Netherlands Standardisation Institute (NEN). The mandate consists of two phases:

- *Phase 1* — to provide the result of a preparatory study and a list of sectors for priority treatment;
- *Phase 2* — based on EC reaction to the output of Phase 1, to provide proposed standardisation work programmes and roadmaps related to the selected sectors.

Phase 1 focuses on obtaining an overview of the current security landscape and listing the sectors for priority treatment to be agreed upon by the Commission services. This phase includes an informal check by the European Commission, after which the draft report has been made available to the stakeholders to comment before the submission of the final report to the European Commission. The report gives the opinion of all involved stakeholders and therefore there can be different points of view.

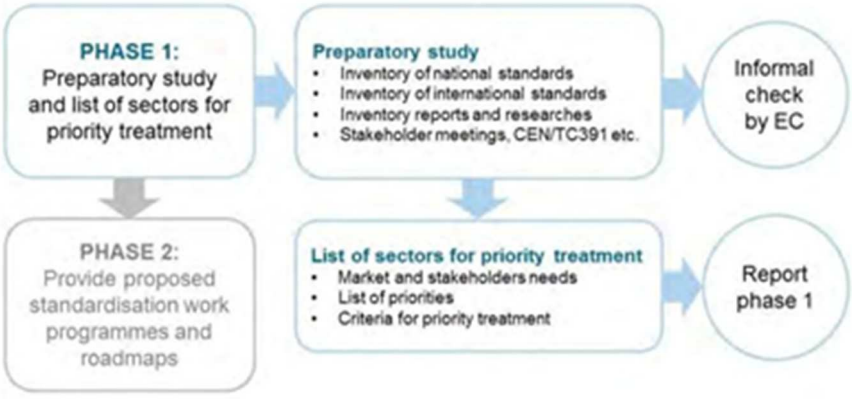

Fig. 1. ESOs Action Plan for phase 1

As the area of security is very broad, boundaries needed to be defined first to establish a framework. Within the area of security, many safety aspects are involved. As there is no clear-cut edge between security and safety, it must be noted that the focus of this work is in the area of security and only includes those aspects of safety that are necessary in relation to security.

In coordinating and handling the response to the mandate, several groups have been set up. An informal coordination group (consisting of representatives of CEN, CENELEC, ETSI, EC and the chairman and secretary of CEN/TC 391) has been established to provide additional support, information and guidance to CEN/TC 391. Furthermore, CEN/TC 391 has established a dedicated Mandate Working

Group, the ad hoc Joint Working Group 'M/487', to support the Phase 1 report. The joint working group is also open for members from CENELEC and ETSI.

Fig. 2. List of security areas defined in the mandate

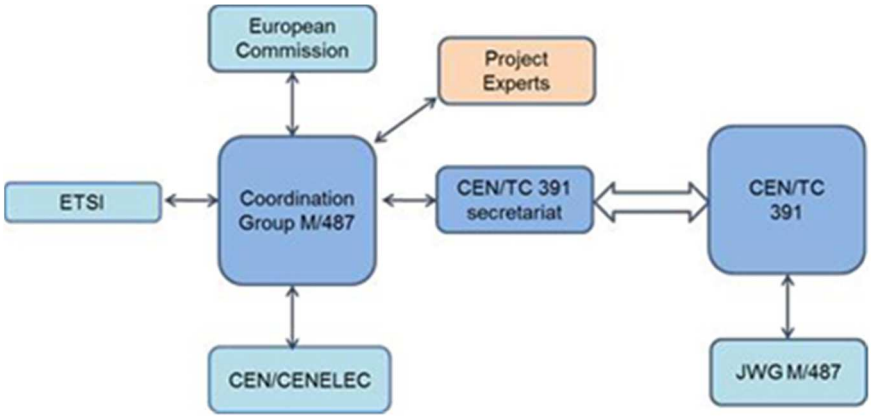

Fig. 3. List of security areas defined in the mandate

National standards

An inventory of the national standards in Europe has been made by means of a survey, which has been sent out to all the members of CEN/TC 391. In total, 12 out of the 18 member countries have responded to the survey. Six countries have submitted their national standards, i.e. Austria, Czech Republic, Germany, Great Britain, the Netherlands and Spain. In total, 203 national standards were found.

International standards

In order to find the existing official European and worldwide standards, a database search has been carried out in two places:

- *Database of the Netherlands Standardisation Institute* — this database contains the standards of the official international standardisation organizations (CEN, ISO, CLC, IEC, ETSI and ITU-T).

  The keywords used for this search were: accident(s), disaster, crime, nuclear accident, disaster, epidem*, pandem*, public safety, border security, fraud, forensic, terroris*, crisis, crises, border control, security biometrics and security guide.

  Combinations of keywords were used for the followings: alarm + terroris*, explosive* + terroris*, explosive* + fire hazard, explosive* + protect*, explosive* + construction, eurocode* + security.
- *'Security Standards Database'* — this database is provided on the website of ITU-T has been used to filter additionally the security standards developed by ETSI and ITU-T as the above mentioned keywords might not be sufficient for a search through these standards.

One of the challenges of this search is to determine which keywords are most relevant and will result in the required outcomes.

Table 1. Overview of submitted national standards on security

Country (no. of standards)	Security area			
	Security of the citizens	**Security of infrastructures and utilities**	**Border security**	**Restoring security and safety in case of crisis**
Austria (16)	4	1	0	11
Czech Republic (1)	1	1	0	0
Germany (57)	30	11	0	17
~~Great Britain (64)~~	~~6~~	~~57~~	~~0~~	~~1~~
Netherlands (47)	41	1	0	5
Spain (18)	n/a	n/a	n/a	n/a
Total (203)	***82***	***71***	***0***	***34***

The sources all indicate that the EU security industry is fragmented, and stress a need for standardisation to improve the European competitiveness of this industry in the world market. There is a lack of standards in many security areas, and a high need for common and European security standards. This is confirmed as security standardisation is mentioned for all the security areas identified within the mandate, making all of these areas relevant for the mandate work. The sources encourage a common understanding of security, research and innovation and to include standardisation in all phases, to support a more harmonised approach.

When looking at concrete standards proposals, many suggestions in each of the areas are given. Striking is still the number of times that standard proposals for personal data protection and border surveillance are mentioned. In general the sources stress the need for interoperability standards in Europe. The sources also stress the need to take the external dimension into account. Next to European standards, the development and promotion of global standards are also emphasised. The global dimension also applies to the development and promotion of European standards to become recognised as global standards. Security standardisation needs to be approached in a more structured way, and the reports argue for a solid security standardisation (and validation and certification) effort at European level. Many suggestions are given how to coordinate security standardisation efforts, and to involve the ESOs in doing so. 'Investing into security research for the benefits of European citizens' have been analysed, and one out of four security research projects cover standardisation in one way or the other. The survey amongst project coordinators shows that most of the project coordinators recognize the importance of standardisation, but they discover that little or no standards are available in the different fields. Reason for that is possibly that there is not that much knowledge of standardisation in the different sectors and therefore the benefits of standardisation have still to be discovered. The project leaders that have thought about standardisation before, all state that standards should be developed in the future.

Main conclusions for phase 1

By analysing the national and international standards and technical committees, the research and reports on security (standardisation), and various meetings and other interactions with stakeholders, this report aims to provide an analysis of the current security landscape. Due to time restraints, it was agreed upon which of the available sources would be assessed. The analysis of the national and international standards shows a variety in published standards and draft standards. In general, standardisation activities have been found in all security areas defined in the mandate. However, no references to national standards in the area of border security were submitted. Furthermore, several 'new' security areas were added during the inventory of international standards. The diversity of the security sector enhanced the challenge to compile a complete list of standards, however time was limited. After using many resources, a large majority is considered to be covered by this report. It should be noted that many national standards are implementations of international standards. Many TCs are involved in this. Particular attention should be given to the new standardization projects in CEN/TC 391 "Societal and citizen security" and ISO/TC 223 "Societal security".

The selected sources and reports on security all indicate that the EU security industry is fragmented, and stress the need for standardisation to improve the European competitiveness of this industry in the global market. There is a lack of standards in many security areas, and an increasing need for European and global security standards. In general, the sources stress the need for interoperability standards in Europe. Furthermore, the sources indicate the need for a structured security standardisation approach, and argue for a solid security standardisation effort at European level. The sources also stress the need to consider the external dimension; apart from European standards, the development and promotion of global standards is emphasised. The global dimension applies to the development and promotion of European standards to become recognised as global standards. This is especially the case for standards addressing interoperability issues. Here the Vienna agreement (an agreement between CEN and ISO on the adoption of each other's standards) can be useful. With regard to security research, the assessed FP7 projects revealed one out of four security research projects relates to standardisation. Project coordinators, once introduced to standardisation, obviously recognise the importance of standardisation and express the need to develop standards.

The stakeholder meetings showed a lot of support for the mandate and the effort to create a roadmap for security standardisation. It also showed the need for coordination of the different activities. The first meeting provided indications from both the industry and the policy side. The second stakeholder meeting resulted in more concrete priority suggestions. Additionally, the working group CEN/TC 391/JWG M487 has provided various inputs on how to approach the mandate work, submitting standards as well as priority suggestions. A general stakeholder analysis has been carried out. The analysis showed that the amount of stakeholders is huge and diverse. This is not surprising as many of the earlier mentioned studies indicated the security sector being large and fragmented. Therefore, when the priority areas are selected in phase 2, a more in-depth stakeholder analysis needs to be carried out. The central focus of standardization efforts is on interoperability, competitiveness, and market defragmentation, while addressing stakeholders' needs. There is a need for a coordinated initiative on European level to stimulate the EU security industry, and the mandate M/487 came at the right time. However, the sooner several standardisation activities are initiated, the better. Various technical committees concerned should be involved. As coordinating technical committee in Europe, CEN/TC 391 'Societal and citizen security', in cooperation with the ESOs, can assist in coordinating and delegating these activities to the appropriate TC.

Priority recommendations

The EU security industry shows that it is highly fragmented. For all security areas there is a need for stimulation and coordination of the standardisation activities. Due to the fragmented character, there is little structure in the large variety of needs and priorities. However, a start can be made using the following list of priority recommendations is compiled, based on this inventory (in random order):

Border security — border security has been mentioned in many of the research reports to be an area for priority treatment, but no standards have been developed until so far, no national or international initiatives. Therefore, this area should be strongly considered to give priority treatment.

Aviation security — standards for conformity testing methodologies (CTMs) of aviation security detection equipment is suggested as a priority. Since performance requirements standards are already in place, this is already foreseen in EU policy, and no harmonised standards are available in the EU. In addition, a fragmented market due to the lack of standards, leads to a high threshold for SMEs to enter the market, to increased costs for manufacturers, to increased time-to-market for providers, to uncertainties for procurers, etc.

CBRNE — few standardisation activities are in the area of CBRNE, while the importance of CBRNE standardisation is also stressed in the 'EU CBRN Action Plan' and the 'Communication on security of explosives', thus the 'E' (explosives) is added to CBRN. Security standardisation in the area of CBRNE is mentioned in the various reports as well as during the stakeholder meeting. Focus in the area of CBRNE is an integral threat assessment and standards for sharing capabilities. In addition, "sampling and detection" and "personal protective equipment (PPE) for first responders" also provide for standardisation opportunities. The latter example is then again overlapping with the priority area 'crisis management' (see next).

Crisis management and civil protection — most importantly in the area of 'Restoring security and safety in case of crisis' is the need to improve the coordination and communication. Reports mention several aspects, such as strengthening response forces, stimulating interoperable command and controlling cooperation and develop standards in the field of education, training and exercises. Other subjects such as mass alert and evacuation should also be considered when exploring this security area.

Personal data protection — throughout many reports and researches the need for standardization for personal data protection is stressed. Yet various issues are related to the different topics, such as 'ethical aspects'; in the absence of a clear EU framework in this area there is a lack of clear guidelines for equipment/technology providers with respect to accepted and acceptable performance requirements.

General coordination of European security standardisation — not mentioned as a specific area of security standardisation, all reports call for combined efforts and coordination of security standardisation. Therefore, this is separately mentioned as an area for priority treatment. Many suggestions have been made on how to coordinate this. These should be looked into when searching for a suitable way of coordination. In addition, special attention should be paid on pan-European acceptance of security standardisation. As mentioned before, the stakeholders recommend the following criteria to the European Commission in selecting areas for priority treatment:

- To protect people and facilities
- To promote EU security industry
- To facilitate the harmonized implementation of EU security policies
- Policy needs

The choice of priorities will be indicated by the industry itself, especially if they feel strongly about it. However, the choice of priorities for work financed by the European Commission is always a political one as well. Therefore a combination of these two is recommended by means of public-private cooperation: industry is needed to elaborate reasonable standards where conspicuous industry experience is needed for, and to indicate the major stumbling blocks to European competitiveness. At the same time, security solutions and services are not developed or deployed in a political vacuum, and efforts to support Europe's security should be informed by the security objectives set by the EU and the Member States in the ESS, ISS and national security strategies. Finally, the advantage of standards only emerges when they are actually applied in practice. Especially for new standards some kind of incentive may be beneficial to stimulate actual use and implementation. This could be achieved for example by including standards as a basis for pre-operational validation (POV). For the POV instrument pilots have been and/or will be carried out under the 7th Framework Programme. It is expected that POV will get more attention under the new Horizon 2020 programme for the period 2014 – 2020. Also, from a financial point of view, this has advantages due to availability of budget within the Horizon 2020 programme for POV projects.

2.1. Mandate 487 phase 2, Proposed standardization work programmes and road maps (2013)

Standardization is quite a new phenomenon in security industry in Europe, although it can be of great benefit for all stakeholders involved. For other industries that widely apply standardization, research has shown that every EURO invested in standardization yields about 10 to 100 EURO (Berger Institute). Standardization and the benefit of it have been recognized by the European Commission since many years (see e.g. Regulation 2252/2004 and 810/2009 of the European Union). Therefore, it seems only logical that being willing to give a push to the European security industry means investing in standardization. Consequent to Mandate M/487 phase 1, the phase 2 was a first step in a process that should lead to a standardization landscape in the field of security that will be of benefit for the industries involved and contribute to the security of EU citizens and residents. Several common threats emerge from the report and these can be summarized as follows:

- Confidentiality – special attention is required in to standardization on security.
- Integrity on behalf of all stakeholders.
- Risk based work – ISO 31000 is a widely accepted standard in the sector.
- Terms and definitions – clear definitions are needed.
- Standardization and innovation – innovation can benefit a lot from early standardization.

- Timeline- proposals need to be prioritized and the roadmaps are only the start of a development.
- EU-policy – standardization in the security sector is an excellent tool to support EU policy.
- Reactions of stakeholders – stakeholders were generally positive about the mandate and participated actively.
- The need to meet the EU objectives and criteria through consideration by experts.

Confidentiality

One of the problems that stakeholders address when it comes to standardization in the field of security is confidentiality. As standardization is an open and transparent, consensus driven process, it is sometimes difficult to appreciate how it could contribute to making society more secure since classified information should not be openly accessible since it could assist criminals and terrorists. European standards (EN) and other deliverables can **not** be confidential. However, for military or business reasons an open standard can be combined with a confidential annex solely for the purpose of work by military organizations or special businesses.

Openness/ loyalty to the principles of standardization

There is one important thing that should be mentioned in the whole process of standardization, but maybe also in a wider context – that is integrity. Without integrity, security standardization or standardization in general is not possible. Of course, all stakeholders have their own agenda, but standardization as a consensus-driven process that makes cooperation possible. It is also clear that stakeholders gain more from participation than they would have achieved if they had tried to solve a problem on their own.

Risk based approach

A risk-based approach has been the starting point for the proposals in this report. This because experience has shown that whatever model is used, the determination of risk is always part of the analysis. ISO 31000 'Risk management' has proven its value since its publication in 2009 and there is a trend that all management standards in the sector are based on this standard.

Terms and definitions

There are several definitions of the words security and safety. It is a challenge to make a good distinction between safety and security. In some of the EU languages, safety and security are the same or almost the same. In addition, related definitions such as crisis management, emergency management and resilience have different definitions in different countries. It is not surprising than that all the experts that participated to this report have mentioned one specific need: to develop a common language within the selected sectors. In this report, no definition of safety or security is given. However, here safety is used as the umbrella for the technical aspects including technical failure. Security is 'the rest' including intentional and unintentional aspects. It will have to be part of the follow-up to develop the common language. There have been some efforts to harmonize all terms and definitions for security like the terms and definition standard in ISO (ISO 22300), in biometrics (ISO 24779 and ISO/IEC 2382-37:2012) and the CBRN glossary in Europe. However, even within ISO there are contradicting definitions.

Standardization and innovation

During recent years standardization has proven its value not only for products and systems that have been in place and use for several years, but also for innovative new products and systems. Those can benefit much from including standardization in the process of development as market introduction becomes much easier if one can prove that a product meets certain requirements when it enters the market. The European Commission has adopted this for many years, and many projects that are carried out within the research agenda Framework 7 (FP7) include standardization form the beginning. All stakeholders recognized the importance to the work in line with the future Horizon 2020 research program. Not only the development of standards and methodologies in the field of the security industry is important, training of the end users, those who will bring those standards and methodologies in practice, is also an important issue. To ensure that all the end-users are educated in the same way, it is to be considered to develop training standards on the various subjects.

Timeline

For each workshop, proposals were invited, discussed and prioritized (see 2.2). For the roadmaps, proposals have been chosen as priority that have the most impact in terms of benefit for industry and better security and can be developed on short term.

EU-policy (implementation)

It is evident that in the security sector not only industry and the public are major stakeholders, but also policy makers. In the New Approach standardization is an important tool for policy makers as they set the (performance) requirements, and standards describe how these can be measured or proven. It is therefore evident that the roadmaps have been developed in cooperation with staff of several Directorates of the European Commission, as these roadmaps should support European policies and programs such as Horizon 2020.

Reactions of stakeholders

This report has been widely spread for review amongst stakeholders. More than 350 comments on the draft version of the report were received. The outcomes of the workshops are the opinion of those who participated and therefore are presented in the report. CEN/TC 391 offered the possibility to all stakeholders to forward their ideas and comments to improve the report. This would make it easier for the European Commission to judge what proposals have the most support and respectively, impact.
The workshops were evaluated and the participants were positive about the way the workshops and the process were organized.

Meeting the EU objectives and criteria by expert judgement

All participants at the workshops were invited to give their opinion on why the proposals were going to meet the EU objectives and criteria. The results were judged by the three experts and discussed with a number of stakeholders in interviews and the results of this expert judgement is given in a table for each of the three priorities of the Mandate M/487.

Main conclusions for phase 2

What is needed is *better instead of more information sharing*. The challenge is not so much that information is not shared within the EU or with third countries, or that focus is needed on ways to enable 'more' data sharing in the EU. Instead, priority should be given to assessing the reasons *why* that 'information' was not used by the relevant national authorities, to ensuring better targeted and more accountable information exchange, and to boosting EU operational cooperation and joint (cross-border) investigations. The politics of 'more data' as the solution were re-confirmed by the Joint Statement issued by the member state ministries of justice and home affairs following the Brussels attacks. Among other initiatives, the Joint Statement calls for improvements in the collecting, checking and connecting of information in the field of counterterrorism. It reiterates the need to adopt the EU Passenger Name Record (PNR) Directive "as a matter of urgency", and to find ways to secure and obtain more quickly and effectively "digital evidence". However, more data is not a panacea. Studies have shown that the intelligence shared by national law enforcement authorities is often not used because it may lack proper procedural guarantees to ensure that it is not the fruit of a poisonous tree, i.e. sourced from unlawful investigations, searches and seizures. Nor does intelligence meet the requirements for it to be considered 'evidence' before a court of law in criminal proceedings. Moreover, more information does not always make the work of law enforcement authorities easier or more effective. Large volumes of data cannot identify potential terrorist plots, yet greatly increase the possibility of false positives and negatives.

The actual dilemma is therefore in finding and devising more effective ways to ensure a *better* and *more targeted* information exchange that meets the EU's rule of law standards, which chiefly include respect of the fundamental rights of the defence and fair trial. If nothing else, the Brussels attacks have illustrated the difficulties of guaranteeing that the large volumes of predictive information and 'intelligence' gathered and shared among state authorities are useful for law enforcement practitioners on the ground. Can this information be trusted as evidence and therefore be used to incriminate a particular suspect before an independent judge? Is that 'information' compatible with the EU rule of law standards applicable in criminal justice proceedings?

The EU could play a more active role in facilitating *better* information sharing. This should be preceded by a higher degree of supranational accountability and rule-of-law evaluation tools concerning what is already there, what works and what does not. A key obstacle to ensuring 'more EU added value' in the field of counterterrorism policies has been the limits of EU legal competence in questions related to 'national security' and the activities of intelligence services. Member state representatives have often used the national security doctrine as a way to prevent 'more EU' in counterterrorism. Examples of this could be seen in the aftermath of the 2013 Snowden revelations of large-scale surveillance and member states' cooperation with the US National Security Agency programme, and their complicity in the US-led CIA extraordinary renditions programme. In both cases, the national security doctrine has prevented proper supranational scrutiny of EU member states' actions and a meaningful discussion of whether existing Union policies are fit for purpose. It is true that the EU Treaties tell us that "national security remains the sole responsibility of each member state" (Art. 4.2, Treaty on the European Union). This provision has been interpreted as referring to the activities of intelligence services. Despite its increasingly popular use by national governments, the actual meaning of 'national security' is far from evident and consensual. Research has demonstrated that this notion varies greatly from one state to another. The concept has blocked effective accountability by courts and parliaments of what national governments and their intelligence services have done in countering terrorism domestically and in cooperation with third countries.

That notwithstanding, 'national security' has not prevented the EU from developing, for more than the last two decades, a whole series of large-scale databases. Among them are the Schengen Information System II (SIS II), a centralised EU database used in particular to refuse entry to or subject individuals to specific checks at the EU's external borders. Another one, arising from the Prüm Decision, is a decentralised system for the exchange of information for preventing and investigating criminal offences. These systems have been accompanied by the set-up of EU home affairs agencies (such as Europol, the EU's law enforcement agency and Eurojust, the EU's Judicial Cooperation Unit) with ever-expanding competences over counterterrorism-related policies. Very little is known about the effectiveness, proportionality or added value of this EU counterterrorism architecture, its tools or actors. There are some general results found during the project Mandate 487 phase 2:

1. Standardization, both the deliverables and the process, are not well known in the security sector. This is something that should be changed as all stakeholders that were involved in this project underline the importance of standardization and the potential benefit the security market in Europe and worldwide can have using standardization.
2 Interoperability and communication were two very important items in all interviews and workshops. Therefore this should also be one of the priority things looked at via standardization.

3. EU Projects under the principles of the Mandate 487

Many projects are run under the principles of Mandate 487 (FP7 or H2020 funding) and especially under the areas of Security of the Citizens, Security of Infrastructures and Utilities, Border Security, Restoring Security and safety in case of crisis, Security systems integration, Interconnectivity and interoperability, Security and Society, Security Research coordination and structuring. In accordance to the EU Research for a Secure Society catalogue (2014), more than 250 projects are contributed to the topic. Respectively, under the Horizon 2020 Work Programme 2016 -2017 for the "14. Secure societies –Protecting freedom and security of Europe" many actions are funded, among which the ERNCIP Project European Reference Network for Critical Infrastructures). The specific action is supporting the implementation of the Security Industrial Policy and Action Plan through the European Reference Network for Critical Infrastructure Protection (ERNCIP). With the publication of the Security Industrial Policy and Action Plan - COM(2012) 417, the European Commission has underlined the need and its ambition to foster the global competitiveness of the EU security industry, e.g. by promoting EU-wide standards of security technologies, tests and evaluations of security equipment, and respective certifications. ERNCIP, set up in the context of the European Programme for Critical Infrastructure Protection (EPCIP), is a direct response to the lack of harmonised EU-wide testing or certification for products and services (in the area of critical infrastructure protection), which is a barrier to future

development and market acceptance of security solutions. This action should focus on linking the relevant work of ERNCIP with the implementation of the Security Industrial Policy and Action Plan, by supporting the uptake and promotion of identified activities. Relevant legislation on European and Member State level need to be taken into account appropriately, including potential ethical, societal and privacy issues of the proposed activities. Special thematic areas with correlated thematic groups like Chemical & Biological Risks in the Water Sector, Detection of Explosives & Weapons at Secure Locations, Detection of Indoor Airborne Chemical-Biological Agents, Radiological and Nuclear Threats, Resistance of Structures to Explosion Effects, are contribute to the production of harmonized protocols and common methodologies in the CIP standardization topics.

4. Summarising advantages and future challenges

The Paris and Brussels terrorist attacks of November 2015 and March 2016 respectively provoked widespread political condemnation and public outrage. The events have brought to the fore past discussions regarding the limits of member states' counterterrorism policies and the extent to which the EU could play a role in shaping more effective responses to these acts of violence.

A closing collaboration gaps needed. The quest for better information sharing should concentrate on ways to improve the use and added value of existing EU databases in relation to controlling the acquisition and possession of firearms and explosives, and the national implementation of existing EU rules in these domains. Criminal justice and police investigations need evidence that is useable, i.e. 'admissible', before an independent judge. By contrast, information qualifying as 'intelligence' encompasses all information, regardless of the quality or reliability of the sources. Intelligence faces significant obstacles for it to be admissible before a court, as there are no proper way to ensure that it is not tainted, as in the above-mentioned case of the US-led extraordinary rendition and unlawful detention programme. All the stakeholders (Manufacturers/Suppliers in CBRNE detection, European Organisation for Security (EOS), Standards Development Organisations (SDO)-CBRNE, Government/Regulatory Agencies, R&D/Testing Laboratories, Military (EDA, NATO), Procurers/Users, Public Safety Organizations(PSO), First responders (FR), should strongly involve to this.

According to Sherif (2001) they 'proceed in lock-step with implementations that test the specifications before adopting them. This incidental benefit can be an important factor in spurring innovation'. Using the approach of participatory standardization more frequently, particularly in security fields in which this approach is optional, is regarded as beneficial (Wurster, 2013). As the "Development of minimum standards for Law Enforcement/First Responders CBRN preparedness and response and their promotion in all EU Member States" is one of the strongest requests from the CBRNE stakeholders, regarding the next steps in the New EU CBRN-E Agenda , please take a look in the attached file of the "Discussion Paper on further steps in the implementation of the CBRN-E Agenda" (DG HOME AFFAIRS, Directorate D: Internal security, Unit D.1: Counter Terrorism and Crisis Management). The mains actions for the New EU CBRN-E Agenda could include:

1. Better exchange of information
2. Increased operational cooperation
3. Stronger cooperation with 3rd countries and international organizations and Initiatives
4. Supporting action: training and exercises, funding, research and innovation.

As highlighted in the document, the above list is not exhaustive. Issues such as insider threat, security of CBRN materials or tracking hazardous substances remain relevant and should be looked at. Moreover, as mentioned, there is a need for close civil-military cooperation. The potential in this area is significant: starting with research and standardisation through sharing of information to detection and logistical support in case of a CBRN incident. Common areas of interest, where cooperation is possible should be identified by both sides.

The development of EU policies emphasising the increased exchange of intelligence could furthermore entail profound challenges to the EU with respect to ensuring that foreign intelligence that is tainted or unlawful is not used or processed by EU member states and European agencies. Therefore, EU policy should call for better information so as to improve the exchange of data qualified as 'evidence' in criminal proceedings and which could lawfully be used to incriminate suspects. European

cooperation in the field of counterterrorism must take place within the remits of European scrutiny in order for counterterrorism policies to be efficient. This is the only way to build trust in the EU as regards cross-border and international cooperation in counterterrorism. Proper and high-level guarantees concerning the quality of information, its soundness and compliance with fundamental rights should be provided by all EU member states in cross-border cooperation. Better information exchange and robust checks against EU rule of law standards must go hand in hand – one cannot exist without the other for the Union to facilitate common responses to terrorism. More EU accountability for member states and their national security policies should also be the approach for ensuring legitimate public policy responses. Otherwise, EU measures will continue to fail in both countering terrorism and in ensuring respect for the rule of law and fundamental rights.

Acknowledgments

The work of this paper was conducted at the Joint Research Centre (JRC) during my mandate as SNE (seconded national expert).

I would like to show my gratitude to the CEN and its' experts for sharing their pearls of wisdom with me during the training course of "StandarDays" that I followed the last September of 2015.

I very thank all the exceptional Expert Members of the ERNCIP Thematic Groups (RSExEf, RN, CB Water) the meetings of which I had the honor of participating as a facilitator.

I thank all the colleagues from DG JRC and ERNCIP project for their collaboration the two years of my secondment in the EC JRC IPSC G.5.

References

1. Chenard, B. (Project Officer, G4) (2014): *Policy and Research in Security EU Security Industrial Policy & Standardisation*. "*Strengthening Science-Policy-Industry links in the CBRN-E sector*", presentation EC, Brussels, 30th January 2014
2. Chenard, B. (Project Officer, G4) (2015): *Innovation and Industry for Security DG Migration and Home Affairs*. "*Standardisation activities in the security area-M/487 to establish security standard*", presentation EC Brussels, 5th May 2015
3. Loos, M., Bueno Diaz, O. (Dec 21, 2012): *Principles of European Law: Mandate Contract*. @sellier european law publishers, ISSN 1860-0905, ISBN (eBook) 978-3-86653-970-9, https://books.google.it/books?id=EG730lY-mnAC&pg=PA107&dq=mandate+487&source=gbs_toc_r&cad=3#v=onepage&q=mandate%20487&f=false)
4. Spring, M.B., Grisham, C., O'Donnell, J., Skogseid, I., Snow, A., Tarr, G., Wang P. (2016): *From Courtship Dance to Lawyering: Working with Bulldogs and Turtles*. Department of Information Science, University of Pittsburgh, Pittsburgh, PA 15260, spring+@pitt.edu. Available at http://www.sis.pitt.edu/spring/papers/improve.pdf
5. Quevauviller, P. (2015): *Strengthening cooperation in the disaster risk and crisis management sectors – Perspectives within Horizon 2020*. Innovation and Industry for Security, presentation EC DG HOME, 2015. Available at http://ec.europa.eu/echo/files/civil_protection/civil/pdfdocs/infoday2015/DG_HOME.pdf
6. Quevauviller, P. (2015): *DRS - 2015 topics*. DG Migration and Home Affairs, DG Communication Networks, Content and Technology, Brussels, 26 April 2015, presentation EC DG HOME/B/4. Available at http://ec.europa.eu/rea/pdf/sec_infoday_2015/drs_2015_infoday_wp2015_drs_.pdf
7. Quevauviller, P. (2014): *First Science-Policy-Industry meeting on CBRN-E – Introductory words*. Security Research and Industry, DG Enterprise and Industry, Brussels, 30th January 2014
8. Wurster, S., Egyedi, T.M., Hommels, A. (2013): *The Development of the Public Safety Standard TETRA: Lessons and Recommendations for Research Managers and Strategists in the Security Industry*. (8th International Conference on) Standardization and Innovation in Information Technology (SIIT), DOI: 10.1109/SIIT.2013.6774584
9. Poustourli, A., Kousoulidou, M., Tsoukala, V. (2015): *Security in Urban Critical Infrastructures: Contribution of Standards for a Holistic Approach of Protection and Resilience*. Proceedings of the 14th International Conference on Environmental Science and Technology p. cest2015_01442, GLOBAL NEST, ISSN 978-960-7475-52-7, http://cest.gnest.org/cest15proceedings/public_html/papers/cest2015_01442_oral_paper.pdf
10. Poustourli, A., Ward, D., Zachariadis, A., Schimmer, M. (2015): *An Overview of European Union and United States Critical Infrastructure Protection Policies***.** Proceedings of the 12th International Conference "Standardization, Protypes and Quality: A means of Balkan Countries' Collaboration", p. 549-557, KOCAELI UNIVERSITY FOUNDATION, ISSN 978-605-83983-0-6, Turkey
11. Poustourli, A., Ward, D., Zachariadis, A. (2015*): European Policies and Programs for the Security of Building*

Constructions. Proceedings of the Construction in the 21st Century-Changing the Field Changing the Field: Recent Developments for the Future of Engineering and Construction (Thessaloniki, Greece), CITC-8, ISBN 978-0-9894623-7-2, http://www.citcglobal.com/citc-8.html

12. Poustourli, A., Kourti, N. (2014): *Standards for Critical Infrastructure Protection (CIP) - The Contribution of ERNCIP*. EURAS proceedings 2014 (Cooperation among Standardisation Organizations and the Scientific and Academic Community) (11th International Conference "Standardisation, Protypes and Quality: A Means of Balkan Countries' Collaboration"), p. 181-195, EURAS Contributions to Standardisation Research, ISBN 978-38-60-73305-2, http://publications.jrc.ec.europa.eu/repository/handle/JRC91182
13. ***: *EU Data Base of Mandates*. http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=472. Accessed: 2016-04-22
14. ***: *New Approach and European standardisation in the Internal Market*. http://www.newapproach.org/, Accessed: 2016-04-22
15. ***: *Commission sets out path to digitise European industry*. http://europa.eu/rapid/press-release_IP-16-1407_en.htm, Accessed: 2016-04-22
16. http://ec.europa.eu/dgs/home-affairs/financing/fundings/pdf/research-for-security/security_research_catalogue_2014_en.pdf
17. Discussion Paper on further steps in the implementation of the CBRN-E Agenda, European Commission
18. DIRECTORATE-GENERAL HOME AFFAIRS Directorate D: Internal security Unit D.1: Counter Terrorism and Crisis Management
19. ***: *The European Agenda on Security*. COM(2015) 185 final, http://ec.europa.eu/dgs/homeaffairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf
20. Public Safety Communication Europe (PSCE)/024-2013, Mandate M/487 to Establish Security Standards Final Report Phase 2, Proposed standardization work programmes and road maps, European Commission, 10-10-2013
21. Mandate M/487 (2012). *Mandate M/487 to Establish security Standards*. Final Report Phase 1 (*Analysis of the Current Security Landscape*). EC DG EI-SRD, 9 May 2012
22. Mandate M/487 (2013): *Mandate M/487 to Establish security Standards*. Final Report Phase 2 (*Proposed standardisation work programmes and road maps*). EC DG EI-SRD, 5 July 2013. Standardisation (M/487 has been accepted by the European Standards Organizations (ESOs)/ The work has been allocated to CEN/TC 391 'Societal and Citizen Security' whose secretariat is provided by the Netherlands), Standardization Institute (NEN), 05-07-2013
23. European Commission, Programming Mandate addressed to CEN, CENELEC, and ETSI to establish security standards, M/487, Brussels 17.02.2011