Leveraging R&D&I to develop capability and enhance security industry sub-sectors

Report of the Horizon 2020 Protection and Security Advisory Group (PASAG)*

December 2017

SUMMARY

To enable the European security industry, and particularly small and medium enterprises (SMEs), to best respond to user requirements and succeed on the global market, Europe should enhance its capability to innovate and invest to remain competitive.

This requires, an open and continuous dialogue across users, industry and the research community; a common understanding of the technology and capability gaps and opportunities; and a short to longer-term vision on how to achieve the intended outcomes, while preserving the necessary market and competitive dynamics.

The **Horizon 2020 Protection and Security Advisory Group (PASAG) has focused this report** on security areas where industrial participants, technology requirements and user/market needs and solutions have been identified to address current shortcomings, focusing mainly on **novel organisational approaches that generate effective synergies**.

The report also addresses emerging needs and the required flexibility to respond and anticipate new threats.

Different models could be applied depending on the sector:

- the Chemical, Biological, Radiological, Nuclear (**CBRN) "cluster" approach**;
- **PPPs** (Public Private Partnerships) such as the Cyber PPP;
- and possible future **European Innovation Platforms** (EIPs);

that can be supported by facilities such as the Network and Information Security facilities, experimentation in the US or the EC Digital Innovation Hubs, when relevant.

The PASAG recommends future "cluster-like" initiatives, in the following fields:

- Border Surveillance, supported by a Coordination and Support Action (CSA) and a complementary set of projects;
- future **police or first responder protection** initiatives;

and proposes that:

- the future **outputs of the CBRN cluster** are properly reviewed, and
- **lessons learned** are drawn for future initiatives incorporating similar approaches.

* More information about the PASAG can be found here: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3010

Objectives

For this report, the PASAG is focusing on how best to leverage Research, Development and Innovation to develop capability and enhance the security industry. It seeks to examine successful approaches and provide guidance on how to identify and meet technology and product gaps in security industry sub-sectors to address user requirements in the future. It will examine how industry clustered approaches, such as CBRN, have been effective in delivering security innovation and how this model could be extended to other areas in future work programmes[1].

This report analyses the major relevant industry needs and similar initiatives, within the H2020 Secure Societies theme or in other fields, to propose options applicable to security areas.

It also recommends monitoring progress in the CBRN cluster, providing feedback of a strategic nature with regards to its design and implementation, also for the benefit of other potential cluster initiatives.

1. The security industry and market sub-sectors

Several security market studies and industry analyses have been conducted at the EU level and globally (ECORYS[2], ISDEFE[3], NIS WG3[4], IPACSO[5], etc.), but there is no commonly agreed typology applicable to the security market and often the different market segmentations overlap, depending on the objective of the study, whether focused on the demand side (categories of customers and users) or on the supply side (market sub-sectors).

---

[1] In the Commission Staff Working Document {SEC(2008)2637} annexed to Commission Communication towards world-class clusters in the European Union (COM(2008)652), a **cluster is broadly defined as a "group of firms, related economic actors, and institutions that are located near each other and have reached a sufficient scale to develop specialised expertise, services, resources, suppliers and skills"**. In this PASAG report, the relevant region covers the entire EU and Associated Countries, where appropriate. The clusters are market driven (or at least demand driven when the market is not yet structured) and should ideally include a demand-side agency (ies), where it exists. They can also include forward-looking public policies, business initiatives, universities and research institutes. They should address short- to longer- term challenges and related activities such as education, dissemination, exploitation and market support.

A cluster in the Chemical, Biological, Radiological and Nuclear areas is a group of specialist enterprises, a "community of suppliers" that includes large companies, SMEs (Small and Medium-sized Enterprises), RTOs (Research and Technology Organisations) and academia, and users and practitioners which cooperate to achieve better response to users' needs, improved EU competitiveness, and opportunities for market development. It includes two participation levels:

- a CSA consortium (as large and representative as possible) that will build upon existing capabilities and knowledge to develop a shared vision and roadmap and a catalogue of technologies that need to be developed to integrate them into the existing and planned toolkits and solutions,
- several IAs (Innovation Actions) led by SMEs with a CBRN focus, responding to the technology and integration requirements.

This definition can be adapted depending on the theme addressed.

[2] http://www.ecorys.com/news/ecorys-building-community-users-secure-safe-and-resilient-societies

[3] https://www.isdefe.es/noticias/improving-use-european-funds-innovation-management?language=en

[4] https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/business-cases-and-innovation-paths-final-version-1.1/view

[5] http://ipacso.eu/34-ipacso-innovation-process-themes/market/market-analysis/market-overview/172-horizontal-vertical-market-analysis.html

Users/customers are typically organised by category: public (agencies, regional or local organisations, practitioners…), private or semi-private (operators, NGOs…, individuals).

As an example, the report, "Competitive Analysis of the UK Cybersecurity Sector", which was compiled by Pierre Audoin Consultants[6] for the UK Department of Business, Innovation and Skills (BIS), identifies four distinct market segments in Cybersecurity, with different requirements and supply chains:

1. Defence and intelligence,
2. Government, other than Defence & Intelligence,
3. Enterprises,
4. SMEs and consumers.

User/customer requirements can also be organised by theme or mission, while industry can be classified by participation level (suppliers of components, equipment, systems and solutions, or operations and services), or by functions along the main risk management phases (from preparedness and training, to long term recovery).

This approach is used in various projects, for instance the EDEN CBRNe Demonstration Project[7], or globally in the IMGS (Integrated Innovation Mission Groups on Security) or in the Community of Users (CoU), animated by DG HOME (Directorate-General for Migration and Home Affairs).

It is not the objective of this report to propose a market or user segmentation for the security sector, nor recommend the aggregation of security technologies or applications in groupings to facilitate the application of funding or innovation initiatives.

This report attempts to identify, based on actual experiences with EC funded relevant projects, and drawing from the expertise of the PASAG members, opportunities for improving the relevancy of market responses to user requirements in delivering security solutions, while meeting the challenges of developing technology solutions in a cost- and time-effective manner. It is not intended to be exhaustive, but only a first step in drawing from the growing number of case studies, based on the outcome of funded projects, that can provide a road map to guide the direction of future research and funding programmes.

2. Main innovation and market related gaps in security industry sub-sectors to address user requirements and develop the market

The security industry sub-sectors (with the exclusion of private or personal security) share similar needs and gaps, related to the effectiveness of innovation and exploitation of market opportunities:

- **Customer and demand-side**:
    - Evidence suggests that properly **organised and effective communities of customers, users and policy makers, offer the best opportunity to join-up common demand-side interests** and create market-relevant scale;

[6] https://www.gov.uk/government/publications/cyber-security-competitive-analysis-of-the-uk-sector

[7] https://eden-security-fp7.eu/

- A disparate, expansive and complex **supply chain needs reliable and consistent mechanisms to enable a clear and common understanding of user needs** and potential market opportunities, including financial, economic and regulatory constraints;
- **Users and providers need a common understanding** to identify and plan for new solutions and products, as well as to ensure their timely implementation through relevant evaluation, testing and training, which can be supported by standards, offering a common understanding of requirements;
- A unique characteristic of this sector is its **constant state of emergency** that requires that the supply chain is short-wired to respond frequently to customers' urgent operational requirements;
- The **shorter-term focus of security practitioners** requires supporting policy and financial incentives to ensure new technology and innovative solutions are encouraged through initial buys and receive access to testing within end-user environments.

- **Research and supply-side** (including academia and RTOs, SMEs, industries, service **providers):**
  - **Communities of suppliers**, organised around sub-sectors of security, offer the **most effective supply-side approach** to improve the customer interface opportunity, particularly with regard to a **shared and common understanding of future requirements**, planning and procurement cycles, testing and commissioning environments, administrative and regulatory constraints. To ensure broad stakeholder consultation and uptake, these requirements may be supported by European standards. These communities will need to address the safeguarding of intellectual property rights and the assurance of a competitive marketplace;
  - Open market access to ensure global competitiveness and access to state of the art technologies and enablers, to **identify gaps and opportunities**;
  - **Road-mapping research** to ensure incremental technology development aligned with customer planning cycles, encouraging private investment by addressing larger markets in the EU and export opportunities abroad;
  - Introducing and **experimenting with new innovation models and agile development** methodologies, including engaging with demand-side users to demonstrate, prototype and test new capabilities through rapid technology insertion models;
  - Encourage the right **balance between the short and longer-term roadmap** and plans and the urgent operational requirements (through updated roadmaps, fast tracks and quick product adaptations);
  - Maximize **Intellectual Property exploitation** to develop successful innovations through sustainable exploitation after completion of the research activities, by using open source technologies to minimize the costs or by leveraging other IP sources;
  - Support **innovation validation and first implementation in operational environments**, R&I monitoring and results dissemination, also through targeted investment incentives;
  - Create **EU-wide events** that showcase research results and encourage innovation by promoting active interaction with users and practitioners, including funding challenges for rapid deployment of capability;
  - Increase **information flows** between supply-side research and technology and innovation initiatives (including, seed and venture capital, incubators, accelerators and mentoring);

- Monitor and support the access to and **availability of relevant talent and skills** through joint initiatives between industry and academia;
- **Encourage** the development of CEN or CENELEC **standards** or other international standards, as a market tool supporting the deployment of innovation.

3. Case studies: the CBRN Cluster, other PPPs, EIPs and other relevant models

- **The CBRN Cluster origin**

CBRN is a theme that has been aggregated into a **recognised sub-sector of security**, principally as a result of its highly sensitive and high-risk attributions, as it addresses a potentially devastating threat to the civil population. Its strategic significance for EU Member States has focused both the demand- and the supply-side into forming communities of interest with strong bonds and committed intent. The result has been a **concentration of efforts** that have successfully assembled the scientific, industrial and operational expertise necessary to address the relevant technological challenges, including the need for significant basic research, with important contributions from across the EU. In this respect, the **CBRN experience has been almost unique**, not just in the approach, but in the effectiveness of the outcome, in terms of both ensuring a uniform and consistent messaging from the Member States (MS) authorities involved, and corralling the best resources to address the requirements.

In this regard, the CBRN experience offers a **useful benchmark** against which to measure the effectiveness of the broader security sector in translating user requirements into technology solutions. It also provides **insight into some of the deficiencies of the current delivery models**, suggesting where these can be improved. These include:

- the current mechanism in place with MS and the EC for the selection of topics in subsequent calls is not always satisfactory, because it does **not offer a clear follow-on process from one call to the next,** within the same topic area;
- the **evaluation** and the detailed project/programme monitoring can best be achieved only **by true experts** in the field;
- some key categories are currently very reluctant to participate in EU collaborative R&I, partly because of **limited IP rights**;
- both **confidentiality and neutrality** must be guaranteed.

The ***triangle*** **EC - Programme Committee - PASAG may not have all the required expertise** to identify the overall research and technology roadmaps and agree the innovation opportunities to pursue. A cluster of professionals, formed in close dialogue with the relevant stakeholders is an option, but it should include a representative, authoritative and comprehensive sample of the provider categories (industry, SMEs, academia, service operators), to avoid bias to competition, and ensure neutrality.

Existing clusters which have had a degree of success in achieving their objective, are possible models, considering that each case is specific: the **FP7 Space clusters**, for instance, where the technical expertise is elevated and specific, both on the part of industry, as well as the space agencies, play a key role in identifying and supporting the space technology roadmaps.

The significance of the CBRN cluster cannot be overstated, particularly given its impact in perpetuating the science and the industrial base required to deliver the technology solutions specific

to this domain. This is very important in an otherwise very narrow field of expertise that could unwittingly be disbanded and be almost impossible to replicate when needed, without the continued and consistent support and commitment of all its stakeholders.

- **Other relevant models for cluster-like initiatives, such as PPPs, EIPs…**

The most relevant example of a cluster approach in the broader security area is the **Cybersecurity cPPP** (contractual Public Private Partnership), launched in 2016 under the auspices of DG CNECT (Directorate General for Communication Networks, Content and Technology).

It is expected to bring together participants from throughout the EU and across the diverse segments of the economy and society, engaged in the development of a secure and trusted digital market (e.g. technology and solution suppliers and service providers, public and private sector customers and users, policy makers and public administrators) in pursuit of an agreed and coordinated strategy and policy initiative aimed at:

- Protecting the (development of the) European Digital Single Market from cyber threats;
- Structuring, consolidating and strengthening the European cybersecurity market with trustworthy and privacy aware technologies, products services and solutions;
- Supporting the development of European capabilities to bring to market innovative cybersecurity technologies and building a strong, resilient and globally competitive European cybersecurity industry with a strong European-based offering, in an open and competitive marketplace;

The objective of the cPPP is to **bridge the gap between capacity building and the deployment of trusted European cybersecurity and ICT solutions** on the European and the international markets, creating new business opportunities for European industry, while addressing the cyber challenges faced by Europe and ensuring that EU principles of privacy of its citizens are protected.

This objective substantiates the commitment to build a sustainable, secure and trustworthy ICT industry in Europe, even beyond the scope of the EC's cPPP, by developing a long term industrial strategy to achieve specific outcomes, monitored through Key Performance Indicators (KPIs).

The proposed **initiative is closely aligned with the objective of establishing a European information ecosystem** underpinned by the exchange of experiences, competencies, pooling of resources, raised general awareness, general education/specific training programmes, etc.

The Cybersecurity cPPP joins-up several stakeholders, including:

(a) Large companies (directly represented): cybersecurity solutions/services providers;
(b) National and European Membership Organisation/Associations (gathering among others, large companies, SMEs, RTOs, Sectoral organisations, public bodies) representing interests at national or European/International level;
(c) SMEs (as per the EC definition) solutions/services providers directly represented;
(d) Users/Operators (where cybersecurity technology/solutions/services provision is not one their business activities);
(e) National and pan-European standards agencies;
(f) Regional/Local public administrations (with economic interests);
(g) Public Administrations at national level (national strategy/regulatory/policy issues, including R&I coordination);

(h) Research Centres (large and medium/small), Academies/Universities (directly represented, not via an associative body).

It is organized by themes initially addressed by the following first Working Groups:

- Standardisation, Certification/Labelling/Supply Chain Management;
- Market development/Financing Export;
- Sectoral demand (market applications);
- Support SME, East EU…;
- Education, training, awareness, exercises;
- SRIA (Strategic Research and Innovation Agenda): Technical areas, Products, Services areas.

4. Main advantages of a "cluster" approach

The main advantages of instituting a "cluster" or adopting other similar approaches, would include:

- **Improving the overall effectiveness of the H2020 instrument and its impact, particularly the approach to selecting priority topics in future calls, by**:
  - **extending the vision** applicable to the technology solutions from short- to medium-term to medium- to longer-term, in alignment with EU policy requirements and global market conditions;
  - **improving continuity and consistency** in pursuing the end-objectives, in terms of both capabilities and solutions (not "one shot" projects without a coherent follow-on), and to provide industry and SMEs the necessary forward visibility to support investments **(road mapping);**
  - **ensuring a phased approach** to progressing to maturity and addressing emerging market requirements (incremental advances from components to systems, with contributions from Human & Social Sciences…) **(master plan with milestones and deliverables),** including **recommending further steps and funding beyond H2020;**
  - enabling faster processes and **accelerated innovation**, including by avoiding re-discussing the objectives, and **through new interdisciplinary understanding** and synergies embedding security solutions more firmly in complex matrices of user and societal needs;
  - ensuring the responsiveness to policy briefs on specific or urgent issues and **promptly answering unexpected and unpredicted threats by calling on expert community support** through research and innovation activities or identifying short term procurement solutions;
  - **guaranteeing neutrality and innovation**, also by running parallel competitive solutions in response to key topics challenges;
  - monitoring progress (at a minimum the FP7/H2020 projects main outcomes, with links to the national projects, by a neutral organization/consortium) to optimize follow-on work and exploitation;
  - training users on the innovations, testing and **demonstrating the tangible benefits to the users and the procurement agencies in their own environment at the national and EU levels.**

  The key objective should be to **develop affordable solutions meeting user and wider societal needs, and guaranteeing their sustainable development. Having agencies (particularly EU agencies where feasible, and national agencies) involved directly in the process with clear**

incentives for participation, would provide a helpful reference in the market and represent an important measure of success that would help secure a stronger market position for providers.

- **A more effective support to improve industry/SME competitiveness** to accelerate development of competitive and innovative products and services for the EU market and, where possible, internationally, through a coordinated effort with users/procurement agencies and commercial customers (especially large operators). This requires:
  - **understanding of the full range of capabilities from critical technologies to integrated demonstrators, with an assurance of access to fundamental enabling technologies** (security specific critical technologies in the Secure Societies theme, and possible links with other Key Enabling Technologies (KETs) where relevant);
  - including both oriented R&I and disruptive R&D and innovations;
  - defining and implementing a **detailed process with milestones, budgets and funding** with long term plans;
  - identifying, where relevant, **short-term needs and procurement opportunities** that can be addressed through other funding sources and agencies;
  - **demonstrating and exhibiting the most promising innovations and products** from EU industry/SME to potential users and customers (i.e., an annual exhibition bringing together the wider community, field demonstrations and training, etc.);
  - **dedicating more effort to "day-to-day" initiatives** (more activities on prevention and recovery, linking safety and security, with other applications such as health or transport…) to ensure the commercial viability of the developed capabilities;
  - Increasing access to **seed and venture capital funds, as well as incubators and accelerators.**

  This will likely require better coordination with other H2020 areas and **close links with the relevant scientific community, especially when validation or "certification" (EU label) is needed.**

  An **overall vision**, provided by this organized "community of interests", including relevant customers, researchers and suppliers, creating **a dialogue with all the stakeholders**, would be an **important unifying element**. This could be achieved through an **overarching CSA**, if recommendations are collectively approved and implemented **as a first step**. An EIP (European Innovation Platform) could be implemented in specific cases, as a second step.

  Where possible, links with other innovation and procurement instruments for later exploitation, while preserving competition and fairness rules, would be helpful. The **use of other EC funding sources for testing, exploitation and some level of procurement,** would be a significant incentive particularly for **end-users and procurement agencies at national level**.

  To facilitate and encourage a successful market exploitation, while bearing in mind national sensitivities, MS agencies and users should participate in the initiatives as early as possible in "**mirror group**" organizations, with a **key driving role for EU agencies**, where possible, to prepare future procurement and delegation agreements.

5. Criteria and processes for other "cluster" selections

Topic selection criteria could be:

- **EU policy driven;**
- **sound commercial perspective and competitiveness (considering some level of assurance of security of supply in the EU), based on:**
  - **Relevance**
  - **Innovation**
  - **Scalability**
  - **Market**
  - **Maturity**
  - **Skills**
- **need for a critical mass at EU level to address the global market;**
- **improved effectiveness of a community working jointly to develop the capabilities and the market (academia, industry, SMEs, and possible communities of interest of customers and other stakeholders).**

6. Relevant implementation models

Each selected area (large enough when scaled to EU level), could be approached with ad-hoc models.

An overall CSA per area would ensure implementation of the technology road maps, the development of master plans and the monitoring of execution, ensuring a high-level review of projects outputs, confirming that real progress is achieved.

It should be run by a focused and dedicated group tasked to deliver the end user/market requirements, while ensuring neutrality of the R&I supply chain.

Depending on the theme, it should include public organisations representing the users, operators, RTO and academic networks and industry/SME trade associations.

The following are examples that can represent models or benchmarks:

- The FP7 **Future Internet PPP**[8] is already implemented as a full programme, with significant private sector engagement.
- In the H2020 Space theme (competitiveness of European space technology), there are two Strategic Research Clusters (SRC), based on CSAs referred to as "Programme Support Actions", that are expected to recommend how a work programme is run. PSAs can be operated under agency or industry leadership, with all stakeholders involved.
- Within H2020 Secure Societies the **"CBRN cluster" (SEC-05-DRS-2016-2017), has two parts: the cluster itself,** including support for further integration and standardization of interfaces **(Part A) and associated RIAs (Research & Innovation Actions) expected in a second call (Part B).**

More generally, such "clusters" can be implemented, when relevant, **under article 41 complementary grant agreements,** allowing coordination between grant agreements, exchanges of foreground IP and synchronisation of activities.

[8] Future Internet Public Private Partnership: https://www.fi-ppp.eu/

7. Short term "cluster" candidates and recommendations

As potential candidates, the PASAG has identified the following themes that would be suitable and more effective under a cluster-like approach:

- **Border Surveillance - Proposal for a security "cluster" approach in the H2020 Secure Societies theme implemented by a CSA and a complementary set of projects**

The **implementation of the European Border Guards Agency**, as envisaged under European Commission policies in the EUMSS (European Union Maritime Security Strategy) and other specific border control governance, will generate an associated impact in the **management of the overlapping competencies and responsibilities** between the EU agency and the national authorities with missions in border management.

Moreover, the need to **seamlessly share patrolling and intervention assets**, the **aspiration to move from the acquisition of assets to a services approach** and the unavoidable standardization issues, are all aspects that require a close and well-structured interaction between the end-user community and the supply chain, to achieve the necessary coherence and continuity of approach.

The **Border Surveillance** theme has all the characteristics of a **strategic area**, with a strong industry component and significant scientific and operational content. For these reasons, it needs to address potential risks that could undermine implementation, such as:

- **Border control investments may not match the evolving end-user needs** or R&D outcomes are not translated into security solutions;
- The **lack of standardization** in border control solutions limits the commercial dissemination of the research outcomes in the market globally;
- The need to **adopt a holistic approach** encompassing all the socio-technical aspects of the solution require that regulations and legal constraints need to be managed in parallel while evolving the technical solution;
- The experience derived from **initiatives** taken across the EU are **not properly shared** and benchmarks are rarely identified, with the risk of "reinventing the wheel" each time;
- Shifting from classic procurement towards a **service-based model** through a Public Private Partnership arrangement can be complex if not properly coordinated, engaging all parties involved.

A **cluster approach connecting experts, recognized end-users and industry** can be the vehicle to achieve the necessary critical mass to meet these challenges by identifying and agreeing the main requirements and standards, and planning the implementation of the necessary research and innovative solutions.

***The main objectives of a Border Surveillance cl*uster** approach should include:

- **Structure topics of the next calls** addressing an appropriate mix of RIA, IA and PCP (Pre-Commercial Procurement) aligned to a long-term vision shared by EC and MS representatives;
- **Foster and improve the supply chain engagement** in participating to the competitive process for the border control topic;
- Address rapidly changing and unexpected threats by **leveraging the support of expert communities**;

- **Monitor the results** and apply corrective actions in the next security call waves,
- Support industrial and SMEs competitiveness;
- **Promote standards** and apply cross sectorial guidelines for ICT related aspects;
- **End-user** need to be more engaged in the definition and validation of the results, as well as in the development phase, **sharing with the industry the associated development risks**;
- The potential for **dual-use applications** is key considering the blurred distinction in technologies between civilian and military solutions for border surveillance.

Possible process for selection of specific focus areas in the Border Surveillance cluster

Border surveillance raises important issues about technology options: currently, major requirements include the provision of persistent surveillance in specific geographic areas and crossings, based on a value for money proposition. In the future, these priorities could be addressed with service-based business models.

Topic selection criteria may therefore include:

- Readiness **for service oriented applications**;
- **Adherence to evolving standards** or proposals for new standards to facilitate seamless integration and data exploitation at European level;
- EU Policy driven approaches;
- **Commercial attractiveness** and competitiveness (competition pressure worldwide to be considered to guarantee some security of supply in the EU);
- Need for a **critical mass at EU level** to address the global market;
- Existence and need for a **homogeneous community** (academia, industry, SMEs, and possible communities of interest of customers and other stakeholders).

Relevant implementation models for a Border Surveillance cluster

A **multi-annual umbrella framework** covering a CSA, RIAs, IAs culminating in PCP-style implementation could provide the best combination to address the main objectives above.

- **Border-linked Police cluster**

As a consequence of the growth and evolution of the terrorism threat and of anti-immigration sentiments, coupled with a dynamic approach of EU countries to Schengen rules or national policies for managing EU entry points, **a flexible and robust capability for data exchange among EU and National Administrations** has become an urgent requirement to improve the monitoring and the prosecution processes related to the unlawful entry into the EU and movement within the area.

The urgency of the **problem no longer allows for a lengthy process** for the development of an EU standard enabling a structured data exchange among authorities in charge of managing regular and irregular migrants in a context of Schengen/non-Schengen rules.

From a supply-chain perspective, it is important to shorten the time to market and the rapid assimilation of significant technological advances into daily operational processes.

In this context*,* **a community** of border/frontier control operators and industry and research providers **can be of high benefit to shorten the time for solutions deployment** related to this crucial EU challenge.

A cluster approach is recommended because it **institutionalises the collaboration between interested parties** and incentivises the introduction of new solutions in a timely fashion with the participation, contribution and engagement of all the key stakeholders. This is particularly important in an area as sensitive as this one, with the challenges imposed by personal data information management, to ensure a seamless but controlled monitoring of the flow of individuals entering and leaving EU borders.

Such a cluster could be an extension of the Border Surveillance Cluster or have its own focus as a dedicated cluster.

The key objective of creating such a group is in the need to ensure an EU capability to secure the identification of all those who enter the EU, including accessing and collecting their relevant background information.

The **European Border Guard** and National Border Police forces should have a **preeminent position in the management of such a cluster**. The objectives of the cluster would be focused on **fast-track introduction of high TRL[9] solutions** and technologies into the end-user operational systems. The PPP/PCP appears to be the best mechanism to support such an initiative.

Additionally, but subsequently, the following topics could be considered for a cluster approach:

- **A (wider) police cluster;**
- **A First Responder Protection cluster.**

8. CBRN Cluster evaluation, implementation monitoring and assessment

The CBRN cluster Step 1 is part of the 2016 call.

The selected project(s) started in spring 2017, with first short term results within a few months to guide the first Step 2 calls. Monitoring and evaluation of these projects should include:

- **Representativeness** of the stakeholder community in the project(s);
- **Leveraging** previous or current research and innovation **results**;
- **Synergies** with other programmes (other H2020 themes, other EU, national, regional, international), to reduce duplications and focus efforts on priority needs and solutions;
- Level of **private investment**;
- **IP** generated and a committed plan for **exploitation**, including the development or contribution to standards;
- **Business Model Outline (agile potential business plan)**;
- First Implementation in **operational systems** for **validation and testing**.

A possible evolution towards an EIP in CBRN would demonstrate the success of the initiative with political and industrial endorsement.

[9] Technology Readiness Level