IMG-S – EARTO Joint Position Paper on RTD, Innovation and Industry for Secure Societies

This document presents a joint position from members of the Integrated Mission Group for Security (IMG-S) and the European Association of Research and Technology Organisations (EARTO) on the analysis of the RTD, Innovation and Industry for Secure Societies.

This position paper has considered the following background information:

- the overall policy goals of the **Europe 2020 Strategy**, the European Union (EU) growth strategy for the next ten years supporting the European ambition to become a smart, sustainable and inclusive economy with associated societal and economic benefits in terms of safety, security, quality of life, well-being, productivity, employment and social peace;
- the **EU Security Industrial Policy**, promoting innovation and competitiveness in the security industry sector, with one of the highest growth and employment potential in Europe;
- the principles and guidelines set out in the **EU Internal Security Strategy** (ISS) for dealing with security threats, namely organised crime and cross border illegal activities, through an integrated strategy;
- the respect of privacy and civil liberties as outlined in the **European Cyber Security Strategy** for secure information sharing and processing, upholding EU's core values and fundamental rights, including the protection of personal data.

Moreover, it is acknowledged that the **H2020 Secure Societies** is a key instrument to achieve the European vision, strategy and policies. It should support innovations that are promising (potentially market disruptive) and/or concrete (close to market) and capable to reach and succeed on the global market. These innovations need to be affordable and appropriate to the existing and future market needs, including dealing with the new forms of threats and required resilience, especially due to the increasing interdependencies between the physical world and IT-platforms (e.g., cyber physical systems)

Communities of Users, comprising key stakeholders, namely policy-makers, end-users, industry, academia, RTOs and citizens, have to work together in a trustworthiness platform to establish shared views on roadmaps, programmes and commitment in the relevant fields of activity. The Communities of Users should detail the security priorities as well as the innovations that ensure a prompt response to the security market demands and the society's security challenges. In addition, it is noted that the the security domain in particular requires an extensive discussion of technology impact assessment, user acceptance and societal impact research.

The "Joint Position Paper on RTD, Innovation and Industry for Secure Societies" was elaborated by:

EARTO SRG: Géraud Canet (CEA, FR), Luis Emaldi (Tecnalia, SP), Andrea Nowak (AIT, AT), Veikko Rouhiainen (VTT, FI) and Helmut Schwabach, (AIT, AT)

IMG-S: Sergey Babichenko (TA6, LDII, EE), Federico Barcio (TA6, Thales, IT), Alberto Bianchi (TA1, Finmeccanica, IT), Willy Bohn (TA6, BOLASER, DE), Federica Di Camillo (TA6, IAI, IT), Michal Choras (TA7, iTTi, PL), Geert De Cubber (TA6, RMA, BE), Vincenzo Cuomo (TA1, CNR, IT), Evrim Anıl Evirgen (TA1, Havelsan, TR), Clemente Fuggini (TA1, TA2 and TA4, D'Appolonia, IT), Alessandro Garibbo (TA2, Finmeccanica, IT), Clive Goodchild (SRT, TA4 and TA6, BAES, UK), Bartlomiej Jankiewicz (TA6, WAT, PL), Artur Krukowski (TA4, Intracomm, EL), Marco Manso (IMG-S Chairman and TA2 co-chair, Rinicom, UK), Jean-Claude de Miscault (TA6, MI, FR), Maarten Nieuwenhuizen (TA6, TNO, NL), Bart Nys (TA6, NICC/INCC, BE), Antonio Palucci (TA6, ENEA, IT), Stefano Pasquariello (TA5, Finmeccanica, IT), Paolo Proietti (TA2, Finmeccanica, IT), Roberto Rossi (TA1, Thales Italia, IT), Francesco Soldovieri (TA1, CNR, IT), Krzysztof Samp (TA2, iTTi, PL), Brigitte Serreault (SRT and TA6, Airbus, FR) and Vyta Vinciene (TA6, CENTRAS, LT).

1. Key Assumptions to Address the Security Challenges

The H2020 instruments and mechanisms should be used in order to successfully explore and exploit the innovations that will assist Europe in attaining its main security objectives, as established within the main European strategies and policies.

That successful exploitation entails a number of key assumptions to address today's and future security challenges:

- The need to adopt a **holistic view of security** and to address the **whole security lifecycle**, including prevention and restoration;
- The relevance of creating **Communities of Users**, bound to long-term visions on how end-users, policy-makers, industry, RTOs and academia and citizens can respond to security and societal challenges;
- The importance of establishing **short-to-long term frameworks** that combine the perspectives of the industry, research and SMEs to provide answers to security challenges, allowing co-funding and strengthening commitment;
- The strong focus on the research and development of **disruptive technologies** to address security challenges, namely tackling the added value of the integration of surveillance, monitoring and resilience technologies, among others.

2. Impact

The main impact of enabling H2020 instruments and mechanisms to address security challenges will be the opportunity for stakeholders in the security sector to share knowledge and experience and capitalise on the multiplier effect of their activities to the benefit of secure societies. Furthermore, it will highlight the excellence of the science and research being conducted in the security sector, as well as the successful viability of the EU security industrial and technological base, leveraging the opportunity for many innovations to timely reach the European and global markets, while fostering end-users adoption and social acceptance by EU citizens.

Aside from contributing to further enhance the EU member states' resilience, the H2020 instruments and mechanisms would empower a successful implementation of EU external security actions, including assisting the development of third-world countries, considering their culture and habits. This would then perform an essential part within Europe's credibility, sustainability and long-term security.

A comprehensive approach to Security would result in a better-prepared European Union, able to provide on social stability, economic growth and sustainable development.

In addition it is important to note, that in particular the security market is characterized by national domains. Therefore demonstration, validation and harmonization activities as well as stakeholder-strategy planning are essentially necessary for ensuring concerned market impacts.

3. Security Priorities

The analysis of today's global context and particular threats highlights the following security priorities:

- Protection and rescue of citizens;
- Surveillance, monitoring and control of borders;
- Emergency and disaster response;
- Cyber-security;
- Privacy for the upcoming networked society
- Chemical, Biological, Radiological, Nuclear and Explosives (CBRNe);
- Cross-cutting initiatives.

On the protection and rescue of citizens, a number of actions should be considered:

- **To establish effective policies and shared mechanisms at the EU-level to deal with the refugees and migration flow in Europe** (both technologically and policy-wise). In one hand, there is a need for collaboration between EU, neighbouring states and originating countries in view of monitoring and controlling immigration into Europe. This could be achieved both by deploying technological means to early detect boats' departures and by liaising with originating countries to prosecute ruthlessly the criminal networks that profit from these activities. Furthermore, it is critical for the security of citizens and the European society to properly assess and establish the conditions to confer the status of economic victims and war refugees, clearly distinguishing eligible people from occasionally suspect individuals or infiltrated terrorists; the latter with the declared purpose of radicalising and recruiting volunteers and conduct terrorist attacks in Europe[1]. It is needed to establish reliable migration records (see in the following) that can be shared across the appropriate entities in Europe and within the appropriate legal framework. Finally, it is fundamental to timely ensure the protection of the migrants' human rights, including providing medical support and preventing the spread of epidemics.
- **To implement actionable intelligence and information sharing to prevent and combat migrant smuggling**[2]. The information and intelligence would enable the identification of suspicious vessels that can be used by smugglers and warrant depriving smugglers of their profits, while enhancing operational cooperation against migrant smuggling and information gathering and exchange in third countries. The EU could ensure full use of all available tools to gather information, such as human field reports and the monitoring of the internet content in order to develop a knowledge base, which would provide capacity building and training to third countries.
- **To gather activity-based Intelligence** (e.g., HUMINT, OSINT), exploiting Big Data to foresee new threats (e.g. terrorism) and future expansion of crime trends particularly in selected areas and referred to specific religious groups. EU needs to consider a comprehensive approach, including non-traditional security stakeholders (e.g. critical infrastructure operators), use of non-conventional sources (e.g. social media) and societal dimension (e.g. inclusiveness, risk of segregation and radicalisation).
- **To speed-up and build awareness in search and rescue operations**. The conduct of cross-border exercises and the promotion of interoperability between neighbouring Member States is relevant in improving the performance, effectiveness and efficiency of emergency services and authorities. For example, the possibility to transmit in real time search and rescue operations videos to relevant control centres would provide enhanced awareness. This would require the necessary bandwidth virtually anywhere through e.g. 5G communications technology, possibly by using deployable access and networking resources, as well as SATCOM facilities).
- **To ensure the safety of EU citizens in the light of increased networking as well as increased usage of autonomous systems technologies,** a fundamental redesign of internet technologies is necessary: we need a new form of privacy because today only a view global players like google , apple,… have access to all produced data - direct and indirect - of the citizens. We need no means, methodologies and tools, which the individual can actively manage his personal data, to ensure democracy and basic values of our society in the future digital universe.
- **To protect EU citizens travelling outside of EU** since EU citizens are frequently travelling outside of EU for business and personal purposes. However, the changing social and political situation in various regions may

[1] In the recent terrorist attacks in Paris, one of the perpetrators "may have travelled to Europe on a Syrian passport along with the flow of migrants". Source: http://www.nytimes.com/2015/11/15/world/europe/paris-terrorist-attacks.html.

[2] See "EU Action Plan against migrant smuggling (2015 - 2020)".

cause that they will be in danger (e.g. from pirates, terrorist groups, etc.) and adequate support should be provided.

On border security, relevant activities should involve:

- **To implement effective Blue and Green Border monitoring and surveillance.** The European Union would benefit from enhanced systems, equipment, tools, procedures and methods to support the border control authorities in ensuring the security of the EU external blue and green borders.
- **To provide tools assuring the concept of Smart Border.** EC proposed a 'smart border package' to speed-up, facilitate and reinforce border check procedures for foreigners travelling to the EU. Currently It consists of two items: Registered Travellers Programme (RTP) and Entry/Exit System (EES). However, there is a need to work on technologies and solutions which will allow to implement this package and in future to extend it with new mechanisms.

On emergency and disaster response, the emphasis should be:

- **To adopt a whole lifecycle approach in emergency and disaster management linking pre-hazard and post-hazard phases**. From risk assessment (including gap analysis) to resilience characterisation (risk awareness), mapping and screening of countermeasures (SWOT analysis), preparedness and planning (requisite for the implementation of interoperable modules/tools), response (including early warning, fast assessment and damage identification), recovery (logistics and insurance involvement) and redundancy (post-disaster management, lesson learnt and co-sharing of knowledge), all phases of emergency and disaster management should be considered in EU's action.
- **To increase proactive collaboration between civil and military organisations**. The creation of a common framework of operations and the conduct of joint exercises between civil and military organisations is fundamental to improve interoperability in case of large-scale emergency or disaster.
- **To introduce Earth Observation as a key enabling technology in the emergency and disaster management loop**. Earth Observation techniques are highly useful in acquiring insight capable of supporting enhanced situational awareness throughout the whole lifecycle of emergency and disaster management.
- **To create the EU First Responder**. Within the EU landscape, international cooperation is paramount to handle large-scale incidents exceeding national capacity. The effective involvement of multi-national assets, namely First Responders (FRs), depends on interoperability, which in turn may result from pan-European standards that have to be developed covering concepts of operation, functions, protocols, interfaces/plugs and information exchange. Furthermore, the development of training methodologies and procedures for First Responders and decision-makers is required. In this context, concepts like those of the Software Defined Radio and the Cognitive Radio should be taken into account in conjunction with the development of 5G Communications standards for interoperability and spectrum optimization.
    - The IMG-S has produced the **Report on Futures of First Responders Systems (R06)** that identifies research needs for the next five years in FR systems, addressing areas such as communications, location, situation awareness, (physical) protection, decision support, search and rescue, cyber-security, training and simulation. The report is included as annex.
- **To develop a knowledge management system** for acquiring and sharing the lessons learnt in the area of crisis management at various organisational levels, i.e. first responders, policy-makers, public authorities.

On cyber-security, activities should encompass:

- **To continuously reinforce cyber-security**. Cyber-security has been based on strong perimeter defences (firewalls, intrusion detection and prevention) but, in the currently distributed and always connected world, this paradigm is changing. Networks and systems, as well as the information/data of an organisation itself, must

be continuously hardened and protected. Moreover, cooperation between organisations is increasingly dynamic and will impose a softer or more open perimeter to allow more flexibility and agility. In this context, it is noted the important growth trend of on-demand ICT services. To address this new scenario, cyber-security should focus more on data and processes than on IT infrastructures.

- **To monitor emerging technologies that pose challenges to cyber-security management**. Common across multiple sectors as well as in emerging application domains, specific key technological trends create considerable challenges for cyber-security management. The most important areas for future developments should include:
    - **Secure cloud-based systems**: this new way of providing ICT requires more efficient security features for virtualisation systems by means of guest virtual machines and cloud components monitoring functions and also better performing cryptographic hardware to allow cloud providers and customers to implement end-to-end confidentiality with no latency delay;
    - **Secure mobile devices**: malicious agents and attack techniques are designed specifically to target mobile devices. Malware is commonly installed on a device through the Internet and it performs activities without the user's awareness or permission. Thus, improved tools for mobile malware detection and inspection are required;
    - **Application security**: "non-critical" applications have no implications concerning safety or information confidentiality and, consequently, are rarely designed to be secure. In order to foster resilience to attacks, security has to be 'built into' the applications. To this end, security methods are needed to be closely linked to software modelling, development and testing; likewise, the definition of improved methods of measuring applications' security and privacy are needed;
    - **Secure Internet-of-Things**: this application typically collects a large volume of very sensitive information, exchanged between machines and devices; as consequence, authentication is one of the most important priorities, but also network security and segregation are areas of particular interest;
    - **Secure social networks**: once information is posted to a social networking site, it is no longer private; for this reason, social network systems generate many concerns on privacy. Also, social networks systems expose their users to the highest concentration of online security threats. As consequence, features to ensure regulatory compliance of these systems and to evaluate trust in the information shared should be considered as priority challenges;
    - **Secure industrial control systems**: in this area, well-funded and organised attackers operate; they own knowledge and capabilities to take advantage of unknown or zero-day vulnerabilities and bypass signature-based virus detectors and intrusion prevention/detection solutions. Thus, improved techniques of attack detection and systems evaluation are required. The development of 'Industry 4.0' paradigm should be exploited to improve inner security of industrial plants and facilities;
    - **Define methodologies and procedures** that will guarantee adherence to civil society principles (like privacy, freedom, independency and neutrality of cyber security operators) and operative efficiency against cyber-attacks.
    - **Nationwide security awareness**: in order to frontage large-scale politically motivated attacks, an effective cooperation and communication between nations, authorities and infrastructure stakeholders is required. A continuous collaboration between industries, research centres, civil and military authorities should deliver decisive means for the collective creation of complete and timely knowledge of the cyber scenario that would enable criteria for an early warning and a rapid and comprehensive reaction to attacks. This need is also highlighted in the Network and Information Security (NIS) Directive, already adopted by the European Commission.

On CBRNe, it is important:

- **To set a specific theme on CBRNe within the EU's strategy and policies**, eventually with the creation of a strong CBRNe organisation with a dedicated budget. This necessary step would enable to overcome the current crisis in this sector and then to develop a strong European CBRNe activity, with support to relevant industry, research and SMEs;
- **To create effective synergies with safety, health and environment communities**. Because these communities are too disparate and function autonomously, it would take a significant effort on coordination and networking to establish a reference framework (including Terms of Reference) to enable understanding of concepts and priorities.

On cross-cutting initiatives, it should remain a priority:

- **To exploit and improve further the Copernicus services** for security applications in three main domains: border surveillance; maritime surveillance; and support to EU external action;
- **To develop secure communications as a *de facto* standard for smart cities**. Smart mobility and smart communication in case of public events and large concentration of citizens in public areas are becoming increasingly indispensable assets (i.e. a smart secure city depends on the security and availability of telecommunications);
- **To promote the development of components and systems deployable for multiple missions and capabilities**. Because their utilisation may be shared amongst different stakeholders (end-users), these components and systems, which can be considered a high-tech and high-value component of the emerging sharing economy, generate economic and financial advantages to the security sector, enlarging the market, reducing market fragmentation and contributing to reinforce the European industrial base.
- **To develop Pan-European standards and procedures** to promote interoperability (cross-border, multinational) on a number of domains, including crisis response, first-responders, border security, cyber security and EU-external missions.

4. Technology as a Game Changer

To effectively address security priorities, RTD and Innovation programmes should be attentive to:

- Critical technologies that ensure a competitive and more independent European positioning in the market;
- Disruptive emerging technologies that represent innovations but also new threats;
- Prevention technologies that follow a sound legal and ethical guidance;
- Multiple use technologies and systems that improve security and account for economic sustainability (cost sharing);

Still, the activities should build on existing capabilities and benefit the most from available components and systems. Furthermore, in order to increase the European resilience and efficiency, public pooling and sharing should be explored, including synergies with other actions and sources of funding.

5. Bottlenecks, Barriers and Opportunities

Currently, the security sector faces as **main bottlenecks** the economic crisis, the environment uncertainty and the political and regulatory difficulties. This context translates into a limited adequacy of the Secure Societies calls to the existing and future needs, in terms of affordability, flexibility and adequacy of the projects' results. A **solution** should be the implementation of structured programmes defined by the multiple involved stakeholders, allowing for fast track actions when needed and focusing on critical technologies.

Indeed, the lack of funding and support at the product development stage is a well-recognised **barrier** to market success in the security sector. In this case, **solutions** on procurement support might play an important role to increase the probability of market success.

In addition, different national interests, national security and legal issues, including IPR, and fragmented standardisation are considered titanic **barriers** within the European security market. Amongst relevant **solutions**, it is possible to highlight the political consensus amongst Member States that should be sought in key areas; the fostering of policy and standards in ethics and privacy-by-design that should be primary requirements for technology development in order to attain societal acceptance and use case implementation; and the need for Europe to drive international standards.

In conclusion, EU regulation activity is perceived as the **opportunity** to create solutions for existing bottlenecks and barriers, carefully considering the social acceptance dimension. In the long-term, European regulation, ethics and standardisation would become an added-value with respect to non-European technologies as well as a competitive advantage in export markets that are not yet mature.

6. Leveraging the EU Knowledge Base for Innovation

The **strongest potential** to leverage the EU knowledge base for innovation in the security sector lies in the actions that require a European dimension (political support, collective commitment and critical mass) and a European technological R&D and industrial/SME capability. Continuous top-down and bottom-up approaches should be achieved by implementing both long-term vision and open calls for innovation within clusters, partnerships or platforms.

Human and social sciences should be an integral part of security activities, giving way to **fully integrated teams**. Reciprocally, **links** should also be established to other societal challenges, involving these themes' operators, industries and institutes (energy, food and water, chemical and pharmaceutical, climate change) in the security communities or platforms and vice-versa.

In the mid-term, technical, political and societal synergies should also be developed with the defence sector to effectively address **civil-military** response to EU external security challenges.

Specific actions to leverage the EU knowledge base for innovation for the benefit of Secure Societies should consider:

- **The implementation of a "master plan" or a strategic research and innovation roadmap by domain** to sensibly prioritise solutions while addressing the different markets in the security sector with different timeframes, and reserving resources for short, medium and long-term solutions.
    - The formation of clusters and European Innovation Partnerships (EIPs) in specialised areas (such as CBRNe, surveillance, identification, communications, human and social sciences, resilience, information management and cyber-security) should provide a more structured innovation model to prioritise capability needs and have innovation calls to accelerate market entry. Specialised clusters and expert communities should be involved in the definition of future work programmes and strategic research and innovation roadmaps.
- **The creation of synergies with Smart Specialisation Strategies, Structural Funds and related instruments** to overcome the highly fragmented demand and boost innovation in the public sector. Public Private Partnerships (PPPs) and Public Procurement of Innovation (PPIs) should accelerate market uptake through the established links with users (mainly public authorities and governmental organisations), which should be particularly useful when solutions are close to market and may be supplied if clear requirements and sufficient demand is expressed by the market. The generated market potential therefore will reinforce and strengthen industrial competitiveness in Europe. In other cases, research and development should still help to

reduce the risk of technologies and to benchmark competing solutions before committing to large-scale deployments (PCP). PPIs and PCPs should impact on:

  - Joint procurement of innovative solutions;
  - Better coordinated dialogue between procurers and suppliers;
  - Competence building in the public sector;
  - Coherent basis for progressive step changes to regulation, standardisation and public procurement practice;
  - Implementation of procurement contracts and final assessment of the procurement outcomes.

- **The funding of several small/medium-scale projects in synergy with large-scale projects** to accelerate results and bolster impact. Successful small/medium-scale projects should provide building blocks for large-scale projects, so that the industry is encouraged to use the results of previously developed small/medium-scale projects under the Horizon 2020 programme.
- **The support to industrial stakeholders by means of Flagship Projects** (or similar solutions) to overcome the fragmentation of the European supply chain and allow the European industry to leverage the global market opportunities for the next years. In **Flagship Projects**, large European industrial champions should create innovation with SMEs and RTOs/academia in an interoperable, scalable, secure and trustful vertical integrated supply chain focused on specific Security Missions.
- **The support to market-driven innovation actions with clear rules, attractive timescales and funding for industry and SMEs**. A percentage of the budget in each work programme should be assigned to short-term needs in form of:
  - Quick and flexible security dedicated innovation topics, in particular to address emerging threats;
  - Critical technologies ensuring the European security of supply chains and competitiveness.
- **The development of growing and effective links between R&D (RTOs and academia), enterprises (market) and end-users (potential buyers)**, where industrial stakeholders should be recognised as full partners by end-users (e.g., being involved in exercises and tests). The end-users' involvement in governmental security is a crucial point to reinforce EU policies in this field, to export the EU model abroad and to reinforce the competitiveness of the European industrial excellence. Pivotal role of RTOs is crucial in that regard.
- **The fostering of cross-fertilisation initiatives**, involving other sectors/technologies/policies by geo-clustering approaches to enable the take-up of technologies and best practices, the definition of pre-requisites for standardisation; the road-mapping at European and international levels and the transfer of policies/standards/solutions/activities from other sectors.
- **The overcoming of non-technical barriers such as certification and standards in emergency and disaster management** that still represent constraints to the introduction and acceptance of innovative technologies (e.g. unmanned systems). The lack of certification and standards represent the first barrier towards a solid industrial policy.
  - In the case of unmanned systems, whether as a tool or a threat (or both), a long-term strategic vision should be agreed. At the moment, developments are being driven by players such as Amazon, Google or iRobot. Europe should assume leadership and provide an overall vision and leadership (see eu.Robotics - http://www.eu-robotics.net/index.html);
  - Where regulations exist, there should be an effort to harmonise it across Europe and to define non-technical boundaries (e.g. ethics, privacy, safety) for the use/availability of specific technologies/components.
  - In domains such as Air Transport Information, security should be internationally harmonised and agreed upon.

- **The tackling of Intellectual Property Rights (IPR)**[3]. If the right IPR rules are not set, organisations may lose the incentive and/or interest to invest in research and development, which will compromise the long-term competitive value and sustainability of European Innovation Champions. Until the H2020, IPR rules were clear and well-accepted by participants: entities have full rights to their background and foreground IP generated within EU-funded actions. Where collaborative research took place, joint IP ownership applied. Rules of participation and model grant agreement as close as possible to the existing ones should be applied to all the instruments and no special IPR provisions should be included in the work programme. Upon the acknowledgement that there should be a fair and competitive market and pricing, these instruments should include special modalities on a case-by-case basis. In the case of IPR, there should be fair and reasonable commercial terms and only for what is necessary to exploit the foreground IP generated under the instrument.
- **The encouragement of interoperability, scalability, secure and trustful transparency between tiers** to address the security market fragmentation**.** The EU should define, develop and adopt (open) standards empowering each stakeholder to be a part of a larger integrated industrial capacity that is able to face EU (security) missions.
- **The reinforcement of cooperation with non-EU countries through different instruments.** Nowadays, the balance of defence and security spending is shifting from the West to the East, a trend that is expected to accelerate in the coming years. China and India, ranked second and fourth in 2020, respectively, are both investing in defence and security and will account for 23% of total spending of the top 20 nations by the end of the decade. Different EU programmes have addressed cooperation with non-EU countries and instruments that should be considered are:
    - Joint programmes and partnerships with emerging countries as scientific/technical cooperation (a good precursor for international export);
    - Partnerships with the USA.
- **The creation of Coordination and Support Actions (CSAs) targeted to specific countries** in order to build a strategic map preparing future joint collaborations and access to markets, following the model used in the ICT and Transport calls.
- **The assessment of international policies for non-EU markets to support exports**. In this sense, the regulation on dual use (Reg. CE 428/2009 modified by reg. UE 1232/2011) of technologies should play a key role in the near future. New policies are needed in liaison with concepts such as ethics and privacy-by-design (e.g. dual use by design).
- **The foundation of an EU body or representation in countries worldwide**, with the mission to promote and support the European industry and the overall research development capabilities of RTOs and academia.
- **The exploitation of multi-use technologies to attain synergistic effects** in terms of investments, competences and capabilities, but also with respect to market enlargement in the security and defence sectors and considering other fields such as ICT, space, transportation and health.
- **The definition of a mandatory requirement establishing that outcomes of research and development and H2020 funded programmes generate market innovation and sustainability**, in order to obtain the right value-for-money when marketing products and innovations.

[3] This paragraph is taken from "IMG-S position paper Recommendations for H2020" (R01).

7. Annex I – About Contributing Entities

EARTO represents 350 research and Technology Organisations from 23 countries. RTOs are key players in the innovation chain, bridging the gap between basic research and practical applications. The EARTO Security Research Group (SRG) is an experts workgroup dedicated to security issues, including 14 RTO's security experts discussing EU security research topics.

www.earto.eu/

The Integrated Mission Group for Security (IMG-S) is a wide multi-disciplinary European professional network bringing together experts from Industry, SMEs, Research and Technology Organisations (RTOs), Academia and End-users. It has more than one hundred entities from 24 European countries. IMG-S aims to support the European Commission and its Member States to build world-class European technological capabilities. By defining research priorities for the security domain at all levels, from fundamental research to mission capabilities and system integration, IMG-S contributes to ensure that short, mid- term and long-term security needs are addressed.

http://imgs-eu.org