MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Interagency Security Research Support System Policy of the Czech Republic for 2017 to 2023 with a view to 2030

Department of Security Research

1.4.2017

CONTENTS

POLICY FOR THE DEVELOPMENT OF A SECURITY RESEARCH SUPPORT SYSTEM

INTRODUCTION

On June 27th, 2008 the Government adopted, by its Decree No. 743, the Interagency Concept of Security Research of the Czech Republic up to 2015 (MKBV2009). It was the first complex roadmap pertaining to this agenda. It reflected on changes in the structure of the entire system of public support of research, development and innovations (R & D & I). The Concept contained a number of important subjects, which have been shaping the security research agenda so far. The list of system management principles was expanded and a dedicated link was made to the national security system. The authorities strove to enhance rational use of available scientific capacity via complementary programmes of public support and supported the idea of much wider use of bilateral and multilateral cooperation as well as socially responsible approach to the security research agenda. This Interagency Security Research Support System Policy of the Czech Republic for 2017-2023 with the view to 2030 (MKBV2017+) is well built on the above notions. Its key ambition is to develop the system – it envisages evolution rather than revolutionary changes.

On June 8th, 2015, the National Security Council adopted, by its Resolution No. 32, an extensive Evaluation Report on the implementation of the MKBV2009. Moreover, the Report stipulated a development roadmap for security research 2017+. Analyses and evaluations were complemented by other analytical texts, research papers by the Technology Centre of the Academy of Science, which drew a complex picture of the research environment in the areas of interest for the security research support, and Ministry of the Interior´s own texts developing on specific aspects of interaction between security research and the envisaged security system´s development path. 170 respondents, primarily representatives of research or user communities, answered questioners which were a part of an extensive opinion research.

The entire process started with an evaluation of the implementation of the MKBV2009. It revealed long-term challenges in respect of stability of financing, human resources, or setting of priorities outside the organisational structure of the responsible provider. The above Resolution stipulated directions of the future development, including a vision for stability, reliability, affordability, and scope of the system of security research support within the limits given by the research capacity and social needs in the Czech Republic.

Following the evaluation of the Policy, the authorities started the process of evaluating programs under the umbrella of the previous programming period. This exercise was to reveal the process of setting priorities and describe relations amongst various support instruments. These program evaluations were complemented by conclusions from the pilot run of the so-called capacity profiling of research organizations supported by the Ministry of Interior. Both the Methodology of evaluation of research organizations 2017+ as well as the Ministry of the Interior confirm the added value of evaluating highly specialized organizations supported by a particular provider; the nature of the organization concerned must also be taken into account. The list of background papers and printed matter ends with a broad research paper on security research that proposes a number of measures in domains such as international co-operation in security research, human resources development, communications and dissemination of information, or support programs. The paper is based on a broad empirical research.

For an outline of development needs as formulated by the background texts, see Annex No. 5, including synergies with measures stipulated by this Policy.

Based on the background printed matter, the authorities designed development concepts for the entire system of security research support, which were negotiated by the Security Research Advisory Committee of the Minister of the Interior (for members, see page 58). Based on these concepts, the Advisory Committee issued recommendations for the MKBV2017+. The final text is therefore fully based on the current situation, stakeholders´ preferences and on a number of other strategic documents, which pose, directly or indirectly, further requirements on the system of security research support.

The submitting authority strives to make the MKBV2017+ a „living document ", which will, despite regular upgrades, always comply with the defined principles and vision of the system functioning, which it has helped formulate. This approach is necessary to ensure at least theoretical stability of the system of security research support and its consistent reflection in other policies. That´s why the submitting authority decided to uphold the principle of portfolio management[1] and strives to introduce in the system of security research support elements of flexibility, continuous streamlining, and regular reviews. Last but not least, this Policy is a measure to improve the current situation and guarantee efficient and stable system of financing of security research.

DEVELOPMENT OF A SECURITY RESEARCH SUPPORT SYSTEM

WHY ARE WE DOING IT?

Security and innovation fields have never been this close, it is therefore right to assume that the convergence of both domains is a current social trend and not just a result of our static observations (the UK Ministry of Defence, 2014, or Steinmueller, 2013). In addition, this concerns a two-way interaction, which poses new challenges (e.g. CIA, 2017) but also promises new solutions (e.g. MSB, 2013, Envisioning, 2016). There is a strategic relationship between research and security. This relationship, however, reaches beyond mere tactical intervention, short-term operational needs, or academic research. The logical response is thus support targeted to applied security research.

In 2008, the Czech Republic became one of the few European countries that responded to this dynamic relationship with focused support of security research, development and innovations at the national level. The primary objective of this support is to gain and develop innovative knowledge, methods and technology which would enable the Czech Republic's security system and its stakeholders to face current and future challenges arising from the changing security environment. [2]

[1] It makes free use of the MoP® methodology (Axelos GBP, 2011).

[2] This concerns primarily, but not exclusively, trends which increase risks deriving from threats in the TESS spectrum (terrorism, espionage, subversion, sabotages) in different contexts and the risk of organised crime engaged in old as well as new types of crime; epidemics, risk of industrial disasters, and other large disasters or emergencies having impact on large groups of inhabitants.

In light of recent international and domestic development, this mission has been gaining momentum quickly. This is also evidenced by the relatively rare consensus across strategic and conceptual security policy materials that have repeatedly labelled security research as one of the main opportunities to enhance security. The National Security Audit (Ministry of the Interior, 2016) serves a good example of this approach. It stipulates security research as an opportunity across almost all chapters. Selected provisions of security policy documents also elaborate on specific tasks related to the management of security research support, particularly with emphasis on the need to transfer results into practice (in paricular the NBÚ, 2015, Ministry of the Interior-GŘ HZS ČR, 2013, PP ČR, 2016, Ministry of the Environment, 2015).[3] The documents complement one another and allow for multiple synergies.

The capacity to meet such wide expectations is directly linked to efficient management processes in respect of security research support management and their transformation. Entities engaged in R & D act as suppliers. The world of R & D is, however, very dynamic and its ever-changing nature will always have a major impact on all chapters of public support. The Interagency Security Research Support System Policy of the Czech Republic 2017-2023 with the view to 2030 serves a proper tool for transformation management.

WHAT ARE WE DOING?

This document provides a general framework for the systematic development of the system of public support for security research, development and innovation, as part of the official research, development and innovation policy, but implemented in favour of the Czech security system. In this context, MKBV2017 + responds to a number of dynamic changes in the setting of relevant policies, but also to changes in the external context and its long-term trends.

If designed properly, security research not only develops security forces´ capacity but also responds to the security needs of the public. Whilst security forces must develop their capabilities, both horizontally and vertically, particularly in areas such as force protection, resource efficiency, or in specialized technology and practice; the society has different needs, such as protection of privacy, availability of adequate assistance and quick response to threats, social and economic stability, availability of infrastructure services, existence of early warning systems and availability of information in crisis situations. Needs of the society and security forces´ capabilities must be reflected in the security system´ organizational structure, tasks and scope. Thanks to dynamic innovations, support of security research

In the scientific environment, security research support facilitates communication between the research environment and the users. Thanks to security related research to improve security, **research activities provide benefits to the society** and **researchers may receive stimulating financial resources on a competitive basis**. On the other hand, the fact that security research is closely connected to the research environment enables the security system to meet its own needs while maintaining know-how and secondary benefits in the home environment

[3] The broad context and the width of potential impact is also documented by the fact that security research explicitly refers to documents from areas which are, at the first glance, detached from the security policy (e.g. the Ministry of Industry and Trade, 2016 or the Ministry of the Environment, 2016).

The Czech Republic is lucky to have a large and diversified research base that has recently been dynamically developing and building new skills. The Ministry of the Interior has a number of external research tools available to them. In the 2022 plus programming period, the situation will change dramatically and focus will shift on the efficient use of these capacities. The ambition of this Policy is to adequately prepare for this situation and to continue developing synergies, instead of supporting subordinate relations between security research support on one hand and research and development policy on the other.

Many stakeholders in the security system have been increasingly more aware of the importance of research, development and innovations as part of the development of one's own capabilities. Numerous references across a range of conceptual and strategic materials in this area serve as evidence of this trend. In addition, these end-users of safety research results have become increasingly more active as partners of the Ministry of the Interior, which, thanks to their involvement, has become a provider enjoying the most advanced system of involvement of experts in activities designed to give the research support the right direction. This and other constructive partnerships need to be further deepened.

Security research is clearly an agenda at the intersection of science and security policy. It has significant limits as well as broad potential for each both of them. Let´s not forget that the tools in support of security research and the very essence of research work allow for tracking of these benefits in the medium or long term perspective. This portfolio must be managed as a part of research, development, and science policy. **Workplaces responsible for security research play a difficult role of a moderator of the exchange between users and research environment**. To do so, they must have specific competencies and tools.

Foreign experience shows a number of key issues outside direct research support, which are indispensable for successful delivery of the desired social benefits in the security area. These issues include so-called responsible research and innovations, social acceptance and impact of security technology, and security culture in research organizations. In the Czech context, we´ve been striving to develop the knowledge economy and maximize the economic contribution of R & D support. In this context, we must protect the innovation sphere against risks associated with strong economic competition. This text seeks to introduce key measures to address at least some of these challenges and to launch a dialogue on the remaining ones.

WHERE DO WE WANT TO BE?

To develop the key capabilities of the security system, Czech security research will make full use of creativity and potential of the research and innovation sector, its individual components and the partner community The authorities will develop a flexible system of **dedicated support tools** that will help research activities focus on the most important security challenges, develop new solutions or initiate **international cooperation of security research teams**.

Security research will remain at the intersection of science and security policy. The Ministry of the Interior will therefore build an **effective partnership** with a number of actors to secure its position of a facilitator and moderator between these two very different worlds. It will manage the support system adequately to maintain its social **responsibility**. These efforts have included and will include targeted concentration on sustainability of the entire security research support system and its evolutionary development.

This Policy strives to introduce and maintain high level of stability, availability, and reliability. All respective activities must be in a scope allowing for maximum impact on the target environment and the efficiency of the funds used. This implies introducing and embedding principles of proactive management, realistic expectations and adaptive review of priorities as well as of portfolio of activities that must match the range of available tools and the status of security research support system's manager, which is primarily a facilitator of the interaction between security and research environment.

What are the proposed solutions?

The proposed solution is based on the assumption that the system development so far, i.e. the dominant focus on extracting the capabilities of the research area for security purposes, has met its purpose within the external constraints. The system can become significantly more efficient, if we adjust targeting of programming tools and formulation of new tools, which had been identified as potential development direction as early as 2008. The ambition of the proposed Policy is to take advantage of the strengths of the system to suppress the potential problems arising from the development of the external context. This is an evolutionary, not a revolutionary approach, which involves efforts to gradually build and deepen the key capabilities of the support provider.

This is why this Policy must be an interagency text, which elaborates on a wide range of subjects at different decision-making levels, from access to program management to broader research policy. Based on the process described above and on a wide range of evaluation backgrounds, the material defines the following goals for the development of the security research support system:

A. Deepening the social benefits of security research support;

B. Flexible support;

C. Development of international activities;

D. Working partnerships;

E. Responsible R & D;

F. Sustainable support system.

These goals are further developed into 18 partial goals and 58 measures.

The document which you are now reading, **is not only a declaration of principles and approach to security research, but primarily a Ministry of the Interior´s (and others) roadmap to support and fully utilise the research and development potential to** continuous development of security system´s capacity and capabilities and to increase resilience of the Czech society. The chosen approach to a comprehensive security research organization structure that links all initiatives in this field into a single and seamless entity, makes MKBV2017 + a document defining the right direction and helping Ministry of the Interior, as the manager of the security research support, and other stakeholders gain better orientation in this complex issue.

DIVISION OF RESPONSIBILITIES

Responsibility for the MKBV2017 + rests upon the Ministry of the Interior which, in the effort to implement the previous Policy, has built a dedicated workplace that concentrates on security research support system´s development, including the implementation of supporting tools. The document envisages cooperation of a number of partners. Their competences and responsibilities for the individual parts of the R & D and innovation support agenda will remain unchanged. For detailed division of roles and responsibilities for individual measures, see Annex 1.[4]

VALIDITY

The Policy life span ends in 2023. Until then, the authorities will have performed a thorough review of individual measures and either draft amendments to its text or draft a completely new concept. All measures should be implemented before the end of 2022 to improve the synergies between the concept and programmes under the umbrella of the management of system of security research support. To best reflect the new system parameters embedded in the Policy, most programmes will be introduced in the second half of the Policy life span.

MILESTONES

The evolution of the public support system is principally never ending and there is no final date. However, key changes that this text seeks to introduce, must be implemented before the end of European subsidies into research and development. The Action Plan (Annexes 1 and 2) defines not only responsibilities and deadlines, but also, where appropriate, implementation milestones. This plan also serves as a basis for an evaluation of the overall implementation of the Policy. The evaluation will follow the indicators below:

- Indicator 1: Measure milestones complied with,
- Indicator 2: Measures met in line with the timetable (for the outline of milestones and schedule, see Annex 2).

Successful implementation of the Policy will be reflected in the quality of transformation process output (see Image 5 and the accompanying text), especially in the evaluation of individual programs,[5] which

[4] With the help of RASCI matrix.

[5] Program evaluation focuses on performance of the support system in the part of the portfolio defined by the programme.

derive from the Policy, and also in characteristics of the security research fields, which are going to be regularly monitored in line with the Policy.[6] The evaluation is complemented by stakeholders´ feedback.

COSTS

Similarly to the first MKBV2009, which was based on the long-term development of financing, this text builds on recent development and experience. So far, security research has enjoyed support which has allowed for implementation and stabilization of this type of support within the limits of the long-term impact of austerity measures introduced to help tackle the financial crisis. A number of strategies and concepts show a wide consensus on the need for further development and extension of this support. The range of supported subjects and their potential impact is wide (e.g. NBU, 2015, Ministry of Industry and Trade, 2016, Ministry of the Interior, 2016). Based on the above, this **Policy requires an increased budget to successfully introduce pre-defined levels of security research support under the umbrella of the national framework of support of R & D & I up to 2020**. The funds allocated to research, development, and innovations in 2017 should be around 1.24% per cent of the national budget. Financing is further developed by a partial initiative No. F.1.

SECURITY RESEARCH SUPPORT SYSTEM IN THE CZECH REPUBLIC

WHAT IS SECURITY RESEARCH?

The current and still functional definition formulated by the European Security Research Advisory Board (ESRAB),[7] envisages safety research at the intersection of the environmental, economic and social context of sustainable development. Security research means research, development and innovation activities aimed at identifying, preventing, preparing and protecting against unlawful conduct or activities with the intention to cause harm to (European) communities, human beings, organizations or structures, tangible and intangible assets and infrastructure. Security research also tackles subsequent operational activities after such threat or harm and measures to mitigate their consequences (also applicable to natural disasters and industrial accidents) (ESRAB, 2006). This definition includes the two main defining elements that characterize security research: the objectives of a wide range of security benefits and a focus on security threats.

Targeting security threats

The Security Threats List is defined by security strategies and concepts. Relevant threats can be, despite their scope and the inclusion of many sub-issues, different levels of analysis, and a range of subjects that

[6] For reference, we used the field analysis as stipulated by the Technology Centre of the Academy of Science of the Czech Republic and outlined in other background material supplied by the provider, implemented as part of the process of drafting of this concept (for details, see measure A.3.4).

[7] *European Security Research Advisory Board*

have relevance for many different threats,[8] divided to 9, respectively 10 categories. For the categories, see Image 1. The tenth (unlisted) category contains military threats that we do not elaborate on for the purposes of defining security research. However, let´s not forget that there is a close link between military and non-military threats through some horizontal subjects or through the recent conceptualization of conflicts.

It is obvious that **this is a large area of interest having complex inner dynamics,** a notion relevant to the most important security research related issue, i.e. prioritisation. At the same time, these subjects must become fully operational to properly target security research on program and project levels.[9] It is therefore recommended to expand the current range of security research parameters and add security benefits.

Targeting results to security benefits

In respect of the above definition, we should widen our analysis of security research view to also consider **benefits which are directly relevant to the catalogue of threats in order to facilitate a targeted view of priorities and stabilize them in a long term horizon**. If we define safety benefits as increased security while maintaining high resource intensity or decreasing resource intensity to secure the current level of security, it is primarily necessary to make all elements necessary to increase security fully operable. We understand the expected benefits of individual supported activities and results for security in the medium and long term as follows:

- improved planning, co-ordination and regulation (i.e. improved preparedness for crisis situations / incidents);
- increased availability of security system services (i.e. range or quality of services);
- reduced threat (i.e. limiting probability of a negative impact of a crisis situation / incident);
- streamlined early warning systems (in particular, prolonging the reaction time, increasing warning reliability);
- Improved safety of intervention teams and individuals;
- increased efficiency of interventions;
- mitigation of consequences (i.e. limiting the intensity and scale of the impact of the crisis / incident / phenomenon[10]).

[8] The security policy printed matter review identified over 90 different security issues that are relevant for the Czech security policy. See Image 1 for their categories, which are compatible with the European system (Ecorys, 2015).

[9] The problem is what to answer to a question of what should be the subject of research for the purpose of, for example, "fighting terrorism". Without further information, one can say almost anything.

[10] Due to the range of subjects and the differences in terminology, these terms will be used in the text more freely and without reference to specific context of user organizations or legislation.

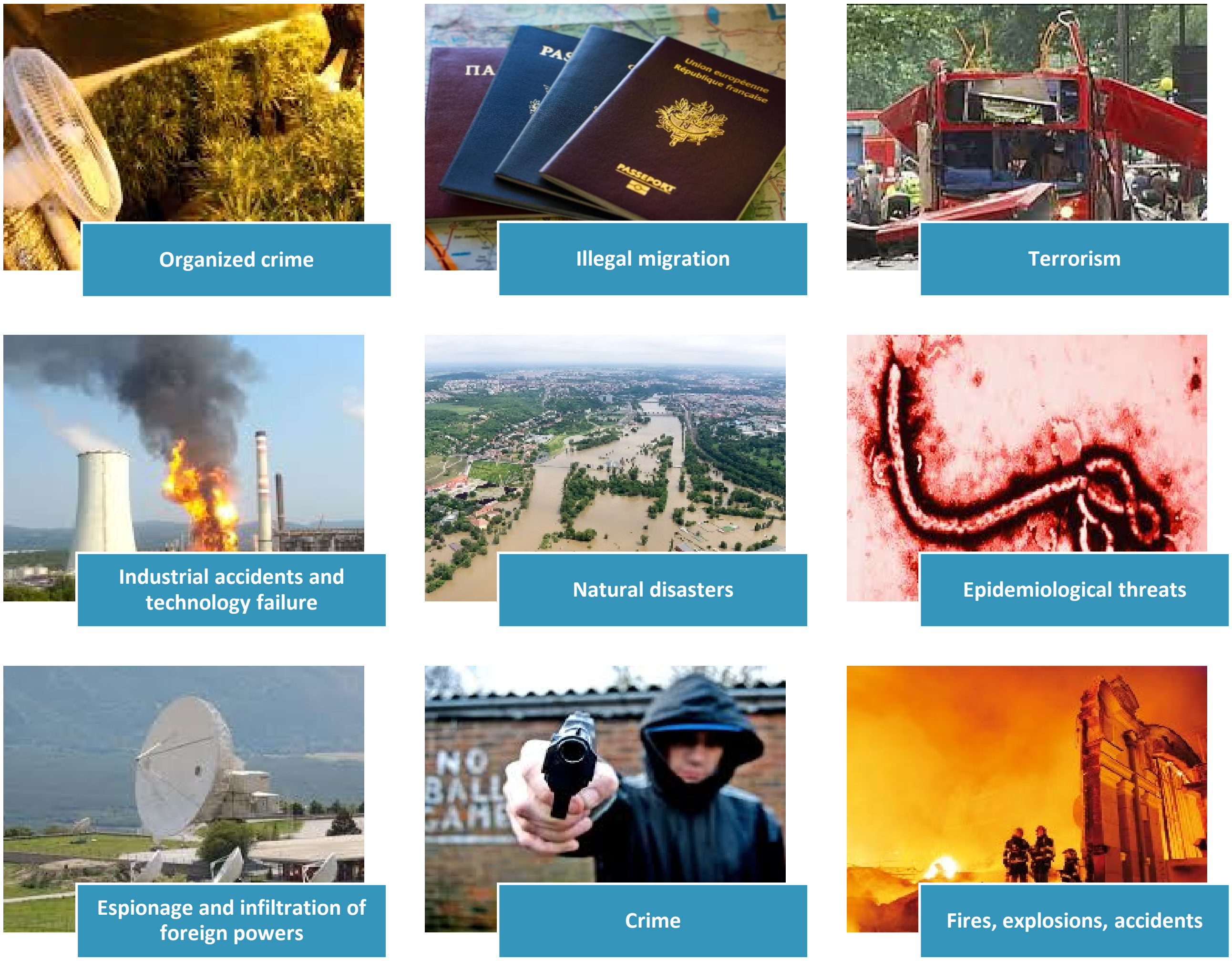

Organized crime
Illegal migration
Terrorism
Industrial accidents and technology failure
Natural disasters
Epidemiological threats
Espionage and infiltration of foreign powers
Crime
Fires, explosions, accidents

Image 1: Reference catalogue of security threats

SECURITY RESEARCH IN THE CZECH REPUBLIC: TARGETING KEY CAPACITIES

An axis of security research support priorities serves as a useful tool to help determine whether the issue falls under the area of interest. We can use the axis to outline almost all public policy issues. These issues may be further broken down to segments following their relevance in respect of individual strategic goals. This picture of overlays and interfaces also makes it possible to evaluate the focus of individual R & D support programs to reduce the risk of duplication or inefficient financing.

Priorities of security research respond to the need for long-term stabilization and emphasis on safety benefits as they are based on the Czech Republic's security system's structure and tasks. The Czech Republic's security system is the main national tool to maintain security as a public good. It also serves as a framework for research, development, and innovations programmes under the competence of the Ministry of the Interior as well as other programs, regardless of their guarantor.

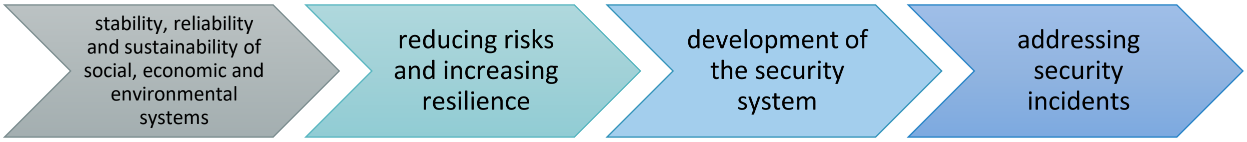

stability, reliability and sustainability of social, economic and environmental systems
reducing risks and increasing resilience
development of the security system
addressing security incidents

Image 2: Priorities of security research

The limited resources that are available to support security research in this context must be well targeted and their impact on key capabilities and deficits in the capabilities of the security system must be maximized.[11] Therefore, the exclusive responsibility of the Ministry of the Interior shall include the following priorities:[12]

- addressing security incidents,
- developing the capabilities of the security system.

The "mitigation of risk and enhanced resilience" priority is an area where we see overlapping responsibilities of individual public support providers. The Ministry of the Interior takes full responsibility of selected issues only.

Although issues, such as enhanced stability, reliability and sustainability of social, economic and environmental systems may have security elements to them, the Ministry of the Interior does not engage in focusing them or implementing their support. These issues therefore fall under responsibility of other relevant public support providers.

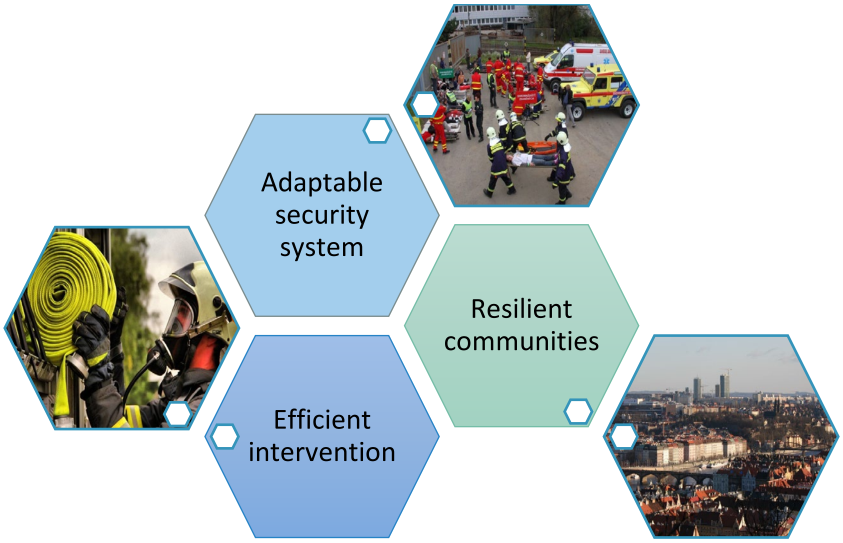


Image 3: Priority objectives of the security system

[11] It is clear that only some of them are appropriate to address research and development activities, and their role may also vary significantly in individual cases.

[12] Coordination rules are guided by Measure D.2.1.

In line with the predefined priorities, we may therefore stipulate the following long-term priorities of the security research:

1) **Efficient intervention** (an objective related to the priority of addressing security incident)
   Future intervention teams and individuals must be able to identify without any delay the threat or an existing incident, analyse the situation and respond, in the shortest time possible, adequately and in a coordinated manner; such adequate and coordinated approach is necessary both during and after the incident and must be in line with the intervention teams' responsibilities. To do this, the teams must be well trained and equipped with appropriate means and tools, including protection gear, which shall always meet all strict requirements for functioning in challenging conditions but which, at the same time, do not limit attention or otherwise hamper physical or cognitive capacity of each intervening individual.

   Under this priority objective, the following areas of interest shall be developed:
   a) Early warning and situation overview
   b) Efficient intervention
   c) Investigation of incidents
2) **Adaptable security system** (an objective related to the priority of developing of the security system)
   Predictive analysis, on-going risk analysis, modelling, simulations, and evaluation are the basis of safety considerations. The future security system will benefit from the above and translate their conclusions into regulations and planning at all levels of decision making. Individual security forces and components of the security system will develop internally and will optimize their own plans, procedures, management processes, and costs to stand ready to perform their tasks in the required quality and scope and to actively improve their performance by learning from experience. Their direction will be proactive; they will operate in an environment where critical decisions will draw on accurate, reliable, and precisely and analytically processed information from the widest possible spectrum of relevant resources.

   Under this priority objective, the following areas of interest shall be developed:
   a) Security policy and crisis management
   b) Internal capacity of the security system
   c) Security information management

3) **Resilient communities** (an objective related to the priority of reducing risks and increasing resilience
   Security has impacted our considerations in many fields, including services, the environment, and society. Our living space, communities, and key support systems have been proactively involved in measures to reduce the risk of disasters or anti-social phenomena while preserving a significant degree of risk tolerance. We´ve been developing conditions necessary to secure continuity of services, the free access to such services, and respect for the basic social values and needs of vulnerable population groups during the crisis situation or under increased threat of

anti-social phenomena in the society. Infrastructure and its critical elements as well as the public space are designed and built to resist natural disasters, accidents and manifestations of anti-social behaviour. Moreover, they allow for flexible and controlled use in times of crisis and in support of fast recovery. Proactive security control as an element of increasing resilience is tailored to handle dynamic movement of people and goods, respect human rights standards and people´s dignity. Communities affected by a major safety incident should be able to react quickly and successfully and duly minimize immediate as well as long-term or chronic consequences.

Under this priority objective, the following areas of interest shall be developed:

(a) Safe public space
(b) Infrastructure safety
(c) Environmental safety

SECURITY RESEARCH IN THE CZECH REPUBLIC – SUMMARY

The above focus of the security research is the best possible one, since it is **built on a relatively stable list of security system´s capacities and partners**, which could help solve almost any security problem. The Policy based on capacities allows us to respond to the so called Security Threat Catalogue (Image 1) and evaluate the impact of their potential, partial as well as substantial, changes on the security research support tools. It also enables us to define priorities, since capabilities of the security system are more targeted and, at the same time, constitute the primary national tool to maintain security. The much wider issue of risk mitigation, however, involves a number of partners and measures, often outside the scope of the security system. At the same time, we can define selected capabilities within this objective, which are key in the context of the above mentioned catalogue of security threats.

The viewgraph summarizing the subject matter of security research (Image 4) shows the security research broken down to the areas of interest (triangles) and provides information on hierarchy of individual priorities (the circle, priority is increasing towards the centre of the circle).

The security research area of interest can be therefore broken down to:

- Issues exclusively under responsibility of the Ministry of the Interior (inside the blue circle), targeting priority goals of "Efficient Intervention" and "Adaptable Security System" (blue fields); the Ministry of the Interior is an exclusive provider of issues which are at the core of priorities of security research support;
- Subjects of dual use (inside the green circle), targeting priority goals of "Mitigation of risk and Improved resilience"; some of these issues are under competence of the Ministry of the Interior (green fields) and the Ministry of the Interior accepts potential overlaps and synergies with other providers´ activities,
- Issues having potential security outreach from other activities; the Ministry of Interior neither supports them nor leads, for there are other adequate tools in the Czech Republic´s public space (grey circle).

Thus, the whole concept of factual definition becomes properly anchored and reasonably flexible. In line with the definition, it maintains the interagency scope of the security research and conveys a clear message of what security research actually is and what it is good for.

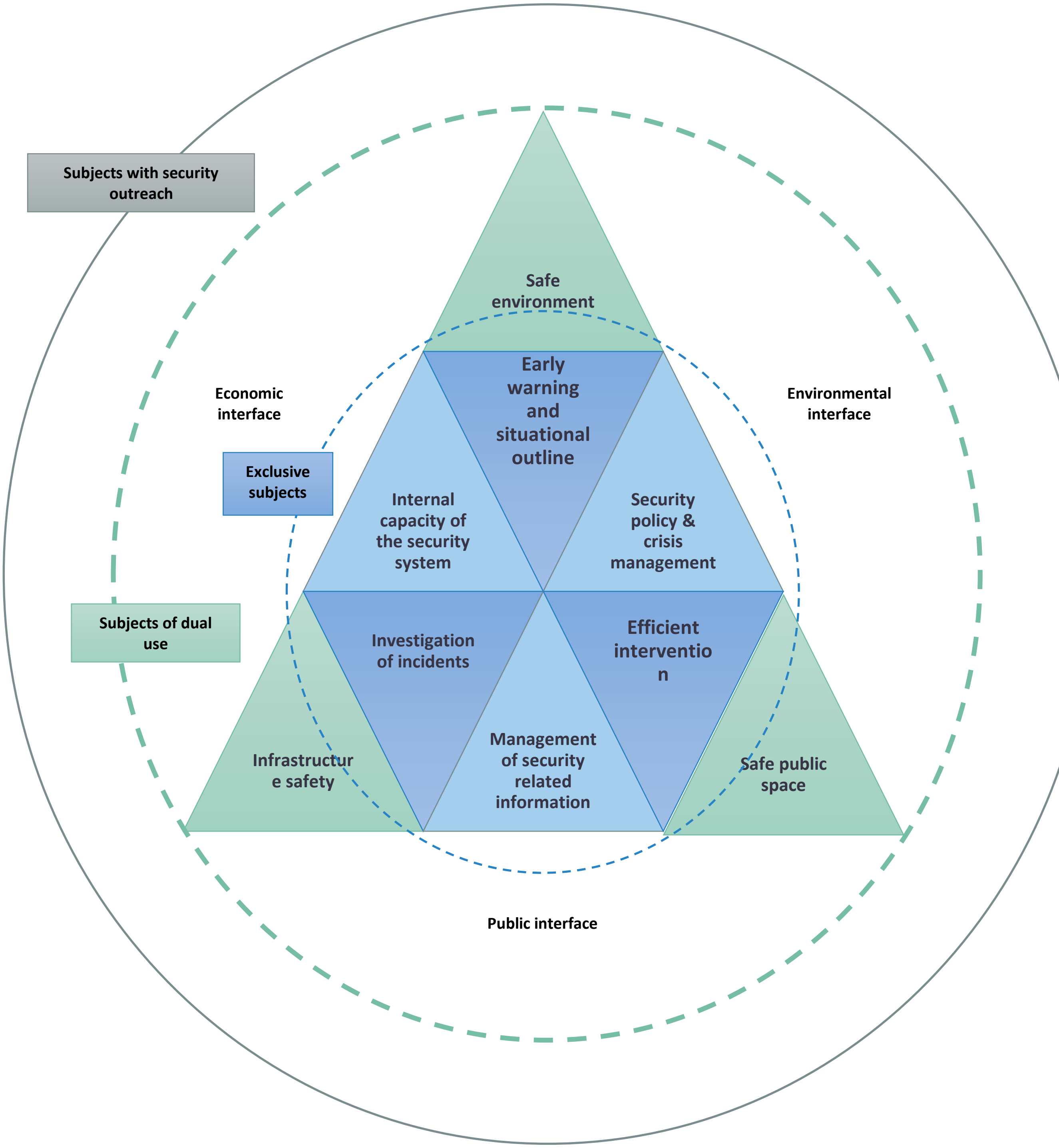

Subjects with security outreach
Safe environment
Early warning and situational outline
Economic interface
Environmental interface
Exclusive subjects
Internal capacity of the security system
Security policy & crisis management
Subjects of dual use
Investigation of incidents
Efficient interventio n
Management of security related information
Infrastructur e safety
Safe public space
Public interface

Image 4: Outline of security research in the Czech Republic

FORMAL MODEL OF THE SYSTEM OF SECURITY RESEARCH SUPPORT

DEFINITION

From the beginning, the Czech system of security research support[13] (under responsibility of the Ministry of the Interior) has been perceived primarily as **controlled financing of the development and implementation of multidisciplinary scientific and experimental research, aiming to achieve high level of expertise and technical and technological knowledge that would enable the Czech Republic to acquire, maintain and develop specific capacity needed to maintain security of the state and its population** (Ministry of the Interior, 2009).

System entries are based on the potential of targeted research activities to meet social needs. In line with the above definition, we are looking for these opportunities at the intersection of security and research policy. These concerns primarily definition of issues or subjects, relevant long-term objectives and limitations (especially financial and administrative).

The transformation process facilitating transformation of these entries into functional support tools and subsequent research projects can be divided into the following five subsystems:

1) A managed and operated subsystem management provider to facilitate efficient use of public funds for security research and development, preparation and design of support programs and their parameters;
2) A program implementation subsystem (managed and operated by the provider) for the implementation of support programs to ensure circulation, selection and implementation of security research calls and projects. The subsystem should establish rules, limitations and procedures as well as standardized project implementation;
3) A subsystem to help implement the support (managed and operated by the provider) and to directly and indirectly develop research capacity, define directions of sustainable development, support instruments and their limitations;
4) A subsystem to provide functional feedback (managed and operated by the provider) to direct and develop security research portfolio through learning from experience at all relevant decision levels;

[13] It should be noted here that terms like "security research system" are difficult to define meaningfully; on the contrary, it is necessary to explicitly separate the BV support system and the system of innovation management in the security system (or its individual parts), to which BV support can deliver inputs.

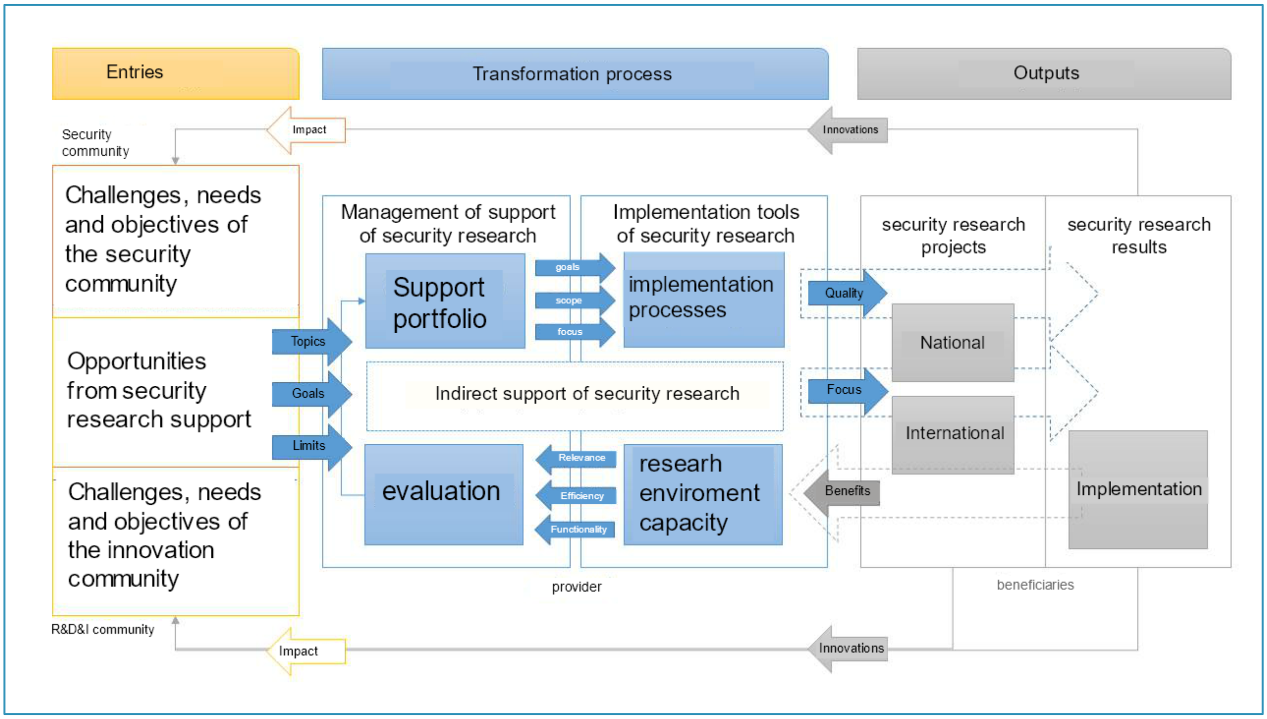

Entries
Transformation process
Outputs
Security community
Impact
Innovations
Challenges, needs and objectives of the security community
Management of support of security research
Implementation tools of security research
security research projects
security research results
Support portfolio
goals
scope
focus
implementation processes
Quality
National
Topics
Goals
Limits
Opportunities from security research support
Indirect support of security research
Focus
International
Relevance
Efficiency
Functionality
evaluation
researh enviroment capacity
Benefits
Implementation
Challenges, needs and objectives of the innovation community
provider
beneficiaries
R&D&I community
Impact
Innovations

Image 5: System of security research support

5) A subsystem of indirect support (managed by the provider and operated in cooperation with external partners) to develop quality, intensity and benefits of security research. The subsystems should help design and implement program related activities, help disseminate information and raise awareness of other activities targeted at the main stakeholder groups.

This Policy tackles the transformation process directly and influences and shapes its future functioning with the intent to maximize quality of outputs and to align its focus with the needs resulting from wider social development and its interactions with the user environment.

Outputs of the support system are in the form of security research projects, respectively their results. These projects are implemented by national or international research community, and their results strive to deliver the above-mentioned security benefits. It is achieved by implementing results of research into practice, i.e. their dissemination to end-users or further development.

The security research support system is closely connected to a myriad of subsequent systems, which can be collectively presented as innovative. They include, among others, the following:

- some elements of technology transfer (although we are mostly involved in the process of implementing the results);
- turning research ideas into reality, i.e. transforming results into true innovative products or services,
- innovation management for the benefit of the user, i.e. decisions on desirable directions for innovation, finding appropriate innovations and making decisions about such innovations, including full integration of the new technology or service into existing user practice.

Table 1: CATWOE analysis of security research support system

CATWOE		Content
C	customers	Beneficiaries
A	actors	provider and other relevant entities operating support services
T	transformation process	problems, needs and goals of owners transformed into valuable research support projects
W	world view	the R & D & I research capacity is an opportunity that can be used with a high (non-financial) added value to enhance security in the current and future context
O	owners	State
E	environmental constraints/external limits	organizational, procedural and financial constraints of R & D & I policy, research environment capacities, legal limits for security research support tools

For support system´s conceptual model, see Image 5~~Image 5~~. It is the most meaningful level of analysis based on 5 defined subsystems. It does not, however, reflect on the nature of other elements of this system as separate subsystems (such as individual programs), which are unrecognizable for this model. For the purposes of potential review of the MKBV or partial changes to the methodology, it would be appropriate to repeat the analysis with a higher level of detail (see, for example, Checkland & Scholes, 1999). An analytical description of the subject system is given in Table 1: CATWOE Analysis of security research Support System.

PERFORMANCE MEASURES

Every system based on human activity requires mechanisms of performance monitoring and rectification of detours. On a conceptual level, there are three types of indicators:

- Functionality, is the desired transformation there?

- Efficiency, i.e. costs (not necessarily financial) compared to system outputs; does the system have an added value?

- Relevance, i.e. does the system achieve long-term goals?

As part of the formal model of the security research support system, these indicators are summarized in Table 2. This performance evaluation model is transferable to individual subsystems and serves as a basis for further evaluation performed in the course of setting up the security research support system. This concerns, but is not limited to, the assessment carried out at the level of the security research support instruments.

Table 2: Security research support system efficiency

Title	Term	Contents

E^1	Functionality	Are challenges and projects implemented? If so, with what intensity?
E^2	Efficiency	What is the quality of the results and their potential impact? What are projects´ secondary benefits? (compared to costs) Is there a clear concentration of support in selected fields and objectives?
E^3	Relevance	Are outputs consistent with needs and predefined goals? Are there still some opportunities to support security research?

POLICY FOR THE DEVELOPMENT OF A SECURITY RESEARCH SUPPORT SYSTEM – OBJECTIVES AND MEASURES

A. SECURITY RESEARCH SUPPORT AND ITS CONTRIBUTION TO PUBLIC BENEFITS OF SECURITY RESEARCH

Expanding the social benefits of supporting security research and development activities is logically the first initiative of this Policy. It is clear that support for research, development and innovation may never address all security needs and problems, especially at the time of their dynamic transformation. On the other hand, in the security area we regularly observe phenomena common to the social development. For this support to be successful, it is crucial to capitalize on the opportunities offered to benefit from R & D support, i.e. to fully utilise synergies between the research capacity and the security system's needs. It is appropriate to concentrate support through various instruments to those areas, where opportunities are the greatest, so that benefits are used as efficiently as possible.

In the future, social benefits will expand thanks to two sub-initiatives:

1) Creating tools to manage security research's support portfolio, in particular by effectively prioritizing key capabilities and deficits in program development and management;
2) Effort to gradually develop the pro-innovation environment in the security system and to remove innovation constraints.

A.1. MANAGING PORTFOLIO OF SECURITY RESEARCH SUPPORT

Portfolio management requires more work. The above targets must be reflected into the support programs and not just simply accepted. This activity should be based on systematic building of our capacity to analytically process the whole security research field supported, on formative use of information obtained in the course of program design and targeted efforts for mutual synergy across all programs.

Measures:

A.1.1. Formalizing the process of drafting research and development programs

For the purposes of preparation of the new programming period, we will develop a process of prioritisation of program subjects and subjects of program challenges, thus linking deficits and needs of the security system, security trends and strong research/industry in the Czech Republic. The grid below will help coordinate programs (Image 6).

We anticipate that programs will primarily focus on projects developing **strategically important** capabilities, i.e. those that focus on developing security system **capabilities** having a long-term critical importance for the future and respecting trends and current development in the security environment. In the second most important group, we envisage projects focusing on the development of capabilities that, due to the development of the security environment, have a **high potential** for future benefits. The third priority group contains projects focusing on key

operational capabilities, i.e. those that currently are and will be in the future necessary to fulfil the security system´s mission. However, projects that develop **support capabilities**, that is, those that are relevant for security research but are not critical for it, fall in the least significant group. The grid categorizes the portfolio cutting across programs and subjects.

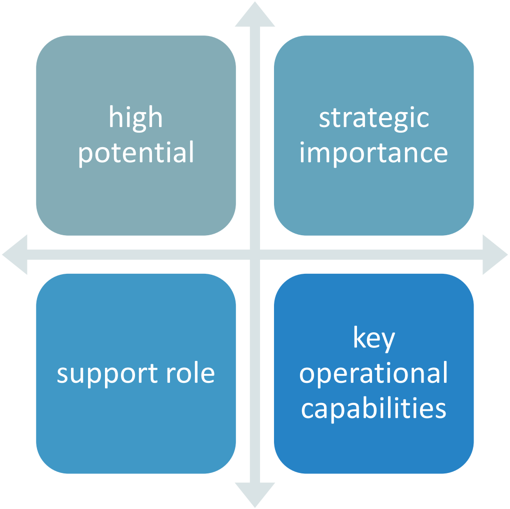


Image 6: security research portfolio categories

A.1.2. Designing research and development programmes

Identifying program objectives and targeting program challenges will always take into consideration security system´s capabilities, social needs (security threats) and the potential of scientists and the science institutions. In relation to, in particular, measure A.1.1. and E.2.1., the process of defining contents of the programs will consist of 5 separate steps:

1) Field Definition (executed in this document)
2) Field analysis (conducted by the provider in cooperation with users)
3) Program definition (sets out the programs´ objectives in terms of measure A.1.1.)
4) Definition of vertical elements of the program (sets partial targets in accordance with E.2.1)
5) Prioritization (defines final program priorities)

A.2. DEFINITION OF PRO-INNOVATION ENVIRONMENT

Innovations are primarily a feature of the security system itself (acquisition) and industry (production of what was designed). The system of support for security research in these complex relationships can neither play a leading nor managerial role, if only because the fragmented security technology market includes a wide range of industry fields and products, various targets, technology and non-technical innovations. Innovation is thus supported primarily by the development of R & D activities and sub-measures aimed at facilitating mutual communication and the transfer of knowledge and results amongst end-users, research projects and business entities - suppliers of innovations to the security system. Nevertheless, the pro-innovation environment, which allows for efficient and rapid acquisition and use of new technologies, procedures and knowledge, is considered as a necessary precondition for success of security research support and should be paid proper attention to (Ministry of the Interior, 2009).

In course of the development of pro-innovation environment, we shall therefore focus our research and development activities on specific requirements of end-users and identify barriers to innovations which must be removed. Moreover, we shall concentrate on acquiring knowledge of the security technology market and its trends relevant to targeting R & D & I cooperation with an emphasis on maximizing the use of available research results.

Measures:

A.2.1. Managing participation of the Ministry of the Interior in R & D

The Ministry of the Interior will draft a regulation of the involvement in research projects (not only in security research) of its individual departments and units as the most important end users of the research results and carriers of know-how and needs. This regulatory framework will include the process of selection, discussion, and decision on their engagement in the extent corresponding to one of the steps shown in Image 6. Individual forms of engagement will differ in respect of the demands on the relationship between those who implement the project and the user involved. The regulation should also serve as a standard for security research programs and recommendations for a wider community of users who are relevant to the security research support system

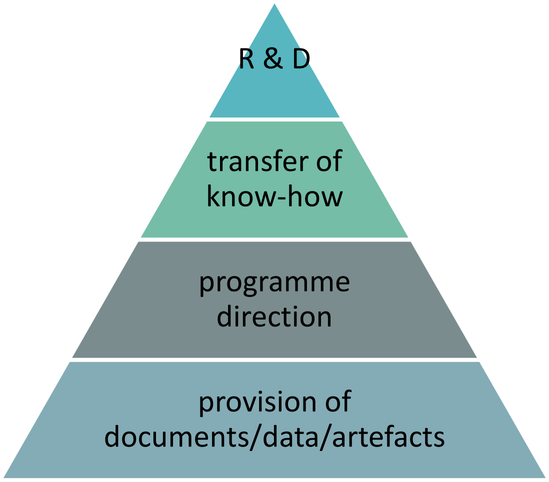


Image 7: Involvement of users in R & D

A.2.2. Innovation platform for security

The Ministry of the Interior will continue to develop, in line with the current National Policy on Research, Development and Innovation (R & D & I), the Policy of the Innovation Platform for Security as a tool to facilitate expert discussion involving all relevant stakeholders with outreach to this area of social challenges. The issue is rather extensive and the authorities will establish a support network of working groups (D.1.1.) and introduce a number of communication channels. This platform will become the central focal point to cover security innovations in respect of RIS3 and activities defined by R & D & I policy.

A.2.3. Evaluating users´ innovation management

Well founded pro-innovation environment requires proper end users´ innovation management. There is no long-term systematic development without a well-functioning system for identifying, prioritizing, securing, implementing and evaluating innovations. A well-functioning system is also a prerequisite for proper introduction of long-lasting and internationally verified tools of innovation-oriented support, whether in the form of a fund for the acquisition of specialized or small-scale products urgently needed to strengthen the capabilities of security forces, or a tool for development, testing and production support known as (PCP pre-commercial procurement), which is operable only in conjunction with medium- and long-term acquisition planning. Quality of end users´ innovation management will be monitored and evaluated after 2020 in order to support decisions on potential implementation of some of these tools and their parameters.

A.2.4. Active search for opportunities for the development of industrial cooperation

In the course of the implementation of this Policy, there will be a number of promising projects completed and ready for commercial use or further development of market-based products. Therefore, the authorities strive to actively seek and develop industrial cooperation initiatives, in particular to (1) facilitate transfer of results to potential producers, or to (2) seek other forms of commercialization of results. In this area, there is a strong synergy with the Ministry of Defence's activities, that should support the security research similarly to the Technology Centre of the Academy of Science or knowledge transfer and innovation support services that have emerged across the research sector thanks to the European funds.

A.2.5. Establishing a retroactive licensing process for the results of public R & D procurement

In line with the level of interest on the side of beneficiaries, the authorities will, pursuant to the Ministry of Defence's best practice, introduce a process of retroactive licensing of rights to output of public procurement in research and development. The use of output will require, in individual cases, an active consent of the commissioning authority (i.e. the entity whose research needs are to be solved by the research exercise).

A.2.6. Legal empowerment to support innovations in the security system

Since the state is the main facilitator and guarantor of safety as the public good, there are many considerable specific limitations the use of R & D activities to meaningful innovations if the production period is overcome. The innovation cycle of dedicated users is thus prolonged, thus reducing the potential added value for safety. There are also a number of results with great potential out of reach of the security system. It is therefore appropriate to consider not only the formulation of the PCP program (see A.2.3), but also the direct support of innovation in the security system and their integration into existing practice. This can only be done in response to adequate legal authority and to the implementation of measures A.2.3.

B. FLEXIBLE SUPPORT

The key to the success of security research's support is the ability to select and hierarchize project subjects within a range of tools that can specifically support different types of activities. Individual aid instruments must be perceived not as stand-alone resources, but as complementary elements in support of security innovations. To target programs properly, it is important to consider not only their subject matter but also their individual roles in the support instruments´ portfolio and their specifics, such as the legal title to results, potential use of results, their technological excellence, or the scope and speed of project implementation. Successful functioning requires the following:

1) use of the existing R & D capacity with the focus on its strongest elements,
2) diversification of the portfolio to include various types of programs,
3) stable support for research capacities established primarily to meet security challenges.

B.1. USE OF CURRENT R & D CAPACITY

The system of support of security research is built around the current research and development sector,[14] its capacity, human resources, equipment, organisational structure, and, primarily, knowledge and expertise. The research and development sector´s efforts concentrate into applied research and development and its orientation is strongly pro-innovation. That´s why the support to be provided in line with this Policy does not offer primarily funds into institutional development (with the exception of the highly specialized capabilities of the security system), the development of human resources, academic mobility, infrastructure construction and other goals collectively understood as development of the research area in general. On the contrary, security research offers space for meaningful and socially beneficial use of these capacities in cooperation with business entities and end users. However, in security research programs we monitor the impact on areas of interest in the context of the development of the research sector, because such impact is often there as a secondary effect of support. security research programs are thus linked to a broader set of National R & D policy objectives and not limited to those aimed at supporting applied research and development only.

Measures:

B.1.1. Development of security research monitoring

Following the experience with the implementation of supporting materials for this Policy, we plan to develop a set of permanent absolute as well as relative indicators to monitor the security research field in the following aspects:

- Financial stability and the role of security research in research financing
- Structure and dynamics of receiving entities
- Results and their quality and application
- Intensity of international cooperation in security research
- Human resources and dynamics of team involvement in security research
- Activity of infrastructure in national and international security research

[14] Business entities, respectively their innovation divisions, are also considered as elements of the research environment.

These indicators will be aggregated in the subjects under Chapter A.1, respectively, according to the factual definition, in relation to the stakeholders´ needs, following the disciplines/groups of disciplines in line with the Frascati manual (OECD, 2015), and in line with the particular type of beneficiary.[15]

B.1.2. Market research of security technology

The Ministry of the Interior, in cooperation with the Ministry of Defence, have conducted a comprehensive analysis of security and defines technology in the Czech Republic with a focus on small and medium-sized business entities and innovative companies. This analysis will help target activities in security and defines research and industrial cooperation in the right direction. The study will complement the official EU analysis to ensure comparability (e.g. Ecorys, 2015). Selected analytical method of the exercise will facilitate regular repeatability for the purposes of drafting of potential follow-up concepts (not only in the field of security research) thus providing for series of comparable analytical papers over a sufficiently long period of time.

B.1.3. Introduction of the process of monitoring global trends in technology

Respective authorities will draft a review on the future of security research, respectively one of its relevant elements. Results of the review be published in order to stir pro-innovation thinking among stakeholders. At the same time, experts will perform a review of foreign strategic analyses, which can be used in the process of program drafting as examples of best practice. Thus, the Ministry of the Interior will have an opportunity to determine whether it is worthwhile to monitor technology and social trends to manage security benefits of security research support.

B.2. DIVERSIFIED SUPPORT TOOLS

Benefits of security research support can be maximized solely in an environment of complementary support tools, which allow for support of the entire spectrum of potential types of project activities. There must be adequate selection, control, and evaluation mechanisms in place, which recognize and appreciate diversity of project attributes and solutions. Programmes under responsibility of the Ministry of the Interior by should cover the whole scale starting with the policy development all the way up to testing and evaluation of results under real conditions. Such programmes should also develop on integration of results into wider and more complex panels designed to cater to specific targets, and, potentially, even wider activities to demonstrate solutions relevant for the whole scale of capacities of interest.

For the system of support of security research to function as a meaningful portfolio, the current system based on two programmes as defined by MKBV200 shall be extended (public competition and public procurement). The two programs represent the core operational capabilities of the security research

[15] This list is indicative; we will strive to maximize overlaps with a background paper drafted for this concept and building of time path; monitoring of the security field along with program evaluations helps evaluating benefits of MKBV.

support system and the level to which the system can always return if it is not sufficiently financed. In line with the above concept, the security research portfolio will create 4 complementary targeted support programs, focusing on different types of activities and institutional support (see chapter B.3). The role of these programs in the process of concentrating support to individual categories of projects in the portfolio is summarized in Image 8.

The picture shows that three projects of strategic importance draw on support of three programme tools, which present completely different types of projects, different approach to end user involvement and varying degree of long-term interaction with projects. The same is true for projects with high potential for future benefits, which develop particular technology and approach. They are also supported from three different programming tools. Both groups of projects therefore promise a number of possibilities for development starting with applied research and ending with highly advanced product development. Projects can be either longer-term or relatively short and their results may be disseminated to users inside as well as outside the security system.

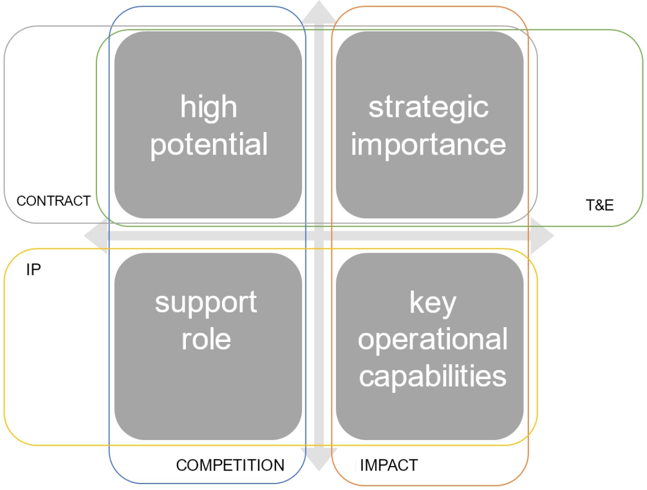


Image 8: Role of programmes in the security research portfolio

Projects targeting competencies having key importance for basic functioning of the security system draw on support from two tools only. The first tool is the institutional support. Security system is setting up research organizations to maintain some key operational capabilities. Therefore, development projects are equally relevant from this point of view as is the purpose-oriented support. Similarly, projects having a support role can also draw on support through two programs, including institutional support.

Measures:

B.2.1. Introduction of IMPAKT programme

The IMPAKT I program helps develop research capacity in areas of strategic importance for security research. However, the bulk of the support will focus on projects that are of key operational importance in the context of the current security system. We envisage implementation of 3 sub-programs of diverse activities:

- The first sub-program will support activities which require long-term interagency cooperation and/or coordination; these activities will focus primarily on integrated solutions implemented in close cooperation with users or for the benefit of international organizations.[16] Supported activities will be grouped in project clusters (programmes), and their focus, including relatively detailed content, will be developed in a roadmap which will be one of the program implementation prerequisites.
- The second sub-program responds to the need for medium and long term development of human resources (Office of the Government, 2015, see also Annex 6). We envisage that the key target group should be young post-doctoral researchers who'd be building and developing their expert teams working in areas having potential for application in the security research.
- We are also planning to implement a smaller sub-program to develop activities targeting indirect support for security research. Successful implementation of the sub-program requires initial search for new project formats and new possibilities for cooperation with end users. We may consider assessment exercises targeting specific tasks.

The requirement to launch a program pursuant to Section 6, Article (5)a of Act No. 130/2002 Coll., on the Research, Development and Innovation Support from Public Funds and on the amendment to certain acts (the Act on Research and Development Support), as amended (hereinafter only the "Act No. 130/2002 Coll.") forms an annex to MKBV2017+.

B.2.2. Introduction of T&E I programme

The T&E[17] I programme makes the portfolio capable of supporting projects, which are exceptional for their development features and significant focus on testing and evaluation in real conditions, with the objective to complete the new product together with its functional capacity. Targeting areas of strategic importance and areas of high potential should provide for high added value in terms of safety of supported results and use of the latest available technology.

This approach can have a positive impact on other goals of this Policy, notably the objective to remove innovation constraints. It can also help facilitate streamlined and informed communication between researchers and end users. The requirement to launch a program pursuant to Section 6, Article (5)a of Act No. 130/2002 Coll. forms an annex to MKBV2017 +.

B.2.3. Drafting of the follow-up programme SOUTĚŽ III

The SOUTĚŽ III programme has a double role in the portfolio. On the one hand, it supports the development of less complex technology applications in areas with high potential. On the other, it opens space for non-technical sub-projects. Similarly to the current program, the follow-up programme will focus on partial solutions and their limited integration. The public competition

[16] For example ENFSI, EDA, MAAE, OPCW, UNODA, etc.

[17] Testing and evaluation of technology, the program designation is for illustration only.

programs have a stabilizing role in the system and they are therefore expected to last longer.[18] Project duration , however, should not exceed four years so that we secure high security benefits of their results. We envisage to implement two sub-programmes

- A sub-program results of which can be disseminated freely or directly transferred to the end users
  This sub-program will serve primarily as an umbrella for subjects and ideas which are intended primarily for the public use and results of which don´t have to be checked in the light of copyright or title. Assignments will be reasonably detailed and elaborated in cooperation with end users; it would be best if they were defined individually for each call.[19]

B.3. DEDICATED R & D CAPACITY OF THE SECURITY SYSTEM

Security research in the Czech Republic builds on specialized research organizations established primarily for scientific support of selected elements of the security system. These organizations play a specific role in maintaining security (primarily fieldwork related tasks). They are also specific in the context of the research system, or better say, in the security research system, since their research activities focus primarily on strategic priorities. Their capacity and infrastructure are unique in the research sector and their permanent cooperation and coordination with the user community is also exceptional.[20] Thanks to that, this group of organizations can play a significant role in shaping the security research agenda while providing dedicated infrastructure and know-how to other research organizations. Their activity is many reasons also vital and irreplaceable outside the security system. Their continued development has thus become a security issue, too.

Measures:

B.3.1. Methodology for profiling of ministerial research institutes´ R & D capacity

In line with the text of M2017+, the Ministry of the Interior will draft a methodology necessary for profiling of research institutes in the organisational structure of various ministries. The methodology should take into consideration that institutional support targets primarily the development of research capacity, activities of each supported organization vary significantly, and all of them are closely linked to the security system. The implementation will take place in line with the roll out or the evaluation process pursuant to M2017+. The next round of profiling will be conducted in 2022. In agreement with the organizations concerned and the Government

[18] Under this measure, we plan to extent the VI program by 2 more years in order to synchronize both programs effectively and to stabilise them; the program is expected to last 8 years with a two-year overlap of the follow-up programs.

[19] A method similar to the activities of the Strategic Research Council of the Finnish Academy.

[20] These program evaluations were complemented by conclusions from the pilot run of the so-called capacity profiling of research organizations supported by the Ministry of Interior in 2016.

Council for Research, Development and Innovations, the Ministry of the Interior will consider piloting of 2022 data profiling exercise with the involvement of foreign evaluators.

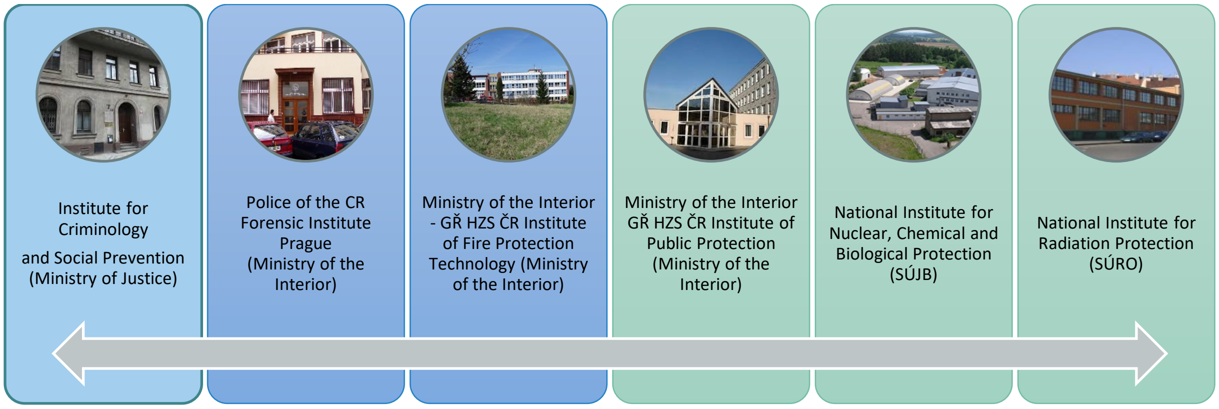

Institute for Criminology and Social Prevention (Ministry of Justice)
Police of the CR Forensic Institute Prague (Ministry of the Interior)
Ministry of the Interior - GŘ HZS ČR Institute of Fire Protection Technology (Ministry of the Interior)
Ministry of the Interior GŘ HZS ČR Institute of Public Protection (Ministry of the Interior)
National Institute for Nuclear, Chemical and Biological Protection (SÚJB)
National Institute for Radiation Protection (SÚRO)

Image 9: Specialized research institutes under the umbrella of government agencies [21]

B.3.2. Roll out of the institutional support program

To manage the institutional support at the Ministry of the Interior, we will regularly draft, in relation to the implementation of the process of profiling of research capacity of ministerial research institutes, a programme document, which will determine relations to other supported fields under the umbrella of the institutional support outside the security research. It will also provide a list of supported organisations, determine budget forecasts, and outline wider goals for the given phase (period between individual profiling rounds). The document will also serve as a background paper for negotiations with the Government Council for Research, Development and Innovation on budget allocated to the institutional support of security research, respectively, institutional support of the Ministry of the Interior.[22]

B.3.3. Priorities of ministerial research institutes´ development

[21] This concerns organizations set up by three different central administrative authorities, the term "agency" is used here as defined by the Guidelines for the Evaluation of Results of Research Organizations 2017+ (M2017 +, Office of the Government of the Czech Republic, 2017)

[22] The document is definitely necessary, if only for the fact that, besides the above-mentioned institutions, the Ministry of Interior has also been supporting one public university (Police Academy of the Czech Republic in Prague) and the National Archive, respectively the field of record-keeping. The current relatively complex situation must be regulated in the long term perspective, especially given the fact that universities are assessed separately (not with the help of agency guidelines) and the assessment is not synchronized with the sector research organizations´ support phases.

Based on the pilot round of profiling of research capacity of the research institutes,[23] which enjoy institutional support under the umbrella of the security research agenda, we have determined the following priorities (in hierarchical order) for their development activities:

1. Sustainable capacity and infrastructure
    a. Development of the organization´s human resources, respectively, cooperation on their human resources´ development in the field, including foreign internships, education and training, or higher academic qualifications
    b. Maintaining and developing infrastructure and equipment of the organization, especially specialized workplaces, which cannot be replaced by providing access to other institutions´ infrastructure
2. International cooperation in research and development
    a. Making use of extensive international contacts to initiate and extend participation in the EU Framework Programs in other fields but the strictly defined field of security research
    b. Making use of extensive international contacts to involve foreign researchers in our research efforts, including their internships in the Czech Republic
3. Public awareness and presentation of research output
    a. Planning, implementation and development of individual organizations´ communication strategies
    b. Development of tools necessary for public communication, including the development of human resources in this area or active participation at open foreign events.

To meet these priorities, we have planned, under measure F.1.1., to increase institutional support dedicated to the long-term development of research institutes and their concepts. The increased support shall be distributed in line with procedure defined by measure B.3.2. and their use shall be tied to the above priorities.

C. INICIATING INTERNATIONAL COOPERATION AND ACTIVITIES

International co-operation in security research is a world of significant and ever growing opportunities, especially thanks to the enormous support in the EU and worldwide as well as close links with the growing security technology market. This favourable trend and the well documented high potential of Czech research organizations and innovative business entities should help us broaden the range of research activities, diversify resources, or expand the scope of application for specialized workplaces. Access to foreign know-how, new partners and challenges posed by international cooperation have had a positive impact on the development of overall quality of the R & D environment. We assume that this

[23] The expert panel evaluation carried out by MV's own procedure in parameters M2017 +; priorities are based on the recommendation of 4 sector-specific panels that have been evaluated by individual organizations. However, the outputs reveal repeating elements which form the basis for such priorities.

phenomenon manifests itself even more strongly in the field of security research, especially as a result of participation in dedicated and highly specialized foreign programs.

Even though responsibility for most international activities rests with the responsible government agency (Ministry of Education, Youth and Sports), we can introduce measures to initiate, develop and sustain international activities in the field of security research and adopt and implement tasks related to the development of strategic development of international cooperation in the security research. We could, in particular, introduce measures in respect of:

1) Sustainable division or roles and responsibilities,
2) Defining areas of interest for such cooperation,
3) Continue creating conditions necessary for proper use of international opportunities, which fall outside the framework of Ministry of Education, Youth and Sports support or may complement such support, especially in areas of security research special interests

C.1. DIVISION OF ROLES AND RESPONSIBILITIES

As previously established, the Ministry of the Interior facilitates primarily, in cooperation with the Ministry of Education, Youth and Sports, international strategic negotiations concerning directions to be jointly undertaken to promote security research (especially negotiations of future direction of relevant parts of the Framework Programs). Our experience has shown that it is correct not only continue in this practice to but also deepen this principle. This strategic position should be formulated in close connection with other national security research activities to ensure complementarity.

The Ministry of the Interior further supports compliance with duties arising from international conventions and membership of the Czech Republic in expert groups and international organizations, which operate in the field of home affairs and disaster risk mitigation, with special focus on key elements of international cooperation. These commitments often include cooperation or activities in R & D.

The Ministry of the Interior has been stimulating the international dimension of security research through indirect instruments, which do not constitute R & D support. These are mainly well-targeted initiatives to help build mutual relations between research communities engaged in security research in the Czech Republic and abroad. The Ministry of the Interior also provides a stable information background and a central contact point for activities of entities active in this field.

Measures:

C.1.1. Interagency coordination task force on international cooperation in security and defines research – a joint activity of the Ministry of Education, Youth and Sports, the Ministry of the Interior and the Ministry of Defence

The authorities will establish a permanent coordination task force to meet biannually. The membership will be open to other stakeholders and the task force´s primary activities will be as follows:

- To assess international cooperation in security and defines research and protection of information,

- To evaluate the process of implementation of measures stipulated in this chapter, the relevant chapter of the Defence Research Concept and the Interagency Concept of International Cooperation, or other relevant documents,
- To design further measures to strengthen international cooperation in security and defines research,
- To examine absorption and operational capacity, objectives, and management of the programme to support international cooperation in security and defines R & D.

C.1.2. Appointing a delegate to the Programme Committee for security research in FP9

The delegate proposed by the Ministry of the Interior will be appointed by the Ministry of Education, Youth and Sports. The agencies shall act in concert and potential disagreements will be negotiated and solved.

C.1.3. Creating expert background for a delegate in H2020/FP9 for security research

The Ministry of the Interior will create and manage an expert workplace for the delegate in the extent necessary to comply with the security research focus in FP9 after it has been finally negotiated. In the course of its implementation, this measure will be tied to D.1.1 to the maximum extent possible.

C.1.4. Competences to the European Network of Law Enforcement Technology Services (ENLETS)

Responsibility for representing the Czech Republic in ENLETS will return to the Police Presidium of the Czech Republic, which is closely linked to and subordinated to the *Law Enforcement Working Party*. The extent of future involvement in ENLETS will be solely on the Police Presidium of the Czech Republic. ENLETS is not further referred to in the context security research support system.

C.2. KEY AREAS OF INTEREST IN RESPECT OF INTERNATIONAL COOPERATION

Topics meeting two equally important criteria should be in the core of the national position and the additional activity under the umbrella of the security research support system. Firstly, the identified subjects should build on the competitive national research capacity in the Czech Republic or their significant potential. If these subjects are adopted, we assume involvement of Czech entities. It is positive, that the number of competitive research entities at the national level keeps growing and we can find real synergies between the national environment on one hand and preferences and capacity of foreign partners on the other. Secondly, results of such priority activities must be applicable in the Czech Republic and must either be used by end-users or to their indirect support. They can also be used to help develop national capacity for security research in high quality comparable to that of foreign entities. Based on these criteria, past experience and expert consultations, we have defined four priority areas and sub-themes for the development of international research cooperation in security research, outlined in Image 9 below.

This list of priorities serves as a framework for the strategic position of the Czech Republic in negotiations on matters pertaining to the European Framework Programs. It also supports international activities of the Ministry of the Interior and other entities that have been developing activities within the framework of the security research support system.

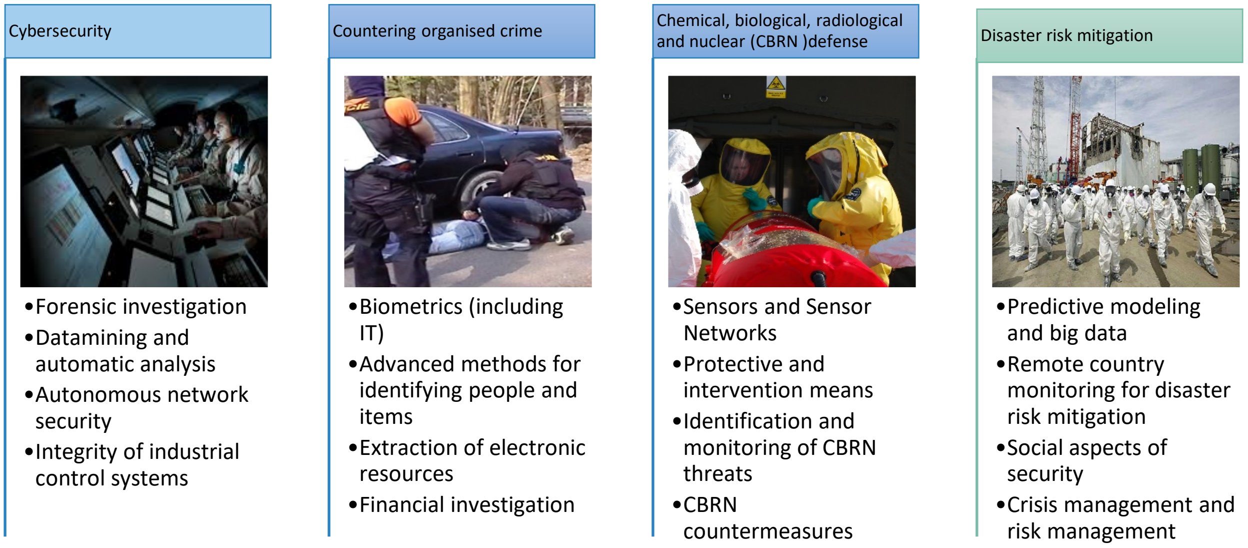
Measures:

C.2.1. Security research as a separate priority of the Interagency strategy for international cooperation (or a similar document)

The Ministry of Education, Youth and Sports will, similarly to the previous strategy, incorporate the conclusions of this chapter into the Interagency strategy for International Cooperation (or a similar document) as a separate priority. A requirement for an annual monitoring exercise will be also stipulated. This requirement should also be reflected in any follow-up activities, in particular indirect support activities for participation in EU framework programs. Such activities should be monitored and evaluated more frequently than now and the authorities shall also seek feedback from the research community.

C.2.2. Security research actively promoted as priority subject of bilateral cooperation

In their negotiations concerning future direction and focus of bilateral R & D cooperation, the Ministry of Education, Youth and Sports and other stakeholders have taken into account the fact, that security research have been given top priority in the national context. They have actively sought to include priority subjects under this chapter in their specifications of bilateral cooperation. The United States, Israel, the United Kingdom, Switzerland and the Scandinavian countries are priority partners for international co-operation in security research, France and the Netherlands are seen as good partners also in respect of disaster risk mitigation.



Cybersecurity

- Forensic investigation
- Datamining and automatic analysis
- Autonomous network security
- Integrity of industrial control systems

Countering organised crime

- Biometrics (including IT)
- Advanced methods for identifying people and items
- Extraction of electronic resources
- Financial investigation

Chemical, biological, radiological and nuclear (CBRN)defense

- Sensors and Sensor Networks
- Protective and intervention means
- Identification and monitoring of CBRN threats
- CBRN countermeasures

Disaster risk mitigation

- Predictive modeling and big data
- Remote country monitoring for disaster risk mitigation
- Social aspects of security
- Crisis management and risk management

Image 10: Priorities of international cooperation

C.2.3. Identification of other relevant international activities and active steps to involve entities from the Czech R & D sector

Our search for relevant international activities and resources has been a continuous process. We dissemination information gathered in this process primarily to the most important actors in the structure of the security research support system as well as through a platform created under the D.3.1. measure. Activities that bring synergy to the security research priorities in the Czech Republic and those which will employ strong R & D players in the Czech Republic are considered relevant. The responsible agency itself will take proactive steps or use facilitators to negotiate involvement of Czech R & D entities in identified opportunities of strategic importance.

C.3. OPPORTUNITIES IN FOREIGN COOPERATION

The main instrument for increased involvement of Czech entities in international security research is their participation in EU framework programs, which increasingly more often include issues such as security research, in which the Czech research institutes have a lot to offer. The second major tool is the support of research projects implemented in cooperation with international partners, which are under responsibility of the Ministry of Education, Youth and Sports. Participation of Czech entities in such instruments should be supported widely, especially by providing information to them or facilitating cooperation for them. Only in exceptional cases and on the case-by-case basis (in particular is the entity´s activity has a special focus or in the context of international expert cooperation of research centres focusing on security research), we can allocate ad hoc funding to allow for Czech participation in research activities carried out for the benefit of international organizations and working groups.

Measures:

C.3.1. Drafting of a list of activities under the umbrella of international cooperation programmes

Pursuant to measure C.1.1., we will draft a plan for designing or redesigning of programmes of international cooperation which would respond to the needs of security and defines related research.

C.3.2. Preparing an action plan to use tools to support scientific diplomacy to develop contacts between key security research stakeholders in priority regions

The Ministry of the Interior will initiate negotiations with the Ministry of Foreign Affairs and Office of the Government of the Czech Republic, Section for Science, Research and Innovations, in order to draft a realistic plan for the use of instruments in support of the economic and scientific diplomacy to internationalize security research in the Czech Republic. This measure should benefit from the network of science counsels stationed abroad, which we are currently establishing, and from an existing network of representatives responsible for related agendas (especially CzechInvest). Our priority partners for international co-operation in security research are the USA, Israel, the Great Britain, Switzerland, and Scandinavian countries.

C.3.3. Pilot communication activities for international cooperation

To initiate international cooperation, we should both launch new initiatives as well as redirect or reactivate the current ones. By the end date of this Policy, we will have implemented the first communication activities in cooperation with partners supporting our participation in the EU framework programs to facilitate participation of Czech entities in various consortia and to open a viable source of information on development in this area. The second group of pilot activities will be listed in the action plan under measure C.3.2.

C.3.4. Coordination of end users´ involvement in security research related projects under the EU framework programs

We will draft a mechanism for involving key end users at the Ministry of the Interior into projects within the EU Framework Programs. The mechanism will introduce a formal process and a single point of reference to handle requests for such involvement.

D. EFFICIENT PARTNERSHIP

The Ministry of the Interior must pay continuous attention to the process of building functional partnerships with a wide range of organizations and individuals. Regardless of whether this may concern internal or external partners, user community, industry stakeholders, research organizations, or service providers, the Ministry of the Interior will focus on proper targeting of security innovations instead of managing or controlling them. This means in practice that it will not dictate which activities are or are not to be implemented, but it will direct its own support into the preferred areas and manage the risk of potential overlaps of initiatives. The Ministry of the Interior is in the core of the cooperation network, it helps create proper conditions for partner activities and enables them to develop towards the objectives of the security research support system. The Ministry neither strives to assume a position at the top of the hierarchy, nor aspires to get absolute control over all activities in the areas of interest. On the contrary, its pro-development efforts focused on activities that have proven themselves as viable in the R & D & I support environment and capacity of which can be used in favour of security research.

This approach should be beneficial especially in respect of:

1) More efficient support through improved communication with end users,
2) Reduction of program related risks in security research as well as in other areas of support through targeted coordination and synergy building,
3) Exchange of information among all parties concerned.

D.1. ENHANCED INVOLVEMENT OF USERS ON ALL LEVELS

Direct communication with security personnel directly responsible for introducing new technologies or practices into practice is an irreplaceable element of the security research support system´s management. That’s why we emphasise the long-term and targeted development of tools for security personnel to be involved on various decision-making levels, from database of opponents and involvement in control activities through participation at program advisory bodies and input to program calls to broader conceptual roles at other advisory platforms. Security research, due to its close relations with the end-user community, is different from other supported areas (except for the defence research) in the national R & D & I support system. Primarily, we strive to develop partnerships with user communities in the areas of (1) law enforcement, (2) public protection and crisis management, (3) cyber security,[24] with a view to potential extension to critical infrastructure (4) areas, safety of so-called soft targets and the public space (5), and disaster risk reduction (6)[25].

[24] In close connection with the coordinating role of the National Security Authority (NBÚ) in targeting the R & D activities related to cyber security in line with the National Cyber Security Strategy for 2015-2020.

[25] We can use the National Platform for Disaster Risk Mitigation, an advisory body of the Minister of the Environment, who is responsible for disaster risk mitigation in the Czech Republic. In the field of disaster risk mitigation, this is the only platform that is part of the international platform system under the umbrella of UN ISDR.

Measures:

D.1.1. Expert advisory bodies

Through the concept of interest communities, we will develop a network of advisory bodies under the umbrella of the Innovation Platform for Security (A.3.2). Interest communities gather users as well as the most active R & D entities in the given area of interest and participate, in particular, in the process of drafting program priorities or other expert texts. There can be different interest communities´ formats with varying activities. The Ministry of the Interior will keep examining thoroughly the possibility of using existing platforms to avoid wasting of forces.[26] Under the umbrella of this measure, we will unify our approach to these communities, describe them, develop a system of their involvement in activities in respect of security research management and facilitate interaction with security innovation platform. We will initiate similar platforms to fill gaps. These groups, which will be primarily responsible for formulating directions of research efforts, will not have any design-making powers in respect of support allocation.

D.1.2. Programme committees composed of members - users

The Ministry of the Interior successfully piloted a model of programme advisory bodies composed of renowned representatives of the user community, i.e. primarily the security forces and central administration bodies. Programme councils will be organised on a under principle with the exception of areas with special orientation or programme policy. Regardless of the membership key, all members of programme councils must be strictly impartial (see Measure A.3.2.).

D.1.3. Executive branches of user organisations to be involved in the process of priority drafting

In the model of participatory formulation of programs (A.1.1., E.2.1.), we will involve representatives of the user community. There will be special emphasis on the executive branches of user organizations. Such approach should provide us a unique picture of ideal capacities and visions of their development (see Royal and others, 2014, etc.).

D.2. SYNERGY WITH OTHER ACTIVITIES IN THE INTEREST AREA

The interagency setup of security research and the already mentioned (within the primary thematic area) variety of research activities to be implemented make us search invites us search

[26] For the law enforcement purposes, we will use the R & D & I task force at the Police Presidium of the Czech Republic, for cybercrime, we have several active academic groups, and for public safety and crisis management, there are activities under the umbrella of the MV-GŘ HZS ČR.

for overlaps and synergies with other R & D actors who can enhance the security research capacity to transfer results into practice at the level of individual projects and to support further efforts of this Policy, e.g. help initiate international cooperation. An active search for these synergies is an endless process, which must at some point bear fruit and result in particular actions to capitalize on such overlaps of interest. See the viewgraph below for examples of potential overlaps with a number of R & D actors.

The previous Policy, which is still in force, envisaged high level of coordination between security and defence research. Such cooperation must be maintained and intensified. The institutional support of research institutes having complementary capabilities provided by the Ministry of the Interior, the Ministry of Defence and the Ministry of Health makes these particular ministries especially fit to seek cooperation and search for issues of common interest. The shouldn´t concentrate on targeted support only. Similarly, we can consider thematic overlaps between interest security research subjects and AV21 priority subjects, which show potential for mutual enhancement. Similarly, there are many different activities to promote technology transfer, production of research output, or other forms of their market application, where other actors may play a significant role.

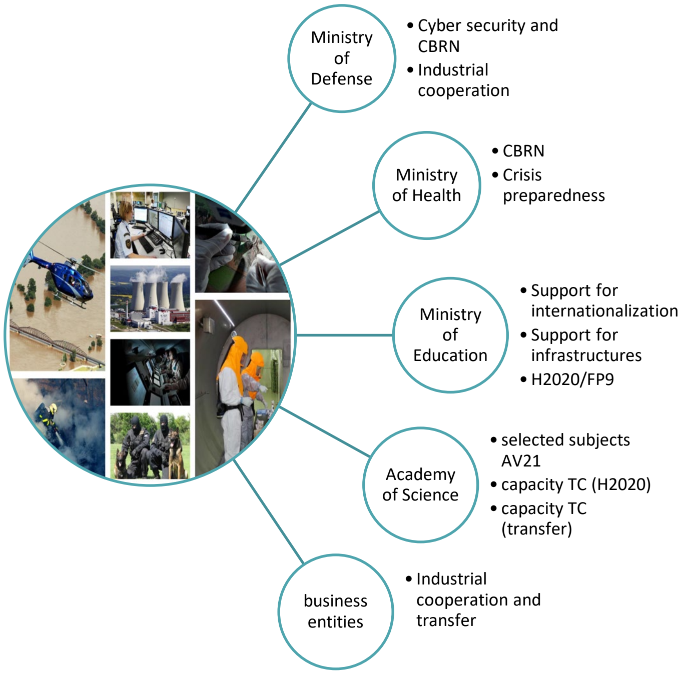


Image 11: Examples of potential overlays between security research and other activities

Measures:

D.2.1. Coordination with other providers

For the Ministry of the Interior to play the key role in coordinating security research and related issues in the context of research, development, and innovations´ support, we have decided on the following distribution of responsibilities for individual groups of subjects in line with the definition of individual security research chapters:

- Primary subjects will be fully and exclusively under responsibility of the Ministry of the Interior.
- Dual subjects, where there are overlaps with other providers, will be under responsibility of the Ministry of the Interior as well as other providers, who will be determined in programme documents.[27]
- Themes with security outreach will be outside the Ministry of the Interior´s scope of responsibility.[28]

To prevent unwanted programme overlaps, the Ministry of the Interior requires compliance with the above parameters and overlaps with its own programmes under the umbrella of the interagency rounds of comments. Program specifications must be complied with to allow for efficient use of the public budget. That´s why subjects under the umbrella of security research cannot be financed from other support tools, unless previously agreed on with the Ministry of the Interior.[29]

There is an exception from this rule: programmes and activities of the Ministry of Defence, for which the authorities plan to introduce and develop a more intense coordination regime.

D.2.2. Proper definitions of results

To maximise benefits from any dedicated research, we must concentrate on results which respond to needs and conduct of the user environment. To maximise benefits from security research support (and to facilitate stronger involvement of social and other science), it is recommended to introduce the following changes to the result definitions:

- With results H_{konc}, we should remove the limiting request for a link to the R & D & I policy, which prevents wider use of research results in the course of implementation of various agency policies. We should also depart from the principle that a project may be implemented solely via public procurement, which is absolutely unsubstantiated.
- On the other hand, with H_{leg} results, we should introduce a limiting principle, that a project must be implemented solely via public procurement, because such results are closely related to the legislative process and its specific nature. The end user, which must participate on the project from the very beginning to ensure success of the activity, is

[27] For a subject to fall under the responsibility of the MV, it must meet at least two of the following characteristics: a subject targeting a BV related target in this subject area (resilience building), strives to deliver one or more BV related benefits, or prevents security threats /risks (see subjects under the umbrella of BV).

[28] Such subjects are to be found primarily in the areas of safe industry and transport processes, safety of means of transport, protection against environmental damage and environmental impact of industrial production, material engineering, occupational safety (other than security services), etc.

[29] Apart from duplicity, the main argument is that security issues are fully dependent on the expertise of end-users who put research results into practice. The low awareness of the operational environment or other relevant demands poses a significant risk of inefficient funding.

also specific and realistic and binding compliance with all requirements can be secured only should be chose the public procurement regime.

- Introduce a special type of results (recommendation for public authorities), in a form of a policy paper, as one of the applied results generated by targeted support and ineligible for M1 M2017 + evaluation of entities, as it is practically the most widely used modus of presenting results of applied research in social science worldwide.[30]
- Consider introducing of an applied result in the form of "further research tools" (databases, techniques, samples, models, markers, etc.), as this concerns a so far widely ignored group of research results that are emerging across projects. These tools can be utilised by other research teams and may therefore have much wider impact on the society. In the context of the security research, these tools have had significant results, since some key issues often cannot be solved using real matter, which may be prohibited of its use restricted by international treaties and agreements. The development of models, in some cases, have gradually become a separate development discipline.

Results, which are in the secret regime, fall under a separate measure (E.1.2.), in which we also describe results in the form of a ´research paper´.

D.2.3. Synergy with current activities

Before the launch of new initiatives we prefer to fully utilise the existing tools and their capacity, especially in respect of foreign and industrial cooperation. Moreover, the security research system keeps actively seeking synergies with the wide spectrum of strategic documents of all types, which it reflects upon, to the extent permitted by missions and objectives of the security research, in the course of preparing programmes and programme calls.

D.3. FUNCTIONABLE COMMUNICATION

Thanks to the fact that R & D & I support is one of the dynamically growing areas of public support importance of which, in the context of economic development, shows a progressive trend, we have succeeded in developing a number of information platforms and tools to increase domestic and international awareness of the Czech R & D & I sector´s capacity. However, these information platforms tend to promote interests of their operator instead maximizing their information value. Currently, there are only two channels available to security research for disseminating information: the Ministry of the Interior web and the Business Journal, respectively electronic marketplaces. Supply of information on potential for involvement, results and status of projects is thus fragmented and the same is true for

[30] We proposed the following definition: The Recommendation for the public sector shall implement the original results of research and development reached by the researcher or the team they were a member of. The Recommendation shall stipulate comprehensive and theoretically and empirically justifiable proposal supported by precise guidelines of at least 3 different solutions of comprehensive and well identified public policy challenges. It shall also deliver a feasibility assessment of these options in practice, including explicit justification for the selection/recommendation of one of them. The document shall include, as its inseparable part, a review report and the end-user acceptance report.

other important information and popularization sources.[31] We should change this situation and consolidate information resources on security research, including potential for foreign cooperation. We wish to introduce a single streamlined information source which will be connected to other information and promotion platforms.

Measures:

D.3.1. Introduction of a Single information source for security research

To tackle the information deficit and fragmentation of resources, the Ministry of the Interior, in cooperation with external partners having responsibility for security research information, will draft a plan for a single information source in the online environment, which will join under one platform all information resources for both national and international security research. This measure entails drafting, implementation, and concept of the Single information source development to introduce extended functions, such as information deriving from other measures within this Policy, interaction between security research and defence research and connectivity to other information sources on the Czech research environment.

D.3.2. Dissemination of information about results

To build on measure D.3.1., we wish to present to the public the projects which have already been implemented, develop guidelines for project publicity, and allocate adequate funding from the project budget. Some project formats will include planning of interactions with users (Vauhkonen, 2016) as one of the typical project activities.

D.3.3. Comprehensive approach to security research and its presentation

We shall create a comprehensive strategic approach to security research presentation including visual identity of security research as a whole as well as individual programmes. The comprehensive approach will guide all public activities related to the security research, especially to the design of the single information source (D.3.1.). After having finalized comprehensive strategic approach and the single source, we will launch an active presentation of security research, which will contain regular online bulletin, publishing of security research latest news from home and abroad and presentation of Czech security research related data. This presentation initiative will be implemented in cooperation with partners within the public administration as well as others.

E. RESPONSIBLE RESEARCH AND DEVELOPMENT

Security research is a sensitive area in respect of ethics (potential misuse of results for unlawful ends, a wider issue of legitimacy of certain aspects, and responsible R & D management) as well as non-standard approach to presentation of results. Contrary to the common practice in the academic environment,

[31] This deficit is to a wide extent covered also by the current version of the Public Protection Strategy.

where research results are proudly presented to the wide audience, security research results tend to hidden and, moreover, actively protected so that they can generate results as expected by the end user. The sensitive nature of the security research means special requirements on targeting, performance, administration, evaluation, and use of security research results. Due to this special regime, the system of security research support will be always perceived as rather enclosed and secretive. That´s why we should pay special attention to the following:

1) Security aspects of R & D,
2) Agenda of responsible research and security and ethical aspects related to support of security research in general.

E.1. SENSITIVE RESEARCH

For drafting purposes, sensitive research shall mean research, development and innovation which we assume, based on our current knowledge, will generate knowledge, information, products or technology (outcomes) that could be directly misused to cause harm to the public health, agriculture, fauna and flora, the environment, or community or national security. Potential impact of such research, development and innovation may be wide and damaging or compromise national strategic security interests and methods, procedures or technology used to combat serious crime that are not in the classified information regime under a special legal instrument.[32,33]

Even though the most sensitive research activities of this kind may potentially fall within the category of classified information pursuant to Act No. 412/2005 Coll., on protection of classified information and security capacity and on the respective implementing bylaws, there is a relatively wide spectrum of activities, which cannot be included into this strictly defined category, but free distribution of their results can have significant negative consequences.[34] In the most serious scenario, such activities output be abused by groups engaged in proliferation of weapons of mass destruction or preparing for research and development of such weapons,[35] individuals or groups perpetrating cybercrime or seeking access to forensic or investigation methods. These are special categories of sensitive research, too, such as handling of crisis management related data or data necessary for early response to crises or ready access to infrastructure which serve as background information for the purposes of sensitive security or

[32] Based on a definition used in the United States (US Government, 2014); extended by a category related to other areas and areas of potential abuse; the final wording of the definition to be announced

[33] Act No. 412/2005 Coll., on protection of classified information and security capacity

[34] A separate category of such information are "special facts" under Section 27 of the Act

No. 240/2000 Coll., on crisis management and on amendments to selected other acts (the Crisis Act)

[35] It is not a completely new agenda, but the first comprehensive picture of such agenda in the Czech R & D & I policy environment; the US-based approach to its activities has been adopted by the United Nations (control regime) and the EU (CBRN Risk Mitigation Centres of Excellence). Obviously, it is well recognized and transferable example of best practice (Rychnovská, 2016).

defence research. Such data should never be revealed to teams or individuals acting to the benefit of foreign powers.

Therefore it´s high time to start debating these complex issues actively[36] with the objective to create and develop secure environment in the research sector and to support responsible approach to sensitive research and its final results. Our conduct must be based on well informed evaluation of risks and potential negative impact (National Science Advisory Board for Biosecurity, 2007). Foreign experience has shown, that is proper to follow the approach based on professional standards, guidelines and recommendations which are both prepared and complied with by the research community. Such approach is more viable than strict regulatory approach. This, however, doesn´t exclude considerations of a basic regulatory framework or its potential introduction in the future.

Measures:

E.1.1. Recommendations on approach to and management of sensitive research

Office of the Government of the Czech Republic, Section for Science, Research and Innovations, will, in cooperation with the Ministry of the Interior, set up an interagency task force of stakeholder representatives to prepare an initial report on sensitive research in the Czech Republic. The report will include the following:

- A brief description of the extent of security research in the Czech research sector;
- A risk analysis of individual fields and areas of interest;
- A description of foreign practice;
- A concept of regulatory measures;
- A description of minimum standards of measures to protect sensitive research.

When the task force will have completed their work, the authorities may decide to establish a permanent task force to develop this issue at an adequate level. If there will be a decision made to establish such task force, it will fall under the responsibility of the Ministry of the Interior. Should there be a Ministry of Science and Research set up in the future, the agenda will be transferred to this newly established agency.

E.1.2. Revised approach to addressing classified information in the R & D & I policy

At their earliest convenience, the authority responsible for the concept of definitions of research institutes´ results will draft comprehensive guidelines for handling of R & D output protected under Act No. 412/2005 Sb., on protection of classified information and security capacity, as amended, or under other legal instruments as stipulated by the dedicated regime of handling sensitive information. The guidelines will stipulate at least the following:

- In principle, in the confidential regime, we may perform research and development activities leading to any type of applied research results or other results – technical

[36] The conflict between open nature of information and free access to information as the basic academic rule on one hand and strict requirements posed by protective measures on the other add extra complexity to this issue.

output, publications or others[37], with the exception of those, which by definition cannot be presented as confidential. That means that any result may be protected in the confidential regime[38], should it comply with requirements of Section 3 of Act No. 412/2005 Coll., on protection of classified information and security capacity, and falls, for its nature, to one of the categories stipulated by the Government Regulation No. 522/2005 Coll., guiding the list of confidential information, as amended, in its full scope .[39] Results which constitute ´special circumstances´ under provision of Section 27 of Act No. 240/2000 Coll., on crisis management and on amendments of selected other acts (the Crisis Act), will be approached accordingly.

- Confidential research and development activities are implemented solely through the R & D & I support instruments under the competence of the Ministry of the Interior, Ministry of Defence and Ministry of Health. These competent providers keep protocols on classified results. Data formats must comply with requirements for transfer to R & D & I information system.
- Protocols drafted by providers in line with the above may be submitted, to the extent necessary, to authorised staff of the Office of the Government of the Czech Republic, Section for Science, Research and Innovations, responsible for budgeting and managing R & D and innovation support.
- Special provisions designed to protect results as classified information do not, in any aspect, reduce requirements for safety of results as stipulated by respective definitions. Their verification is entirely under responsibility of the provider.
- Pursuant to this measure (i.e. only should it be implemented), the definition of a result, which is now the "Research report" will be changed to the "Expert paper".[40]

E.2. RESPONSIBLE RESEARCH

Responsible research agenda[41] has been a priority for all stakeholders especially in the context of research financing. Security research is highly specific and poses numerous challenges in respect of financing. Therefore, the system of security research support cannot simply strive to widely implement

[37] Workshop, conference, etc.

[38] Unless it contradicted its defining features deriving from other legislation.

[39] Due to the interagency nature and overlaps with programmes of the providers listed below.

[40] We propose the following definition: ´A research paper shall implement the original research and development results which the author or a team of experts the author was a member of arrived at. The research paper shall provide a targeted analysis of a properly identified problem area or a specific issue. The analysis shall be based rigorous methodology. The research paper will be longer that a standard journal article, but not as long as a book. The research paper shall meet all the requirements of an expert text. The context should be standardized and include an analysis of the initial state of affairs, footnotes, and literature. An integral part of the research paper will be an independent expert review.´ This result will be used in research to meet national needs.

[41] *Responsible Research and Innovation* (RRI)

measures in support of this agenda. On the other hand, the system of security research support may promote development of responsible research and innovation in the environment of the security research. The only exception would be the *Open Access*, which cannot be reasonably developed in the security research sector. There are two of five inherent attributes of responsible research and innovation which are relevant for the security research – the role of ethics[42] in research and decision on financing of such research.[43] In these aspects, we should further develop and enhance the system of security research support.

Measures:

E.2.1. Enhanced involvement of experts in the management of support

There are many potential ways for experts to be involved in the security research[44]. So far, third parties have been involved in the security research related decision making as follows: (1) participation on decision making related to project financing in public tenders where experts acted as members of advisory bodies, and (2) participation on defining projects the in public tendering process through so called research needs. In both, participation concerns primarily the project level.

In line with the fact that the Ministry of the acts as a facilitator of the debate between the research environment and the end users, we shall strive to enhance the structured involvement of both communities in project preparation process (A.1.2.). We assume primarily involvement of security forces' staff, which do not come in contact with the R & D & I management and thus represent the expert public (D.1.). Their participation will be facilitated with the help of a concept transferred from the CASI andESPONDER4 projects. For details, see the viewgraph below.

For dual use subjects, we shall act accordingly and involve users and the public at large.

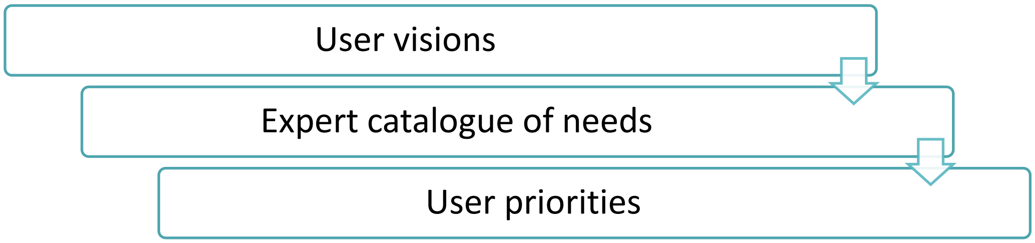


Image 12: Concept of participative decision-making

[42] We can learn, for example, from the ethical screening of project applications in the European framework programs. It is quite heavily regulated, but still allows for responsible approach of, primarily, support providers. It also serves, to a large extent, as an alternative paradigm for sensitive research.

[43] *Public engagement in R&D*

[44] For more information, see the public consultation process pursuant to the CASI project (Bedstedt, 2016) or guidelines for priority setting of the purposes of security research in the USA, Responder 4 (Royal & Jennings, 2014).

E.2.2. Gender

Measures to include gender point of view will be introduced under the umbrella of elements of participative decision-making (E.2.1.). Gender related aspects will be most visible in respect of security research agenda setting, primarily in the social interface.

In the programme of institutional support, respectively in the process of research capacity profiling, gender issues remain in the centre of attention already in the pilot phase and will be a part of the subsequent methodology. Indicators for this specific criterion will be developed to allow for better and more complex understanding of situation in the organisations to be evaluated.

Gender related issues will be most visible within the IMPAKT programme. The Ministry of the Interior has been promoting, on a long term basis, higher involvement of women in all activities and it will continue doing so in the future.

E.2.3. Ethical screening

To enhance the current requirement for ethical conformity of projects, which operate with human or animal element, we plan to introduce an ethical screening with the objective to identify projects which pose a threat of potential abuse of results or know-how for criminal purposes or in the context of which we can expect higher risk of negative impact on the society. In their evaluation, users will develop on the level of risk and protection against such risk of criminal abuse and aspects related to the potential impact on the society will be under responsibility of the programme council. Screening methodology will be based on potential risk analysis and proportionate measures in case of an increased level of risk.

E.2.4. Open access

Pursuant to the Czech National Strategy for Open Access to Scientific Information for 2017-2020, security research may opt for an exemption from the duty to introduce Open Access into supported projects. This exception will be assessed in the framework of the interim report on the implementation of this Policy with a view to finding options for selective application, e.g. in relation to the current recommendations for the sensitive research. It is obvious , that there is a number of subjects in the security research field, in which partial (or within a certain community) or full enforcement of the Open Access principles would deliver positive results. On the other hand, there are major security risks that must be taken in consideration.[45]

F. SUSTAINABLE SUPPORT SYSTEM

The entire security research system is very broad, highly specialized, and, to a great extent, unique and specific. As such, it poses high demand on logistics and organisation, processes, resources and information. The support can be flexible primarily thanks to the existing R & D facilities and the

[45] We plan to implement this measure in cooperation with the working group at the Technology Centre of the Academy of Science of the Czech Republic.

competition for spare capacity. That’s why we need to engage in a long-term monitoring of this field, secure its long-term financial stability and progressive streamlining of internal processes with the aim to maintain and develop high quality research workplaces without which the security research support system in the framework of the security research agenda and the acquisition of new experts and scientists with high potential in terms of quality and originality would not be possible. On the other hand, security research as a highly sensitive field requires careful selection, supervision, and evaluation, as these processes are essential for the provider's ability to achieve (in particular programme related) goals.

To sustain the system of security research support, the Policy proposes initiatives in the following fields:

1) Long-term financial planning,
2) Increased efficacy of administration,
3) Learning from experience,
4) Development of evaluation.

These initiatives should help us stabilize the system, develop it systematically, and reduce risks in the portfolio. User as well as partner comfort should increase substantially.

F.1. ADEQUATE FINANCING

Security research, for its high degree of specialization, the crucial role played in its implementation by ministerial research organizations (not only the Ministry of the Interior´s capacity) and the relatively high number of research organizations involved in comparison to the handful of small and medium-sized business entities, must draw its financial support with two important aspects on mind. Firstly, financial participation will relatively low, and, second, absorption capacity will be limited. That´s why security research requires, for the efficient functioning of the system, stable financial forecasts and the ability to respond systematically to portfolio fluctuations, in particular at the level of program challenges and subject changes. By all means, proper functioning of the system requires more than mere financing, it won´t work without its proper and meaningful allocation. Nevertheless, it is necessary to keep increasing the budget and maintain a stable flow of financing not to lose high quality research capacity.

Measures:

F.1.1. Budgetary framework

The budgetary framework respects the limitations of the public budget, but takes into account the range of tasks and subjects of the security research support system. The optimal level of financial security is at CZK 900 million of annual targeted support (given the current R & D & I total budget) and CZK 135 million in annual institutional support (if we plan to finance over 50 per cent of research related costs incurred by the supported organizations). The key goal of this measure is to achieve the above financing level and to stabilize financial flows in the long term horizon.

Table 3: Financial forecast of security research support

	2017	2018	2019	2020	2021	2022	2023
purpose-oriented support for security research	500	740	800	880	880	880	880

in total	000	000	000	000	000	000	000
security research in total	568 176	883 321	946 047	1 028 828	1 031 665	1 034 558	1 038 509
Share of the Ministry of the Interior R & D & I related to the security research	1,74 %	2,53 %	2,74 %	2,98%	2,99%	3,00%	3,01%
Share of the Ministry of the Interior on the purpose-oriented support	3,07 %	4,26 %	4,53 %	4,99%	4,99%	4,99%	4,99%

F.1.2. Risk management 1 (triggered by: lower relative budgetary coverage of security research)

The 2009-2015 evaluation displays budgetary instability and a decline in financing of security research. Requirements on security research, on the other hand, increased. This is the key risk also for the upcoming periods and as such, it must be managed. To that end, we stipulated the following levels of overall relative support for security research and measures in case of non-compliance:

% of security research in R & D & I chapter of public budget	**Coverage**	**Measures**
> 2,5 %	Full	Support implemented to the extent that it covers the full range of subjects of dual use.
2 % - 2,5 %	Sufficient	Support implemented to the extent that it includes the full range of primary security research subjects and a part of the range of subjects of dual use (infrastructure protection, public space safety and future of security).
< 2 %	Basic	Support implemented to the extent covering solely the primary subjects of security research.

F.1.3. Risk management 2 (triggered by: lower relative budgetary coverage of the security research purpose oriented support)

The 2009-2015 evaluation displays budgetary instability and a decline in financing of security research. Requirements on security research, on the other hand, increased. This is the key risk also for the upcoming periods and as such, it must be managed. To that end, we stipulated the following levels of overall relative support for security research and measures in case of non-compliance:

% of target oriented support in	**Coverage**	**Measures**

R & D & I chapter of public budget		
> 4 %	Full	Program tools implemented in full.
3 % - 4 %	Sufficient	Program tools implemented to a limited extent, the T & E programme reduced, and the VS (public procurement) programme not fully covered.
< 3 %	Basic	Program tools limited to the basic level of the security research support system, i.e. IMPAKT and VZ (public tenders) are the only programmes to be implemented, the VS programme not fully covered and calls implemented as long as resources become available; the T & E programme not implemented.

F.2. EFFICIENT ADMINISTRATION

Support administration must always respond to the needs and responsibilities of both parties involved - providers and beneficiaries. Key parameters of the administrative process are therefore relatively hard to modify, since all provider´s responsibilities to the public budget must be met and rules for the provision of subsidies, R & D & I policy evaluation requirements, and audit trail for the regulatory bodies must be complied with (while keeping the operational costs or investments as low as possible). However, it is essential to keep simplifying the process systematically and introduce technology improvements to streamline the process. The major positive role in these efforts should play the Security Research Information System, which needs to be dynamically developed to enhance digitization and support other similar R & D & I policy initiatives. This process gets even more important in the light of the fact that the implementation of new programming tools will inevitably lead to an increased workload of the responsible entity.

Measures:

F.2.1. Human resources to work on the security research agenda

For an activity to be efficient, it must be fully implemented. Full implementation of tasks is not possible without dedicated workforce and efficient working processes. The current responsibilities on the side of the provider require a relatively strong human resources background, especially in the field of administrative and control activities, which cannot be modified to reduce necessary staff. Volume of activities keeps growing hand in hand with the growing number of supported projects, respectively the volume of aid allocated. In 2015 and 2016, we covered this deficit from the internal resources of the responsible agency.

There is a growing demand on providers´ quality and conceptual and analytical capacity and sills (especially in respect of various analyses and evaluations), which contributes to the hunt for skilled personnel. Most workplaces were understaffed and required staff increase in 2017. Now, there are sufficient human resources available to facilitate efficient functioning of security research.

The development program for the years this Policy has been drafted for envisages implementation of two new support programs and their further split to sub-programs. Such exercise will require increased program management activity. Therefore, we will need to add four more service positions of program managers. The increased volume of aid to be distributed will require enhanced financial control and generate more administrative and control tasks. For that reason, it will be necessary to add three more service positions.

Year	**2017**[46]	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**
Personnel	+4	+7	0	0	0	0	0
Total	21	28	28	28	28	28	28

A.1.1. Risk management 3 (triggered by: new scope of provider´s responsibilities)

Personnel requirements are based on eight years of the provider´s experience from implementation of interagency and interdisciplinary programs of R & D & I support. The requirements reflect the current provider´s responsibilities. Personnel requirements may change in case provider´s responsibilities changed as a result of implementation of public tenders in R & D & I, which have been and will remain the key tool of allocation of support to security research or should there be more extensive financial control introduced.

- The new requirement beyond the framework of measure F.2.1. should the system introduced processes adequate to administrative procedure in public tendering process in a scope wider than in 2016 is plus 2 service positions in the specialized field of service (in the year following after the year of change);
- The new requirement beyond the framework of measure F.2.1. in case of more extensive financial control is plus one service position in the specialized field of service (in the year following after the year of change)

A.1.2. Transition to a new security research information system

The key measure to improve procedures is the new security research information system. This system is not only a big step forward to streamline and simplify administrative processes of all stakeholders, but also a precondition for increased and improved absorption capacity of provider's organisation to implement new programme related tools.

The new security research information system should facilitate the following capacity on the side of the provider:

[46] Implemented in relation to the Government resolution No. 477/2016 to the draft security research budget for R & D & I for 2017, with the view to 2018 and 2019.

- parallel asynchronous competitions having different document and work related parameters,
- support of all participating roles throughout the project and program lifecycle,
- digitization of the process of managing changes and other communication between the provider and the beneficiary
- maintaining the audit trail for projects and programs,
- connectivity to the record-keeping service of the Ministry of Internal Affairs and the R & D & I information system (in particular the Central database of research, development and innovation projects)
- interface to measure D.3.1.

A.1.3. Database of experts

The database of experts will become an integral part of the new security research information system. It will include a feature enabling an automated pre-selection of opponents for individual events, an algorithm for evaluating key performance indicators of the opponent's activity, and a monitoring tool to increase reliability of expert opinions. The program administration will be partially digitized and job contracts will be automatically processed.

A.1.4. Publication of key data on public procurement

In respect of above measures (D.3.1. and F.2.3.), the authorities plan to significantly simplify and streamline the process of dissemination of information on calls to all stakeholders, especially to the authors of drafts and bidder´s organisations, to the Central database of projects, and to the public. The minimum requirement is an automated process of submission of opponent reports and publication of key statistics on the calls in every stage of its implementation.

A.2. LEARNING FROM EXPERIENCE

Any system will be sustainable only should it keep developing at least as dynamically as the changes of the context in which the system exists. One of the key tools of organisation development is learning from experience. Any organisation, which can learn from its success as well as mistakes can use its full potential. We must keep in mind, however, that the learning process must peak with an action and that it is not enough to just identify the problem or its cause. An on-going process of learning by experience requires a functioning structure, process, and tools necessary to identify, analyse, and use information on processes, activities, tasks, resources, and risks faced by such organisation.

Measures:

A.2.1. Review of contractual terms and conditions of support allocation to research, development, and innovations across the entire spectrum of providers

To improve the entire R & D & I support policy in the security field, we must both adopt crosscutting measures as well as learn from the implementation of the individual regulatory instruments. Therefore, we must develop an analysis of contractual terms and conditions across the entire spectrum of providers, including an assessment of experience gained from each of the respective instruments. The analysis will summarize our past experience, risks and minimum requirements for the grant agreement. The grant agreement should pose minimum administrative burden for the research entity and allow the provider to comply with all regulatory requirements. We will emphasise a maximum level of digitization of all necessary aspects of contract management and monitoring of the contractual relationship.

A.2.2. Introducing a process of learning from experience

The process of learning by experience, which has been so far applied only ad hoc, will be formalized. The guidelines will stipulate the process, tasks and competences, process objectives, and benchmarks. The guidelines will be based on a dedicated NATO standard (Eaton, 2016).

A.3. EVALUATION

The monitoring and evaluation culture is being systematically developed within the entire security research support system. However, the diversity of subjects, benefits and efficiency measures that can be applied to security research as well as the varying nature of individual projects´ focus and planned use of results, have rendered more general evaluations virtually impossible and hard to interpret. Evaluation procedures must target primarily the quality of projects. Other evaluation processes can play a formative role in the security research support system and must respect the limits posed by security research. Given the fact, that we are formulating a new approach to the security research support system which we envisage as a comprehensive portfolio, it is recommended to coordinate evaluation and reporting mechanisms and to link the activity reports with the monitoring of more holistic indicators of system development.

Measures:

A.3.1. Development of decision-making processes in programmes

In line with the ambition to continuously increase the efficiency of financing, we will develop a framework for program evaluation mechanisms based on portfolio analysis. This new tool will result enable us to sort projects to be supported more efficiently. The basis for this framework is the evaluation of the costs to benefits ratio instead of the current "project quality" based evaluation model. Opponent evaluation will become means of measuring benefits in the following aspects:

a) scientific
b) user.

Project results in these categories should be accommodated based on costs (e.g. following Davis, et al, 2009). This framework needs to be further verified with the help of historical data from VI and VH programmes. After that, the authorities will decide on its implementation or partial implementation, or it will be abandoned.

A.3.2. Unbiased programme advisory bodies

Decision making processes shall remain fully transparent. Transparency will be maintained and deepened beyond the basic framework stipulated by Section 1(21) of Act No. 130/2002 Coll. Membership of programme advisory bodies established pursuant to Section 4 (21) of the above Act, must comply with the conditions below:

- No research institutes to be nominated
- More than half of the members must represent the user community outside the Ministry of the Interior, i.e. other central public bodies, security and emergency services, professional associations or chambers, or other significant end users of results[47]
- In case of a bias on the side of any member, such member must be excluded from such advisory body[48]
- Any exceptions from these rules must be duly justified and enforced by special nature of the programme in question.

A.3.3. Development of the process of monitoring of project results

The current monitoring process will be developed into a coherent and uniform process applicable across all public procurement activities in respect of security research support. The system is designed to monitor the use of project results without having to burden beneficiaries excessively (e.g. Wooding, 2009). The process of implementation monitoring should have three phases - monitoring, evaluation and follow-up measures. The evaluation phase should include an impact assessment carried out on a sample of supported projects and with the help of case studies. We should also develop an approach to projecting implementation success to other programs and to the project evaluation. We need a similar stand-alone system for the purposes of the public procurement which requires specific implementation.

A.3.4. Comprehensive structure of evaluation documents

Security research related monitoring and evaluation reports shall have the following structure, periodicity, and framework content:

- **Interim report on the system of security research support**
    - Provides information on the implementation of the Interagency Policy of Security Research and on other responsibilities of the provider deriving from other R & D & I policy documents (especially the National policy for research, development and innovations),

[47] In the nomination process, the key aspect is the subject of the programme

[48] I.e. replaced by another member, not only excluded from the consideration on the given application

    - Issued in the middle of the implementation timetable of the Interagency Policy of Security Research
    - Contains the following:
        - Information on the process of implementation of measures stipulated by the current Interagency Policy of Security Research
        - Monitoring/final reports on support programmes, including IP
        - Information on the process of implementation of completed projects´ results (A.2.3.)
        - Information on the process of implementation of measures stipulated by the current National policy for research, development and innovations
    - To be submitted for information to the Government Council for Research, Development and Innovation and the National Security Council, via the Civil Emergency Planning Committee (VCNP),[49]
- **Evaluation report on the system of security research support**
    - A analytical background material for the following Policy
    - Issued at the end of the implementation timetable of the Interagency Policy of Security Research
    - Contains the following:
        - Information on the process of implementation of measures stipulated by the current Interagency Policy of Security Research
        - Information on the process of implementation of measures stipulated by the current National policy for research, development and innovations
        - Report on external environment trends relevant for security research (A.2.2.)
        - Report on security research environment (B.1.1. and B.1.2.)
        - Monitoring/final reports on support programmes, including IP
        - Reports on implementation of completed projects´ results (F.4.2.)
        - At least three visions of the potential development of the system of security research support
    - To be submitted for information to the Government Council for Research, Development and Innovation and the National Security Council, via the Civil Emergency Planning Committee (VCNP) to adopt the recommended solution
    - The Evaluation report on the system of security research support is to be directly followed by an amendment to the Interagency Policy of Security Research to harmonise with the adopted vision; the amendment will be debated in the National Security Council (Civil Emergency Planning Committee) and subsequently adopted by the Government.

[49] See Article 2 (f), Statutes of the Civil Emergency Planning Committee, adopted by the Government Repulsion No. 544/2014.

VIEW TO 2030

While the first MKBV2009 responded to the need for securing support for the key capacity of security research support at the operational, programme and conceptual level, this MKBV2017+ strives to consolidate and develop the already well-established and anchored system of security research support system and provide it with comprehensive ability to focus security research in the right direction with the help of a complementary system of tools which all belong to one coherent portfolio. Although our capacity of forecasting development for the years 2023 to 2030 is rather limited, we can assume that stakeholders will benefit from the experience and the new approach embedded in this Policy. We believe the system will adapt to the new reality without having to expand significantly.[50]

After 2023, we must concentrate our efforts primarily on aspects of proper interface between support and end users´ innovation management.[51] It will be a challenge to manage innovation oriented programmes and support their implementation. We assume that the spectrum of security risks will change nationally; risks posed by perpetrators of crime will change with their flexibility and ability to dynamically innovate their modus operandi using the newest development in industry, automation, and autonomous systems.

The system of security research support will be further shaped, similarly to all other systems of R & D & I support, by the end of operational programmes´ financing. The end of OP financing will introduce significant changes in R & D & I environment which will have to fight for sustainability. Targeted support should pay a significant role in this context. Last but not least, we should strive to expand international cooperation in the field of R & D & I and compete for foreign financing.

FRAMEWORK DEVELOPMENT PATHS

- Transformation of a part of programme related activities into the system of pre-commercial procurement calls, especially to develop strategic capabilities.
- Flexible re-orientation of the programmes´ direction to respond to the goals defined by this Policy while taking in consideration the output of strategic analysis of trends in the target area.
- Evaluation of the IMPAKT type projects and a new road map for the next period.
- Development of bilateral instruments of international cooperation in security research while focusing on program activities which are outside the EU Framework Programs.
- Expanding of tools necessary for implementation and protection of sensitive research as well as for development of international co-operation in this area with special focus on European partners.
- Enhanced protection of innovations (if implemented).
- Full optimization of provider and programme processes based on selected dedicated methodology (MoP®, MSP®).

[50] With potential exception in the field of international cooperation

[51] To a certain extent, this is the most challenging agenda in the context of security research support in the European context.

SECURITY RESEARCH ADVISORY COMMITTEE OF THE MINISTER OF THE INTERIOR

- Mgr. Monika Pálková, MPA, Deputy Minister of the Interior managing Section of Social and Health Security, Security Research and Program Management

- JUDr. Petr Novák, Ph.D., Head of the Security Research and Police Education Department, Ministry of the Interior,

- PaedDr. Jan Vykoukal, Head of Security Research Unit at Security Research and Police Education Department, Ministry of the Interior,

- Ing. Dana Drábová, Ph.D., Chair of the State Office for Nuclear Safety,

- Mgr. Arnošt Marks, Ph.D., Deputy Prime Minister for Science, Research and Innovations; Representative of the Council for Research, Development and Innovations,

- Mgr. Vladimir Zimmel, Deputy Minister of Justice for Criminal Policy,

- Brigadier General Ing. Miloš Svoboda, Deputy Director General of the Fire Rescue Service of the Czech Republic responsible for Prevention and Civil Emergency Readiness,

- prof. RNDr. Pavel Danihelka, CSc., Delegate of the Czech Republic to the Horizon 2020 Program Committee for "Safe Society", Member of the Advisory Committee of the Minister of the Environment, Department of Security Engineering, Mining University - Technical University of Ostrava,

- Col. Ing. Jaromír Kadlec, CSc., Chancellor, Security Information Service,

- Mgr. Marek Šimandl, MPA, Deputy Director and Security Director, National Security Authority,

- Col. Mgr. Monika Mezuliáníková, Head, Office of Projects and European Funds, Police Presidium of the Czech Republic,

- Lt. Col. JUDr. Mgr. Jan Urban, MPA, General Directorate of Customs, Representative of the Council of Security Research for National Purposes 2016-2021,

- Luděk Moravec, MSc (Econ), Department of Security Research and Police Education, Ministry of the Interior, national contact person for the European Network of Law Enforcement Technology Services,

- Mgr. Marek Liška, Department of Security Policy and Crime Prevention, Ministry of the Interior,

- Assistant professor Ing. Blahoslav Dolejší, CSc., Ministry of Defence,

- Ing. Radek Holešínský, representative of the Association of Research Organizations of the Czech Republic,

- Ing. Dušan Švarc, representative of the Association of the Defence and Security Industry of the Czech Republic,

- Retired Col. Prof. MUDr. Josef Fusek, DrSc, doctor honoris causa, Department of Military Health, University of Defence,

- Ing. Michal Pazour, Ph.D., Head of Strategic Studies, Technology Centre of the Academy of Science of the Czech Republic,

- PhDr. Miloš Balabán, Ph.D., Head of the Security Policy Centre, Department of Social Science, Charles University Prague,

- Assistant Prof. Mgr. Oldřich Bureš, MA, Ph.D., Head of the Centre for Security Studies at the Metropolitan University of Prague,

- Ing. Miroslav Chlumský, Ministry of Industry and Trade,

- Bc. Jan Schneider, Representative of the Council for Security Research Program of the Czech Republic in 2015-2020.

LIST OF ACRONYMS

AV - Academy of Science of the Czech Republic
AV 21 - Strategy of Academy of Science of the Czech Republic AV21 (document)
BRS – National Security Council
BV - security research
CBRN - Chemical, Biological, Radiation and Nuclear (Substances, Threats ..)
CEP - Central database of research, development and innovation projects
EDA - European Defence Agency
ENFSI - European Network of Forensic Research Institutes
ENLETS - European Network of Law Enforcement Technology Services
ESRAB - European Security Research Advisory Board
EU - European Union
FP9 - 9th EU Framework Program for Science and Research
GŘ HZS ČR - General Directorate of the Fire Rescue Service of the Czech Republic
HZS ČR - Fire Rescue Service of the Czech Republic
H2020 – 8th EU Framework Program for Science and Research Horizon 2020
IP – institutional support
IS VaVaI – Information system for research, development and innovations
M2017+ - Methodology of evaluation of research organizations and evaluation of targeted support programs (document)
MAAE – International Atomic Energy Agency (IAEA)
MKBV2009 – Interagency Policy of Security Research in the Czech Republic by 2015 (document)
MKBV2017+ - Interagency Policy of Security Research in the Czech Republic for 2017–2023 with outreach to 2030 (document)
MSB – Swedish Civilian Crisis Management Agency
MŠMT – Ministry of Education, Youth and Sports
MO – Ministry of Defence
MVČR – Ministry of the Interior
MZd – Ministry of Health

MZV – Ministry of Foreign Affairs

NBÚ – National Security Authority

NP VaVaI – National R & D & Innovation Policy (document)

OECD – Organization for Economic Cooperation and Development

OPCW – Organization for the Prohibition of Chemical Weapons

OSN – United Nations

OV – security research

PCP – Pre-Commercial Procurement

PP ČR – Police Presidium of the Czech Republic

RVVI – Government Council for Research, Development and Innovation

SR VaVaI – national budget for research, development and innovations

SÚJB – State Office for Nuclear Safety

TC AV – Technology Centre, Academy of Science of the Czech Republic

UNODA – United Nations Office for Disarmament

UP – purpose-oriented support

UV SVVI – Office of the Government of the Czech Republic, Section for Science, Research and Innovations

VaV – R & D – research and development

VaVaI – R & D & I - research, development and innovations

VCNP – Civil Emergency Planning Committee

VF – Program of Security Research for Public Purposes 2010-2016

VG – Security Research Program of the Czech Republic for 2010–2015

VH – Program of Security Research for Public Purposes 2016-2021

VI – Security Research Program of the C 2015-2020

VS – public competition

VO – research institute

VZ – public procurement

REFERENCES[52]

Academy of Science (2015). *Strategie AV21: Špičkový výzkum ve veřejném zájmu.* Praha: Akademie věd ČR.

(Academy of Science (2016). Strategy AV21: Top research in the public interest, Prague, Academy of Science of the Czech Republic)

Axelos GBP. (2011). *Management of Portfolios.* London: TSO.

Bedstedt, B. (2016). *How to engage citizens in definingresearch priorities?* Získáno 05. 01 2017, z Public Participation in Developing a Common Framework for Assessment and Management of Sustainable Innovation: http://www.casi2020.eu/casi-policy-conference-2016/agenda/

CIA. (2017). *Global Trends: Paradox of Progress.* Langley, VA: Office of the Director of National Intelligence.

Davis, P. K., & Drever, P. (2009). *Portfolio Analysis Tool.* Santa Monica, CA: RAND Corp.

[52] In the document, we also use photographs and images made by the Police of the Czech Republic, Fire Rescue Service of the Czech Republic and individuals who participated in the "Firemen as photographers and their objects" award in 2015 and 2016, KUP, SUJCHBO and SURO, as well as photos taken by anonymous authors and downloaded from the Internet.

Eaton, J. (2016). *The Joint Analysis and Lessons Learned Handbook (4th revised edition).* Lisabon, PT: NATO ACT JALLC.

Ecorys. (2015). *Study on the development of statistical data on the European security technological and industrial base.* Downloaded on September 25th, 2016, from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/security/reference-documents/docs/security_statistics_-_final_report_en.pdf

Envisioning. (2016). *Autonomous Defence Project*. Downloaded from envisioning.io: http://envisioning.io/deftech

ESRAB. (2006). *Meeting the Challange: European Security Research Agenda.* Brusells: European Commission.

Ministerstvo vnitra -GŘ HZS ČR. (2013). *Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030.* Praha: Ministerstvo vnitra.

(Ministry of the Interior - GŘ HZS ČR. (2013). Policy for Public Protection up to 2020 with the view to 2030. Prague: Ministry of the Interior

Checkland, P., & Scholes, J. (1999). *Soft Systems Methodology in Action.* New York: Wiley.

Ministerstvo průmyslu a obchodu. (2016). *Iniciativa Průmysl 4.0.* Praha: MPO.

(Ministry of Industry and Trade. (2016) Initiative Industry 4.0. Prague: Ministry of Industry and Trade

Ministerstvo vnitra. (2009). *Meziresortní koncepce bezpečnostního výzkumu ČR do roku 2015.* Prague: Ministry of the Interior.(2009). Interagency Concept of Security Research in the CR up to 2015. Prague: Ministry of the Interior

Ministerstvo vnitra. (2016). *Audit národní bezpečnosti.* Prague: Ministry of the Interior.

Ministry of the Interior. (2016) National Security Audit. Prague: Ministry of the Interior

Ministerstvo životního prostředí. (2015). *Aktualizace Koncepce environmentální bezpečnosti a to na léta 2015-2020 s výhledem do roku 2030.* Praha: MŽP.

Ministry of the Environment. (2015). Updated Policy of Environmental Safety for 2015 to 2020 with a view to 2030. Prague: Ministry of the Environment.

Ministerstvo životního prostředí. (2016). *Strategie adaptace na klimatickou změnu.* Praha: MŽP.

Ministry of the Environment. (2016). Strategy of adaptation to climate changes. Prague: Ministry of the Environment.

MSB. (2013). *Strategic challenges for societal security: Analysis of five future scenarios.* Stockholm: Swedish Civil Contingencies Agency (MSB).

National Research Council. (1983). *Scientific Communication and National Security.* Washington, D.C.: National Academy Press.

National Science Advisory Board for Biosecurity. (2007). *Proposed Framework for the Oversight of Dual-Use Life Sceinces Research: Strategies for minimizing the potential misuse of research information.* Bethesda, MD: NSABB.

NBÚ. (2015). *Národní strategie kybernetické bezpečnosti pro období let 2015-2020.* Praha: Národní bezpečnostní úřad.

National Security Authority (2015). National Strategy for cyber security for 2015 to 2020. Prague: National Security Authority

OECD. (2015). *Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development.* Paříž: OECD Publishing.

OSN. (2015). *Sendai Framework for Disaster Risk Reduction 2015-2030.* Sendai:*UNISDR*

PP ČR. (2016). *Koncepce rozvoje Policie ČR 2016-2020.* Praha: Ministerstvo vnitra.

PP ČR. (2016). Police Development Policy 2016 to 2020. Prague: Ministry of the Interior

Royal, M., & Jennings, D. (2014). *Project Responder 4: 2014 National Technology Plan for Emergency Response to Catastrophic Incidents.* Falls Church VA: Homeland Security Studies & Analysis Institute.

Rychnovská, D. (2016). Governing Dual-Use Knowledge: From the politics of responsible science to the ethicalization of security. *Security Dialogue, 47*(4).

Steinmueller, K. (2013). *Future Dimensions of Public Security: Security 2025 – Four Scenarios.* Koln: Z-Punkt.

UK Ministry of Defence. (2014). *Global Strategic Trends - Out to 2045 (5th Edition).* Londýn: Doctrines and Concepts Development Centre.

Úřad vlády. (2015). *Národní politika výzkumu, vývoje a inovací ČR na léta 2016 - 2020.* Praha: Úřad vlády ČR.

Office of the Government: National Policy for R+D+I for 2016 to 2020. Prague, Office of the Government of the CR

Úřad vlády. (2016). N*árodní strategie otevřeného přístupu ČR k vědeckým informacím na léta 2017* to 2020.Praha: Úřad vlády ČR.

Office of the Government: *National Strategy for open access to scientific information for 2017–2020.* Prague, Office of the Government of the CR

Úřad vlády. (2017). *Metodika hodnocení výzkumných organizací a hodnocení programů účelové podpory (verze pro meziresortní připomínkové řízení).* Praha: Úřad vlády ČR.

Office of the Government. (2017). Methodology of evaluation of research organizations and evaluation of targeted support programs *(version for the interagency round of comments.* Prague: Office of the Government (2017).

US Government. (2014). *United States Government Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern.* Washington, D.C.: US Government.

Vauhkonen, J. (2016). *Evaluation of Societal Interaction Case of Strategic Research Funding in Finland.* Downloaded on January 15, 2017, from Public Participation in Developing a Common Framework for Assessment and Management of Sustainable Innovation: http://www.casi2020.eu/casi-policy-conference-2016/agenda/

Wooding, S. (2009). *Mapping the Impact: Exploring the Payback of Arthritis Research.* Cambridge, UK: RAND Europe.

ANNEXES

1) Action plan – implementation of measures: division of responsibilities
2) Action plan – implementation of measures: timetable milestones
3) Requirement to launch the IMPAKT programme (Art. 6 (5)a of Act No. 130/20002 Coll.)
4) Requirement to launch the T&E programme (Art. 6 (5)a of Act No. 130/20002 Coll.)
5) Summary of recommendations of analytical documents and their inclusion into MKBV2017+
6) Background papers of the Technology Centre of the Academy of Science

Obrázek ze strany 18

Image 5

Entries	Transformation process	Outputs
Security community *šipka* Impact		*Šipka* Innovations
Challenges, needs and objectives of the security community	Management of support of security research Implementation tools of security research	security research projects security research results
Opportunities from security research support *Šipky* Topics Goals Limits	Support portfolio *šipka* goals implementation processes *šipka scope* *šipka focus*	*Šipky* Quality Focus Benefits
	(5) Indirect support of security research	
	Šipky Relevance Efficiency functionality~~functionality~~	Implementation
	(4) evaluation (3) research environment capacity	
Challenges, needs and objectives of the innovation community		
R&D&I community	provider	beneficiaries
Šipka Impact		*Šipka* Innovations

Obrázek ze strany 27

Image 8

	High potential	Strategic importance	
Procurement			T&E
IP			
	Support role	Key operational importance	
	Competition	Impact	