Federal Ministry
of Education
and Research

Civil Security Research in Europe

Ensuring a Secure Life for All in the Future

This paper supplements the "German discussion paper in preparation for the 10th EU Framework Programme for Research and Innovation" of the Federal Government, which was published and submitted to the European Commission by the Federal Ministry of Education and Research (BMBF) in May 2024. It is thus part of a series of papers by the BMBF that more closely address individual aspects of Germany's provisional position on the next EU Framework Programme for Research and Innovation.

European Civil Security Research must be established within the 10th EU Framework Programme for Research and Innovation (FP10) in a way that its role as a driver and shaper of innovation meets the current and future challenges civil security faces. The following conditions are essential to achieving this:

- Civil security must be considered a political priority of the 10th EU Framework Programme for Research and Innovation.

- Civil Security Research encompasses technological and social approaches and integrates these. Europe's technological sovereignty is fundamental for the European Union's civil security. Social innovations strengthen the resilience of societies.

- Civil Security Research is a key contributor to the innovative capability of security practitioners in Europe. Strengthening applied research and innovation will, in turn, substantially strengthen authorities and organisations with security responsibilities and critical infrastructure operators.

- Improved coordination of the key European Civil Security funding instruments will enable more efficient use of funding and the transfer into application.

- The digital transformation and European digital sovereignty require a continuous focus on Cybersecurity Research. Cybersecurity forms part of European Civil Security Research.

- Civil Security Research contributes to ensuring that the role of civil defence can be performed in full in the overall defence of Europe.

Civil Security Research covers a wide range of topics that need to be expanded in the coming years in order to include an applied focus on hybrid threats and on the protection of democracy. The protection of society and democracy against crime and terrorism, the protection of critical infrastructures, the safeguarding of the supply for the society, the capability to act in the event of natural and man-made disasters and cybersecurity all remain essential.

This focus paper complements the "German discussion paper for the preparation of the 10th EU Framework Programme for Research and Innovation" that was published by the Federal Ministry of Education and Research in May 2024 and submitted to the European Commission. It raises the following demand:

> *"In light of the Zeitenwende (turning point in history) and increasing geopolitical tensions, which are accompanied by hybrid threats, attacks on our critical infrastructures and rising extremism, FP10 must be even more effective in exploiting the potential of R&I to strengthen European security."*

This paper addresses the demand of strengthening European security in more detail. It does not state a position on the European Commission's Dual-Use White Paper, the content of which is being evaluated and submitted separately by Germany. Instead, it sets out requirements for future European research funding from a civil security perspective.

Security and Civil Security Research: A Need for Action and Innovation

In recent years, Europe has faced multiple challenges (including a war in Europe, extreme weather situations, transnational crime, extremism and terrorism, a pandemic, hybrid threats to critical infrastructure, fake news and disinformation, cyber-attacks, threats to democracy, issues at the EU's external borders). These challenges are not expected to fade.

Research and innovation are essential components in strengthening civil security. Civil Security Research is the basis for these innovations. The duty of protecting the people of Europe entails specific requirements which must be met. Authorities and organisations with security responsibilities, critical infrastructure operators and other system-relevant actors must, at all times, be able to respond to challenges with the latest approaches and technologies. Furthermore, they must be able to take preventive measures and, at all times, maintain a focus on the complexity of a given situation. To meet these needs, they must continue to benefit from social and technological innovations which are independently developed (and enhanced) in Europe. Our industrial players must have a constantly updated set of tools and options for action available in order to protect themselves. The population must not only feel safe but must also be equipped to actively engage in enhancing their ability to provide for themselves, to act confidently in a digital environment and to increase their resilience. This not only supports civil security in general but also makes a key contribution to the non-military element of Europe's overall defence. For this reason, civil security must be a political priority of the 10th EU Framework Programme for Research and Innovation.

Security Affects All Areas of Life: Research is Needed in a Wide Range of Themes

European Civil Security Research already covers a wide range of themes in the current research framework programme. All the issues for which research has been funded to date continue to be important and should both remain and be enhanced as an active part of European Civil Security Research. A new, visible addition should be research on protection against hybrid threats and on civil protection (protection of civilians in the event of tension and defence) both as an independent research field and as a cross-cutting aspect relevant in all areas of Security Research.
Findings and solutions should strengthen the resilience, independence and self-sufficiency of the population and its infrastructures and contribute to the overall defence of Europe as a civil element in defence.

Greater consideration than previously should be given to the protection of critical infrastructures, not least in view of the increased threat posed by hybrid attacks. While operational protection has already been restructured in Europe by means of the Critical Entities Resilience Directive and the NISII Directive, the funding of innovation in this area has not yet received the necessary attention. This is problematic in the face of the diversity of the infrastructures needing protection and the potential threat scenarios. Research must always consider the physical and digital aspects of resilience together.

Research on the various aspects of disaster prevention and crisis management involving the population also in the digital space, should be expanded. In order to enable European responses to crises and disasters, isolated solutions must be avoided to ensure interoperability in European cooperation between emergency services and, with that, strengthen resilience. The needs of emergency services who risk their lives for the population should be met by research-driven innovation based on the best technological and tactical equipment. This includes research on the acceptance of new technologies within organisations and the population. The population should always play an active role in research projects where the focus is on their resilience. The warning of the population should be researched, as should the population's contribution to risk mitigation, self-protection, supplying itself and involvement in disaster and defence situations.

Further on, research in areas relevant to police forces as well as research about police is important for European Civil Security Research due to cross-border crime, and in the context of European cooperation. In addition to researching forms of crime, crime prevention and the social environment also play a crucial role. Police actors have to keep pace with digital transformation and the use of digital tools by criminals, terrorists and government agencies poses a major challenge. Research into structures that preserve or endanger democracy is also of great importance, especially in the context of police research.

The digital transformation and the path towards European digital sovereignty can only succeed if cybersecurity continues to be a focus of specific research activities as well as on a broader scale. A stronger bridge to applied research in other areas of Civil Security Research is desired to ensure cybersecurity in particular for security sensitive applications. The various stakeholders in the field of cybersecurity often address different, sometimes competing requirements (e.g. data protection vs. data analysis). For this reason, it is important to clearly define the requirements in the respective application areas in order to develop a comprehensive requirement profile at an early stage. More attention should also be paid to cyber-resilience in terms of the societal use of digital services. More reliable and more secure information and communication systems are essential and will continue to play an important role in a functioning economy and in almost all areas of our highly interconnected society. Cyber-resilience is essential to ensure protection against hybrid threats including both physical and cyber-based attacks on critical infrastructure.

Research on the management of European borders should be broadened in future. This should include both new approaches to the optimal implementation of freedom of movement in Europe and to the management of migration within Europe. The individual and human rights should be at the centre of the research interest.

Transdisciplinarity, including a strong role for Social Science and Humanities in the projects, is a fundamental constant of Civil Security Research and must be maintained and strengthened. In particular, the direct participation of civil society organizations and affected social actors in research should be further developed in the future. Only research which also takes social and societal aspects into account can strengthen the resilience of security actors and society to an equal degree. Addressing the inter-sectoral and multi-sectoral nature of Civil Security Research in an appropriate manner is a challenge in the current research framework programme due to the strong thematic structure. For example, the threat of the release of CBRN-E is relevant in many areas of application and for many security actors (civil protection, police, operators of critical infrastructre), which are currently addressed in different destinations. New approaches to dealing with complex crises and systemic risks can only be conceived in an overarching manner, taking into account hybrid threats, the threat posed by criminal actors, climate-related changes and digitally connec-

ted structures, and should also be researched in this manner. This can be implemented through a scenario-based approach that aims to reproduce this complexity and test solutions in a combined way. In addition, an open capability-driven approach can also be useful to provide knowledge and technologies usable across different fields of application, to create cross-sectoral comparability within Security Research and to avoid thematic silos. A capability-based approach can help practitioners and end-users shape research proceses. In general, it is therefore necessary to find a good balance between research with a broad horizon and a focus on complexity and interrelation-ships on the one hand, and projects that seek the solution to very specific problems at a detailed level on the other.

Practitioners in European Civil Security Research: Key Role, but Scope for Improvement

Civil Security Research is characterized by its strong orientation on application. Practitioners in Civil Security Research are authorities and organisations with security responsibilities such as police, fire brigades and emergency services, operators of critical infrastructures, civil society organisations which are active in the various areas of Security Research, and other actors such as regional authorities. Already today they are playing a central role in European Civil Security Research. In addition to their mandatory involvement as project partners, there have already been approaches, over the duration of the Horizon Europe programme, to allow more practitioners and end-users not directly involved in the project to access the funded projects and/or the project results. These approaches should be evaluated and, if assessed positively, continued in the next research framework programme. In addition, there should be a strong focus on those practitioners – and on their involvement – who have a key role in the phenomenon being addressed.

Civil Security Research strengthens cross-border cooperation between researchers, companies and practitioners. Nonetheless, establishing contact between them is still a challenge.
This challenge, however, must be resolved in order to have the entire range of practitioners represented in the research programme and to ensure the operationalisation and scaling up of relevant research results. The necessary accompanying networking of the primarily regional and national security actors is essential.

However, this networking should not be funded in the form of projects as these are not permanently available and are not sufficiently open to new actors. Networking initiatives should be easy and affordable to access for national actors, they should address specific thematic and cross-cuttingissues and bring existing national practitioner networks into contact with each other. In order to make projects effective in the long term, it is useful to cluster them in order to facilitate exchange with and beyond them, and to make their results available beyond the end of the project. Besides (hybrid) exchange events, demonstrations of project findings are also useful. The measures currently implemented in the Community for European Research and Innovation for Security (CERIS) are not sufficient as the networking provided in this case does not reach new practitioners and, due to its nature of concentrating on project presentations, does not entirely meet the goal of enabling networking.

The successful integration of practitioners is dependent on researchers and industry collaborating with practitioners at an early stage on a level playing field and in a manner which values their contribution. Successful integration is dependent on the involvement of practitioners in all phases of the project. This fundamental requirement for all civil Security Research projects should be given even greater emphasis and should encourage research institutions to be better prepared for collaboration. This concerns the handling of content which needs to be treated as confidential. This is because practitioners are only able to fully contribute themselves and their information if appropriate security measures are planned within projects to ensure that confidentiality and freedom of research are reconciled.

Relationship Between Civil Security Research and Defence Technology Research

Germany is committed to a holistic concept of security which includes civil security and military defence as central elements. In the future, Civil Security Research and Defence Technology Research must continue to be funded in a complementary manner with the aim of leveraging synergies between the two areas and ensuring that the respective processes and technologies interact smoothly. As explained in the beginning, this paper cannot comment on the European Commission's proposals for better defining the future role of dual use in the European research funding landscape.

In addition to all efforts in this area, however, it is important to emphasise that Civil Security Research is an independent research area tailored to the needs of a broad user group and clearly defined as civilian. Ideally, its findings can be implemented in both areas. Defence Technology Research, which is currently being addressed in the European Defence Fund, is tailored to military practitioners.

However, the next research framework programme should develop the interfaces between the programmes, and synergies should be more strongly established. Spin-in calls could thus potentially be created in both directions. Regarding defence, military and civil aspects should be considered to be on an equal footing in European research. On the one hand, this is based on a constructive, continuous dialogue between the two funding areas regarding their future interface work and, on the other, on a structural and budgetary separation of funding in both areas in order to be able to adequately serve the needs of society. At the same time, the aim is to enhance synergies between military and civil research.

Strengthen Scientific Progress in Civil Security: Interfaces and Synergies

The relationship between European Civil Security Research and other areas of research should be redefined. In this regard, Civil Security Research – already multi-sectoral, transdisciplinary and cross-cutting – forms the core that needs to be closely linked with other areas of research and innovation. Topics and findings from other research areas should be incorporated into Civil Security Research in order to explicitly investigate security aspects and – for example in the case of societal issues – develop strategies for action for security actors based on the latest scientific findings. The transfer of findings into Civil Security Research could be realised as a spin-in possibility. A reflected approach to cooperation with other areas of European research funding could also serve to support delineation and the allocation of responsibilities. This applies to synergies with the future cultural and social science programme part of the 10th EU Framework Programme for Research and Innovation in the area of democracy research and with other areas of the programme, as well as with respect to research on health (e.g. pandemic control, water quality), nutrition (e.g. food and water security, agro security, biodiversity), energy (e.g. resilience of

decentralised networks), mobility and living environment (e.g. safety of transport infrastructures such as railways, roads, bridges or waterways and everyday infrastructures such as schools, shopping centres or other public spaces) and the climate (e.g. previously unseen extreme weather events, water shortages, flooding, heat waves) as well as adapting to the consequences of climate change (Green Transition). In technology-oriented research areas, a spin-in could be used to foster the focus on application, for example with regard to industrial (e.g. drones and robotics) and digital technology (e.g. digital euro, end-to-end encryption) as well as aerospace (e.g. satellite technology, Galileo).

EU programmes of all kinds should complement each other and feed into each other in a targeted manner. Civil Security Research should harness synergies with EU operational programmes implementing policies which are explicitly related to civil security (e.g. Union Civil Protection Mechanism supporting disaster resilient societies, Digital Europe Programmes on CyberSecurity, EU Agency for Health Emergency Preparedness and Response (HERA)) or marginally related (e.g. Green Deal Industrial Programme; IRIS²). Programmes that scale and apply research results should be extended and the links between programmes should be improved in their structure.

The Transfer Challenge: Measures that are Creative and Diverse, Focus on Policy-Making

The transfer to application poses a challenge due to the fragmented European market and the low equipment budgets of civil security authorities and actors, to which even greater focus should be given in the next research framework programme. On the one hand, transfer is integral to the existence of Civil Security Research at EU level. It legitimises Civil Security Research's role of addressing practitioner needs and showing ways to innovate in civil security. On the other hand, the outcome of European Civil Security Research, by definition, cannot be a completed transfer process. There are currently already measures in this area of conflicting priorities which, despite their complexity, should be continued such as the tendering of pre-commercial procurement projects or the specific funding of SMEs. Incremental improvements can be made to these tools. A prerequisite for a successful transfer is that projects take into account a systemic view of the solution's

adaptability to the subsequent operational context, which also includes organisational and structural requirements. This comprehensive validation should already be evident in the project application.

Creativity is required when designing new measures because, on the one hand, there is no single silver-bullet for transfer into practice and, on the other hand, all conceivable solutions should be tested and evaluated. For example, procurers, who are usually part of the practitioner organisation, could be involved in projects with a medium level of technological maturity in order to include the procurement perspective in considerations. Insurers could play a role in projects with a higher level of technological maturity, as they can both feed data into projects and, in effect, act as quasi-regulators as they set standards through insurance activities. The preference for open source solutions to subsequently facilitate provision of innovations to a broad range of practitioners would have to be examined here in the same way as the granting of rights of use to the practitioners involved in the project.

There should be a stronger emphasis in the design of funding policy on not viewing projects from the outset as complete individual measures in themselves, but as part of a process. Projects with lower and higher levels of technological maturity can build on each other. A clear separation should be made where competitive tender processes take place and where ongoing funding is based on a positive evaluation. Close coordination is necessary so that other programmes can provide funding opportunities at the right time and to the right extent, for example to provide networking opportunities to practitioners and to consolidate their needs in advance of a call for tender in European Civil Security Research, or for scaling up after a project with a high level of technological maturity.