GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

www.SIFO.de

Informationsbrief zur zivilen Sicherheitsforschung 2/17

Veröffentlicht: 20.03.2017

1. Ergebnisse der Aufrufe aus dem Jahr 2016 im Bereich „Sichere Gesellschaften“ des europäischen Forschungsprogramms „Horizont 2020“

Akteure aus Deutschland haben sich in der jüngsten Auswahlrunde der europäischen Sicherheitsforschung sehr gut platziert.

Im Bereich „Sichere Gesellschaften“ wurden im Jahr 2016 drei Aufrufe (Calls) zur zivilen Sicherheitsforschung veröffentlicht: „Critical Infrastructure Protection (CIP), „Security“ (SEC) und „Digital Security Focus Area“ (DS).[1] Dabei war der SEC-Call in die vier Bereiche „Disaster Resilience“ (DRS), „Fight against Crime and Terrorism“ (FCT), „Border Security and External Security“ (BES) und „General Matters (GM)” unterteilt.

In den drei Calls wurden 48 Projekte zur Förderung ausgewählt. Deutsche Antragsteller sind an 33 der 48 zu fördernden Projekte (entspricht 68,8 Prozent) beteiligt, wobei insgesamt 62 Projektpartner aus Deutschland gefördert werden sollen. Im Call „Security“ sind Partner aus Deutschland sogar an 80 Prozent aller zu fördernden Projekte beteiligt (20 von 25 Projekten).

Gemäß einer vorläufigen Budgetauswertung erhalten die erfolgreichen deutschen Projektpartner in den genannten Calls eine Gesamtfördersumme von ca. 25,9 Mio. Euro (entspricht ca. 12,9 Prozent). Davon entfallen auf den Bereich „Security“ allein 17 Mio. Euro (entspricht ca. 14,3 Prozent der Mittel in diesem Call). Deutschland steht damit sowohl für den Call „Security“ als auch in der Gesamtbetrachtung der drei Calls auf Rang zwei.

Die Überzeichnung der Fördermittel ist stark zurückgegangen. Insgesamt ergibt sich eine 7,1-fache Überzeichnung gegenüber einer 11,6-fachen im Vorjahr. Der Rückgang fällt im Call „Security“ mit einer Halbierung der Überzeichnung noch stärker aus. Betrachtet man ausschließlich diesen Call, wurden ca. 6,7-fach mehr Fördermittel nachgefragt als zur Verfügung standen, wobei die Überzeichnung im Vorjahr noch bei einem Faktor von 12,5 lag.

Deutsche Beteiligung an den zu fördernden Projekten

Insgesamt wurden zu den Calls im Bereich „Sichere Gesellschaften“ 325 gültige Vorschläge eingereicht. 48 der 325 Projektvorschläge, d. h. 14,8 Prozent, wurden positiv evaluiert und sollen gefördert werden. Die Erfolgsquote ist damit im Vergleich zu 8,1 Prozent im Vorjahr wesentlich gestiegen. Betrachtet man ausschließlich den Call „Security“, so fällt die Steigerung noch höher aus: Die Erfolgsquote liegt bei 15,2 Prozent gegenüber 7,8 Prozent im Vorjahr.

Unter diesen 48 erfolgreichen Projekten in den Calls zu „Sichere Gesellschaften“ befinden sich 62 Beteiligungen aus Deutschland. Davon stammen allein 42 Beteiligungen aus den 25 Projekten, die im Call „Security“ gefördert werden (siehe Abbildung 1).

An 33 der 48 zu fördernden Projekte sind deutsche Partner beteiligt (siehe Abbildung 2). Dies entspricht 68,8 Prozent aller erfolgreichen Projekte. Im Call „Security“ sind deutsche Partner sogar an 80 Prozent aller zu fördernden Projekte beteiligt (20 von 25 zu fördernden Projekten).

[1] Diese Auswertung berücksichtigt nicht das KMU-Instrument.

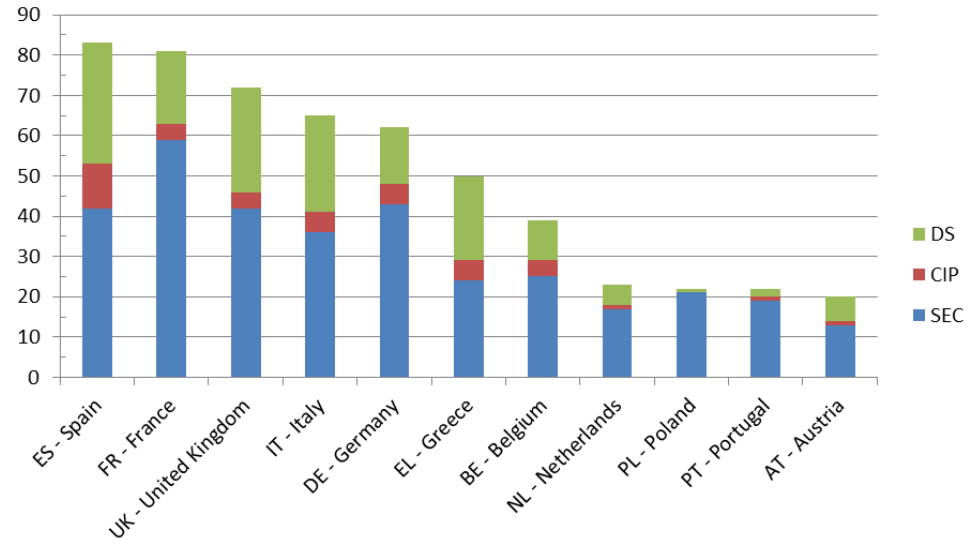

Abb. 1: Anzahl der Projektpartner in zu fördernden Projektvorschlägen (nur Länder mit mindestens 20 Partnern).

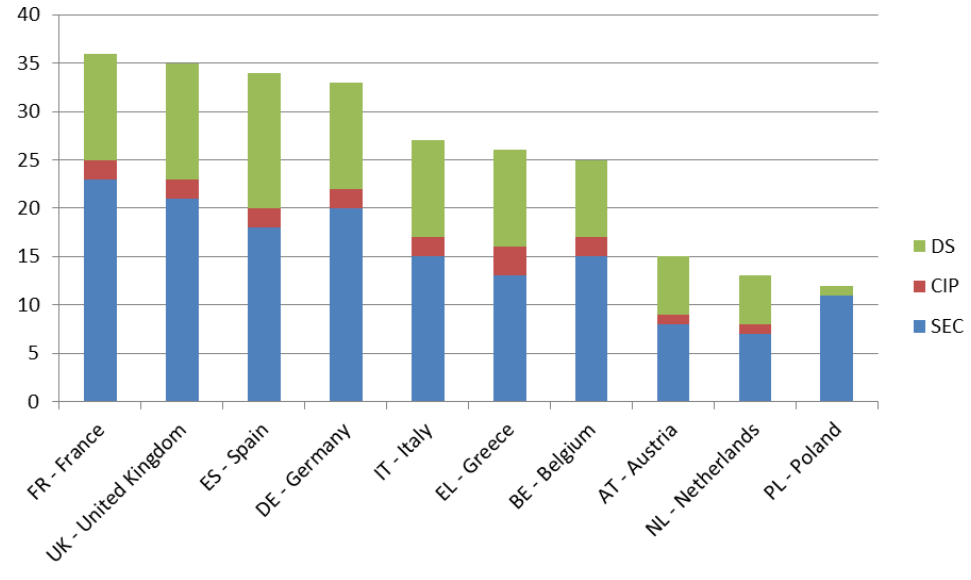

Abb. 2: Beteiligung an zu fördernden Projektvorschlägen (ein oder mehrere Partner eines Landes sind am Projekt beteiligt; nur Länder mit mindestens 12 Projektbeteiligungen).

Vorläufige Budgetanteile

Mit den eingereichten 325 Verbundprojekten wurde eine Gesamtfördersumme von ca. 1.422 Mio. Euro nachgefragt. Als Ergebnis sollen in den drei Calls Projekte mit insgesamt 201,2 Mio. Euro gefördert werden. Die Überzeichnungsquote hat sich für Antragsteller damit positiv entwickelt. In diesem Jahr ergab sich eine ca. 7,1-fache Überzeichnung, während dieser Faktor im Vorjahr noch bei ca. 11,6 lag. Noch deutlicher fällt der Rückgang im Call „Security“ aus, in dem sich die Überzeichnung fast halbiert hat (von einer ca. 12,5-fachen auf eine ca. 6,7-fache Überzeichnung)[2].

[2] Unter Berücksichtigung der korrespondierenden Calls „FCT“, „DRS“ und „BES“ für das Jahr 2015.

Die Gesamtfördersumme der Partner aus Deutschland in den zu fördernden Projekten liegt insgesamt bei ca. 25,9 Mio. Euro, d. h. ca. 12,9 Prozent, (siehe Abbildung 3) bzw. für den Call „Security“ bei ca. 17 Mio. Euro, d.h. ca. 14,3 Prozent, (siehe Abbildung 4).

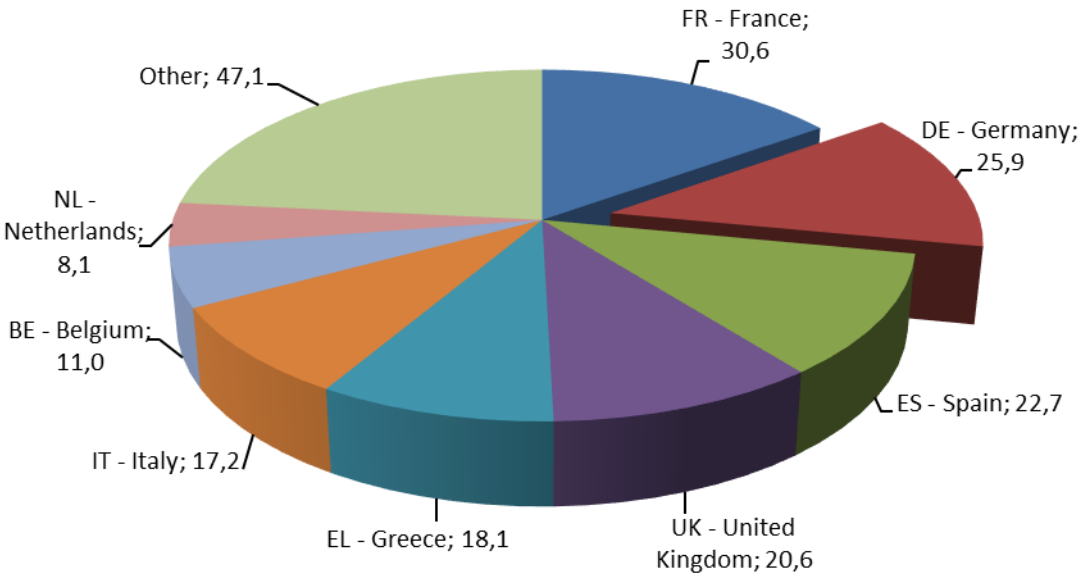

Abb. 3: Gesamtfördersumme für den gesamten Bereich „Sichere Gesellschaften“ in Mio. Euro (basierend auf den ausgewählten Projekten; nur Länder mit mehr als acht Mio. Euro).

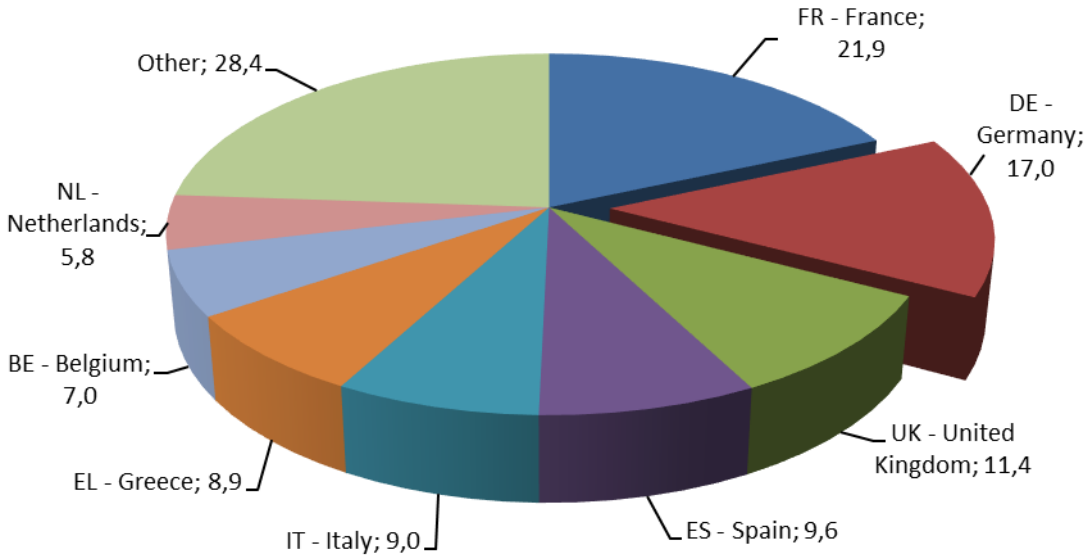

Abb. 4: Gesamtfördersumme für den Call „Security“ in Mio. Euro (basierend auf den ausgewählten Projekten; nur Länder mit mehr als fünf Mio. Euro).

Themenzuordnung

Eine Zuordnung der 48 ausgewählten Projekte zu den ausgeschriebenen Topics findet sich in den Tabellen 1, 2 und 3 (siehe S. 5 ff.).

Zu allen ausgeschriebenen 19 Topics wurden Projektvorschläge zur Förderung ausgewählt. Die vollständige Abdeckung aller Topics konnte insbesondere dadurch erreicht werden, dass im Arbeitsprogramm 2016/2017 einzelnen Topics oder Gruppen von Topics Budgets zugeordnet sind, was die maximale Anzahl von Projekten je Topic einschränkt. Zudem ist für einige Topics oder Subtopics die maximale Anzahl zu fördernder Projektvorschläge explizit begrenzt. Nähere Informationen hierzu können dem Abschnitt „Conditions for the Call“ entnommen werden, der sich im Arbeitsprogramm am Ende der jeweiligen Calls befindet.

Antragsteller aus Deutschland sind in allen Calls des Jahres 2016 erfolgreich. Die 33 Projekte, an denen Partner aus Deutschland beteiligt sind, decken, mit zwei Ausnahmen im Bereich DS, alle ausgeschriebenen Topics ab.

Tab. 1: Zuordnung der eingereichten und zu fördernden Projekte im Call “Critical Infrastructure Protection“ zu den ausgeschriebenen Topics

Call – Critical Infrastructure Protection					
CIP-Topic	**Titel der ausgeschriebenen Topics**	**Typ**	**Eingereichte Vorschläge**	**Zu fördernde Vorschläge**	**Zu fördernde Vorschläge mit DE-Partnern**
1	Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe	IA	34	3	2

Tab. 2: Zuordnung der eingereichten und zu fördernden Projekte im Call „Security“ zu den ausgeschriebenen Topics

Call – Fight against Crime and Terrorism[3]						
Themenbereich	**SEC-Topic**	**Titel des ausgeschriebenen Topics**	**Typ**	**Eingereichte Vorschläge**	**Zu fördernde Vorschläge**	**Zu fördernde Vorschläge mit DE-Partnern**
Disaster-resilience: safeguarding and securing society	1	Integrated tools for response planning and scenario building	IA	19	2	2
	2	Situational awareness systems to support civil protection preparation and operational decision making	CSA	6	1	1
	3	Validation of biological toxins measurements after an incident: Development of tools and procedures for quality control	IA	2	1	1
	5	Chemical, biological, radiological and nuclear (CBRN) cluster	CSA	3	1	1
Fight against crime and Terrorism	6	Developing a comprehensive approach to violent radicalization in the EU from early understanding to improving protection	RIA	21	4	2
	7	Human Factor for the Prevention, Investigation, and Mitigation of criminal and terrorist acts	RIA	20	1	1
	8	Forensics techniques on: a) trace qualification, and b) broadened use of DNA	RIA	7	1	1
	11	Detection techniques on explosives: Countering an explosive threat, across the timeline of a plot	RIA	6	1	1

[3] Diese Auswertung berücksichtigt nicht das KMU-Instrument und auch nicht das Instrument „Fast track to Innovation“.

	12	Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism	RIA	33	4	3
Border Security and External Security	14	Towards reducing the cost of technologies in land border security applications	RIA	7	1	1
	19	Data fusion for maritime security applications	IA	6	1	1
	20	Border Security: autonomous systems and control systems	IA	10	2	1
General Matters	21	Pan European Networks of practitioners and other actors in the field of security	CSA	16	5	4

Tab. 3: Zuordnung der eingereichten und zu fördernden Projekte im Call "Digital Security" zu den ausgeschriebenen Topics

Call – Digital Security					
DS-Topic	**Titel der ausgeschriebenen Topics**	**Typ**	**Eingereichte Vorschläge**	**Zu fördernde Vorschläge**	**Zu fördernde Vorschläge mit DE-Partnern**
1	Assurance and Certification for Trustworthy and Secure ICT systems, services and components	CSA	5	1	-
		IA	4	2	2
		RIA	28	4	3
2	Cyber Security for SMEs, local public administration and Individuals	IA	43	5	4
3	Increasing digital security of health related data on a systemic level	RIA	11	2	1
4	Economics of Cybersecurity	RIA	22	3	1
5	EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation34	CSA	13	3	-

zurück

2. Wichtiger Hinweis: Einschränkung der offenen Topics und weitere Informationen für die Calls in 2017

Für die Antragstellung zu den in 2017 geöffneten Calls „Critical Infrastructure Protection“ und „Security“ sind wichtige Hinweise zu berücksichtigen, die im Folgenden kurz zusammenfassend dargestellt werden. Eine ausführliche und rechtsverbindliche Übersicht über die zu beachtenden Hinweise können bezogen werden unter https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-cip-2016-2017.html sowie unter https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-sec-2016-2017.html.

Einschränkung von Themenbereichen ausgeschriebener Topics

Zu einigen in 2017 ausgeschriebenen Topics in den Calls „Critical Infrastructure Protection“ und „Security“ konnten bereits in 2016 Projektvorschläge eingereicht werden. Zu den bereits in 2016 erfolgreich adressierten Themenbereichen dieser Topics wird in 2017 keine Einreichung von Projektvorschlägen mehr möglich sein. Daher sind bei den in 2017 ausgeschriebenen Topics folgende Einschränkungen zu berücksichtigen:

- CIP-01-2016-2017 (Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe):
  Zu den folgenden Kritischen Infrastrukturen können Projektvorschläge eingereicht werden:
  - „Communication infrastructure“
  - „Health services“
  - „Financial services“

  Die Infrastrukturen „Water“, „Energy“ und „Transport“ sind bereits in 2016 erfolgreich adressiert worden und daher nicht länger geöffnet.
- SEC-07-FCT-2016-2017 (Human Factor for the Prevention, Investigation, and Mitigation of criminal and terrorist acts):
  Die folgenden Sub-topics bleiben geöffnet:
  - Sub-topic 2 „New methods to prevent, investigate and mitigate cybercriminal behaviours“
  - Sub-topic 3 „New methods to prevent, investigate and mitigate corruption and financial crime to fight the infiltration of organised crime in the European Union (licit) economy“
  - Sub-topic 4 „New methods to prevent, investigate and mitigate high impact petty crimes“
  - Sub-topic 5 „New methods to prevent, investigate and mitigate high impact domestic violence“

  Das Sub-topic 1 „New methods for the protection of crowds during mass gatherings“ ist bereits in 2016 erfolgreich adressiert worden und ist daher nicht länger geöffnet.
- SEC-12-FCT-2016-2017 (Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism):
  Die folgenden Sub-topics bleiben geöffnet: - “Others“

  Die Sub-topics 1 bis 3 („cyber-crime: virtual/crypto currencies des-anonymisation/ tracing/impairing where they support underground markets in the darknet“,„detection and neu-

tralization of rogue/suspicious light drone/UAV flying over restricted areas“ und „video analysis in the context of legal investigation“) sind bereits in 2016 erfolgreich adressiert worden und sind daher nicht länger geöffnet.

- SEC-21-GM-2016-2017 (Pan European Networks of practitioners and other actors in the field of security):
  Für die einzelnen Netzwerktypen gelten folgende Bedingungen:
  - Netzwerktyp A (same discipline and from across Europe) – bereits adressierte Disziplinen, die nicht länger geöffnet sind:
    firefighters, police
  - Netzwerktyp A (same discipline and from across Europe) – noch nicht adressierte Disziplinen, die weiterhin geöffnet bleiben:
    „intelligence bodies; border guards, coast guards, and custom authorities; explosive specialists; forensic laboratories; medical emergency teams; think-tanks on security; etc.“
  - Netzwerktyp B (from different disciplines in a particular geographical area) – bereits adressierter geografischer Bereich, der nicht länger geöffnet ist:
    „Danube river basin“
  - Netzwerktyp B (from different disciplines in a particular geographical area) – noch nicht adressierte geografische Bereiche, die weiterhin geöffnet bleiben:
    „the Mediterranean region (including the Black Sea), the Arctic and North Atlantic region, the Baltic region“
  - Netzwerktyp C (demonstration and testing sites, training facilities): Dieser Themenbereich wurde bereits erfolgreich adressiert und ist daher nicht länger geöffnet.

Zu berücksichtigende Ergebnisse laufender Projekte

Weiterhin ist bei der Antragstellung zu bestimmten Topics auf Ergebnisse bereits laufender Projekte Bezug zu nehmen. Die Europäische Kommission hat hierzu Dokumente zur Verfügung gestellt, in denen die zu berücksichtigenden Ergebnisse zusammengefasst sind. Die Informationen aus diesen Dokumenten sind bei der Antragstellung zwingend zu berücksichtigen:

- SEC-04-DRS-2017 (Broadband communication systems):
  Für die Antragstellung sind die Erkenntnisse aus dem CSA-Projekt BROADMAP zu berücksichtigen, das zum Topic DRS-18-2015 gefördert wird (Projektnummer: 700380). Das Projekt hat Erkenntnisse darüber generiert, ob oder ob nicht die Einrichtung einer neuen Organisation vor der Phase 1 eines PCP erforderlich ist. Zudem hat das Projekt Spezifikationen sowie für eine Ausschreibung relevante Dokumente erarbeitet. Diese Informationen können von folgender Website bezogen werden:
  http://ec.europa.eu/research/participants/data/ref/h2020/other/guides_for_applicants/h2020-sec-techspec-tenderdoc_en.pdf
  Im Nachgang zur Veröffentlichung der Dokumente und unter Berücksichtigung der Projektergebnisse wird die Europäische Kommission in Kürze über eine Änderung des Calls zum Topic entscheiden.

- SEC-05-DRS-2016-2017 (Chemical, biological, radiological and nuclear (CBRN) cluster):
  Der für die Antragstellung relevante Katalog, der eine Liste zu berücksichtigender Technologien enthält und auf den in der Topic-Beschreibung verwiesen wird, kann von folgender Website bezogen werden:
  http://ec.europa.eu/research/participants/data/ref/h2020/other/guides_for_applicants/h2020-sec-tech-catalogue_en.pdf
- SEC-13-BES-2017 (Next generation of information systems to support EU external policies):
  Die relevanten Erkenntnisse aus dem CSA-Projekt CIVILEX (Projektnummer 700197), das zum Thema BES-11-2015 gefördert worden ist und auf das in der Topic-Beschreibung verwiesen wird, können von folgender Website bezogen werden:
  http://ec.europa.eu/research/participants/data/ref/h2020/other/guides_for_applicants/h2020-sec-civilex-findings_en.pdf

Verpflichtende Einbindung von Endnutzern

Wie bereits in 2016 ist auch in 2017 die Rolle von öffentlichen und privaten Endnutzern in den Calls „Critical Infrastructure Protection“ und „Security“ deutlich gestärkt. Neben einer entsprechenden thematischen Schwerpunktsetzung werden zu den einzelnen ausgeschriebenen Topics Mindestbeteiligungen von Endnutzern als vollwertige Projektpartner vorgeschrieben. Die entsprechenden Bedingungen werden im Abschnitt “Conditions for the Call“ zum jeweiligen Call aufgelistet und sind zwingend zu berücksichtigen.

Die Europäische Kommission nutzt zur Beschreibung der Endnutzereinbindung den Begriff „Practicioner“. Diesen Begriff hat die Europäische Kommission für eine Antragstellung in 2017 nun näher definiert: „A practitioner is someone who is qualified or registered to practice a particular occupation, profession in the field of security or civil protection. Applicants are invited to identify clearly which members of the consortium they consider "practitioners" in the specific context of their proposal, and to include a clear description of their respective role and added-value as practitioners.”

Die Hinweise zum Begriff „Practicioner“ sollen bei der Antragstellung zwingend berücksichtigt werden. Die Mitarbeiterinnen und Mitarbeiter der Nationalen Kontaktstelle (NKS) Sicherheitsforschung beraten Sie gern zu Fragen zur Endnutzereinbindung wie auch zu anderen Fragen der Antragstellung.

Ihr **Ansprechpartner in der NKS Sicherheitsforschung** bei der VDI Technologiezentrum GmbH ist:

Dr. Thorsten Fischer
Telefon: +49 211 6214-628
E-Mail: fischer_t@vdi.de

zurück

3. Links

www.sifo.de – BMBF-Seite zur zivilen Sicherheitsforschung

www.sifo-informationsbrief.de – Informationsbrief zur zivilen Sicherheitsforschung

www.sifo-securityresearchmap.de – Landkarte zur zivilen Sicherheitsforschung

www.sifo-nks.de – Nationale Kontaktstelle für die EU-Sicherheitsforschung

www.sifo-dialog.de – Fachdialog Sicherheitsforschung

zurück

Herausgeber:

VDI Technologiezentrum GmbH, VDI-Platz 1, 40468 Düsseldorf
E-Mail: vditz@vdi.de, Internet: http://www.vditz.de
Geschäftsführer: Dipl.-Ing. Sascha Hermann
Amtsgericht Düsseldorf HRB 49295, USt.-ID: DE 813846179

Ansprechpartner:
Dr. Andreas Hoffknecht - Projektträger des BMBF - Programm "Forschung für die zivile Sicherheit"
Telefon: +49 211 6214-456, E-Mail: hoffknecht@vdi.de

Dr. Thorsten Fischer - Nationale Kontaktstelle Sicherheitsforschung
Telefon: +49 211 6214-628, E-Mail: fischer_t@vdi.de

Der Informationsbrief wird im Auftrag des Bundesministeriums für Bildung und Forschung (BMBF) herausgegeben.

VDI Technologiezentrum

NKS Sicherheitsforschung
Nationale Kontaktstelle für das Europäische Forschungsrahmenprogramm

PROJEKTTRÄGER FÜR DAS
Bundesministerium für Bildung und Forschung