BEAUFTRAGT VOM

Bundesministerium
für Bildung
und Forschung

SIFO.de

Informationsbrief zur zivilen Sicherheitsforschung 12/20

Abgesagt: Security Research Event / Innovationsforum Zivile Sicherheit 2021

Leider müssen wir Ihnen mitteilen, dass aufgrund der Entwicklung der Corona-Pandemie das Bundesministerium für Bildung und Forschung (BMBF) und die Europäische Kommission entschieden haben, die **für 2021 geplante gemeinsame Konferenz „Security Research Event / Innovationsforum Zivile Sicherheit" abzusagen**.

Ursprünglich war die Konferenz für den 24.-26. November 2020 in Bonn geplant und sollte dann ins Frühjahr 2021 verschoben werden.

Allen Beteiligten ist diese Entscheidung nach einer mehrjährigen Vorbereitungszeit sehr schwergefallen. Die aktuelle Corona-Krisenlage hat jedoch verdeutlicht, dass die Planung dieser internationalen Konferenz mit zu vielen Unwägbarkeiten verbunden wäre.

Dem bekannten Zweijahres-Rhythmus folgend, wird das BMBF aller Voraussicht nach im Jahr 2022 wieder ein „Innnovationsforum Zivile Sicherheit" organisieren. Wir würden uns freuen, Sie auf diesem Innovationsforum begrüßen zu dürfen.

zurück

Online-Stammtisch des Graduierten-Netzwerks am 16. Dezember 2020

Am **16. Dezember 2020** lädt das **Graduierten-Netzwerk „Zivile Sicherheit"** von 19:00 Uhr bis 20:30 Uhr zum **9. Online-Stammtisch** ein. Der Online-Stammtisch dient der Vernetzung von Nachwuchsforscherinnen und -forschern aus Wissenschaft und Praxis im Kontext der zivilen Sicherheit in Deutschland.

Sollten Sie Interesse haben, am Online-Stammtisch teilzunehmen, wenden Sie sich bitte unter Angabe ihres individuellen Hintergrunds (Fach- bzw. Arbeitsgebiet) mit einer kurzen E-Mail an friedrich.gabel@izew.uni-tuebingen.de, um die Einwahldaten zu erhalten. Oder treten Sie der „Xing-Gruppe Graduierten-Netzwerk „Zivile Sicherheit" bei.

Alle Interessenten sind herzlich willkommen.

Weitere Informationen erhalten Sie auch auf www.sifo-graduierte.de.

zurück

Digitale Veranstaltungsreihe: fit4sec für Horizont Europa von 13. bis 15. Januar 2021

Vom **13. bis 15. Januar 2021** bietet das Brandenburgische Institut für Gesellschaft und Sicherheit (BIGS) im Rahmen der Unterstützungsmaßnahme fit4sec zum „Aufbau Europäischer Konsortien für die Sicherheitsforschung" eine **digitale Veranstaltungsreihe** zum Austausch über das neue Forschungsrahmenprogramm „Horizont Europa" (2021-2027) an.

Derzeit wird noch verhandelt, welche Themen im nächsten europäischen Sicherheitsforschungsrahmenprogramm behandelt werden. Dennoch zeichnet sich ab, dass die Bildung von Konsortien und die Einreichung von Projektanträgen 2021 zügig voranschreiten müssen. Die Frist für die Einreichung wird voraussichtlich unverändert bei Ende August 2021 bleiben.

Die digitale Veranstaltungsreihe soll Experten aus Industrie, Wissenschaft, Zivilgesellschaft und öffentlichen Einrichtungen zusammenbringen, um die Schwerpunkte der anstehenden europäischen Sicherheitsforschungsagenda zu diskutieren. In geplanten „Break-out Sessions" werden eine Reihe nationaler und bilateraler Projekte vorgestellt, um eine Synthese mit anderen europäischen Initiativen herzustellen und das Potential für das kommende europäische Sicherheitsforschungsprogramm zu erkunden.

Weitere Informationen zum Veranstaltungsprogramm finden Sie auf der folgenden Webseite: www.fit4sec.de.

Anmeldung und Fragen bitte per E-Mail **bis zum 11. Januar 2021** an caroline.vdheyden@bigs-potsdam.org.

Bleiben Sie auf dem Laufenden und melden Sie sich für den fit4sec-Newsletter an, damit Sie über die kommenden Veranstaltungen im Jahr 2021 informieren können: www.fit4sec.de/en/contact/newsletter-registration.html.

zurück

Bescheinigungsstelle Forschungszulage (BSFZ) mit virtueller Roadshow

Zum 1. Januar 2020 ist das **Gesetz zur steuerlichen Förderung von Forschung und Entwicklung** (FZulG; BGBl I S. 2763) in Kraft getreten. Das Gesetz ermöglicht die steuerliche Begünstigung von Forschungsausgaben von steuerpflichtigen Unternehmen in Deutschland und soll Anreize setzen, in Forschung und Entwicklung zu investieren. Ziel ist es, den Investitionsstandort Deutschland zu stärken und die Forschungsaktivitäten insbesondere kleiner und mittlerer Unternehmen anzuregen.

Seit dem 16. September 2020 können forschende Unternehmen ihre Forschungsvorhaben zertifizieren lassen und mit einer entsprechenden Bescheinigung eine steuerliche Forschungszulage beim Finanzamt beantragen. Im Auftrag des BMBF übernimmt die Prüfung der Anträge und das Ausstellen der Bescheinigungen die neu eingerichtete **Bescheinigungsstelle Forschungszulage (BSFZ)**, die gemeinsam von der VDI Technologiezentrum GmbH, dem DLR Projektträger und der AiF Projekt GmbH gebildet wird. Entsprechende Anträge können online unter www.bescheinigung-forschungszulage.de eingereicht werden.

Die BSFZ prüft, inwieweit es sich bei den eingereichten Vorhaben um förderfähige Forschung und Entwicklung im Sinne des Forschungszulagengesetzes handelt. Grundsätzlich können alle steuerpflichtigen Unternehmen – unabhängig von Größe, Rechtsform und Branche – die Forschungszulage in Anspruch nehmen. Die Zulage ist zudem themenoffen.

Derzeit veranstaltet die BSFZ gemeinsam mit dem Bundesministerium der Finanzen eine **virtuelle Roadshow**. Ziel ist es, Unternehmen alles Wichtige rund um die Steuerliche Forschungsförderung zu präsentieren und Fragen der Teilnehmerinnen und Teilnehmer zu beantworten.

Sie erhalten Informationen zu folgenden Themen:

- Einführung Steuerliche Forschungsförderung und Forschungszulagengesetz: Anspruchsberechtigung, begünstigungsfähige FuE-Vorhaben und das zweistufige Antragsverfahren
- Das Antragsverfahren bei der BSFZ: Antragsformular, Prüfkriterien und Beispiele für FuE-Tätigkeiten
- Der Antrag auf Forschungszulage: Förderfähige Aufwendungen, Bemessungsgrundlage, Fördersatz und das Verfahren beim Finanzamt

Die Teilnahme ist kostenlos.

Interessierte können sich unter www.bescheinigung-forschungszulage.de/veranstaltungen über aktuelle Termine der Roadshow informieren.

zurück

SmartResilience – Neue Wege, die Resilienz kritischer Infrastrukturen in Europa zu bewerten

Die europäischen und nationalen Gesetze definieren kritische Infrastrukturen als Einrichtungen oder Anlagen, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind. Durch ihren Ausfall oder ihre Beeinträchtigung treten erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit ein.

Der Schutz kritischer Infrastrukturen ist für staatliche wie privatwirtschaftliche Akteure immer wieder mit neuen Herausforderungen und Risiken verbunden. Daher müssen die Widerstands- und Anpassungsfähigkeiten bzw. die Resilienz kritischer Infrastrukturen

kontinuierlich weiterentwickelt und evaluiert werden.

Das SmartResilience-Projekt

Infrastrukturen werden zunehmend „intelligent“ – ganze Städte werden in Zukunft mit der voranschreitenden digitalen Vernetzung von Abläufen zu sogenannten „smart cities“. Dies hat klare Vorteile im normalen Betrieb, da beispielsweise Strom- oder Verkehrsnetze in Echtzeit und zentral überwacht werden können. Dennoch muss sichergestellt werden, dass solche intelligenten Infrastrukturen auch in kritischen Situationen sicher und störungsfrei arbeiten. Eine zentrale Forschungsfrage ist hierbei: Wird die erhöhte Komplexität, z.B. infolge der Einführung von zusätzlichen intelligenten Systemen, zu neuer Verletzbarkeit führen?

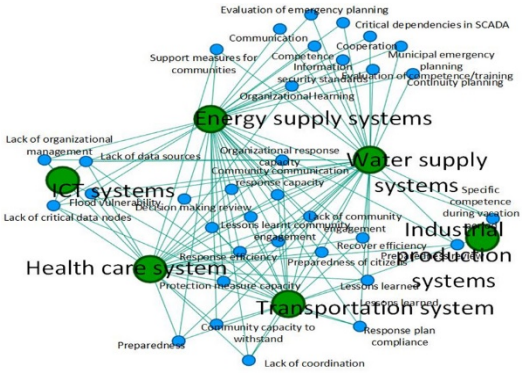

Abb 1: Kritische Infrastrukturen sind in unserer vernetzten Welt mehr denn je voneinander abhängig.
© SmartResilience 2020

Die Untersuchung dieser und damit verbundener weiterer Fragestellungen zur Entwicklung eines zukünftigen Resilienz-Managements kritischer Infrastrukturen stand im Mittelpunkt der 2015 veröffentlichten EU-Ausschreibung „Disaster-resilience: safeguarding and securing society, including adapting to climate change“. Das im Rahmen dieses Aufrufs geförderte Projekt SmartResilience entwickelte ein entsprechendes, ganzheitliches und indikatorenbasiertes System zur Messung und Abschätzung der Resilienz „smarter“ Infrastrukturen. Das vom Europäischen Risiko und Resilienz Institut (EU-VRI) koordinierte Projekt wurde von einem Konsortium mit über 20 Partnern aus 12 Ländern durchgeführt, darunter sieben Betreiber kritischer Infrastrukturen.

Der Weg zur Verbesserung der Resilienz von kritischen Infrastrukturen in Europa

Um das Konzept umzusetzen, hat das Projekt über 5.000 verschiedene Resilienz-Indikatoren identifiziert. Auf denen, die für ein Szenario relevant sind (etwas weniger als 100) basiert dann die Analyse, Bewertung und Resileinzabschätzung. Dabei berücksichtigte Indikatoren können z.B. die Qualifizierung von Sicherheitsmaßnahmen, Anzahl und Art von Schutzeinrichtungen, Überwachung von Risiken oder die Häufigkeit von Cyber-Attacken sein. Für die Bewertung von „smarten“ kritischen Infrastrukturen war vor allem die Identifikation von Indikatoren entscheidend, die auf „Big Data“ beruhen. Kern des Projekts war die Entwicklung und der Test von drei Bewertungs-Methoden: „3D Resilienz-Würfel“, „5 x 5 Resilienz-Matrix“ und „resilience landscape“ (Abb. 2). Durch die Kopplung dieser Methoden wird es nicht nur möglich, die Resilienz einer kritischen Infrastruktur zu einem bestimmten Zeitpunkt zu bewerten, sondern auch sie kontinuierlich zu überwachen, zu optimieren und mit anderen Infrastrukturen zu vergleichen.

Darüber hinaus lässt sich über diese ganzheitliche Methodik bei Bedarf das Verhalten einer Infrastruktur während einer Krise bzw. eines Krisen-Szenarios detailliert analysieren. Ebenso werden die wechselseitigen Abhängigkeiten zwischen den Infrastrukturen quantifiziert und Maßnahmen zur Optimierung der Resilienz (z. B. durch Investitionen in neue Sicherheitsmaßnahmen, Ausbildung usw.) aufgezeigt.

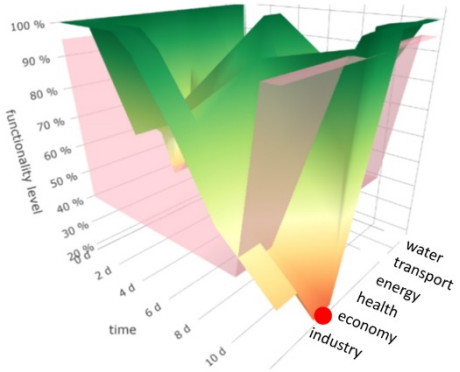

Abb. 2: Resilienz einer Infrastruktur mit „Resilience landscape“ abbilden: Wo sind die kritischen Stellen während einer Krise?
© SmartResilience 2020

Die im Projekt entwickelten Methoden in einem „ResilienceTool“ zusammengeführt. Das Tool wurde in über 25 Fallstudien unter Smart-City-ähnlichen Bedingungen getestet und validiert, dabei wurden u.a. Energie-, Verkehrs-, Gesundheits- und Wasserinfrastrukturen, aber auch Produktionsanlagen einbezogen und Kaskadeneffekte berücksichtigt. Insgesamt wurden über 250 Bewertungen von verschiedenen Infrastrukturen durchgeführt. Beispielsweise wurde die Resilienz von 122 Krankenhäusern bewertet – was nach Projektabschluss bereits zur besseren Analyse und Optimierung von entsprechenden Maßnahmen in der Corona-Krise beigetragen konnte.

Das ResilienceTool wird z. Z. in Nachfolgeprojekten (zum Beispiel im Projekt InfraStress) weiterentwickelt und steht zusammen mit den Gesamtergbenissen des Projekts Interessierten (inklusive einer eLearning-

Abb. 3: Resilienz mehrerer Infrastrukturen visualisieren: Beispiel Krankenhäuser – jedes Krankenhaus bewertet und analysiert einzelne Szenarien mit Hilfe des SmartResilience Tools.
© SmartResilience 2020

Plattform) frei zur Verfügung. Die Ergebnisse des Projekts fließen zudem in die Entwicklung eines neuen ISO-Standards ein (ISO 31050 „Guidance for managing emerging risks to enhance resilience“). Im Rahmen des Europäischen Clusters von Kritischen Infrastrukturen (ECSCI) leistet SmarResilience auch einen Beitrag bei der Neufassung der aktuell noch geltenden EU-Richtlinie 2008/114 über europäische kritische Infrastrukturen.

Weitere Informationen zum Projekt unter www.smartresilience.eu-vri.eu und www.resilience-tool.eu-vri.eu.

zurück

Presserückschau und Links

Presserückschau

„Pandemien der Zukunft vermeiden“ Interview mit Prof. Dr. Jonas Schmidt-Chanasit zum Verbundprojekt PREPMEDVET, bmbf.de

Soziale Medien

Nachrichten vom Twitter- und Facebookkanal des BMBF

Tweet zum Projekt PREPMEDVET vom 28.11.2020

Facebook-Post zum Projekt PREPMEDVET zum 27.11.2020

Tweet zum Projekt PRÄDISIKO vom 25.11.2020

Links

BMBF-Seite zur zivilen Sicherheitsforschung
www.sifo.de

Informationsbrief zur zivilen Sicherheitsforschung
www.sifo-informationsbrief.de

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

Fachdialog Sicherheitsforschung
www.sifo-dialog.de

zurück

Impressum

Herausgeber und Gestaltung:

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

Ansprechpartner und verantwortliche Redakteure:

Dr. Michael Klink - Projektträger Sicherheitsforschung
Telefon: +49 211 6214-286, E-Mail: klink@vdi.de

Dr. Christine Prokopf - Nationale Kontaktstelle Sicherheitsforschung
Telefon: +49 211 6214-945, E-Mail: prokopf@vdi.de

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

Bildnachweis
Titel: BMBF

Versanddatum: 14.12.2020