



Bundesministerium
für Bildung
und Forschung

Dokumentation

zum

Agenda-Workshop zur Fortschreibung des Programms „Forschung für die zivile Sicherheit“

„Herausforderungen der staatlichen Sicherheitsvorsorge“

17. November 2010

Collegium Leoninum Bonn

Noeggerathstrasse 34

53111 Bonn

Inhaltsverzeichnis

Tagesordnung 3

Ergebnisse 5



Workshop „Herausforderungen der staatlichen Sicherheitsvorsorge“

im Rahmen des Agenda-Prozesses zur Fortschreibung
des Programms „Forschung für die zivile Sicherheit“

Tagesordnung

Termin: 17. November 2010

Ort: Collegium Leoninum in Bonn

Zeit	Thema
ab 10:00	Anmeldung, Begrüßungskaffee
10:30	Einleitung und Ziel des Workshops <i>Dr. Stefan Mengel, BMBF</i>
10:40	Zum Stand der Forschung <i>Prof. Dr. Klaus Thoma, Fraunhofer-Institut für Kurzzeitdynamik</i> Forschungsprojekte des laufenden Programms <i>Dr. Stefan Mengel, BMBF</i>
11:10	Impulsstatements: Sicherheit im Kontext globaler Trends Bedrohungen durch Extremismus, Terrorismus und organisierte Kriminalität <i>Prof. Dr. Christopher Daase, Universität Frankfurt</i> Risiken durch natürliche oder anthropogene Katastrophen und Schadenslagen <i>Prof. Dr. Bernd Appel, Bundesinstitut für Risikobewertung</i> Risiken durch eine technisierte und global vernetzte Welt <i>Prof. Dr. Holger Mey, Cassidian</i> Diskussion
12:20	Einführung in die Arbeitsgruppen <i>Dr. Andreas Hoffknecht, VDI Technologiezentrum GmbH</i>

12:30	Mittagsimbiss
13:30	<p>Identifizierung von Forschungsansätzen (in parallelen Arbeitsgruppen):</p> <p>AG1: „Extremismus, Terrorismus und organisierte Kriminalität“ <i>Prof. Dr. Hans-Jürgen Lange, Universität Witten-Herdecke</i></p> <p>AG2: „Natürliche oder anthropogene Katastrophen“ <i>Dr. Karsten Michael, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe</i></p> <p>AG3: „Technisierte und global vernetzte Welt“ <i>Dr. Mathias Glasmacher, Diehl Stiftung & Co. KG</i></p>
15:15	Kaffeepause
16:00	Vorstellung und Diskussion der Ergebnisse aus den Arbeitsgruppen
17:15	Ende der Veranstaltung

Ergebnisse

Ziel des Agenda-Workshops „**Herausforderungen der staatlichen Sicherheitsvorsorge**“, an dem 72 Teilnehmer aus Industrie, Forschung und dem Endnutzerbereich teilnahmen, war es, die Risiken und Forschungsfragen der zivilen Sicherheit zu diskutieren, die vorrangig **hoheitliche** Aufgaben der zivilen Sicherheit betreffen. Dabei wurde im Workshop vor allem der Einfluss mittel- und langfristiger Trends für den Bedarf an ziviler Sicherheit betrachtet, wie beispielsweise die Erweiterung des Sicherheitsbegriffes, die Privatisierung hoheitlicher Bereiche, die Vernetzung kritischer Infrastrukturen etc. sowie die Auswirkungen globaler Entwicklungen oder Bedrohungen, wie etwa des Klimawandels oder der Erscheinungsformen des transnationalen Terrorismus und der organisierten Kriminalität.

Im Rahmen des Workshops wurden deshalb drei Arbeitsgruppen zu den Themenschwerpunkten „**Extremismus, Terrorismus und organisierte Kriminalität**“, „**Natürliche oder anthropogene Katastrophen**“ und „**Technisierte und global vernetzte Welt**“ gebildet, die die Aufgabe hatten, auf der Basis der in den Themenschwerpunkten adressierten Herausforderungen, **Bedarfs- und Forschungsthemen** mit geeigneten Umsetzungs- und Anwendungsperspektiven zu identifizieren.

Die Ergebnisse lassen sich in vier thematische Bedarfsschwerpunkte fassen:

1. Risiken und Auswirkungen des Klimawandels

- Untersuchung der Auswirkungen des Klimawandels auf kritische Versorgungsinfrastrukturen, z.B. bei der Trinkwasserversorgung
- Entwicklung verbesserter technischer und organisatorischer Schutzkonzepte für (kritische) Infrastrukturen unter Berücksichtigung von klimawandelbedingten Gefährdungen z.B. durch Einbeziehung von Verwundbarkeitszenarien in Planungsinstrumenten
- Entwicklung präventiver Maßnahmen zur Erkennung neuartiger Krankheitserreger und Toxine
- Untersuchung der Folgen des Klimawandels für den Katastrophenschutz (national, europäisch) und Anpassung von Organisationsstrukturen und Schutzkonzepten

2. Kritische Infrastrukturen 2.0

- Erweiterung von „Security by Design“-Lösungen und -Konzepte durch „Infrastrukturresilienz by Design“, z.B. zur Sicherstellung von Minimalfunktionalitäten bzw. Notlaufeigenschaften in kritischen Infrastrukturen
- Lösungen und Konzepte für den Schutz der kritischen Infrastruktur Weltraum bzw. Raumfahrt im Sinne von Sicherheit durch Raumfahrt, aber auch Sicherheit für Raumfahrt(systeme)
- Verbesserte Maßnahmen zum Schutz der kritischen Infrastrukturen Wasserversorgung bzw. Land- und Forstwirtschaft

- Verbesserte Schutzkonzepte gegen elektromagnetische Einwirkung (z.B. verursacht durch Sonnenstürme oder nukleare elektromagnetische Impulse (NEMP)) auf kritische Infrastrukturen
- Entwicklung von Methoden und Lösungen für koordinierte und sektorübergreifende Simulationen und integrierte Modellbildungen in vernetzten Infrastrukturen („Systems of systems“)
- Konzepte und Methoden zur Analyse des Kaskadenverhaltens diversitärer kritischer Infrastrukturen
- Technologische und organisatorische Lösungen und Maßnahmen zum Schutz vor sowie der Erkennung und Bewältigung von biologischen Gefahrenlagen, z.B. über
 - o Entwicklung verbesserter Systeme zur Probenahme und Detektion von B-Gefahrstoffen (z.B. durch den Einsatz generischer Nachweismethoden für unbekannte Proben)
 - o Entwicklung von Verfahren zur evidenzbasierten Einschätzung des Bedrohungspotenzials spezifischer biologischer Agenzien
 - o Entwicklung von verbesserten Verfahren und Konzepten zur Dekontamination und Wiederherstellung kontaminierter Räumlichkeiten, Areale und Personen

3. Menschen, Organisationen und deren Interaktionen

- Technische und organisatorische Maßnahmen und Lösungen zur Erhöhung der Interoperabilität und Kooperation zwischen den Sicherheitsbehörden, den kritischen Infrastrukturbetreibern und der Bevölkerung, z.B. durch verbesserte Notfall- und Kommunikationssysteme für den Krisenfall
- Maßnahmen zur Vernetzung und Abstimmung unterschiedlicher privater oder staatlicher Sicherheitsakteure und Einrichtungen, z.B. durch ein übergreifendes Risiko- und Notfallmanagement. Maßnahmen für den Aufbau effizienter Koordinierungssysteme, z.B. zur Unterstützung kritischer Infrastrukturbetreiber oder die bessere Koordinierung von Rettungs- und Hilfskräften
- Verbesserte Konzepte in der Risiko- und Krisenkommunikation, z.B. im Bezug auf den öffentlichkeitswirksamen Umgang mit Ungewissheit in Krisensituationen, der Rolle der Medien und des Internets oder der intendierten und nicht-intendierten Folgen von Kommunikationsinhalten
- Technologische Maßnahmen (z.B. SelbsthilfeeinFORMATIONssysteme) und verbesserte Sensibilisierungs- und Ausbildungskonzepte zur Erhöhung des Selbstschutzes und der Selbsthilfefähigkeiten der Bevölkerung unter Berücksichtigung neuer interaktiver Lernmöglichkeiten und Szenarien (Stichwort: „Menschen als Betroffene und Helfer“)

4. Übergeordnete Querschnittsthemen:

- Entwicklung von Werkzeugen und Methoden der Risikoanalyse, -bewertung und -priorisierung, z.B. für „proaktive“ Risikoanalysen oder die Erhebung von Risiken
- Konzepte für verbesserte Aus- und Weiterbildungsmaßnahmen für (privates) Sicherheitspersonal
- Entwicklung ganzheitlicher Standardisierungskonzepte und -strategien, z.B. zur Zusammenführung von technologischen Insellösungen oder zur Festlegung einheitlicher Weiterbildungsstandards in BOS und Unternehmen

Wichtige Aussagen aus den Plenumsdiskussionen und Impulsstatements

- Eine zentrale Herausforderung staatlicher Sicherheitsvorsorge besteht darin, auf ein wachsendes Sicherheitsbedürfnis der Gesellschaft so zu reagieren, dass Sicherheit maximiert wird, aber die ebenfalls gewachsenen Anforderungen an Transparenz und Rechenschaftspflicht einer demokratischen Gesellschaft nicht unterminiert werden.
- Eine der weiteren Herausforderungen staatlicher Sicherheitsvorsorge besteht darin, Entscheidungen unter hoher Ungewissheit zu treffen und diese entsprechend zu kommunizieren. Das erfordert eine proaktive Risikopolitik, die das politische Management von Sicherheit und Unsicherheit gewährleistet und bereits im Vorfeld aktiv wird, um die Wahrscheinlichkeit eines zukünftigen Schadens zu reduzieren.
- Neben Vorsorge ist Vorbeugung ein wichtiges Element proaktiver Sicherheitspolitik. Forschung zur Gewährleistung und Erhöhung ziviler Sicherheit muss deshalb sowohl bei den Möglichkeiten zur Vorsorge (also wie lassen sich z.B. die Maßnahmen zur effektiven Strafverfolgung einerseits und zum Schutz der Bevölkerung und zur Reduzierung der Verwundbarkeit strategischer Infrastrukturen andererseits verbessern) als auch bei den Möglichkeiten zur Vorbeugung ansetzen (wie ist im Vorfeld möglicher Gefahren z.B. eine effektivere Aufklärung möglich und wie können soziale Prozesse so beeinflusst werden, dass organisierte Kriminalität und Terrorismus nicht überhand nehmen).
- Ein Teil zukünftiger Sicherheitsforschung sollte sich den institutionellen Herausforderungen staatlicher Sicherheitspolitik widmen und darauf gerichtet sein, wie die Kooperation zwischen nationalen und internationalen, öffentlichen und privaten, zivilen und militärischen Institutionen optimiert werden kann, um dem spezifisch transnationalen Charakter von Terrorismus und organisierter Kriminalität gerecht werden zu können.
- Die zukünftige Sicherheitsforschung sollte sich u.a. auch den politisch-normativen Herausforderungen staatlicher Sicherheitspolitik widmen und die ethischen Kriterien und Standards staatlicher Sicherheits- und Unsicherheitskommunikation sowie das Verhältnis individueller und institutioneller Verantwortlichkeit für Risikoentscheidungen klären.

- Es ist eine weitere Öffnung des Sicherheitsforschungsprogramms nicht nur für die Sozial- sondern auch für die Geisteswissenschaften notwendig, da sie einen wichtigen Beitrag zum Verständnis insbesondere der Herausforderungen staatlicher Sicherheitsvorsorge leisten können. Dabei sollten die Sozial- und Geisteswissenschaften sowohl ihre eigenen Fragestellungen bearbeiten, aber auch – im Sinne einer Gleichstellung institutioneller und normativer Fragen – weiterhin in die technik- und naturwissenschaftliche Sicherheitsforschung integriert werden.
- In einer modernen, durch eine hohe technische Durchdringung geprägten Welt führen u.a. die zunehmende Interoperabilität, Nutzerfreundlichkeit und Effizienzsteigerung technologischer Komponenten zu neuen Risiken. Insbesondere der Einsatz der auf geringe Kosten und Nutzerfreundlichkeit, aber nicht auf Sicherheitsaspekte hin optimierten kommerziellen Massenware (COTS- oder „commercial off-the-shelf“-Produkte) erhöhen die Gefahren möglicher Manipulationen.
- Die Sicherheitsstandards technischer Infrastrukturen weisen ein sehr heterogenes Erscheinungsbild auf. Hier wird es zukünftig insbesondere für den Schutz kritischer Infrastrukturen immer wichtiger werden, entsprechende „Notlaufeigenschaften“ oder Notfallverfahren zu entwickeln, die im Krisenfall zumindest die grundlegende Funktionsfähigkeit technischer Infrastrukturen z.B. nach Cyber-Angriffen gewährleisten können. Einen hohen Stellenwert des zukünftigen Schutzes kritischer Infrastrukturen nimmt auch die Härtung von technischen Systemen und Komponenten sowohl hinsichtlich physischer (einschließlich EMP) als auch „virtueller“ Verwundbarkeiten ein.
- Zukünftige Risiken der Vernetzung gehen u.a. von einer wachsenden Autonomisierung technischer Systeme aus und werden dabei auch von der Ambivalenz vernetzter Systeme bestimmt: So bietet die Vernetzung z.B. dadurch Schutz, dass durch Rerouting-Prozesse Systeme wiederhergestellt werden können, gleichzeitig führt es dazu, dass die Abkopplung einzelner Systeme oder Infrastrukturen z.B. im Falle Cyber-Angriffen nur schwer zu realisieren ist und die geographische Distanz immer weniger Sicherheit bietet. Auf der anderen Seite führt der Einsatz entsprechender Schutzmaßnahmen häufig zu einer Reduzierung der Vorteile der Vernetzung.
- Der Schutz kritischer Infrastrukturen vor zukünftigen Risiken sollte proaktiver ausgerichtet werden, da die Anpassungsfähigkeit kritischer Infrastrukturen nicht mehr Schritt halten kann mit der hohen Veränderlichkeit von Risiken.
- Risikobewertung sollte in Deutschland stärker im Sinne einer Quantifizierung von Risiken verfolgt werden (z.B. über die Definition von Risikoindikatoren).
- Neben den zukünftigen Bedrohungslagen muss in der staatlichen Sicherheitsvorsorge auch die politische Rahmung betrachtet werden (sowohl national als auch international), da neue Risiken und Bedrohungslagen auch immer mit neuen bzw. veränderten Formen von Politik, Demokratie und Staatlichkeit korrespondieren.
- Im Rahmen der staatlichen Sicherheitsvorsorge ist die Erarbeitung einer Entscheidungs- und Bewertungsmatrix für Großschadenslagen und Katastrophen notwendig, damit die zuständigen Behörden und Organisationen bereits im Vorfeld Prioritäten der Sicherheitsvorsorge festlegen können.

- Zur Verbesserung des Technologietransfers und einer marktgerechten Überführung von Projektergebnissen in Produkte sollte bei der strategischen Ausrichtung des kommenden Sicherheitsforschungsprogramms stärker die Entwicklung von Geschäftsmodellen in den Blickpunkt gerückt werden.

Dr. Olav Teichert (VDI TZ)