



Bundesministerium
für Bildung
und Forschung

Dokumentation

zum

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

**„Herausforderungen
für Bürgerinnen und Bürger und das Gemeinwesen“**

13. Dezember 2010

Bundesministerium für Bildung und Forschung

Heinemannstraße 2

53175 Bonn

Inhaltsverzeichnis

Tagesordnung **3**

Ergebnisse **5**



Workshop „Herausforderungen für Bürgerinnen und Bürger und das Gemeinwesen“

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

Tagesordnung

Termin: 13. Dezember 2010

Ort: BMBF, Bonn

Zeit	Thema
ab 10:00	Anmeldung, Begrüßungskaffee
10:30	Einleitung und Ziel des Workshops <i>Dr. Wolf Junker, BMBF</i>
10:40	Zum Stand der Forschung Gesellschaftliche Dimension der Sicherheitsforschung <i>Prof. Dr. Christoph Gusy, Universität Bielefeld</i> Forschungsprojekte des laufenden Programms <i>Reinhold Friedrich, BMBF</i>
11:10	Impulsstatements: Sicherheit im Kontext globaler Trends Ausdifferenzierung der Gesellschaft und demographischer Wandel <i>Prof. Dr. Thomas Görgen, Deutsche Hochschule der Polizei</i> Klimawandel und Globalisierung <i>Prof. Dr. Janos Bogardi, Deutsches Komitee für Katastrophenvorsorge</i> Wandel zur Informations- und Wissensgesellschaft <i>Prof. Dr. Michael Waidner, Fraunhofer-Institut für Sichere Informations- technik</i> Diskussion

12:20	Einführung in die Arbeitsgruppen <i>Dr. Andreas Hoffknecht, VDI Technologiezentrum GmbH</i>
12:30	Mittagsimbiss
13:30	Identifizierung von Forschungsansätzen (in parallelen Arbeitsgruppen): AG1: „Urbane Sicherheit“ <i>Prof. Dr. Dietrich Henckel, TU Berlin</i> Saal 4 AG2: „Gesellschaftliche Widerstandsfähigkeit“ <i>Prof. Dr. Walter Perron, Universität Freiburg</i> Raum 1373 AG3: „Rahmenbedingungen für zukunftsfähige Sicherheitslösungen“ <i>Peter Zoche, Fraunhofer-Institut für System- und Innovationsforschung</i> Raum 1417
15:15	Kaffeepause
16:00	Vorstellung und Diskussion der Ergebnisse aus den Arbeitsgruppen
17:15	Ende der Veranstaltung

Ergebnisse

Ziel des Agenda-Workshops „**Herausforderungen für Bürgerinnen und Bürger und das Gemeinwesen**“ an dem 50 Teilnehmer aus Industrie, Forschung und dem Endnutzerbereich teilnahmen, war es, die Risiken und Forschungsfragen der zivilen Sicherheit zu diskutieren, die sich vorrangig für Menschen **als Individuen** in ihren beruflichen, öffentlichen oder privaten Lebensbereichen und für das **Gemeinwesen** ergeben. Dabei wurde im Workshop vor allem der Einfluss mittel- und langfristiger Trends für den Bedarf an ziviler Sicherheit betrachtet, wie beispielsweise demographischer Wandel, Wertewandel etc. und die Auswirkungen globaler Entwicklungen, wie etwa des Klimawandels.

Im Rahmen des Workshops wurden deshalb drei Arbeitsgruppen zu den Themenschwerpunkten „**Urbane Sicherheit**“, „**Gesellschaftliche Widerstandsfähigkeit**“ und „**Rahmenbedingungen für zukunftsfähige Sicherheitslösungen**“ gebildet, die die Aufgabe hatten, auf der Basis der in den Themenschwerpunkten adressierten Herausforderungen, **Bedarfs- und Forschungsthemen** mit geeigneten Umsetzungs- und Anwendungsperspektiven zu identifizieren.

Das Ergebnis lässt sich in vier thematische Bedarfsschwerpunkte gliedern:

1. Urbane Sicherheit

- Maßnahmen und Konzepte zur Verbesserung der Zusammenarbeit öffentlicher und privater Sicherheitsdienstleister
- Ganzheitliche Konzepte und Lösungen zur Erhöhung der Sicherheit im ÖP(N)V unter Einbeziehung sicherheitskonformer Kriterien bei der Neugestaltung städtischer Verkehrsinfrastrukturen, innovativer Crowd Management-Lösungen sowie relevanter Einflüsse und Faktoren auf das Sicherheitsempfinden von Fahrgästen und Mitarbeitern
- Maßnahmen zum Schutz vor dem Ausfall städtischer Infrastrukturen und Einrichtungen sowie Konzepte der Gewährleistung von Versorgungssicherheit (z.B. der Lebensmittelversorgung) in urbanen Regionen
- Untersuchungen zu den Einflüssen von Urbanisierung und Bevölkerungsdichte im Kontext der potenziellen Auswirkungen, die z.B. von der Verbreitung von Infektionskrankheiten bzw. von biologischen Anschlägen ausgehen können
- Untersuchungen zum „Defensible-Space“-Ansatz oder zu „Gated Communities“, die im Laufe des 21. Jahrhunderts wachsende Bedeutung erlangen könnten
- Untersuchung zu den Ursachen und Auswirkungen räumlicher Verdrängungsdynamiken auf die Sicherheit urbaner Regionen, z.B. hinsichtlich der Auswirkungen auf städtische Versorgungsinfrastrukturen
- Bedeutung und Rolle des Einsatzes neuer sicherheitsrelevanter Technologien (z.B. verteilter und vernetzter Sensorik und deren Anwendungen) im öffentlichen Raum bzw. ihres Einflusses auf die zukünftige Veränderung urbaner Lebenswelten

2. Gesellschaftliche Widerstandsfähigkeit und Resilienzforschung

- Entwicklung von Methoden zur Analyse gesellschaftlicher Widerstandsfähigkeit, beispielsweise zur Durchführung resilienzspezifischer, räumlicher Analysen in städtischen und ländlichen Regionen sowie zur Definition qualitativer und quantitativer Kriterien zur Erfassung und Gestaltung gesellschaftlicher Widerstandsfähigkeit unter Berücksichtigung z.B. intra- und interindividueller Resilienzfaktoren
- Untersuchung der Kosten sowie möglicher negativer Effekte von Resilienz erhöhenden Maßnahmen
- Konzepte und Lösungen zur Erhöhung der Resilienz von Entscheidungs- und Kommunikationsstrukturen zuständiger Behörden und ihrer Führungskräfte im Krisenfall
- Technische und organisatorische Maßnahmen zur Erhöhung der Resilienz der Informationsgesellschaft unter Einbeziehung unterschiedlicher Anwendungsszenarien und Verwundbarkeiten von Bürgern, Unternehmen, kritischer Infrastrukturen sowie staatlicher Behörden und Organisationen
- Entwicklung von Konzepten und Maßnahmen zum Schutz der Gesundheit der Bevölkerung unter besonderer Berücksichtigung von Veränderungen, die z.B. durch den Klimawandel oder die Entstehung oder Verbreitung neuer Krankheiten ausgelöst werden können
- Untersuchungen zum Stellenwert des Einsatzes neuer Technologien zur Förderung von Resilienz

3. Sicherheitskulturen und Sicherheitsarchitekturen

- Untersuchungen zum Einfluss und der Bedeutung des kulturellen Wandels für die Entwicklung von Kriminalitätsrisiken
- Einfluss und Rolle der Risikowahrnehmung der Bevölkerung bei der Anpassung staatlicher Krisenmanagementkonzepte
- Untersuchungen zu sicherheitskulturellen Trends und Fragestellungen, z.B. zur Frage der Akzeptanz von Unsicherheit oder dem notwendigen bzw. erreichbaren Maß an Risikobewusstsein in der Bevölkerung
- Entwicklung von Verfahren und Methoden zur Quantifizierung von Sicherheit bzw. der Evaluierung von Sicherheitsmaßnahmen, einschließlich der Herleitung und Bestimmung von Kriterien für die Legitimität von Sicherheitslösungen
- Technische und organisatorische Konzepte zur Entwicklung robuster und anpassungsfähiger softwaretechnischer Sicherheitslösungen
- Einbeziehung moderner Usability- bzw. Ergonomie-Konzepte zur Erhöhung der Benutzbarkeit bei Entwicklung und Einsatz neuer ziviler Sicherheitstechnologien

- Untersuchung des Einflusses auf die operative Umsetzung von Sicherheitstechnik und -programmen hinsichtlich der Auswirkungen von Sicherheitsgefühl und Sicherheitswahrnehmungen der Bürgerinnen und Bürgern
- Gesellschaftliche Bedeutung und Awareness von Sicherheits- und Fehlerkulturen, beispielsweise im Gesundheits- und Pflegewesen bzw. im Sicherheitsgewerbe

4. Übergeordnete Querschnittsthemen:

- Untersuchungen zum zukünftigen Einfluss des demographischer Wandels, z.B. bei der Entwicklung technischer und organisatorischer Lösungen im Bevölkerungsschutz (z.B. bei der Pandemiebewältigung)
- Entwicklung ganzheitlicher Konzepte der Risiko- und Sicherheitskommunikation, unter Einbeziehung horizontaler und vertikaler Risikokommunikationsstrukturen
- Rolle des Internets oder neuer Mediennutzungsformen (z.B. Social Media) für die Verbreitung von Informationen im Krisenfall bzw. für die Entwicklung neuer Kommunikationsformen und für die Qualität der Einbeziehung der Bevölkerung in ganzheitliche Konzepte der Risiko- und Sicherheitskommunikation
- Moderne Awareness- und Trainingskonzepte, z.B. zur Information und Schulung der Bürgerinnen und Bürger über bestehende Risiken oder zur Kompetenzbildung im Umgang mit Sicherheitstechnologien
- Entwicklung verbesserter Methoden und Verfahren zur Erstellung von Verwundbarkeits- und Risikoanalysen, z.B. im Rahmen von Verwundbarkeitsmodellierungen in der Stadtplanung, Vulnerabilitätsanalysen zur Stärkung der Resilienz bzw. der Selbstschutzzfähigkeiten oder zur Definition und Einschätzung neuer Gefährdungslagen

Wichtige Aussagen aus den Plenumsdiskussionen und Impulsstatements

- Die gesellschaftswissenschaftliche Sicherheitsforschung sollte die im Rahmen des laufenden Programms eingeschlagene anwendungsorientierte Ausrichtung weiter ausbauen. Unter den laufenden Themenschwerpunkten besteht insbesondere im Bereich der Sicherheitskommunikation ein weiterhin hoher Bedarf, Forschungsansätze stärker zu fördern.
- Wichtige derzeit in der gesellschaftswissenschaftlichen Sicherheitsforschung diskutierte Forschungsfelder sind u.a. die Wirkungsforschung (z.B. medialer Inszenierungen und deren Wirkungen), die Resilienzforschung sowie die Europäisierungs- und Globalisierungsforschung, die sich mit sicherheitsrelevanten Fragestellungen in Folge zunehmender internationaler, arbeitsteiliger Vernetzung auseinandersetzt (aktuell unterstreicht z.B. das Thema „Sicherheit der Luftfracht“ die Bedeutung dieser Fragestellung).
- Die gesellschaftswissenschaftliche Sicherheitsforschung wird sich zukünftig stärker mit Fragen der Sicherheit und sich wandelnder Sicherheitsbedürfnisse im Kontext des gesellschaftlichen Wandels

(z.B. soziale Disparitäten, demographischer Wandel, Migration) auseinandersetzen müssen. Wichtige Fragestellungen in diesem Kontext adressieren z.B. mögliche zukünftige Perspektivänderungen sowie die Änderungen von gesellschaftlichen Nachfrage- und Angebotsverhalten, die sich unmittelbar aus den unterschiedlichen Sicherheitswahrnehmungen aller in der Gesellschaft vertretenden Altersgruppen ableiten.

- Die Veränderung der Bevölkerungsstruktur bzw. die Alterung der Gesellschaft wird aller Voraussicht nach in der Zukunft kein höheres Maß an Unsicherheit bzw. eine erhöhte Gefährdung älterer Menschen durch Kriminalität und Gewalt zur Folge haben. Jedoch können neue Risiken u.a. durch die Verringerung von Alltagskompetenzen bzw. die zunehmende Pflegebedürftigkeit älterer Menschen entstehen. Man geht zudem davon aus, dass es in Zukunft zu einer zunehmenden Verlagerung bestehender Kriminalitätsrisiken und Gefährdungen vom öffentlichen in den privaatstaatlichen bzw. privaten Raum kommen wird.
- Praktische Fragestellungen, die sich zukünftig vor dem Hintergrund einer zunehmenden Alterung und Heterogenisierung der Gesellschaft ergeben, sind u.a.:
 - Wie kann die Sicherheit der wachsenden Zahl pflegebedürftiger älterer Menschen verbessert werden?
 - Wie können ältere Menschen unterstützt werden, für ihre Sicherheit selbst zu sorgen?
 - Wie können staatliche oder private bzw. gemeinnützige und ehrenamtlich tätige Sicherheitsakteure in einer alternden Gesellschaft dabei unterstützt werden, Nachwuchskräfte sowohl in ausreichender Zahl als auch mit hinreichender Qualifikation zu gewinnen?
 - Mit welchen Mitteln kann sozialen und ethnischen Separationstendenzen insbesondere in großstädtischen Räumen entgegengewirkt werden?
- Zukünftige Hauptgefährdungen und Herausforderungen im globalen Maßstab sind nicht nur mit dem Klimawandel sondern u.a. auch mit der zunehmenden Beeinträchtigung des globalen Stickstoffkreislaufes sowie dem Verlust der Biodiversität verbunden.
- Bezüglich des globalen Trends der Urbanisierung existieren derzeit noch keine ausreichenden Methoden und Instrumente, um die globalen Auswirkungen von Verstädterung (z.B. in Asien) auf die Governance von Sicherheit vorherzusagen bzw. zu steuern.
- Die Risikowahrnehmung der Bevölkerung und das tatsächliche Bedrohungspotential von Extremwetterereignissen stehen häufig nicht im Einklang. So ist z.B. die zukünftig von Hitzewellen ausgehende Gefahr für die Bürger vielfach als größer einzuschätzen als die in der Bevölkerung und den Medien stärker als Bedrohung wahrgenommene Hochwassergefahr.
- „Cyber-Insecurity“ ist einer der zentralen Bedrohungsfaktoren der zukünftigen Informations- und Wissensgesellschaft. Bereits heute ist eine wachsende Zahl gut vorbereiteter und gezielter Angriffe auf staatliche Infrastrukturen und Unternehmen zu verzeichnen (man spricht in diesem Zusammenhang auch von „Advanced Persistent Threats“), die ohne die Zusammenarbeit der potentiellen Opfer weder erkannt noch verhindert werden können. Zusätzlich verstärkt wird diese Bedrohung durch eine erhöhte Angriffssymmetrie (ein potentiell kleiner Angriffsaufwand steht einem sehr

hohen Schutzaufwand gegenüber) sowie die höhere Verwundbarkeit von IT-Systemen, die durch die zunehmende Standardisierung und Uniformität der Systeme aber auch durch die zunehmende Vernetzung kritischer Infrastrukturen begünstigt wird.

- Bei der zukünftigen Weiterentwicklung des Cloud Computing sind „Public Clouds“ als neue potentiell kritische Infrastrukturen anzusehen, da insbesondere die weitere Verbreitung mobiler Zugangsgaräte dramatische Auswirkungen auf die Sicherheit der Clouds haben wird, zumal diese ausschließlich vom jeweiligen Benutzer kontrolliert und verwaltet werden.
- Wichtige zukünftige Themen im Kontext des Schutzes von IT-Infrastrukturen betreffen u.a. die notwendige Schaffung einer neuen Sicherheits- und Datenschutzkultur — z.B. hinsichtlich der Definition und Machbarkeit einer allgemeinen „IT-Sicherheitsgurtpflicht“ — sowie die Entwicklung vertrauenswürdiger bzw. smarter kritischer IT-Infrastrukturen, die z.B. die Implementierung verbesserter Sicherheitsarchitekturen ohne gleichzeitige Einbußen beim Datenschutz ermöglichen.
- Zukünftig werden deutlich höhere Investitionen in Modellierung, Analyse und Behandlung von cyberphysikalischen Systemen und Angriffen notwendig werden. So kann z.B. die Einführung technologisch sinnvoller Verbesserungen bei der Kontrolle und Steuerung kritischer Infrastrukturen (Bsp. Einführung elektronischer Ventile in öffentlichen Gasnetzen) häufig zu negativen Seiteneffekten führen, die im Falle eines Angriffes frühzeitig erkannt und analysiert werden müssen.

Dr. Olav Teichert (VDI TZ)