

2. Jahrestagung

Public Private Security Schutz Kritischer Infrastrukturen

Berlin

22. und 23. März 2010 - Fachtagung

24. März 2010 - Workshop

www.public-private-security.com



Fachtagung unter Vorsitz von Dr. Heiko Borchert

- Herausforderungen durch interdependente Krisenszenarien
- Konzepte für erfolgreiche Projekte im Bereich Public Private Security
- Bedrohungspotenziale und Szenarien für Kritische Infrastrukturen
- Pandemie: Lessons learned und Prävention
- Koordination von Krisenmanagement im föderalen System

Workshop

Risiken, Krisen und Prävention in interdependenter KRITIS

Dr. Frank Umbach, Senior Associate, Centre for European Security Strategies (CESS)

Mit Fachbeiträgen führender Unternehmen und Institutionen

- Allianz AG
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe BBK
- Bundesanstalt Technisches Hilfswerk
- Bundesinstitut für Risikobewertung
- Bundeskriminalamt
- Bundesministerium des Innern
- Centre for European Security Strategies (CESS)
- Deutsche Lufthansa AG
- Deutsche Post DHL
- Deutsches Rotes Kreuz - Generalsekretariat
- Dutko Worldwide
- International Atomic Energy Agency
- Robert-Koch-Institut
- Senatsverwaltung für Gesundheit, Umwelt und Verbraucherschutz, Berlin
- Zweckverband Bodensee-Wasserversorgung

8.30 Empfang mit Kaffee und Tee
Ausgabe der Unterlagen zur Fachtagung

9.00 Eröffnung des ersten Tages durch den Vorsitzenden,
Dr. Heiko Borchert,
Dr. Heiko Borchert & Co. Consulting & Research

9.15
Der Schutz von Kritischen Infrastrukturen in der Vernetzten Sicherheit
• Definition Kritischer Infrastrukturen für das staatliche Gemeinwesen
• Bedarfsanalyse: Welche Einrichtungen fallen unter die Definition Kritischer Infrastrukturen?
• Deutsche KRITIS in einem internationalen Umfeld
• Unter welchen Umständen ist eine relevante Krisenschwelle erreicht?
• Konsequenzen aus der wechselseitigen Vernetzung von Infrastruktursystemen

Oberst i.G. Ralph Thiele,
Vorsitzender der Politisch-Militärischen Gesellschaft

10.00
Risiken für Kritische Infrastrukturen - Bedrohungen von Außen und Innen
• Was sind die größten Risiken? - Eintrittswahrscheinlichkeiten und Ausmaße aus Sicht eines Versicherers
• Kleine Ursache - große Wirkung: Kettenreaktionen und Systemversagen
• Verdrängung des Worst Case - Beschreibung von verschiedenen Szenarien
• Ausblick: zukünftige interne Ausfallursachen
• Risiken als Schlüssel für neue Chancen - Die Entstehung innovativer Marktchancen und neuer Kritischer Infrastrukturen

Dr. Rudolf Kreutzer,
Allianz Global Corporate & Specialty, Research & Development/Think Tank

10.45 Kaffeepause

11.15
Herausforderungen durch kombinierte und interdependente Krisenszenarien für KRITIS
• Natürliche, soziale, politische, ökonomische und technische Entwicklungen mit Risikopotenzial
• Beispielhafte Einzelereignisse als Impuls für Kettenreaktionen
• Wann ist eine Katastrophendimension erreicht, und was sind die Folgen für die Gesellschaft?
• Informationsunsicherheit vs. Risikokommunikation: Wie kann die Selbsthilfekompetenz der Gesellschaft gesteuert werden?
• Erforderliche Elemente der Vorsorgeleistung

Dr. Alexander Fekete,
II.4 Gefährdungskataster, Schutzkonzepte Kritischer Infrastrukturen, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)

12.00
Koordination von Krisenmanagement unter föderalen Rahmenbedingungen
• Die Rolle des Bundes in föderalen Strukturen des Krisenmanagements
• Unterstützungsleistungen des Bundes bei Schadenslagen von nationaler Bedeutung
• Vorteile vereinheitlichter Führungsstrukturen und ressortgemeinsamer Krisenbewältigung
• Zusammenwirken von Staat und Wirtschaft im Krisenmanagement
• Maßnahmen zur gezielten Schärfung eines Krisenbewusstseins in der Bevölkerung

René Du Bois,
Referatsleiter Koordinierungszentrum Krisenmanagement (KM 1), Bundesministerium des Innern

12.45 Gemeinsames Mittagessen

14.15
An overview of the US Critical Infrastructure Protection (CIP) Model and Activities
• How US CIP efforts are interacting with foreign partners, focusing on transatlantic partnerships
• Dependencies and interdependencies, and the impact on national security
• Infrastructure failures due to all-hazards threats (man-made vs. natural disaster related): what does the US CIP model focus on?
• Possible mechanisms and frameworks by which international CIP partnership may increase resiliency and mitigate/minimize risks
• How to connect public and private stakeholders and establish partnerships

Chris Krebs,
Vice President, Dutko Worldwide

15.00
Gefahren durch Kriminalität für die Kritische Infrastruktur
• Was sind aus Sicht des BKA aktuell die relevanten Bedrohungsszenarien?
• Gefahrenpotenzial durch kriminelle oder terroristische Aktionen
• Wirtschaftskriminalität und ihre Erscheinungsformen: Wer sind die Täter?
• Beobachtungen zu den Tatmustern bei Organisierter Kriminalität
• Mit welchen Instrumenten und Kompetenzen müssen Ermittlungsbehörden ausgestattet sein, um ihren Beitrag zum Schutz der Kritischen Infrastruktur leisten zu können?
• Public Private Security: Wie können sich Staat, Wirtschaft und Gesellschaft wirksam gegen Bedrohungen schützen?

Jörg Ziercke,
Präsident, Bundeskriminalamt

15.45 Kaffeepause

16.15
Elemente leistungsfähiger Organisationen für das Krisenmanagement
• Phasen des Risikomanagements von Planung bis Nachbereitung
• Welche Voraussetzungen müssen für ein erfolgreiches Krisenmanagement im Vorfeld geschaffen werden?
• Wann muss das Krisenmanagement in operative Prozesse von Einrichtungen eingreifen?
• Stärken und Schwächen öffentlicher vs. privater Akteure beim Schutz Kritischer Infrastrukturen

Dr. Johannes Richert,
Bereichsleiter Nationale Hilfsgesellschaft/internationale Zusammenarbeit, Deutsches Rotes Kreuz, Generalsekretariat

17.00
Einsatzmöglichkeiten des THW bei Großschadenlagen
• Gesetzlicher Auftrag, Daten und Fakten zum THW
• Einsatzoptionen des THW bei Großschadenlagen
• Unterstützungsmöglichkeiten und -grenzen für Kritische Infrastrukturen
• Zusammenarbeit des THW mit privaten und öffentlichen Akteuren

Albrecht Broemme,
Präsident der Bundesanstalt Technisches Hilfswerk

17.45 **Zusammenfassung durch den Vorsitzenden und Ende des ersten Tages**

Im Anschluss an das offizielle Programm der Fachtagung lädt die Vereon AG alle Referenten und Teilnehmer im Tagungshotel ein. Lassen Sie den Tag bei einem kleinen Imbiss ausklingen. Nutzen Sie die Gelegenheit, sich in ungezwungener Atmosphäre mit Ihren Kollegen auszutauschen und wertvolle Kontakte zu vertiefen.

9.00

Eröffnung des zweiten Tages durch den Vorsitzenden

9.15

Nuclear Security und Schutz Kritischer Infrastrukturen - die Arbeit der Internationalen Atomenergieorganisation (IAEA)

- Definition von Nuclear Security
- Schlüsselemente eines globalen Nuclear Security Regimes
- Die Wirkung von internationalen Rechtsinstrumenten zur Verbesserung von Nuclear Security
- Wie wirken eine global wachsende Energienachfrage und die Anforderungen der Nuclear Security aufeinander?
- Maßnahmen zur Förderung gemeinsamer Sicherheitsinteressen: Der Beitrag der IAEA

**Karin Burmester,
Senior Nuclear Security Officer, Department of Nuclear Safety and Security,
International Atomic Energy Agency**

10.00

Multilaterale Sicherheitsstrukturen in der Wasserversorgung

- Notwendige Elemente für einen Krisenplan und Ansätze der Public Private Security
- Rollenverteilung im Krisenstab und Aufgabenbeschreibungen
- Wie kann der Zeithorizont von Maßnahmen im Krisenfall möglichst gering gehalten werden?
- Abbildung und Kommunikation von Prozessen in Krisenszenarien
- Herausforderungen in der multilateralen Zusammenarbeit am Beispiel des Dreiländerecks

**Martin Sigle,
Abt. WV (Wasserverteilung), Zweckverband Bodensee-Wasserversorgung**

10.45 Kaffeepause

11.15

Herausforderungen an die Security in der internationalen Logistik

- Aufrechterhaltung der logistischen Netzwerke als Element der KRITIS
- Externe Bedrohungen für logistische Netzwerke - logistische Netzwerke als Mittel für Bedrohungen
- Schleichende Prozesse mit Auswirkungen auf sicheren weltweiten Warenverkehr
- Lageanalyse und Vernetzung von Sicherheitsstrukturen als Instrumente des Risikomanagements
- Anforderungen an die Zusammenarbeit von öffentlichen Akteuren und Wirtschaft aus Sicht eines global agierenden Logistikdienstleisters

**Sabine Wiedemann,
Vice President Corporate Security, Deutsche Post DHL**

12.00 Gemeinsames Mittagessen

13.45

Sicherheit im Luftverkehr - Zusammenarbeit der Systempartner Fluggesellschaft, Flughafen und Sicherheitsbehörden

- Anforderungen an und Herausforderungen für eine Sicherheitsorganisation
 - Aktuelle und künftige Risiken
 - Qualitäts- und Risikomanagement im Bereich Luftsicherheit
- Zu schützende Unternehmenswerte eines börsennotierten und global tätigen Konzerns
- Aufgabenportfolios der LH Sicherheitsorganisation
- Kooperation mit Systempartnern bei der Krisenbewältigung
- Kooperation bei der Krisenprävention
- Zusammenarbeit zwischen Industrie und Sicherheitsbehörden
- Balancing Security: Einklang von Sicherheit, Wirtschaftlichkeit und Kundenfreundlichkeit

**Jürgen Faust,
Leiter Luftsicherheit, Deutsche Lufthansa AG**

14.30

Aktuelle Rahmenbedingungen im Krisenmanagement am Beispiel einer Pandemie

- Entwicklung von Erkenntnissen zu Pandemieszenarien am Beispiel der Neuen Influenza: Welche gesicherten Kenntnisse können Maßnahmen im Gesundheitssystem auslösen?
- Kennzahlen zur Ausbreitung der Neuen Influenza und Stand der öffentlichen Diskussionen im Rückblick
- Besondere Herausforderungen in Notfallplanung und Koordination von Maßnahmen am Beispiel H1N1
- Impfungen im Unternehmen: Rechte und Pflichten
- Zusammenarbeit von Industrie und öffentlichen Einrichtungen im Krisenfall aus Sicht einer dem Bundesministerium für Gesundheit unterstellten Einrichtung

**Dr. Gérard Krause,
Leiter Abteilung Infektionsepidemiologie, Robert-Koch-Institut**

15.15 Kaffeepause

15.45

Präventive Maßnahmen gegen Pandemien im Zusammenspiel öffentlicher und privatwirtschaftlicher Akteure

- Wie viel zeitlicher Vorlauf ist für ein flächendeckendes Impfkonzept erforderlich?
- Auf Basis welcher Entscheidungsparameter müssen die verantwortlichen öffentlichen Stellen entscheiden?
- Grundlagen der Kosten-Nutzen-Betrachtung für die Bevorratung von Impfstoffen
- Maßnahmen durch gesellschaftliche und wirtschaftliche Akteure: Rechte, Pflichten, Empfehlungen
- Lessons learned nach H1N1: Maßnahmen zur kontinuierlichen Weiterentwicklung des Infektionsschutzes

**Dr. Marlen Suckau,
Senatsverwaltung für Gesundheit, Umwelt und Verbraucherschutz, Berlin**

16.30

Reale versus gefühlte Risiken - zielgruppengerechte Risikokommunikation als Strategie

- Subjektive Wahrnehmung von Risiken versus objektiv vorhandene Risiken
- Analyse von Wahrnehmungsmustern und Typisierung von Zielgruppen
- Interaktive Einbindung von Stakeholdern aus den Bereichen Wissenschaft, Wirtschaft, Politik, öffentliche Institutionen, Medien, NGO, Verbände und Verbraucherschaft
- Evaluation von Dialogformaten auf Erreichbarkeit definierter Zielgruppen
- Beispiele erfolgreicher Risikokommunikation
- Vermeiden von Krisen vor ihrer Entstehung (non events)

**PD Dr. rer. nat. Gaby-Fleur Böll,
Leiterin Abteilung Risikokommunikation, Bundesinstitut für Risikobewertung (BfR)**

17.15 **Zusammenfassung durch den Vorsitzenden und Ende der Fachtagung**

8.45 **Empfang mit Kaffee und Tee**
Ausgabe der Unterlagen zum Workshop

Die Pausen werden flexibel festgelegt.

9.00 **Beginn des Workshops**
Risiken, Krisen und Prävention in interdependenter KRITIS

16.30 **Zusammenfassung durch den Workshopleiter**

Ihr Workshopleiter

Dr. Frank Umbach ist Senior Associate und Programmleiter am Centre for European Security Strategies (CESS), München/Berlin, sowie ein unabhängiger Konsultant. Nach seiner Tätigkeit beim BIOST in Köln, im Büro des NATO-Generalsekretärs in Brüssel und mehreren Forschungsaufenthalten in den USA, Moskau und Tokio in den 90er Jahren hat er u.a. das Programm "Internationale Energiesicherheit" in der DGAP von 1996 bis Ende 2007 geleitet. Er ist Regionalexperte zu sicherheitspolitischen Fragen in der EU, der NATO, Russland und Ostasien. Seit 2003 ist Dr. Umbach Co-Chair des European Committee of the Council for Security Cooperation in Asia-Pacific und derzeit u.a. Mitglied einer hochrangigen transatlantischen Expertengruppe zu Energiesicherheit sowie einer zu den künftigen NATO-Russland-Beziehungen. In den letzten Jahren hat er schriftliche Expertisen für die Europäische Kommission, das Europäische Parlament, das Auswärtige Amt, das BMVg, die NATO, das US-Außenministerium, die U.S.-China Economic and Security Review Commission des US-Kongresses sowie das House of Lords (Britisches Oberhaus/Parlament) in London verfasst.

Thema und Ziel des Workshops

Kritische Infrastrukturen: Bedrohungspotenzial und Risikoszenarien

- Gefahrenlage für die Kritische Infrastruktur
- Risikoszenarien für einzelne Elemente der KRITIS in Deutschland
- Schleichende Prozesse vs. Einzelereignisse: Ursachen für Krisen
- Möglichkeiten zur Beurteilung von Schadensausmaß und -dauer

So vielfältig die Elemente der Kritischen Infrastrukturen sind, so vielfältig sind auch die bestehenden Risiken beschaffen. Im ersten Abschnitt geht der Workshopleiter von einer abstrakten Einschätzung der Gefahren zu konkreten Risikoszenarien über. Eine grobe Orientierung bietet dabei u.a. der Leitfaden des BMI zur KRITIS. Gegenstand der Analyse ist weiterhin, Ereignisse und schleichende Prozesse auf ihre Wirkungen hin zu untersuchen. Teilnehmer werden für die unterschiedlichen Vorwarnzeiten sensibilisiert, die sich für einzelne Szenarien ergeben. Ebenso soll - hier noch an einzelnen Vorgängen - dargestellt werden, wie schwer Ausmaß und Gestalt von krisenhaften Ereignissen einzuschätzen sind. In diesem Themenblock nimmt der Workshopleiter Bezug auf die an den vorherigen Konferenztagen erörterten Szenarien.

Interdependenzen und Kaskadeneffekte in vernetzten Elementen der KRITIS

- Ermittlung von Interdependenzen in der Kritischen Infrastruktur
- Risiken für das Eintreten von krisenhaften einzelnen Ereignissen und möglichen Verkettungen
- Entwicklung von Kaskadeneffekten an Beispielen
- Zeitliche Abfolge von krisenhaften Entwicklungen und erforderliche Reaktionszeiten

Interdependenzen und wechselseitige Vernetzung prägen die Elemente Kritischer Infrastrukturen. Ausgehend von einzelnen Ereignissen als Impulse werden durch den Workshopleiter Kaskadeneffekte thematisiert: Was passiert nach einem krisenhaften Ereignis in einer Welt voller vernetzter Strukturen und somit vernetzter Risiken? Diese Kaskadeneffekte werden mithilfe einer Zeitschiene entwickelt, um ein komplexes Bild der tatsächlichen Risiken und weiterreichender Implikationen zu gewinnen.

Maßnahmen zur Krisenbewältigung

- Beteiligte Akteure in Krisensituationen
- Aufgabenverteilung: Wie kann das Zusammenwirken von öffentlichen und privaten Akteuren koordiniert werden?
- Kommunikation von Maßnahmen und Zuständigkeiten unter erschwerten Bedingungen bei Großschäden
- Welche Instrumente der Krisenbewältigung sind verfügbar?
- Erforderliche Ansätze der Risiko- und Gefahrenkommunikation

Im Anschluss an die vollständige Erfassung der Risiken und der ihnen zugrunde liegenden Interdependenzen ermitteln die Teilnehmer des Workshops erforderliche Maßnahmen zur Krisenbewältigung. In einem ersten Arbeitsschritt sollen die Instrumente erfasst werden, wie sie prinzipiell, also in einem Idealszenario, verfügbar sind. Diese Instrumente sollen nun anhand der vorher festgehaltenen Kaskadeneffekte auf den Grad ihrer Funktionsfähigkeit geprüft und gegebenenfalls ergänzt werden. In diesem Zusammenhang werden zugleich die Akteure benannt, die einen Beitrag zur Krisenbewältigung und der buchstäblichen Public Private Security leisten können.

Elemente der Krisenprävention und der Risikominderung für die KRITIS

- Von Krise und Risikobewertung zur Prävention: konzeptionelle Grundlagen
- Leben mit und Kommunikation von Restrisiken
- Akteure und Lösungskompetenzen: Wer kann welchen Beitrag zur Prävention leisten?
- Konkrete Maßnahmen zur Krisenprävention und interne Voraussetzungen

Mit dem Stichwort PPS ist zugleich der abschließende Themenblock eingeleitet, nämlich ein Konzept zur Prävention unter Einbezug aller Akteure. Mit Blick auf den Leitfaden "Nationale Strategie zum Schutz Kritischer Infrastrukturen", den das Bundesministerium des Innern herausgegeben hat, soll ein flexibler Katalog an Maßnahmen in der Gruppe erarbeitet werden. Zielsetzung ist dabei, Risiken wirksam zu reduzieren und im erforderlichen Fall unter Einbezug aller relevanten öffentlichen und privaten Akteure Krisen bewältigen zu können. Die klare Zuordnung von Aufgaben und Zuständigkeiten wird in diesem Abschnitt im Mittelpunkt stehen, ebenso die strukturierte Koordination der Lösungskompetenzen.

Sehr geehrte Damen und Herren,

Staatssekretär Dr. August Hanning hat auf der Fachtagung KRITIS im März 2009 zum Abschluss seiner Key Note formuliert: "Um den Schutz kritischer Einrichtungen weiter zu verbessern, benötigen wir vor allem die Fähigkeit zur Zusammenarbeit aller Beteiligten. Es bedarf eines offenen Dialogs zwischen Staat und Wirtschaft und des Ausbaus der Sicherheitspartnerschaften auf allen Ebenen."

Über hundert Teilnehmer haben im folgenden auf der Veranstaltung diesen Anspruch mit Leben gefüllt. Kooperation zum Zwecke der Erhöhung von Sicherheit - das ist mehr als überschneidende Interessen, es ist angesichts veränderter Bedrohungsszenarien eine Notwendigkeit. Wirksame Konzepte zum Schutz Kritischer Infrastrukturen müssen eine Vielzahl an Akteuren zusammenführen, so dass sich zwei besondere Herausforderungen ergeben: zum einen die Koordination aller Kräfte in Prävention als auch Krisenbewältigung; zum anderen die Berücksichtigung von interdependenten Szenarien, von Kaskadeneffekten. In einer Welt vernetzter Sicherheit sind Risiken wie Lösungskompetenzen engmaschig vernetzt.

Wie die Potenziale konstruktiv genutzt werden können, soll ein leitendes Thema inmitten einer vielschichtigen Fachtagung sein. Gemeinsam mit den Referenten freuen wir uns auf anregende Diskussionen zu den aktuellen Herausforderungen.

Mit freundlichen Grüßen,



Dr. Björn Nehls
Director, Vereon AG

Behörden Spiegel
Unabhängige Zeitschrift für den Öffentlichen Dienst

**CD Sicherheits-
Management**

**DEFENCE.
PROFESSIONALS**

**griephan
global security**

IIMS Sicherheitspolitik • Streitkräfte • Technik
Internationales Magazin für Sicherheit

Wik Zeitschrift
für die Sicherheit
der Wirtschaft

Public Private Security Schutz Kritischer Infrastrukturen

Ja, hiermit melde ich mich verbindlich an für:

Fachtagung und Workshop vom 22. bis 24. März 2010

- Reguläre Teilnahmegebühr 1.895 EUR (zzgl. MwSt.)
- Teilnahmegebühr für Ministerien, Behörden und Institutionen mit besonderen öffentlichen Aufgaben 695 EUR (zzgl. MwSt.)

Fachtagung am 22. und 23. März 2010

- Reguläre Teilnahmegebühr 1.495 EUR (zzgl. MwSt.)
- Ermäßigte Teilnahmegebühr 495 EUR (zzgl. MwSt.)

Workshop am 24. März 2010

- Reguläre Teilnahmegebühr 995 EUR (zzgl. MwSt.)
- Ermäßigte Teilnahmegebühr 395 EUR (zzgl. MwSt.)

1. PERSON

Anrede, Titel

Name, Vorname

Position, Abteilung

E-Mail

Firma

Strasse, Nr.

Postfach

PLZ, Ort

Land

2. PERSON

Anrede, Titel

Name, Vorname

Position, Abteilung

E-Mail

RECHNUNGSDetails

Bestellreferenz

MwSt.-Nr.

Firma

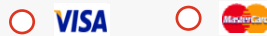
Abteilung

Straße

PLZ, Ort

Datum, Unterschrift

Bei Zahlung per Kreditkarte bitte ausfüllen:



Karteninhaber

Kartennummer

gültig bis

Datum, Unterschrift

VERANSTALTUNGSORT

Esplanade Grand Hotel Berlin
Lützowufer 15
10785 Berlin

Telefon +49 30 25478 0
Web www.esplanade.de

ANMELDUNG

Web vereon.ch
Telefon +41 71 677 8700
Fax +41 71 677 8701
E-Mail info@vereon.ch
Post Vereon AG
Postfach 2232
8280 Kreuzlingen
Schweiz

TEILNAHMEGEBÜHR

Die Teilnahmegebühr beinhaltet die Teilnahme für eine Person. Sie versteht sich inklusive schriftlicher Unterlagen, Mittagessen und Tagungsgetränke zzgl. MwSt. Nach Eingang Ihrer Anmeldung erhalten Sie eine Anmeldebestätigung und eine Rechnung. Diese ist in jedem Fall vor Eintritt in die Veranstaltung fällig.

STORNIERUNG

Sollten Sie an der Teilnahme verhindert sein, so akzeptieren wir natürlich ohne zusätzliche Kosten einen Ersatzteilnehmer. Darüber hinaus ist eine vollständige Stornierung bis dreißig Tage vor Beginn der Veranstaltung kostenlos möglich. Die Stornierung bedarf der Schriftform. Bei späterem Rücktritt oder Nichterscheinen wird die gesamte Teilnahmegebühr fällig. Programmänderungen aus dringendem Anlass behält sich der Veranstalter vor. Jegliche Haftung für hieraus entstehende Schäden oder entgangene Gewinne seitens des Teilnehmers ist ausgeschlossen.

DATENSCHUTZ

Wir behandeln Ihre Daten in Übereinstimmung mit den geltenden datenschutzrechtlichen Bestimmungen. Zum Zwecke der Leistungserbringung speichern wir Ihre Daten. Wünschen Sie eine Löschung Ihrer Daten, so teilen Sie uns dies bitte an info@vereon.ch mit.