

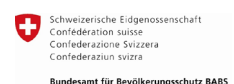
CRN TAGUNGSBERICHT

Naturgefahren & Ausfall von kritischen Infrastrukturen

Praxis-Forum vom 11. November 2010,
Geoprotecta, St. Gallen

26. November 2010

Bundesamt für Bevölkerungsschutz (BABS), Bern
Center for Security Studies (CSS), ETH Zürich
IBCOL Technologies & Consulting AG, Küsnacht



Dieser Bericht ist auf der Webseite www.crn.ethz.ch erhältlich

Center for Security Studies, ETH Zürich

Autorin: Corinne Bara

Adresse:

Center for Security Studies (CSS)

ETH Zürich

Haldeneggsteig 4, IFW

8092 Zürich / Schweiz

Tel. +41 44 632 40 25

Fax +41 44 632 19 41

www.crn.ethz.ch

crn@sipo.gess.ethz.ch

INHALTSVERZEICHNIS

1	EINLEITUNG	2
2	NATURGEFAHREN UND SCHUTZ VON KRITISCHEN INFRASTRUKTUREN: GRUNDLAGEN DES INTEGRALEN RISIKOMANAGEMENTS.....	3
2.1	Die nationale Strategie zum Schutz Kritischer Infrastrukturen	3
2.2	Die kritischen Infrastrukturen der Schweiz und der Begriff der Kritikalität.....	3
2.3	Massnahmen und Umsetzung 2009-2011	3
2.4	Erkenntnisse	5
3	WIE SCHÜTZT MAN KRITISCHE INFRASTRUKTUREN: TIPPS FÜR KRISEORGANE	6
3.1	Klare Methodik	6
3.2	Stufengerechte Planung	7
3.3	Kontinuierliche Verbesserung.....	8
4	HOCHWASSERVORHERSAGEN AN DER SIHL: VON DER VORHERSAGE ÜBER DIE WARNUNG ZUR HANDLUNG	9
4.1	Das Projekt «Hochwassermanagement Zürichsee-Sihl-Limmat».....	9
4.2	Idee: Der Rückhalt von Wasser im Sihlsee.....	10
4.3	Herausforderungen im Hochwasserschutz in Zürich.....	10
5	STROMPANNE 2005: AUSWIRKUNGEN UND LEHREN AUS DER SICHT DES KRISENMANAGEMENT SBB.....	12
5.1	Die SBB und der Schutz Kritischer Infrastrukturen	12
5.2	Das Krisenmanagement der SBB.....	13
6	FAZIT	14
	ANHANG: REFERENTEN	15

1 EINLEITUNG

Am 11. November 2010 trafen sich Vertreter aus Deutschland, Österreich, dem Fürstentum Liechtenstein und der Schweiz von lokalen, kantonalen und nationalen Behörden sowie Führungsstäben, Partnerorganisationen des Bevölkerungsschutzes, Infrastrukturbetreiber und Experten zu einem zweistündigen Praxis-Forum. Im Zentrum stand der Schutz von kritischen Infrastrukturen vor Naturgefahren. Das Praxis-Forum fand im Rahmen der Fachmesse Geoprotecta für integrales Risikomanagement von Naturgefahren und Klimafolgen in St. Gallen statt.

Die Herausforderungen beim Schutz Kritischer Infrastrukturen (SKI) können nur gemeinsam angegangen werden. Das Hauptziel der Veranstaltung war daher, den interdisziplinären, kollektiven Ansatz bei der Zusammenarbeit zwischen Bevölkerung, Behörden, Betreibern und Experten zu unterstreichen und zu fördern. Zwar ist die Kultur des Miteinanders im föderalen System Schweiz durchaus verankert, doch

für die SKI-Verantwortlichen stellen die zunehmende Verästelung der politischen Entscheidungskompetenzen und die Fragmentierung von Handlungsspielräumen auch in der Schweiz eine grosse Herausforderungen dar.

In den vier Referaten wurde das Thema SKI aus vier verschiedenen Perspektiven beleuchtet: Aus der Sichtweise der Bundesverwaltung, einer Beratungsfirma im Bereich Sicherheits- und Risikomanagement; eines Fachexperten in der kantonalen Verwaltung und aus der Sicht eines Infrastrukturbetreibers.

Die zentrale Rolle des integralen Risikomanagements (siehe Abb.1) zog sich als roter Faden durch das gesamte Praxis-Forum. Während der Veranstaltung kristallisierten sich noch weitere wichtige und übergreifende Aspekte von SKI heraus; diese werden im Schlussteil dieses Tagungsberichts zusammengefasst.

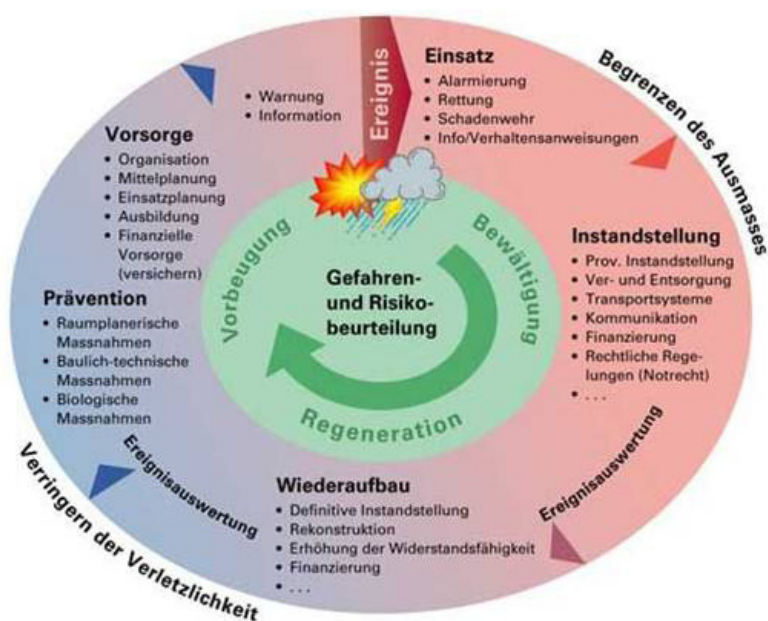


Abbildung 1: Kreislauf des integralen Risikomanagement (Quelle: BABS).

2 NATURGEFAHREN UND SCHUTZ VON KRITISCHEN INFRASTRUKTUREN: GRUNDLAGEN DES INTEGRALEN RISIKOMANAGEMENTS

Präsentation: Dr. Stefan Brem, Bundesamt für Bevölkerungsschutz (BABS)

Das Bundesamt für Bevölkerungsschutz hat beim Schutz Kritischer Infrastrukturen in erster Linie eine Koordinationsfunktion. Das übergeordnete Ziel ist, die Bevölkerung und ihre Lebensgrundlagen zu schützen, wobei Gesellschaft, Politik und Wirtschaft gleichermaßen auf ein funktionierendes Netz von Infrastrukturen angewiesen sind. Während sich viele Stellen in ihrem Zuständigkeitsgebiet seit langem mit dem Schutz von wichtigen Anlagen und Einrichtungen befassen, hat auf nationaler Ebene lange Zeit eine übergeordnete Koordination und ein einheitliches Vorgehen gefehlt. Das BABS erarbeitet daher im Auftrag des Bundesrats eine nationale Strategie zum Schutz Kritischer Infrastrukturen, um diese Koordination und das einheitliche Vorgehen zu gewährleisten.

2.1 Die nationale Strategie zum Schutz Kritischer Infrastrukturen

Im Rahmen des nationalen SKI-Programms wurde vom Bundesrat am 5. Juni 2009 eine Grundstrategie zum Schutz Kritischer Infrastrukturen verabschiedet. Die Grundstrategie ist das Resultat der ersten zwei Phasen des nationalen SKI-Programms. In Phase 1 (Abschluss 2007) wurden zentrale Begriffe erklärt, die für die Schweiz relevanten kritischen Infrastrukturen definiert, ein Überblick über nationale und internationale SKI-Aktivitäten gewonnen und das weitere Vorgehen für die Erarbeitung der nationalen SKI-Strategie festgelegt. In Phase 2 (Abschluss 2009) wurde eine Beispielstudie Erdbeben und SKI-Gefährdungsszenarien erarbeitet und kritische Teilsektoren definiert und entsprechend gewichtet. Auf der Basis dieser Grundstrategie werden nun in der aktuellen dritten Phase (2009–2011) zahlreiche Massnahmen umgesetzt und die nationale SKI-Strategie für 2012 erarbeitet. Das BABS koordiniert die Tätigkeiten zur Erarbeitung der SKI-Strategie und leitet die SKI-Arbeitsgruppe, in der 29 Bundesstellen aus sieben Departementen sowie der Bundeskanzlei und zwei Kantone vertreten sind. Zentrale Grundsätze im nationalen SKI-Programm sind ein umfassendes Gefährdungsspektrum, die Orientierung am integralen

Risikomanagement, die Subsidiarität, die Verhältnismässigkeit des Mitteleinsatzes (Sicherheitsoptimierung) und die Resilienz (Widerstandsfähigkeit).

2.2 Die kritischen Infrastrukturen der Schweiz und der Begriff der Kritikalität

Der Bund hat in den ersten zwei Phasen 10 kritische Sektoren und 28 kritische Teilsektoren identifiziert und diese nach ihrer Kritikalität gewichtet. Die 10 identifizierten Sektoren (siehe Abb. 2) decken sich in etwa mit kritischen Sektoren anderer Länder im internationalen Vergleich.

Die **Kritikalität** ist dabei ein zentraler Begriff. Die Kritikalität eines Teilsektors wird bestimmt durch dessen Auswirkungen auf andere Teilsektoren im Schadensfall (Dependenz), die Auswirkungen auf die Bevölkerung und die Auswirkungen auf die Wirtschaft. Der Bund ist in seiner Rolle als SKI-Koordinator in erster Linie am sektorübergreifenden Schutz interessiert, weswegen die Kritikalität nichts über die Bedeutung der Teilsektoren «an sich» aussagt, sondern sich an Interdependenzen orientiert.

2.3 Massnahmen und Umsetzung 2009-2011

Die folgenden Massnahmen werden auf der Basis der Grundstrategie von 2009-2011 umgesetzt.

- ♦ **Priorisierung der kritischen Infrastrukturen**
Das Ziel ist ein Verzeichnis von national kritischen Infrastruktur-Objekten. Dieses soll den bisherigen vom Führungsstab der Armee erstellten Objektkatalog zur Sicherstellung existentieller Bedürfnisse (SEB) ersetzen bzw. hinsichtlich berücksichtigter Sektoren, Betreiber, Gefahren und Schutzmassnahmen erweitern. Eine Methode zur Erstellung des Inventars wurde in der Arbeitsgruppe SKI erarbeitet und wird bereits in einigen Sektoren wie Verkehr und Energie angewendet. Die eigentliche Identifikation der Objekte von nationaler Bedeutung erfolgt mit Hilfe von sogenannten Expertenkomitees. In diesen Expertenkomitees sind jeweils die für den Teilsektor zuständigen Bundesstellen, sowie die wichtigsten Betreiber in diesem Teilsektor vertreten.

♦ **Schutz durch umfassende Konzepte**

Der Schutz der kritischen Infrastrukturen soll mit Hilfe von umfassenden Schutzkonzepten gewährleistet werden. Dabei wird auf zwei Ebenen vorgegangen, wobei das Kontinuitätsmanagement jeweils eine wichtige Rolle spielt:

Auf Stufe der kritischen Infrastruktur-Objekte wird unter anderem ein Leitfaden entwickelt, der als Grundlage zur Erarbeitung von Schutzkonzepten dient. Der Leitfaden wird für Objekte aus allen kritischen Infrastruktur-Sektoren anwendbar sein. Er berücksichtigt dabei bereits bestehende Massnahmen.

Auf Stufe der kritischen Infrastruktur-Teilsektoren wird ein Rahmenprozess festgelegt, der als Grundlage zur Sicherstellung der kontinuierlichen Leistungsfähigkeit der kritischen Infrastrukturen, respektive der raschen Wiederaufnahme der Kernprozesse im Fall von Störungen dient.

♦ **Erarbeitung von Grundlagen**

Für verschiedene Herausforderungen im SKI-Bereich, wie etwa wechselseitige Abhängigkeiten und Kaskaden-Effekte im Fall von Störungen,

sind weitere Grundlagenarbeiten notwendig, um wirkungsvolle Gegenmassnahmen treffen zu können. Zu diesem Zweck besteht eine enge Forschungszusammenarbeit mit verschiedenen Schweizer Hochschulen (u.a. ETH Zürich) und europäischen Forschungsinstituten. Ein Schwerpunkt liegt auch hier beim sektorübergreifenden Schutz Kritischer Infrastrukturen und der sektorübergreifenden Risikoanalyse.

♦ **Förderung der Risikokommunikation**

Vielerorts fehlt das Bewusstsein für die Bedeutung von kritischen Infrastrukturen und die möglichen Folgen von Störungen. Deshalb werden Akteure auf verschiedenen Stufen (Bund, Kantone, Betreiber) sowie die Bevölkerung mit Informationsprodukten, Referaten und Ausbildungssequenzen sensibilisiert und über Verhaltensmassnahmen und Schutzmöglichkeiten orientiert. Ein wichtiges Instrument dafür ist die SKI-Homepage (www.infraprotection.ch), auf der über aktuelle SKI-relevante Ereignisse, neueste Publikationen im SKI-Bereich sowie über den Stand der SKI-Arbeiten informiert wird.

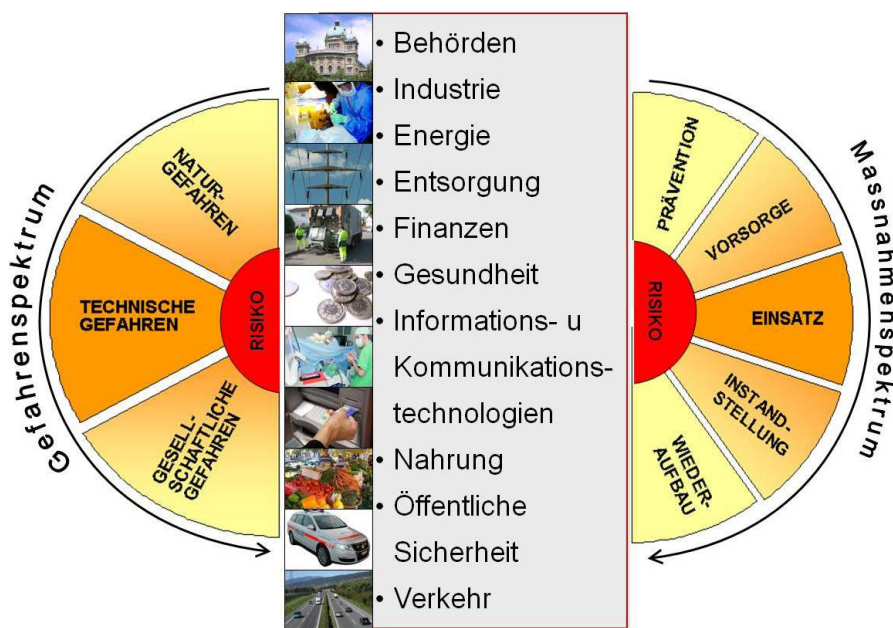


Abbildung 2: Die zehn kritischen Sektoren, das Spektrum der Gefährdungen und das Massnahmenspektrum (Quelle: BABS).

2.4 Erkenntnisse

SKI ist ein Thema mit wachsender Bedeutung. Dabei sind verschiedene Akteure (Staat, Wirtschaft, Bevölkerung) mit unterschiedlichen Interessen zu berücksichtigen. Dies bedingt einen kontinuierlichen Risikodialog, Koordination und Kooperation. SKI ist zudem als Prozess und nicht als Zustand zu verstehen. Da nicht alle kritischen Infrastrukturen jederzeit und hundertprozentig geschützt werden können, gilt es, Prioritäten zu setzen und Restrisiken zu berücksichtigen. In diesem Zusammenhang gewinnt das Konzept der Resilienz von Infrastrukturen und Gesellschaft an Bedeutung. Kritikalität bezieht sich auf

die Interdependenz von Teilsektoren und die Auswirkungen eines Ausfalls auf die Bevölkerung und die Wirtschaft. Sie darf nicht mit Verwundbarkeit oder schon gar mit einer tatsächlichen Bedrohung gleich gesetzt werden.

Der SKI-Prozess ist auf die nationale Gefährdungsanalyse «Risiken Schweiz» (www.risk-ch.ch) abgestimmt. Dabei werden u.a. Gefährdungsdossiers von «Risiken Schweiz» für vertiefende SKI-Gefährdungsszenarien verwendet. Allfällige Erkenntnisse zu Interdependenzen von Infrastrukturen können wiederum in die umfassenden Gefährdungsdossiers aufgenommen werden.

3 WIE SCHÜTZT MAN KRITISCHE INFRASTRUKTUREN: TIPPS FÜR KRISENRGANE

Präsentation: Dr. Urs Cipolat, IBCOL Technologies & Consulting AG

Die IBCOL berät Kunden aus der Privatwirtschaft sowie aus der öffentlichen Verwaltung in den Bereichen Sicherheit, Risiko-, Krisen- und Kontinuitätsmanagement. Aufgrund der Zuspitzung der Bedrohungslagen, der Zunahme von regulatorischen Vorgaben und dem erhöhten Erwartungsdruck von Medien und Bevölkerung ist die korrekte Beurteilung von Risiken, der effiziente Schutz von kritischen Infrastrukturen sowie die effektive Bewältigung von Ereignissen für die öffentliche Verwaltung wie auch für private Unternehmen von zunehmender Wichtigkeit. Bei den Infrastrukturbetreibern und Führungsstäben fehlt es häufig nicht am guten Willen, den Schutz von kritischen Infrastrukturen zu gewährleisten. In der Umsetzung jedoch zeigen sich gewisse Mängel. Dazu gehören fehlende Grundlagen (Einsatzmanuale, Kontinuitätspläne), zögerliche Führung und Projektfinanzierung (Leitung setzt andere Prioritäten), unklare Methodik, insbesondere eine fehlende Abgrenzung von Risikomanagement (RM), Krisenmanagement (KM), Kontinuitätsma-

nagement (BCM) und Qualitätsmanagement (QM), fehlende Fachkenntnisse und ein weit verbreitetes Gärtchendenken. Vor diesem Hintergrund haben sich in der Praxis drei Tipps für Krisenorgane besonders bewährt: Es gilt, sich primär um eine klare Methodik, eine stufengerechte Planung und die kontinuierliche Verbesserung der Reaktionsfähigkeit zu kümmern.

3.1 Klare Methodik

Eine intensive Auseinandersetzung mit methodischen Fragen zahlt sich bei der Umsetzung des Infrastruktur-Schutzes aus. Das betrifft auch die Abgrenzung von Begriffen. So müssen die drei Prozesse Vorbeugung (Risikomanagement), Bewältigung (Krisenmanagement) und Regeneration (Kontinuitätsmanagement) innerhalb des integralen Risikomanagements separat behandelt werden (siehe Abb. 3). Vor allem bei der Massnahmenplanung, aber auch bei der Definition von Verantwortlichkeiten oder bei der Durchführung von Übungen ist diese Unterscheidung wichtig.

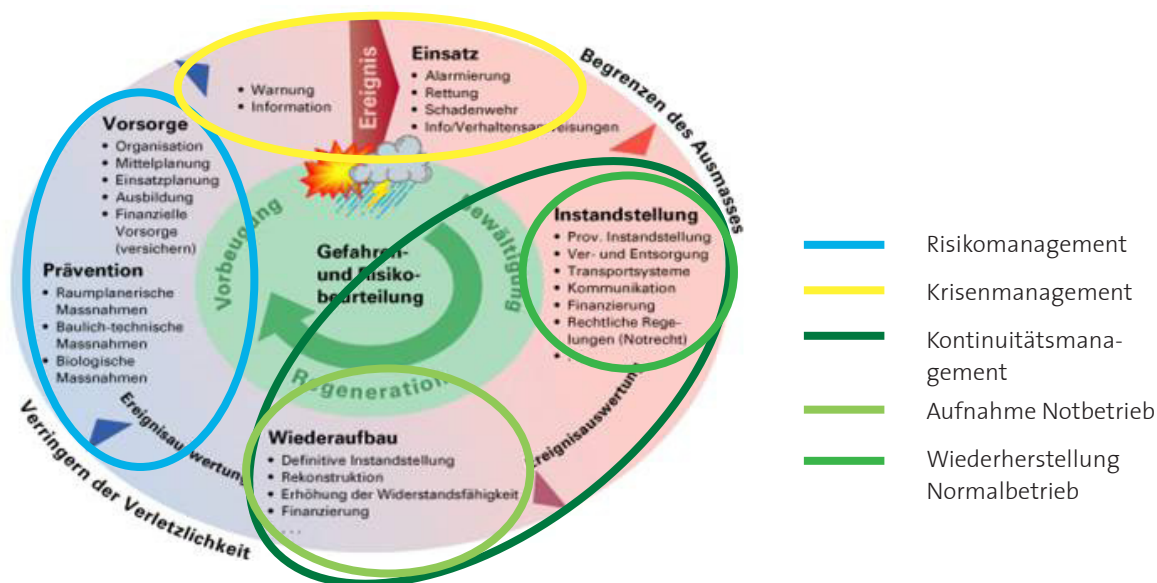


Abbildung 3: Risikomanagement, Krisenmanagement und Kontinuitätsmanagement im Kreislauf des integralen Risikomanagement (Quelle: BABS, angepasst von IBCOL).

Im Kontinuitätsmanagement muss weiter unterschieden werden zwischen Massnahmen zur Aufnahme des Notbetriebs und Massnahmen zur Wiederherstellung des Normalbetriebs. Auch wenn das Kontinuitätsmanagement aus Sicht der Krisenorgane oft «am Ende» der Prozesskette steht, müssen auch in diesem Bereich bereits im Vorfeld von möglichen Ereignissen und basierend auf einer fundierten Risikoanalyse Massnahmen geplant werden. Es gilt, vom Ereignis-getriebenen Krisenmanagement wegzukommen hin zu einem integralen Risikomanagement, mit dem sich der Kreislauf Risikomanagement, Krisenmanagement und Kontinuitätsmanagement schliesst.

3.2 Stufengerechte Planung

Sämtliche Planung soll stufengerecht sein. Jede Stufe (lokal, kantonal, national) muss ihre eigenen kritischen Infrastrukturen unterscheiden und nach deren

Kritikalität bewerten. Was auf lokaler Stufe höchst kritisch ist, muss auf nationaler Stufe nicht notwendigerweise kritisch sein und umgekehrt. Wo es Überschneidungen gibt, müssen die Zuständigkeiten und die Zusammenarbeit kollektiv geklärt werden. Die Zuständigkeiten müssen auch betreffend Eskalation eines Ereignisses geklärt werden. Welches Einsatzorgan beschäftigt sich wann mit welcher Art von Ereignis? Mittels Eskalationsstufen können Zuständigkeiten definiert werden (siehe Abb. 4). Eine zielgerichtete Lagedarstellung nach dem Bring-Prinzip könnte die Krisenorgane dabei unterstützen. Ein weiterer Aspekt, der nur kollektiv geklärt werden kann, ist die Bestimmung der kritischen BCM-Grössen, insbesondere die Frage, wie schnell gewisse Infrastrukturen wieder hergestellt werden sollen. Weil eine schnellere Wiederherstellung letztlich eine Kostenfrage ist, ist die Bestimmung der kritischen BCM-Grössen auch eine politische Diskussion.

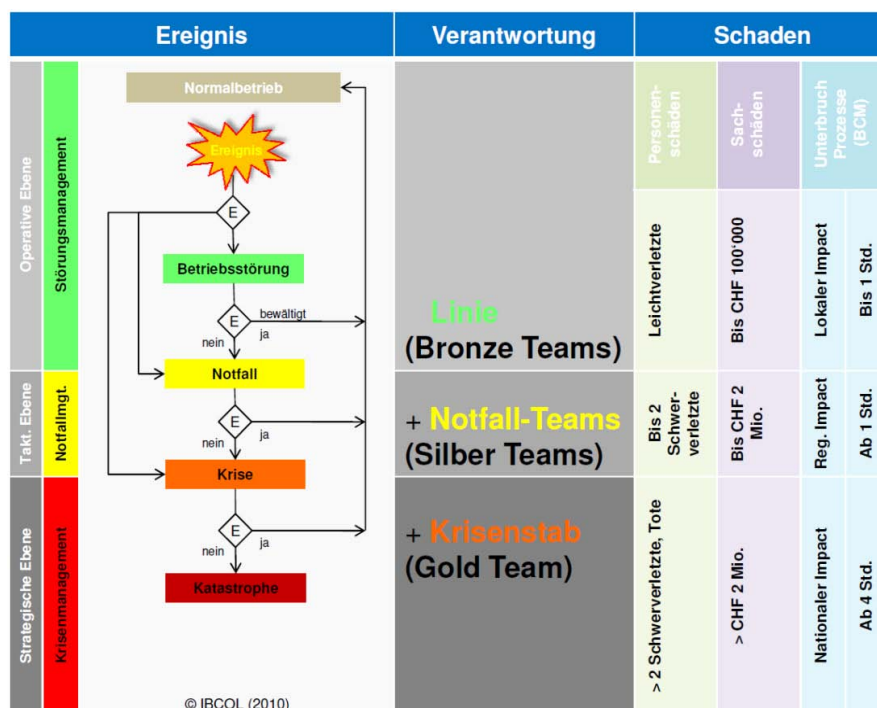


Abbildung 4: Eskalationsstufen und Zuständigkeiten. Aufgaben der Gold-, Silber- und Bronze-Teams (Quelle: IBCOL).

3.3 Kontinuierliche Verbesserung

Für eine kontinuierliche Verbesserung des integralen Risikomanagements und seiner Bestandteile Risikomanagement, Krisenmanagement und Kontinuitätsmanagement bieten sich verschiedene Möglichkeiten an. Im Risikomanagement ist ein Prozessdenken zentral; eine einmalige Risikoanaly-

se reicht nicht, die Risiken müssen regelmässig neu beurteilt werden. Im Krisen- und Kontinuitätsmanagement helfen regelmässige Schulungen, Übungen und Tests bei der Verbesserung. Eine Voraussetzung dafür ist, dass für diese Prozesse Budget zur Verfügung gestellt wird. Neue Software-Tools können ebenfalls in allen drei Prozessen unterstützend eingesetzt werden.

4 HOCHWASSERVORHERSAGEN AN DER SIHL: VON DER VORHERSAGE ÜBER DIE WARNUNG ZUR HANDLUNG

Präsentation: Dr. Matthias Oplatka, Amt für Abfall, Wasser, Energie und Luft im Kanton Zürich

Im Jahr 2005 ist die Stadt Zürich nur knapp einer Hochwasserkatastrophe entgangen. Wäre das Zentrum der Starkniederschläge im Jahre 2005, die entlang des gesamten Alpennordhangs für grosse **Überschwemmungen** gesorgt haben, **über dem Sihl-einzugsgebiet gelegen**, so wären zentrale Gebiete der Stadt Zürich überschwemmt worden. Milliarden-schäden und eine Bahninfrastruktur, die längere Zeit ausser Betrieb gewesen wäre, wären die Folgen gewesen. Dies zeigten Modellrechnungen im Zusammenhang mit der Ereignisanalyse nach dem Hochwasser 2005. Es konnte auch aufgezeigt werden, dass solche Überschwemmungen bereits 1846 und 1910 stattfanden, nur war damals das Schadenpotential wesentlich kleiner (siehe Abb. 5 zum Schadenpotential heute). Das Bewusstsein über diese Gefährdung fehlte bei Stadt und SBB bis vor kurzem weitgehend.

Als Konsequenz aus den gewonnenen Erkenntnissen aus den Hochwasser 2005 hat die Baudirektion das Projekt «Hochwassermanagement Zürichsee-Sihl-Limmat» lanciert. Die Abteilung Wasserbau im kantonalen Amt für Abfall, Wasser, Energie und Luft (AWEL) koordiniert diese Aktivitäten.

4.1 Das Projekt «Hochwassermanagement Zürichsee-Sihl-Limmat»

Mit dem Projekt Hochwassermanagement Zürichsee, Sihl, Limmat werden rund 40 Projekte koordiniert. Diese reichen von der Grundlagenbeschaffung über die Notfallplanung und Kommunikation bis hin zu Langfristmassnahmen, wie die Projektierung eines eventuellen Überlaststollens vom Sihltal in den Zürichsee. Die Projektorganisation besteht aus der Stadt und dem Kanton Zürich, der SBB und der Sihltal Zürich Uetliberg Bahn (SZU). Als Sofortmassnahme wurde ein Hochwasservorhersagesystem



Abbildung 5: Hochwasser-Schadenpotential in der Stadt Zürich heute (Quelle: AWEL).

für die Sihl entwickelt, mit dem Ziel, dass mittels Vorabsenkung von Sihl- und Zürichsee Rückhaltevolumen für Starkniederschlagsereignisse geschaffen werden kann. Parallel dazu mussten die Stadt Zürich und grössere Infrastrukturbetreiber in Bezug auf die Hochwasserproblematik sensibilisiert und Aufgaben, Verantwortungen und Kompetenzen geklärt werden. Ziele bis Ende 2011 sind, die Schutzziele für den Hauptbahnhof und weitere Sonderobjekte der Stadt zu definieren, die Abläufe der Notfallorganisationen abzustimmen, eine Notfallplanung aufzubauen und Sofortmassnahmen umzusetzen, eine Strategie für den langfristigen Hochwasserschutz der Sihl festzulegen, und die Kostenteilung für den langfristigen Hochwasserschutz zu definieren.

4.2 Idee: Der Rückhalt von Wasser im Sihlsee

Um Überschwemmungen in der Stadt Zürich zu vermeiden wird die Idee verfolgt, den Sihlsee als grosses Wasserrückhaltebecken zu benützen (siehe Abb. 6). Wenn ein Hochwasser erwartet wird, wird der See abgesenkt, so dass vor dem Hochwasser steigende Wasserpegel in der Stadt zu beobachten sind. Diese senken sich noch vor dem Hochwasser wieder ab. Beim Hochwasser kann der Sihlsee dann wieder aufgefüllt werden und funktioniert als Wasserrückhal-

tebecken, damit die Sihl nicht über die Ufer tritt. Für dieses Projekt wird als Entscheidungsgrundlage das neue interkantonale Frühwarn- und Kriseninformationssystem IFKIS Hydro Sihl benutzt. In einem nächsten Schritt soll IFKIS aufs gesamte Siedlungsgebiet der Stadt erweitert werden und vom Bund ins eigene Warnsystem (Gemeinsame Informationsplattform Naturgefahren) integriert werden. Allerdings gab es seit der Einführung von IFKIS keine grossen Hochwasser mehr, weshalb noch keine Erkenntnisse über das Funktionieren von IFKIS vorliegen.

4.3 Herausforderungen im Hochwasserschutz in Zürich

Bei der Warnung vor Hochwassern besteht heute die grosse Herausforderung, dass sehr viele Stellen an der Prozesskette, d.h. vom Wettermodell bis zur Feuerwehr beteiligt sind und somit viele Schnittstellen bestehen. Die Wetter- und Abflussinformationen weisen heute zwar einen sehr hohen Stand auf, hingegen fehlt an vielen Stellen das fachliche Wissen, um diese Informationen zu verarbeiten. Insbesondere bereitet die Interpretation der zum Teil unsicheren Wetter- und Wasserprognosen und deren Umwandlung in klare Verhaltensanweisungen Mühe. Wie geht man mit einer Wettervorhersage, die eine 30-prozentige

Rückhalt von Wasser im Sihlsee

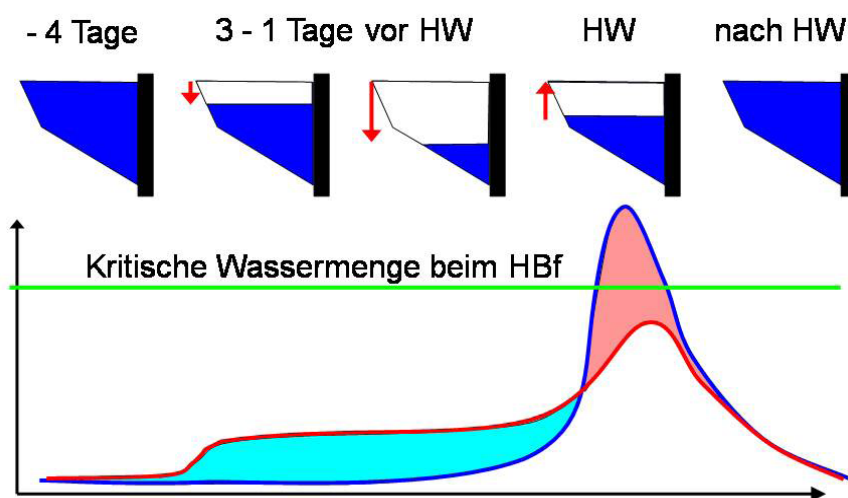


Abbildung 6: Rückhalt von Wasser im Sihlsee (Quelle: AWEL).

Unsicherheit aufweist, um? Wer braucht zu welchem Zeitpunkt welche Informationen? Es gilt entsprechende Schulungen durchzuführen und Personen einander bekannt zu machen. Eine weitere Herausforderung besteht im Umgang mit Medien im Zusammenhang mit dem Infrastrukturschutz. Gerade Gefährdungen im Bereich des Hauptbahnhofs rufen die Medien auf den Plan, weshalb die Medienarbeit

zum Teil sehr viel Zeit in Anspruch nimmt. Eine der grössten Herausforderungen aber ist die Sensibilisierung der verschiedenen in den Hochwasserschutz zu involvierenden Stellen. Die Wichtigkeit der Prävention ist sehr schwer zu vermitteln. Wäre der Hauptbahnhof 2005 tatsächlich unter Wasser gestanden, gäbe es kein Problem, die Leute vom Nutzen des Hochwasserschutzes in Zürich zu überzeugen.

5 STROMPANNE 2005: AUSWIRKUNGEN UND LEHREN AUS DER SICHT DES KRISENMANAGEMENT SBB

Präsentation: Bruno Schärer, Schweizerische Bundesbahnen (SBB)

Bei der SBB hat das Krisen- und Notfallmanagement seit der Strompanne im Jahr 2005 eine stärkere Bedeutung erhalten. Mit dem Aufbau eines professionellen Notfall- und Krisenmanagements, der Errichtung von permanenten Krisenräumen sowie dem Ausbau der Versorgungssicherheit wurden ab 2005 die Grundpfeiler geschaffen, um weiteren Krisen entgegenzuwirken. Auch der Bereich «Schutz Kritischer Infrastrukturen» bekam plötzlich eine weit grössere Bedeutung. So ist der Begriff heute auch im Bereich «Betriebliche Verfügbarkeit» (von Anlagen und Infrastrukturbauten) und im Bereich «Innere Sicherheit» (Unternehmensschutz, Cyberterror, Anschläge) anzutreffen. Das Beispiel SBB macht einmal mehr deutlich, dass oft erst ein einschneidendes Ereignis das Bewusstsein der Verantwortlichen für die Bedeutung des Krisenmanagements und den Schutz Kritischer Infrastrukturen weckt.

5.1 Die SBB und der Schutz Kritischer Infrastrukturen

Die SBB als Systemführerin Schiene betreibt ein über 3000km langes Schienennetz mit einer Auslastung

von mehr als 9000 Zügen pro Tag. Dabei ist die SBB selbst Infrastruktur-Betreiberin (Energie, Schiene, Daten) und gleichzeitig stark von anderen kritischen Infrastrukturen abhängig, insbesondere von anderen Stromanbietern. Die zahlreichen Naht- und Schnittstellen sind für die SBB eine grosse Herausforderung. Diese Herausforderung wird dadurch verstärkt, dass die SBB mit 3% der Fläche der Schweiz (Schienennetz, SBB-Areale etc.) eigentlich den Stellenwert eines Kantons hat, gleichzeitig aber immer auf den einen oder anderen Kanton angewiesen ist, wenn es darum geht, SBB-Objekte zu schützen. Eine weitere Herausforderung ist die Prioritätensetzung beim Schutz Kritischer Infrastrukturen. Wer und was hat Priorität bei der Wiederherstellung des SBB-Betriebes nach einer Panne? Ist, um ein Beispiel zu nennen, der möglichst rasche Transport von Trinkwasser oder der Transport von Erdöl wichtiger? Die Geschwindigkeit der Wiederherstellung hängt von dieser Prioritätensetzung, von finanziellen Mitteln und auch von Sicherheitsüberlegungen ab und ist letztlich auch eine politische Diskussion, die geführt werden muss.

5.2 Das Krisenmanagement der SBB

Vor der Strompanne 2005 kannte die SBB einen Krisenstab und einen Kernstab. Für die Arbeit des Kri-



Abbildung 7: Krisenmanagement und Notfallmanagement bei der SBB heute (Quelle: SBB).

senstabs während der Strompanne musste ein Sitzungszimmer vorübergehend umgestellt werden. Unübersichtliche Strukturen, wenige Hilfsmittel und fehlende Infrastrukturen (z.B. Krisenstabsraum) für die Krisenbewältigung machten sich bemerkbar. Nach der Strompanne wurden im Krisenmanagement der SBB diverse Änderungen vorgenommen. Heute unterscheidet die SBB zwischen Krisenmanagement und Notfallmanagement (siehe Abb. 7).

Notfallmanagement ist operativ und bedeutet Ereignisbewältigung. Für die drei Infrastrukturbereiche Energie, Schiene und Informatik gibt es je einen Notfallstab. Das Krisenmanagement hingegen ist strategisch ausgerichtet. Verantwortlich ist der Krisenstab SBB. Die Trennung von Krisenmanagement und Not-

fallmanagement war wichtig. Die Mitarbeitenden müssen wissen, ob sie für die Ereignisbewältigung oder für die Bewältigung der Zukunft zuständig sind. Bei der Ereignisbewältigung (Notfallmanagement) diktiert das Ereignis die Mittel. Eine Krise hingegen kann unterschiedliche Ursachen haben (siehe Abb. 8) und der Krisenzustand wird vom Management definiert. Bei der Strompanne von 2005 kann wohl in erster Linie von einer Imagekrise gesprochen werden.

Sowohl für den Krisenstab wie auch für die Notfallstäbe sind nach 2005 Handbücher herausgegeben und Checklisten erarbeitet worden. Zudem wurden permanente Krisenräume am Hauptsitz SBB sowie Führungsräume für die Notfallstäbe an den jeweiligen operativen Standorten geschaffen.

Krisenmanagement SBB: Krisenursachen	
Naturereignisse	... wenn ein Hochwasser zu Streckensperrungen führt
Grossunfälle	... wenn es Tote / Verletzte bei einem Zugsunfall gibt
Grossstörungen	... wenn durch techn. Defekt / menschliches Versagen das Netz zusammenbricht
Image	... wenn dauernde Verspätungen zu einem bedeutenden Imageverlust führen
Finanzen	... riskante Investitionen gefährden das Unternehmen

Abbildung 8: Krisenursachen bei der SBB (Quelle: SBB).

6 FAZIT

Das Praxis-Forum zum Schutz von kritischen Infrastrukturen – insbesondere vor Naturgefahren – hat aufgezeigt, dass SKI sowohl für Behörden als auch für Infrastrukturbetreiber eine grosse Herausforderung ist. Es hat aber auch verdeutlicht, dass das Miteinander, die Koordination und Kooperation beim Schutz dieser Infrastrukturen, in verschiedenen Bereichen bereits gut gelingt.

Besondere Herausforderungen für alle Verantwortlichen sind der Kulturwandel hin zu einem integralen Risikomanagement, die Sensibilisierung von Entscheidungsträgern und Partnern, und die Definition von Schutzzielen.

Integrales Risikomanagement: Das integrale Risikomanagement unterscheidet zwischen Prävention und Vorsorge (Risikomanagement), Einsatz (Krisenmanagement), und Instandstellung und Wiederaufbau (Kontinuitätsmanagement). Die besondere Herausforderung liegt darin, eine reaktive, ereignisorientierte Managementkultur in eine Kultur des proaktiven, integralen Risikomanagements umzuwandeln. Ein stärkerer Fokus auf das Kontinuitätsmanagement, das auch die Wiederherstellung des Normalbetriebs plant, bietet sich als Lösungsansatz an. Wichtig ist in jedem Fall, die Prozesse Risikomanagement, Krisenmanagement und Kontinuitätsmanagement methodisch klar zu trennen, aber dennoch einen integralen Ansatz zu verfolgen. Der Begriff der Resilienz (verstanden als Widerstandsfähigkeit und Regenerationsfähigkeit von technischen Systemen und der Gesellschaft) gewinnt in diesem Zusammenhang an Bedeutung. Angesichts der Komplexität und Interdependenz moderner Risiken ist es unmöglich, sich gegen alle potentiellen Ereignisse abzusichern. Ein Ansatz, der sich an der Resilienz ausrichtet, fördert die Flexibilität und Widerstandsfähigkeit eines Systems in einer solchen Art, dass es potentielle Krisen ungeachtet deren Ursprungs gleichermaßen bewältigen kann.¹

Prävention und Sensibilisierung: Prävention ist schwierig zu vermitteln. Die Beispiele des SBB-Stromausfalls und des Hochwasserschutzes in Zürich haben aufgezeigt, dass die Bedeutung von SKI und Krisenmanagement oft erst erkannt wird, nachdem ein Ereignis passiert ist. Die Unterstützung der Entscheidungsträger, sowohl aus der Politik als auch aus dem Firmenmanagement, ist beim Schutz Kritischer Infrastrukturen unerlässlich. Die Sensibilisierung von Entscheidungsträgern für SKI ist denn auch eine zentrale Aufgabe der SKI-Verantwortlichen.

Bestimmung der Schutzziele: Schutzziele beschreiben das Sicherheitsniveau, das angestrebt wird. Welche Ausfallszeit kann bei einer kritischen Infrastruktur toleriert werden? Hier müssen unterschiedliche Interessen und Bedürfnisse koordiniert werden. Die Prioritäten der Infrastrukturbetreiber decken sich naturgemäss nicht immer mit den Prioritäten der Behörden. Vonseiten der Infrastrukturbetreiber wird denn auch immer wieder angemerkt, dass in dieser Hinsicht entsprechende Richtlinien aus der Verwaltung und Politik notwendig sind, die das Gesamtinteresse der Gesellschaft berücksichtigen. Da die Bestimmung der Schutzziele auch immer eine Frage der Finanzierbarkeit ist, basiert die Prioritätensetzung beim Schutz Kritischer Infrastrukturen letztlich auch auf einer politischen und gesellschaftlichen Diskussion.

¹ Siehe Brunner, Elgin M. und Jennifer Giroux (2009): Resilienz: Konzept zur Krisen- und Katastrophenbewältigung. CSS Analyse Nr. 60. Center for Security Studies (CSS), ETH Zürich.

ANHANG: REFERENTEN

Dr. Stefan Brem, Bundesamt für Bevölkerungsschutz (BABS)

Dr. Stefan Brem leitet seit März 2007 den Fachbereich Risikogrundlagen und Forschungscoordination innerhalb des Bundesamtes für Bevölkerungsschutz BABS. Das BABS ist verantwortlich für die Erarbeitung einer nationalen Strategie zum Schutz Kritischer Infrastrukturen (SKI) und koordiniert zu diesem Zweck eine interdepartemental zusammengesetzte Arbeitsgruppe. Als wichtiger Meilenstein konnte im Sommer 2009 die SKI-Grundstrategie durch den Bundesrat verabschiedet werden. Das BABS ist zudem im Dezember 2008 durch den Bundesrat beauftragt worden, eine nationale Gefährdungsanalyse «Risiken Schweiz» zu erstellen. Im Weiteren unterstützt das BABS die Kantone bei der Erstellung von kantonalen Gefährdungsanalysen (KATAPLAN). Zuvor war Stefan Brem zwischen März 2003 und März 2007 als wissenschaftlicher Mitarbeiter am Zentrum für internationale Sicherheitspolitik des Eidg. Departements für Auswärtige Angelegenheiten EDA in Bern tätig. Dort war er u.a. für folgende Themenbereiche zuständig: Schutz Kritischer Infrastrukturen, insb. in den Bereichen Energie, Kommunikation, Transport; Sicherheitssektorreform; Grenzsicherheit und Rolle von privaten Sicherheitsfirmen. Vor seinem Eintritt in die Bundesverwaltung war Stefan Brem Assistent an der Universität Zürich, wo er u.a. zu Rüstungskontrolle und Abrüstung Vorlesungen gehalten hatte. Er hat an der Universität Zürich im Frühjahr 2003 seine Dissertation in Politikwissenschaft abgeschlossen. Zuvor hat er an der Universität Zürich Geschichte, Politikwissenschaft, Staats- und Völkerrecht studiert.

Dr. Urs Cipolat, IBCOL Technologies & Consulting AG

Dr. Urs Cipolat ist zertifizierter Risikomanager ONR 49000/ ISO 31000. Seit 2008 ist er als Berater und Senior Manager für IBCOL Technologies & Consulting AG in Küsnacht tätig. Zu seinen Fachgebieten gehören u.a. das Durchführen von Risikobeurteilungen, Business Impact Analysen und Krisenstabsübungen für private und öffentliche Organisationen sowie das Erstellen von Notfallplänen zum Schutz kritischer

Prozesse und Infrastrukturen. Als Fachexperte in den Bereichen Risiko-, Krisen- und Kontinuitätsmanagement hat Dr. Cipolat in den vergangenen zehn Jahren rund fünfzehn Mandate im In- und Ausland als Projektkoordinator oder -leiter betreut. Daneben hielt er zahlreiche Referate, leitete diverse Workshops und unterrichtete als Gastdozent während acht Jahren an der Universität Berkeley, Kalifornien, wo er 2000 zum Thema Exportkontrollen, Massenvernichtungswaffen und Völkerrecht promovierte.

Dr. Matthias Oplatka, Amt für Abfall, Wasser, Energie und Luft im Kanton Zürich

Dr. Matthias Oplatka arbeitet seit 1997 beim AWEL (Amt für Abfall, Wasser, Energie und Luft) der Baudirektion des Kantons Zürich. Zuerst war er Projektleiter in der Abteilung Wasserbau. Heute ist der Leiter der Sektion Bau in derselben Abteilung. Er ist zuständig für die Hochwasserschutzbauten und die Renaturierungen der grösseren Fließgewässer des Kantons, sowie für die Organisation der Hochwasserfachstelle. Zudem unterstützt er als Fachexperte die kantonale Führungsorganisation. Nach Abschluss des Studiums der Kulturtechnik und eines Nachdiplomstudiums für Siedlungswasserbau und Gewässerschutz arbeitete Herr Oplatka als wissenschaftlicher Mitarbeiter an der ETH-Versuchsanstalt für Wasserbau, Hydrologie und Glaziologie (VAW). Als wissenschaftlicher Mitarbeiter und Doktorand schrieb er dort auch seine Dissertation zum Thema «Stabilität von Weidenverbauungen an Flussufern».

Bruno Schärer, Schweizerische Bundesbahnen (SBB)

Bruno Schärer von Luzern leitet bei den Schweizerischen Bundesbahnen SBB das Krisenmanagement und ist als Stabschef Teil des Krisenstabes SBB. Nach erfolgreicher Lehre als Automechaniker und Weiterbildung im Bereich Elektrotechnik/Elektronik sowie dem Erwerb des Handelsdiploms besuchte er verschiedene technische Hochschulen und erwarb das Diplom zum eidg. Dipl. Betriebsausbildner. Bevor Bruno Schärer seiner heutigen Stelle als Leiter Kri-

senmanagement SBB im 2005 antrat, arbeitete er als Fachlehrer im Führungssimulator 95 der Schweizer Armee in Kriens. Im Jahr 2010 wurde er zum Oberst im Generalstab (Heeresstab, Einsatz als Chef Regie) befördert. Neben seiner beruflichen Tätigkeit besuchte er diverse Weiterbildungen im Bereich Risikomanagement und Security an der ZHAW sowie an der HSLU.

Dr. Myriam Dunn Cavelty (Moderation), Center for Security Studies (CSS), ETH Zürich

Dr. Myriam Dunn Cavelty ist Leiterin der Forschungsgruppe «Neue Risiken» am Center for Security Studies (www.css.ethz.ch) und Dozentin für Sicherheitspolitik an der ETH Zürich und Fellow der Stiftung

neue Verantwortung in Berlin. Sie hat Internationale Beziehungen, allgemeine Geschichte und Völkerrecht in Zürich studiert und absolvierte diverse Forschungsaufenthalte in den USA, Grossbritannien und Skandinavien. 2007 war sie Visiting Fellow am Watson Institute for International Studies (Brown University). Sie publiziert regelmässig in internationalen Fachzeitschriften und ist Autorin und Herausgeberin mehrerer Bücher. Neben ihrer Forschungs- und Publikationstätigkeit berät sie Regierungen, internationale Institutionen und Unternehmen in den Bereichen Cybersecurity, Cyberwar, Schutz Kritischer Infrastrukturen, Risikoanalyse und strategische Früherkennung. Als weltweit nachgefragte Cyber-Expertin gibt sie häufig Vorträge an Fachtagungen und nimmt in Printmedien und am Radio Stellung zu aktuellen Vorfällen.

The Center for Security Studies (CSS) at ETH Zurich specializes in research, teaching, and information services in the fields of international relations and security policy. The CSS also acts as a consultant to various political bodies and the general public. The Center is engaged in research projects with a number of Swiss and international partners, focusing on new risks, European and transatlantic security, strategy and doctrine, state failure and state building, and Swiss foreign and security policy.

The Crisis and Risk Network (CRN) is an Internet and workshop initiative for international dialog on national-level security risks and vulnerabilities, critical infrastructure protection (CIP) and emergency preparedness. As a complementary service to the International Relations and Security Network (ISN), the CRN is coordinated and developed by the Center for Security Studies at the Swiss Federal Institute of Technology (ETH) Zurich, Switzerland. (www.crn.ethz.ch)