# Risikodialog im Internet

**Das immer breiter und komplexer werdende Spektrum moderner Gefahren und Risiken bringt für die sicherheitspolitische Forschung zusätzliche Herausforderungen und einen erhöhten Erklärungs- und Handlungsbedarf mit sich. Das «Comprehensive Risk Analysis and Management Network» (CRN) stellt einen zukunftsgerichteten Versuch dar, per Internet der Mehrdimensionalität moderner Bedrohungen und Verletzlichkeiten gerecht zu werden.**

VON KURT R. SPILLMANN
UND JAN METZGER

Was bedeutet «Risiko» für eine moderne Gesellschaft? Sind die Staaten im 21. Jahrhundert verwundbarer als früher? Und wenn ja, wieso? Wie lassen sich verschiedene Risiken miteinander vergleichen? Wie sieht die zukünftige Rolle des Staates im Bereich der sicherheitspolitischen Gefahrenabwehr aus? Es ist nicht leicht, auf diese Fragen befriedigende Antworten zu geben. Trotzdem lassen sich die gegenwärtigen Gefahren- und Risikotrends auf verschiedene, zugegebenermassen selektive Weisen charakterisieren.

### Gefahren- und Risikotrends

Erstens lässt sich ein Trend von eindimensionalen zu mehrdimensionalen Bedrohungsformen und Verletzlichkeiten feststellen. Das Gefahrenspektrum wird nicht mehr durch eine einzelne Bedrohung dominiert – wie dies während der Zeit des Kalten Krieges weitgehend der Fall war. Die mehrdimensionale Bedrohungssituation hat zur Folge, dass die Frage der Prioritätensetzung für die politischen Entscheidungsträger als sicherheitspolitische Akteure zunehmend schwieriger zu beantworten ist.

Zweitens gibt es nicht nur mannigfaltigere und weniger eindeutig zu priorisierende Gefahren, sondern auch eine Schwergewichtsverlagerung von territorialen hin zu funktionalen Bedrohungsformen und Verletzlichkeiten – gleichsam vom physischen hin zum digitalen Schlachtfeld. Vor diesem Hintergrund des Wandels vom Kalten Krieg zum «heissen Frieden» ist es erstaunlich, dass der Bereich «Information Warfare» innerhalb der schweizerischen Verteidigungsanstrengungen nach wie vor ein vergleichsweise kümmerliches Dasein fristet.

Mit diesem Punkt verbunden ist drittens der geografische Trend von nationalen zu transnationalen Gefahren. Entsprechend kann auch die Abwehr der heute wirklich relevanten Bedrohungen kaum mehr im nationalen Alleingang erfolgreich bewältigt werden. Selbst den Vereinigten Staaten von Amerika werden trotz intensivster Bemühungen im Bereich «Critical Infrastructure Protection» immer wieder die Grenzen autonom-nationaler Einflussmöglichkeiten aufgezeigt.

Viertens verändern sich mit dem Wandel von der Industrie- zur Wissensgesellschaft nicht nur die Bedrohungen an sich, sondern auch die Akteure, von denen diese potenziell ausgehen. Hier gibt es einen Trend von staatlich-zentralen hin zu dezentral-individualisierten, substaatlichen Risikopotenzialen festzuhalten. Ob ein Cyberhacker aus einem terroristischen, einem extremistischen oder einem kriminellen Antrieb handelt, ist weniger entscheidend als der Umstand, dass er uns als einzelnes Individuum dort treffen kann, wo es wirklich weh tut. Die Bedrohung der Industriegesellschaft des 20. Jahrhunderts, beispielsweise durch Chemie- und Biologiewaffen-Terroristen, setzte Staaten oder extremistische Gruppen mit den entsprechenden umfangreichen finanziellen, personellen und logistischen Ressourcen als Akteure voraus. Der Terrorist in der Wissensgesellschaft ist demgegenüber ein hoch leistungsfähiger Einzeltäter.

Mit dieser Individualisierung einher geht fünftens, dass die Verletzlichkeit der kritischen Infrastrukturen moderner Staaten in den letzten Jahren ungemein zugenommen hat und wohl auch weiterhin zunehmen wird – nicht zuletzt durch zahlreiche Privatisierungen im Kommunikations- und Informationstechnologiebereich sowie die gängigen offenen Systemarchitekturen. Der Einzelne kann nicht nur mehr Schaden anrichten; wir als Gesellschaft und der Staat als traditioneller Garant nationaler Sicherheit können immer weniger feststellen, wo und von wem wir bedroht respektive bereits getroffen sind. Die nicht linear ablaufenden Angriffe können nur schlecht an ihren Ursprungspunkt zurückverfolgt werden.

Die Risikotrends sind damit nicht erschöpfend aufgezählt. Sie sind aber real – und das ist nur der Anfang einer sich abzeichnenden Entwicklung. Ein flüchtiger Blick in die Zukunft zeigt, dass im Bereich der Robotik oder auch der Nano- und Gentechnologie noch einiges auf uns zukommen wird.

### Fragen und Folgen für die Sicherheitspolitik

Welche Auswirkungen haben diese Veränderungen auf die wissenschaftliche Disziplin der Sicherheitspolitik und Konfliktfor-

Dr. Kurt R. Spillmann ist Leiter der Forschungsstelle für Sicherheitspolitik und Konfliktanalyse an der ETH und Titularprofessor für Neuere Allgemeine Geschichte an der Universität Zürich. Dr. Jan Metzger ist als Senior Researcher verantwortlich für das Projekt CRN an der Forschungsstelle.

schung? Aus ihrer Sicht wird eine ganze Palette von traditionellen Begriffen und Konzepten inhaltlich zunehmend in Frage gestellt – insbesondere die Differenzierung zwischen nationaler und internationaler sowie zwischen innerer und äusserer Sicherheit.

Weil vertraute Konzepte an Gültigkeit einbüssen, wird die Durchführung bedrohungsgerechter sicherheitspolitischer Verwundbarkeitsanalysen zugleich notwendiger, aber auch ungemein komplexer. Wer soll sie in Angriff nehmen? Der Staat? Die traditionellen vertikaldepartemental integrierten Garanten öffentlicher Sicherheit haben grösste Mühe, die horizontal-bereichsübergreifenden Bedrohungsformen in zeitgerechter Weise überhaupt wahrzunehmen, geschweige denn darauf reagieren zu können. Und die Privaten? Auch ihnen mangelt es zur erfolgreichen Behauptung an der digitalen Frontlinie oftmals an Know-how und strukturell-übergreifenden Kooperationsmechanismen. In jedem Fall gilt es bei einer Diskussion der zukünftigen Rolle des Staates in der Sicherheitspolitik immer auch dem Verhältnis zwischen öffentlicher Sicherheit und individueller Freiheit die gebührende Beachtung zu schenken.

### Virtuelles Netzwerk als Antwort

Das Internet hat ein Janus-Gesicht mit einer guten und einer schlechten Seite. Bis anhin wurde vor allem über die Gefahren gesprochen. Aber so wie jedes Risiko zugleich eine Chance darstellt, bietet sich gerade das Internet als künftiges Medium des sicherheitspolitisch-interdisziplinären Risiko-, Bedrohungs- und Gefahrendialoges an. An diese Vorstellung knüpft das «Comprehensive Risk Analysis and Management Network» (CRN) an, welches sich derzeit an der Forschungsstelle für Sicherheitspolitik und Konfliktanalyse der ETH Zürich im Aufbau befindet. Methodisch und inhaltlich steht es in der Nachfolge des Projekts «Umfassende Risikoanalyse Schweiz», in welchem seit 1993 ein systematischer Dialog über die Erfassung und Bewertung existenzieller Risiken für die Schweiz durchgeführt wurde.

Unter der Leitung und Koordination der Zentralstelle für Gesamtverteidigung (ZGV) waren neben Vertretern aller interessierten Bundesstellen auch Experten aus Politik, Wissenschaft und Wirtschaft am Projekt beteiligt. Im Herbst 1999 beschloss das Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) das Projekt Risikoanalyse zu akademisieren sowie zu internationalisieren (dies im Sinne des Leitspruches des sicherheitspolitischen Berichtes 2000 «Sicherheit durch Kooperation»). Zu diesem Zweck wurde das Projekt der Forschungsstelle für Sicherheitspolitik und Konfliktanalyse der ETH Zürich übertragen.

Angesichts des verbreiterten Gefahrenspektrums moderner Gesellschaften gilt es, Ressourcen von Universität und ETH (beispielsweise das «World Institute for Disaster Risk Management» [DRM] des ETH-Rates) zur Bewältigung sowohl naturbedingter, technischer, machtpolitischer als auch zivilisatorischer Risiken auf einer elektronischen Plattform zu bündeln. Neben zahlreichen Bundesstellen sind verschiedene internationale Partner involviert, insbesondere die Schwedische «Agency for Civil Emergency Planning» (ÖCB). Auch Partnerschaften mit privaten Institutionen werden angestrebt.

### Interdisziplinärer Risikodialog

Der Aufbau des CRN wird bis jetzt vollumfänglich durch das VBS als Bestandteil des schweizerischen Engagements in der «Partnership for Peace»-Initiative der NATO finanziert – dies ebenso wie das «International Relations and Security Network» (ISN), auf dem es vor allem technisch, teilweise aber auch inhaltlich basiert. Das ISN wird zusammen mit dem «Information Management System for Mine Action» (IMSMA) als elektronischer Informationsdienst von der Forschungsstelle für Sicherheitspolitik und Konfliktanalyse entwickelt und betrieben. Die Forschungsstelle wiederum bildet seit 1997 zusammen mit den Professuren für Internationale Beziehungen von ETH und Universität das Zentrum für Internationale Studien (CIS).

Das ISN hat sich mit 300 000 bis 400 000 Hits pro Woche als einer der führenden Informationsdienste im Bereich Sicherheitspolitik im Internet etabliert. In Kooperation mit über 40 Partnerinstitutionen verbindet das ISN Vertreter aus Regierung, akademischen und militärischen Einrichtungen, Presse und Nichtregierungsorganisationen (NGOs) durch eine Reihe von hauptsächlich internetbasierten Diensten. Ziel und erklärte Aufgabe des ISN ist es, den breit verstandenen sicherheitspolitischen Dialog in Europa zu fördern und zu pflegen.

Das CRN stellt inhaltlich eine Ergänzung des ISN dar, indem es auf den interdisziplinären Risikodialog ausgerichtet ist. Angesichts des verbreiterten Gefahrenspektrums moderner Gesellschaften gilt es, bestehende methodische Konzepte und Vorgehensweisen zur Bewältigung sowohl naturbedingter als auch zivilisatorischer Katastrophen und Bedrohungen auf einem Informationsportal zusammenzufassen und interessierten Kreisen nutzbar zu machen. Die Struktur des Portals ist so ausgelegt, dass sowohl risikospezifische als auch interdisziplinäre Inhalte aus Lehre, Forschung, Entwicklung, Training und Ausbildung Platz finden.

Im Rahmen des vierten «International Security Forum» vom 15. bis 17. November 2000 in Genf wird ein Homepage-Prototyp des CRN online geschaltet und das Projekt dadurch erstmalig einer breiteren Öffentlichkeit vorgestellt.