CSS Analysen zur Sicherheitspolitik

CSS ETH Zurich

Nr. 16 • Juni 2007 • 2. Jahrgang

KRITISCHE INFRASTRUKTUREN: VERWUNDBARKEITEN UND SCHUTZ

Die Verwundbarkeit moderner Gesellschaften stellt eine wachsende Herausforderung für die Sicherheitspolitik dar. Der Schutz kritischer Infrastrukturen hat seit den Terroranschlägen vom 11. September 2001 neue Dringlichkeit erlangt. Die Erarbeitung wirksamer Schutzkonzepte erweist sich jedoch als schwierig. Erforderlich sind differenzierte Lageanalysen, ein besseres Verständnis der Verwundbarkeiten und ein politischer Konsens über prioritäre Schutzmassnahmen. Auch innen- und zwischenstaatliche Kooperation sowie funktionierende öffentlich-private Partnerschaften sind unabdingbar.

Informationsinfrastrukturen - Nervenzentren der modernen Gesellschaft *www.istockphoto.com*

Der Schutz von Infrastrukturen hat in der Sicherheitspolitik stark an Bedeutung gewonnen. Dies geht vor allem auf die traumatischen Terroranschläge in New York und Washington (2001), Madrid (2004) sowie London (2005) zurück. In all diesen Fällen instrumentalisierten die Attentäter Elemente der zivilen Infrastruktur für den Zweck des wahllosen Mordens. Bei den Anschlägen in den USA am 11. September 2001 bedienten sie sich der Verkehrsinfrastruktur in Form von Flugzeugen als Waffe. In Europa fungierten Züge, Untergrundbahnen und Bahnhöfe respektive die dort verkehrenden Menschenströme als Angriffsziel. Dieses Vorgehen führte nicht nur die erschreckende Brutalität des «neuen» Terrorismus vor Augen, sondern verstärkte auch die Einsicht, dass traditionelle Konzepte der inneren Sicherheit nicht mehr den Erfordernissen der Zeit entsprachen und einer Anpassung bedurften.

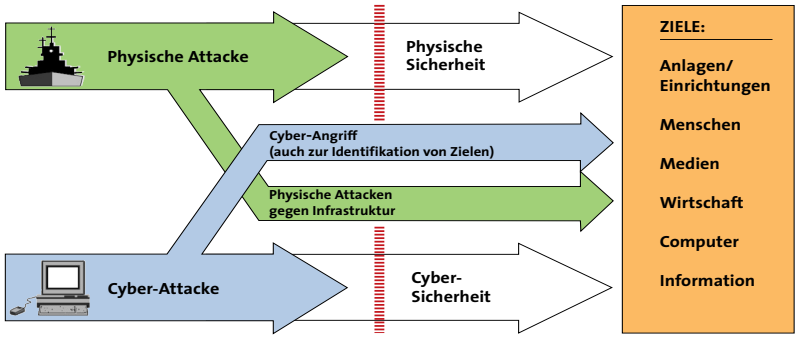
Zwar war der Schutz strategisch wichtiger Objekte im eigenen wirtschaftlich-gesellschaftlichen Rückraum schon früher unter dem Namen «Objektschutz» wichtiger Teil nationaler Verteidigungskonzepte. Der Schutz kritischer Infrastrukturen, meist unter der englischen Begrifflichkeit der *Critical Infrastructure Protection* (CIP) diskutiert, umfasst jedoch ein breiteres Konzept. Zum einen geht es nicht mehr nur um die konkrete Gefahrenabwehr oder die Strafverfolgung nach begangener Tat, sondern zunehmend auch um Gefahren- oder sogar «Sicherheitsvorsorge». Zum anderen ist die moderne Gesellschaft heute wesentlich verwundbarer und das Spektrum möglicher Auslöser von Störungen und Krisen umfassender und diffuser. CIP ist deshalb zu einem Kristallisationspunkt der gegenwärtigen Sicherheitsdebatte geworden.

Von Bedrohungen zu Risiken

Die Entstehung und Etablierung des CIP-Konzepts geht auf zwei zentrale Faktoren zurück. Erstens hat der Wandel der sicherheitspolitischen Lage nach dem Ende des Kalten Kriegs die Schutzbedürftigkeit von Infrastrukturen erhöht. Während des Ost-West-Konflikts wurden sicherheitspolitische Gefahren in erster Linie als militärische und akteurbezogene «Bedrohungen» verstanden. Die Identifizierung und Einschätzung dieser Bedrohungen erfolgte aufgrund des so genannten Bedrohungsdreiecks, bestehend aus dem gegnerischen Akteur, dessen feindlichen Absichten sowie dessen Mittel zur Schadensverursachung. War das daraus resultierende Bedrohungsbild während des Kalten Kriegs relativ klar, so sind die Formen und Verläufe sicherheitspolitischer Herausforderungen seither wesentlich diffuser geworden. Statt einer begrenzten Anzahl «Bedrohungen» ist eine Vielzahl von «Risiken» in den Blickpunkt der Sicherheitspolitik gerückt. Risiken sind gekennzeichnet durch Ungewissheit und Komplexität, die Frage «wer-wie-wo-was-warum-wann» kann kaum mehr beantwortet werden.

Diesem diffusen Lagebild entsprechend wurde der sicherheitspolitische Fokus nach der Zeitenwende 1989/91 weniger auf (schwer identifizierbare) Akteure, sondern auf die generellen Verwundbarkeiten der Gesellschaft gelegt. Diese Debatte

Interdependenzen von Risiken und Verwundbarkeiten



Quelle: PCCIP-Studie 1997, S. 6

bedeutend mitgeprägt hat das US-Militär, das in den frühen 1990er Jahren verstärkt über asymmetrische Bedrohungen nachzudenken begann.

Die zweite Antriebskraft hinter dem CIP-Konzept war die Globalisierung und insbesondere die diesen Prozess wesentlich mitgestaltende und vorantreibende Informationsrevolution. Neue Informations- und Kommunikationstechnologien haben in den 1990er Jahren eine dynamische und tiefgehende Transformation der Gesellschaft ausgelöst, die noch keinesfalls abgeschlossen ist und deren Folgen erst teilweise erkennbar sind. Neben einer Vielzahl von positiven Faktoren sticht in dieser Entwicklung vor allem ein Negativum hervor: Die Verwundbarkeit moderner industrialisierter Gesellschaften durch ihre Abhängigkeit von einer Vielfalt von nationalen und internationalen Informationsinfrastrukturen. Diese sind das vernetzende Führungselement zwischen anderen Elementarbereichen und somit Grundvoraussetzung für das Funktionieren aller anderen Infrastrukturen. Sie machen heute einen zentralen Bestandteil der ökonomischen Wertschöpfung aus. Dabei gelten sie nicht nur als inhärent unsicher, sondern sind auch ganz besonders anfällig für asymmetrische Massnahmen.

Von Hackern zu Terroristen

Für die weltweite Verbreitung des CIP-Konzepts war die 1997 in den USA vorgelegte Studie «Critical Foundations: Protecting America's Infrastructures» der *President's Commission on Critical Infrastructure Protection* (PCCIP) massgebend. Die Studiengruppe untersuchte Schwachstellen der Sicherheit in acht Sektoren: Telekommunikation, Stromversorgung, Gas- und Öltransporte und -lager, Banken und Finanzen, Verkehr, Wasserversorgungssysteme, Rettungsdienste und öffentliche Verwaltung. Sie stellte fest, dass die USA von diesen Infrastrukturen so abhängig seien, dass die Regierung sie durch einen «nationalen Sicherheitsfokus» betrachten müsse, da ein längerer Ausfall gravierende Folgen für die gesamte Nation haben könnte.

Gemäss diesem Ansatz sind kritische Infrastrukturen zu verstehen als materielle und informationstechnologische Einrichtungen, Netze, Dienste und Anlagegüter, deren Störung oder Vernichtung gravierende Auswirkungen auf die Gesundheit, die Sicherheit oder das wirtschaftliche Wohlergehen der Bürger sowie auf das effiziente Funktionieren der Regierung eines Landes hätte. Diese Infrastrukturen können sowohl durch strukturelle Gefahren als auch durch bewusste Angriffe von Akteuren Schaden erleiden. Zur ersten Kategorie von Risiken zu zählen sind etwa Naturkatastrophen, zivilisatorische Katastrophen (z.B. Staudammbruch, AKW-GAU), Personalausfall durch Streik oder Epidemie, organisatorische Mängel technischer oder personeller Natur, menschliches Fehlverhalten, technische Störungen sowie Abhängigkeiten und Versorgungsengpässe. Das Spektrum möglicher Angreifer, die zweite Kategorie, ist weit gespannt und reicht vom gelangweilten Teenager über verärgerte oder unzufriedene Mitarbeiter, Industriespione, organisiertes Verbrechen, Fanatiker und Terroreinheiten bis hin zu feindlichen Staaten.

Vielfältig sind auch die Angriffsoptionen, die Hackerangriffe genauso umfassen wie die physische Zerstörung ziviler oder militärischer Einrichtungen. Das Hauptaugenmerk der frühen amerikanischen CIP-Bemühungen lag jedoch eindeutig auf den noch weitgehend unbekannten Risiken aus dem Cyberspace: die globale Informationsinfrastruktur schien anonyme Angriffe von überall auf der Welt zu ermöglichen und machte gleichzeitig Hackertools für jedermann einfach zugänglich. Aufgrund dieser Bedrohungswahrnehmung bildete sich unter US-Präsident Bill Clinton eine CIP-Politik heraus, die zu einem grossen Teil auf Informationssicherheit ausgerichtet war.

Seit den Terroranschlägen vom 11. September 2001 lässt sich allerdings eine Rückkehr des klassischen Bedrohungskonzeptes in die CIP-Debatte feststellen. Insbesondere aus Sicht der Vereinigten Staaten wird seither eine Reihe von strukturellen Gefahren vermehrt im Rahmen einer akteursorientierten Strategie der Terrorismusbekämpfung angegangen. CIP wurde in den USA zu einem zentralen Bestandteil von *Homeland Security* und wird heute vornehmlich mit Blick auf Strategien gegen den islamistischen Terrorismus diskutiert. Physische Aspekte von CIP sind in den Vordergrund gerückt, Informationsaspekte hingegen haben an Bedeutung verloren. Eine solche auf Terrorabwehr zugeschnittene Ausrichtung von CIP prägt heute auch die Debatten in der EU, die unlängst mit der Entwicklung einer – vor allem die Massnahmen ihrer Mitgliedstaaten koordinierenden – CIP-Politik begonnen hat.

Herausforderungen für eine wirksame CIP-Politik

Das amerikanische Beispiel und die bisherigen Erfahrungen weiterer Länder lassen auf vier, teilweise eng verknüpfte Herausforderungen für eine wirksame CIP-Politik schliessen. Erstens ist eine fundierte Einschätzung von Art und Ausmass der relevanten Risiken und Bedrohungen erforderlich. Statt des derzeit einseitigen Fokus auf den Terrorismus sollte CIP wieder einem breiteren Ansatz folgen und sich mit der Anfälligkeit hochkomplexer Systeme generell befassen. Bezüglich einer differenzierten Lageanalyse kommt den Nachrichtendiensten eine wichtige Rolle zu. Sie ist umso wichtiger, als je nach Gefahr die Verantwortlichkeiten anders liegen und Schutzpraktiken anders zu gestalten sind. Um den Schutz vor Gefahren und Risiken im «normalen» Rahmen – dazu gehören etwa neben Hackerangriffen auch kleinere natürliche Katastrophen – muss der Infrastrukturbetreiber selber bemüht sein. Vom Staat hingegen wird erwartet, dass er Schutz vor Gefahren einer höheren Stufe bieten kann, wie zum Beispiel Angriffe von Terroristen und anderen Staaten.

Zweitens braucht es ein grösseres Verständnis der Verwundbarkeiten, inklusive der Interdependenzen zwischen Infrastrukturen. Es hat sich gezeigt, dass aufgrund hochkomplexer Systeme die bestehende

Methodik nicht ausreicht, um die ganze Spannweite des Problems zu erfassen. In strategischer Hinsicht geht es im Gegensatz zum dominierenden «technischen Zugang» oft weniger darum, Risiken «objektiv» zu quantifizieren und zu messen, als sie in ihrem gesellschaftlichen, politisch-institutionellen, kulturellen oder ökonomischen Kontext zu verstehen.

Drittens gilt es die Frage zu beantworten, was eine Infrastruktur überhaupt «kritisch» macht. Nach 9/11 wurde die Liste von kritischen Infrastrukturen in den USA stark ausgeweitet: Kritisch ist nun auch, was Rückwirkungen auf die Psyche und die nationale Moral haben könnte. Dies führt zu fast unüberwindbaren Problemen für die Konzeption von Schutzmassnahmen: Wie kann man Sicherheit gewähren, wenn potentiell fast alles kritisch und deshalb schützenswert ist? Schwellenwerte zwischen «normal» und «kritisch» dürfen nicht zu tief angesetzt werden. Eine sinnvolle Priorisierung ist zentral. Dies wiederum ist nur mit umfassenden Risikoanalysen möglich. Die hypothetische Verwundbarkeit eines Ziels reicht nicht als Indikator dafür aus, ob dieses Ziel geschützt werden muss. Vielmehr braucht es für die sinnvolle Abwägung von Kritikalität auch Wissen über konkrete Bedrohungen und die Tragweite und Schwere eines möglichen Schadenfalls.

Viertens erfordert CIP umfassende Kooperation. Eine funktionierende Partnerschaft zwischen Staat und Wirtschaft ist unabdingbar. Die Liberalisierung vieler Bereiche des öffentlichen Sektors seit den 1980er Jahren und der Globalisierungsprozess haben dazu geführt, dass sich heute ein grosser Teil der kritischen Infrastrukturen in privater Hand befindet. Der Wirtschaft kommt deshalb sowohl bei der Definition als auch bei der Umsetzung einer Schutzpolitik eine bedeutende Rolle zu. Eine wirksame CIP-Politik bedarf aber auch der Kohärenz zwischen den verschiedenen staatlichen Stellen sowie der internationalen Kooperation. Terroristische Handlungen und sonstige Straftaten wie auch Natur- und sonstige Katastrophen machen nicht an Ländergrenzen halt, weshalb auch Gegenmassnahmen international zu koordinieren sind.

Bedeutung für die Schweiz

Auch in der Schweiz beschäftigen sich auf Bundesebene bereits mehrere Stellen mit dem Schutz kritischer Infrastrukturen, allerdings mit stark unterschiedlichen Blickwinkeln und kaum koordiniert. Folgerichtig wurde das Bundesamt für Bevölkerungsschutz (BABS) Mitte 2005 vom Bundesrat beauftragt, zusammen mit allen beteiligten Departementen den Handlungsbedarf zu identifizieren und entsprechende Massnahmen zu erarbeiten.

Analysiert man den heutigen Stand der Schweizer CIP-Bemühungen anhand der oben identifizierten vier Herausforderungen, so ergibt sich ein differenziertes Bild: Bezüglich der Lageeinschätzung kann die Schweiz im Bereich der Informationssicherheit einen auch im internationalen Vergleich erfolgreichen Ansatz vorweisen. Die Melde- und Analysestelle Informationssicherung (MELANI) hat sich nicht zuletzt aufgrund einer engen Anbindung an den Inland-Nachrichtendienst (DAP) als wirksames Instrument erwiesen. In Bezug auf eine CIP-Strategie sollte auf dieser Basis aufgebaut werden. Darüber hinaus sollte ein breites Netz von Experten zur kontinuierlichen Einschätzung der Bedrohung einbezogen werden.

Ansätze zur Erfassung von Verwundbarkeiten, die über die klassische Risikoanalyse hinausgehen, sollte die Schweiz systematisch auf ihre Nützlichkeit prüfen. Darüber hinaus kann ein besseres und umfassendes Verständnis der Verwundbarkeiten nur über interdisziplinäre und vor allem internationale Forschung erreicht werden, wie sie die EU in ihrem 7. Rahmenprogramm ab 2008 in diesem Themenbereich priorisiert und fördert. Die Schweiz darf diese Entwicklung nicht verpassen und sollte bemüht sein, die entsprechenden Forschungsprogramme aktiv mitzugestalten.

Die Festlegung von Schwellenwerten in Bezug auf die Kritikalität von Infrastrukturen erfordert eine politische Debatte, die in der Schweiz noch nicht stattgefunden hat. Notwendig ist in diesem Bereich auch ein staatliches Informations- und Kommunikationskonzept. Bei der Erfassung von Kritikalität und Verwundbarkeit ist zudem eine departementsübergreifende Vorgehensweise mit einer einheitlichen Methodik anzustreben, die auch nichtstaatliche Akteure einbindet.

Hinsichtlich der Notwendigkeit umfassender Kooperation schliesslich lassen sich im Fall der Schweiz besondere Stärken wie auch beträchtliche Defizite ausmachen. Das schweizerische Milizsystem, d.h. die enge Bindung zwischen Staat und Wirtschaft, gewährt einen wichtigen Vorteil bei der Einbindung des Privatsektors in die Risikoanalyse. Hier wird es darum gehen, bereits bestehende öffentlich-private Partnerschaften auf der Ebene von Bundesämtern auch für eine Schweizer Gesamtstrategie im CIP-Bereich nutzbar zu machen und bestehende Vertrauensstrukturen auszubauen. Handlungsbedarf hat die Schweiz hingegen in der internationalen Zusammenarbeit zum Schutz kritischer Infrastrukturen: Sektorspezifische Vereinbarungen über die Entwicklung einheitlicher Standards, gemeinsame Untersuchungen über CIP, die Ermittlung gängiger Bedrohungsarten und der Austausch bewährter Schutzpraktiken sollten zentrale Elemente einer zukünftigen Schweizer Kooperationsstrategie sein. Gerade weil die Schweiz günstige Voraussetzungen für öffentlich-private Partnerschaften hat, sollte sie die von ihr entwickelten Lösungsansätze auch vermehrt in die internationale CIP-Debatte einfliessen lassen.

CIP-Timeline der Schweiz

- **November 1997:** Strategische Führungsübung 1997 (SFU 97), Übungsszenario setzt schweizerische Informationsinfrastruktur elektronischen Attacken aus. Resultat: Dringlicher Vorschlag, einen Sonderstab Informationssicherheit für Krisenbewältigung auf Stufe Bund einzurichten.
- **Juni 2001:** Übung INFORMO, «Krisen ausgelöst durch Störungen in der Informationsinfrastruktur», Test des Sonderstabs Information Assurance (SONIA).
- **2001:** Die Stiftung InfoSurance führt Roundtables zum Thema „Risiken und Abhängigkeiten in der Informationsgesellschaft" in verschiedenen Sektoren durch, ab 2004 vom Bundesamt für wirtschaftliche Landesversorgung (BWL) übernommen.
- **Oktober 2003:** Gründung der Melde- und Analysestelle Informationssicherung (MELANI).
- **Juni 2006:** Der Bundesrat beschliesst, dass unter der Leitung des BABS als Grundlage für eine zukünftige Strategie der Handlungsbedarf konkretisiert und entsprechende Massnahmen erarbeitet werden sollen. Die Bestandesaufnahme soll u.a. die folgenden Elemente umfassen: Gemeinsames, abgestimmtes Begriffsverständnis, Identifikation der für die Schweiz relevanten kritischen Infrastrukturen und ein Grundset an Gefährdungsszenarien.

- Verantwortlicher Editor: Daniel Möckli
  analysen@sipo.gess.ethz.ch
- Bezug und Mailingliste:
  www.ssn.ethz.ch