Sicherheit im Informationszeitalter

Critical Information Infrastructure Protection (CIIP) als gemeinsame Herausforderung für Politik und Wirtschaft

Myriam Dunn, wissenschaftliche Mitarbeiterin an der Forschungsstelle für Sicherheitspolitik, ETH Zürich, dunn@sipo.gess.ethz.ch

Die Entwicklung offensiver Informationskriegsstrategien hat dazu geführt, dass CIIP heute als eine der wichtigsten Aufgaben im Informationszeitalter wahrgenommen wird.

Pläne zum Schutz strategisch wichtiger Objekte, heutzutage meist als «kritische Infrastrukturen» bezeichnet, waren früher schon wichtiger Bestandteil nationaler Verteidigungskonzepte, ist der wirtschaftlich-gesellschaftliche Rückraum eines Gegners doch seit jeher ein lockendes militärisches Angriffsziel.[1] Diese Schutzkonzepte verloren allerdings wegen der Veränderung in der Bedrohungsperzeption gegen Ende des Kalten Krieges vielerorts an Bedeutung – um nur wenige Jahre später mit umso stärkerem Gewicht und verändertem Fokus in die Sicherheitsdebatte zurückzukehren. Unter dem Schlagwort «Critical Infrastructure Protection» (CIP) hat die Thematik seit einigen Jahren ausgehend von den USA auch in Europa erneut Einzug in die politische Diskussion gehalten. Bei der «Critical Infrastructure Protection» geht es um den Schutz von Infrastrukturen, die als «kritisch» bezeichnet werden, weil ihre Zerstörung oder längere Unverfügbarkeit eine potenziell katastrophale Auswirkung auf die nationale Sicherheit und das wirtschaftliche und soziale Wohlergehen einer Nation haben könnten.[2] Zu dieser Kategorie werden heute gezählt:

- Information und Kommunikation
- Banken- und Finanzwesen
- Elektrizität-, Gas- und Ölversorgung
- Verkehr und Transport
- Wasserversorgung
- Notfalldienste
- Systeme der Regierung und Verwaltung.[3]

Informationsrevolution als treibende Kraft

Der wichtigste Grund für das Comeback der Schutzkonzepte ist die in den 90er-Jahren so richtig in Schwung gekommene «Informationsrevolution». Diese bewirkt eine dynamische, tiefgehende und in vielen Aspekten noch unklare Transformation der Gesellschaft durch Informations- und Kommunikationstechnologien (IKT).[4] Neben einer Vielzahl von ausserordentlich positiven Faktoren sticht aber auch ein Negativum dieser Entwicklung hervor: Die neue und delikate Verwundbarkeit moderner industrialisierter Gesellschaften durch ihre Abhängigkeit von einer Vielfalt von nationalen und internationalen Informationsinfrastrukturen, die als inhärent unsicher gelten. Es sind vor allem zwei Faktoren, die diese Abhängigkeit begründen: Erstens sind IKT-Infrastrukturen zum zentralen Bestandteil der ökonomischen Wertschöpfung geworden und zweitens sind sie das vernetzende Führungselement zwischen anderen Elementarbereichen und somit die Grundvoraussetzung für das Funktionieren aller anderen Infrastrukturen.[5]

Aus diesem Grund rückt neu spezifisch der Schutz kritischer Informations- und Kommunikationsinfrastrukturen («Critical Information Infrastructure Protection», CIIP), insbesondere die Informationsflüsse, die in diesen Netzwerken transportiert werden, sowie die Dienstleistungen und Prozesse, die dadurch ermöglicht werden, ins Zentrum des gesamtgesellschaftlichen Schutzinteresses.[6]

Gefährdung nach dem Kalten Krieg

Diese Entwicklung muss im grösseren Zusammenhang einer substanziellen Verbreiterung des wahrgenommenen Gefahrenspektrums nach dem Zusammenbruch der Sowjetunion gesehen werden. Federführend bei dieser sicherheitspolitischen Neuorientierung waren Strategen in den USA, die den Blick verstärkt auf nichtstaatliche Akteure lenkten, die mit terroristischen Anschlägen eine Bedrohung darstellen könnten.[7]

Beunruhigend an diesem «neuen Gegner» war, dass er nicht mehr klar und mit gängigen nachrichtendienstlichen Mitteln identifiziert

werden konnte. Als Folge davon begann man, Unsicherheitsabschätzungen verstärkt von der wahrscheinlichen Gefährlichkeit der Mittel abhängig zu machen, die zur Verfügung stehen könnten. Dabei wurden neben Massenvernichtungswaffen auch Bedrohungen in Erwägung gezogen, die auf der offenen Struktur der Datensysteme, der unkontrollierbaren Software-Proliferation sowie einem breit vorhandenen *Hacker-Know-how* basierten.[8] So begannen sich bereits in der ersten Hälfte der 90er-Jahre Warnungen zu häufen, dass die nationale Sicherheit durch mögliche Cyber-Attacken auf Kraftwerke, Banken oder die Flugsicherung bedroht sei.

Ziviler Ansatz setzt sich durch

Die wachsende Sorge um die neue Verwundbarkeit war von Anfang an eng verknüpft mit der Entwicklung offensiver Informationskriegsstrategien. Denn je weiter die Diskussion über Angriffe auf die Informationssysteme möglicher Gegner voranschritt, desto offensichtlicher wurde die Verwundbarkeit der eigenen militärischen und zivilen Datennetze gegenüber einer ganzen Reihe von potenziellen Missetätern.[9]

Dass die Thematik heute trotz der anfänglich stark militärisch geprägten Debatte aber in der Regel fast überall zivil angegangen wird, hat verschiedene Gründe. Sicherlich ausschlaggebend waren die Schwierigkeiten, mit denen die bestehenden Sicherheitsorgane aufgrund territorial nicht mehr begrenzter und auf keine identifizierbaren Akteure mehr festlegbarer Bedrohungen konfrontiert wurden. Der unbestimmte und permanente Charakter der neuen Gefahren trägt nämlich dazu bei, dass die Grenzen zwischen innerer und äusserer Sicherheit und so zwischen Aufgaben der Streitkräfte und ziviler Kräfte immer schwieriger auszumachen sind, ja sogar eine neue Aufgabendefinition und Aufgabenverteilung erforderlich scheinen.[10]

Weiter wurde man sich in militärischen Kreisen bewusst, dass eine Fokussierung auf den Schutz eigener militärischer Computernetze nur einen kleinen Teil des Problems zu lösen vermochte. Das Militär steht nämlich auch in grosser Abhängigkeit von zivilen Technologien und Netzwerken, so dass zivile Risiken durch Hacker und ähnlichem auch die militärische Sicherheit bedrohen. Aufgrund dieser Faktoren hob die US-Regierung das Thema aus dem militärischen Kontext heraus und etablierte es in einer breiteren zivilen Umgebung, wo es seither auch weiterentwickelt wird.

Verschiedene Blickwinkel

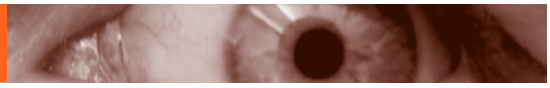
Wie ein Vergleich von gegenwärtigen CIIP-Politikbemühungen in vierzehn Ländern zeigt, wird CIIP heute dementsprechend als gemeinsame Aufgabe diverser Einrichtungen verstanden und meist auch interdepartemental angegangen.[11] Aus dieser Vielfalt an beteiligten Akteuren ergibt sich aber das Problem, dass CIIP unter sehr unterschiedlichen, teilweise disparaten Gesichtspunkten betrachtet wird und folglich sehr unterschiedliche Instrumente zur Problemlösung vorgesehen werden. Idealtypische Beispiele für diese Gesichtspunkte sind zum Beispiel:

In militärischen Kreisen wurde man sich bewusst, dass eine Fokussierung auf den Schutz eigener militärischer Computernetze nur einen Teil des Problems lösen konnte.

- *Die (IT-)technische Sichtweise:* CIIP wird als gleichbedeutend mit IT-Sicherheit verstanden. Es wird angenommen, dass Gefahren gegen die Informationsinfrastruktur ausreichend mit technischen Mittel wie Firewalls, Anti-Virus-Software, Datenverschlüsselung, etc. bekämpft werden können. Obwohl von zentraler Wichtigkeit, greift diese Sichtweise jedoch in einigen nicht-technischen Aspekten zu kurz.
- *Die betriebswirtschaftliche Sichtweise:* CIIP wird mit sicherem E-Business und möglichst permanenter Verfügbarkeit wichtiger Geschäftsprozesse gleichgesetzt. Die Mittel, um dies zu ermöglichen, stimmen im Grossen und Ganzen mit denjenigen der technischen Sichtweise überein. Der Fokus ist aber etwas breiter und umfasst auch organisatorische und personelle

Kurz und bündig

Die aktuelle Informationsgesellschaft befindet sich in grosser Abhängigkeit von hochkomplexen, inhärent unsicheren Informationssystemen, die wesentliche Grundlagen darstellen für Prozesse und Dienstleistungen, die für das Funktionieren der heutigen Gesellschaft notwendig sind. Der durch diese Abhängigkeit entstehenden potenziellen Gefährdung begegnen Staaten mit einer Reihe von Konzepten zum Schutz kritischer Informationsinfrastrukturen (Critical Information Infrastructure Protection, CIIP). Dieses noch im Entstehen begriffene Politikfeld stellt eine substanzielle Herausforderung für beteiligte Akteure dar, verlangt es doch neue Denk- und Schutzansätze und vor allem aktive Zusammenarbeit, nicht nur zwischen militärischen und zivilen, sondern auch zwischen staatlichen und privatwirtschaftlichen Organen.



Faktoren. Auch diese Sichtweise ist in vielen Ländern dominant und politikbestimmend.

- *Die Sichtweise von Strafverfolgungsorganen:* CIIP wird verstanden als Schutz der Gesellschaft gegen Cyberkriminalität, die eine Vielzahl von unterschiedlichen Straftatbeständen umfasst, die mit Hilfe von IKT begangen werden können. Cyberkriminalität wird mit Hilfe von mehr oder weniger traditionellen Strafverfolgungskonzepten bekämpft, wie z.B. Anpassung der nationalen Gesetzgebung.
- *Die sicherheitspolitische Sichtweise:* Diese Sichtweise umfasst verschiedene Ansätze, die CIIP als Politik für den ausserordentlichen Fall und somit für Vorkommnisse, die den Alltag durchbrechen, verstehen. Die gesamte Gesellschaft wird als akut gefährdet angesehen, so dass Aktivitäten auf verschiedenen Ebenen, wie z.B. auf der technischen, der gesetzgeberischen, der organisatorischen und der internationalen, notwendig sind. Wie oben angetönt, ist CIIP im sicherheitspolitischen Sinn nicht als ausschliesslich militärische Aufgabe zu verstehen, sondern als eine interdepartementale und kooperative.

Das Spektrum möglicher Angreifer ist weit gespannt und reicht vom verärgerten oder unzufriedenen Mitarbeiter über Industriespione, organisiertes Verbrechen, Fanatiker, Terroreinheiten bis hin zu feindlichen Staaten.

Auch wenn diese Sichtweisen in Wirklichkeit nie so schematisch und klar voneinander abgrenzbar sind, können divergierende Ansichten doch zu einem konkreten Problem für die Politikformulierung werden, weil weder eine Übereinkunft über die wichtigsten Charakteristika der Problematik noch über «was wann wie geschützt werden muss» besteht. Gleichzeitig ergibt sich eine ganz praktische Abgrenzungsfrage: Wann ist der Schutz kritischer Infrastrukturen eine ganz normale Aufgabe eines individuellen, betrieblichen oder lokalen Akteurs und wann Gegenstand einer nationalen und allenfalls sogar internationalen Sicherheitspolitik?[12]

Alltags- und Sicherheitspolitik

Was die Abgrenzungsproblematik zwischen Alltags- und Sicherheitspolitik noch zusätzlich erschwert, sind die oben bereits angesprochenen Schwierigkeiten, die neuen Verwundbarkeiten der Informationsgesellschaft zu erfassen. Das Spektrum möglicher Angreifer ist weit gespannt und reicht vom verärgerten oder unzufriedenen Mitarbeiter über Industriespione, organisiertes Verbrechen, Fanatiker, Terroreinheiten bis hin zu feindlichen Staaten.[13] Das Spektrum der Angriffsoptionen reicht von Hackerangriffen bis zur gezielten Störung oder Zerstörung ziviler oder militärischer Einrichtungen.[14] Im Ernstfall ist die Einschätzung von Gefahren und somit das zeitgerechte Einleiten von entsprechenden Massnahmen oder Gegenschlägen also ungemein schwierig geworden.

Noch weiter verkompliziert wird die Abgrenzungsproblematik dadurch, dass viele der kritischen Infrastrukturen privatwirtschaftlich teilweise sogar vom Ausland her kontrolliert sind. Tatsächlich verliert der Staat deswegen einen substanziellen Teil seiner Autorität für das Kollektivgut Sicherheit an die Wirtschaft, der dadurch sowohl bei der Definition als auch bei der Umsetzung einer CIIP-Politik eine bedeutende Rolle zukommt.

Allen Initiativen im CIIP-Bereich ist infolgedessen die Anlage eines Kooperationsprogramms gemein, das die Partnerschaft von Staat und Privatwirtschaft beinhaltet.[15] Aber auch wenn viele solche Pläne bestehen und auch einige davon in die Tat umgesetzt worden sind, bleibt die Wegbereitung dieser Art von Kooperation immer noch eine der Hauptschwierigkeiten des Themenbereichs. Denn während der Staat eine nationale Schutzstrategie anstrebt, geht es den Infrastrukturbetreibern meist ausschliesslich um die Sicherheit ihrer eigenen technischen Systeme und damit in erster Linie um lokale Sicherungsmassnahmen.

CIIP als kooperative Aufgabe

Was sich mit Blick auf vorhandene Schutzpraktiken sagen lässt, ist, dass CIIP eine Aufgabe ist, die die vereinten Kräfte von verschiedenen Regierungsbehörden und privaten Akteuren fordert. Dass dies keine einfache Aufgabe ist, wurde oben bereits aufgezeigt. Notwendig ist nicht nur die Ausarbeitung sogenannt defensiver «Information Operations» (IO), die im Kriegs- oder Krisenfall gegen die ganze Palette von offensiven Informationskriegsmitteln wirksam sein müssen. Anzustreben ist vielmehr ein breiterer Ansatz, der staatliche Organe und Privatwirtschaft im fortwährenden Kampf gegen ein ganzes Spektrum von Vorkommnissen vereint, die katastrophale Auswirkungen auf die Informationsinfrastruktur unseres Landes haben könnten.

Um den Schutz vor Gefahren und Risiken im «normalen» Rahmen – dazu gehören 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. Hier ist die Rolle des Militärs in der Führung von defensiven IO als Teil der Informationssicherung zentral.

Das primäre Schutzziel ist dabei nicht der Schutz von Objekten der Informationsinfrastruktur, sondern hauptsächlich die Sicherstellung der Robustheit kritischer Dienstleistungen. Dabei muss die langfristige Überlebensfähigkeit aller relevanten Netzwerke gewährleistet werden. Unterbrüche der Dienstleistungen, die diese Infrastrukturen ermöglichen, müssen von kurzer Dauer und schnell behebbar sein. Dies stellt zu jeder Zeit hohe Anforderungen an die interdepartementale Zusammenarbeit und die Koordination zwischen öffentlichem und privatem Sektor. ■

Fussnoten und Links

1 Vgl. Andrew Rathmell, International CIP Policy: Problems and Prospects, in: Information Security Technical Report, Vol 4, (1999) No. 3, 31.

2 Für eine gängige Definition von kritischen Infrastrukturen, siehe eine der ersten zentralen amerikanischen Publikation zum Thema: President's Commission on critical Infrastructure Protection. Critical Foundations. Protecting America's Infrastructures. Washington D.C., 13.10.1997, B-1. Nachfolgend zitiert als PCCIP Report.

3 Vgl. Definition der Sektoren im PCCIP Report, 3-4. Für Definitionen in vierzehn Ländern, siehe Myriam Dunn / Isabelle Wigert, The International Critical Information Infrastructure Protection (CIIP) Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries. Herausgegeben von: Andreas Wenger / Jan Metzger (Zürich, 2004).

4 Für eine Analyse der veränderten Umstände siehe: Myriam Dunn, Information Age Conflicts: A Study on the Information Revolution and a Changing Operating Environment. Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung, No. 64 (Zürich, 2002).

5 Andreas Wenger / Jan Metzger / Myriam Dunn, «Critical Information Infrastructure Protection: Eine sicherheitspolitische Herausforderung», in: Kurt Spillmann / Andreas Wenger (Hrsg.) Bulletin zur Schweizerischen Sicherheitspolitik (Zürich, 2002), 119-142.

6 Ibid.

7 Vgl. z.B. William S. Cohen, The Report of the Quadrennial Defense Review, Washington D.C., Department of Defense, Mai 1997, Section II: The Global Security Environment. Siehe http://www.defenselink.mil/pubs/qdr.

8 PCCIP Report, 14.

9 R. Anderson et al., Securing the U.S. Defense Information Infrastructure: A Proposed Approach, Santa Monica 1999). Siehe http://www.rand.org/publications/MR/MR993.

10 Vgl. Ralf Bendrath, The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection, in: Andreas Wenger (Hrsg.), The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal, Volume 7, 2001, 80-103.

11 Siehe Fn. 3.

12 Jan Metzger, The Concept of Critical Infrastructure Protection (CIP), in: A.J.K. Bailes / I. Frommelt (Hrsg.), Business and Security: Public-Private Sector Relationships in a New Security Environment, Oxford 2004.

13 Vgl. z.B. Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), Threat Analysis, Number TA03-001, 12. März 2003. Siehe http://www.ocipep-bpiepc.gc.ca/opsprods/other/TA03-001_e.pdf.

14 Ibid.

15 Siehe Fn. 3.