Der Schutz kritischer Informationsinfrastrukturen in der Schweiz: Eine Analyse von Akteuren und Herausforderungen

von Isabelle Wigert

Einleitung

Seit den 1990er Jahren taucht in vielen modernen Staaten unter dem Schlagwort *Critical Information Infrastructure Protection (CIIP)* ein neues sicherheitspolitisches Thema auf. Nach gängigem Verständnis geht es bei CIIP, also dem «Schutz kritischer Informationsinfrastrukturen», sowohl um den Schutz physischer Komponenten der Informationsinfrastruktur – wie zum Beispiel Computer, Satelliten oder Glasfaserkabel – als auch um den Schutz abstrakter und immaterieller Dinge – wie vernetzte Systeme, dem Internet oder IT-Netzwerke und kritische Informationen, die in diesen Netzwerken fliessen. Das Ziel von CIIP ist es, dass Netz- und Systemunterbrechungen selten, von kurzer Dauer, beherrschbar, lokal begrenzt und von geringem Schadensausmass sind.[1]

Der entscheidende Grund für die gegenwärtige Popularität des Themas ist die seit Anfang der 1990er Jahre zügig voranschreitende Informationsrevolution. Während der Schutz kritischer Infrastrukturen, *Critical Infrastructure Protection (CIP),* mitnichten ein neues Thema ist, sondern immer schon Teil nationaler Verteidigungskonzepte war, hat die Abhängigkeit moderner Gesellschaften von Informations- und Kommunikationstechnologien ein verändertes Gefährdungsbild geschaffen. Neu ist insbesondere, dass Informationsinfrastrukturen häufig die Grundvoraussetzung für das Funktionieren aller anderen Infrastrukturen bilden. Das primäre Schutzziel ist heutzutage deshalb nicht mehr nur der Schutz von statischen, oft physischen Objekten, sondern in erster Linie die Sicherstellung der Robustheit kritischer Dienstleistungen, die in der Regel nicht physischer Natur sind, sondern sich im virtuellen Bereich von hoch vernetzten, interdependenten Netzwerken abspielen.[2]

Die enge Vernetzung von Infrastrukturen und Informationsinfrastrukturen macht eine Trennung zwischen beiden oftmals fast unmöglich, so dass es unab-

* Die Autorin dankt Myriam Dunn und Victor Mauer für die wertvollen Kommentare und die Durchsicht des Manuskripts.

1 Joint Economic Committee, United States Congress. *Security in the Information Age. New Challenges, New Strategies.* Washington: Mai 2002, S. 12. http://www.fas.org/irp/congress/2002_rpt/jec-sec.pdf.

2 Wenger, Andreas/Metzger, Jan/Dunn, Myriam. Critical Information Inrastructure Protection: Eine Sicherheitspolitische Herausforderung. In: Spillmann, Kurt R./Wenger, Andreas (Hrsg.). *Bulletin 2002 zur schweizerischen Sicherheitspolitik*. Zürich: Forschungsstelle für Sicherheitspolitik und Konfliktanalyse, 2002, S. 119–142.

dingbar ist, CIP und CIIP als eng miteinander verknüpfte Konzepte zu begreifen. Für einen umfassenden Schutz der Informationsinfrastrukturen müssen andere kritische Infrastrukturen miteinbezogen werden: Wenn zum Beispiel die Transportsysteme zusammenbrechen und Arbeitnehmer ihren Arbeitsplatz nicht mehr erreichen können, dann nützt die beste betriebsinterne Notfallvorsorge für Computerausfälle nichts. Die grossflächigen Stromausfälle in Italien und im Osten der USA haben zudem gezeigt, dass sich ein anfänglich kleiner Zwischenfall durch Interdependenzen schnell zu einer nationalen Krise ausweiten und zahlreiche kritische Infrastrukturen in Mitleidenschaft ziehen kann.

Gerade die Schweiz als ein seit langem in der Informationstechnologie führender Wirtschaftsstandort hat im Falle einer grösseren Störung in der Informationsinfrastruktur viel zu verlieren: Mehr als 70 Prozent der Erwerbstätigen arbeiten im Dienstleistungssektor, und nicht nur die Wirtschaft und der Staat, sondern die Wohlfahrt aller Bürger sind immer stärker von diesen «digitalen Nervensystemen» abhängig. Gemäss Schätzungen würden bei einem Totalausfall der Informatik 25 Prozent der Unternehmen Bankrott gehen, wenn der Schaden nicht innerhalb kürzester Zeit behoben werden könnte. Bei einer Bank zum Beispiel wäre dies schon nach zwei Tagen ohne IT-Systeme der Fall, bei einem Handelsunternehmen nach höchstens drei Tagen.[3] Diese Abhängigkeiten und die damit verbundenen Risiken und Gefahren für die Gesellschaft, die Wirtschaft, den Staat und die nationale Sicherheit werden zunehmend erkannt. Der Staat, gemäss Bundesverfassung für «die gemeine Wohlfahrt» seiner Bürger verpflichtet,[4] ist als Anbieter des Kollektivguts Sicherheit vor neue Herausforderungen gestellt.

Durch die Liberalisierung und Privatisierung vieler lebenswichtiger Bereiche der öffentlichen Hand (Wasser, Strom, Transport, Telefon) seit den 1980er Jahren befindet sich auch in der Schweiz ein Grossteil der kritischen (Informat ions)Infrastrukturen in privaten Händen. Somit stellt sich die zentrale Frage, in welchen Situationen und Bereichen der Staat beziehungsweise der Privatsektor für Massnahmen und Vorkehrungen im Rahmen der nationalen Sicherheit verantwortlich ist.[5] Firmen, bei denen Information der zentrale Produktionsfaktor darstellt, schützen sich zwar selbst intensiv, tendieren aber dazu, informations-

3 Online Interview mit Reto Stäheli, Head of Business Continuity Services, Swisscom IT Services: http://www.swisscom.com/Assets/e-tools/printversion/printversion1.jsp?oid=10862&site=it.

4 Artikel 2, Absatz 2.

5 Henriksen, Stein. The Shift of Responsibilities within Government and Society. Und: Andersson, Jan Joel/ Malm, Andreas. Minding the Gap: Reconciling Responsibilities and Costs in the Provision of Societal Security. In: *CRN-Workshop Report. Societal Security and Crisis Management in the 21st Century.* Stockholm 2004, S. 60–63 bzw. S. 33–52.

technischen Schutz, der über ihr unmittelbares Umfeld hinausgeht, nicht als ihr «business» zu betrachten[6] – auch und nicht zuletzt weil viele Privatfirmen unter dem steigenden Druck von Kostenminimierung und Gewinnmaximierung weniger Ressourcen für Sicherheit und Krisenmanagement zur Verfügung zu stellen bereit sind. Dabei stellt sich eine ganz praktische Abgrenzungs- und Zuständigkeitsfrage: Wann ist der Schutz kritischer (Informations)Infrastrukturen eine Routineaufgabe privater oder betrieblicher Akteure, und wann ist er Gegenstand einer nationalen und allenfalls sogar internationalen Sicherheitspolitik? Dabei wird Sicherheitspolitik als «Politik des Ausserordentlichen» oder als «Politik existentieller Bedrohungen» verstanden.[7]

Die Interessen der Privatwirtschaft und des Staates bei CIIP sind im Prinzip dieselben: Im Mittelpunkt stehen das reibungslose Funktionieren und die permanente Verfügbarkeit der Informationsinfrastrukturen. Die negativen Auswirkungen einer längeren Unterbrechung sind für beide Akteure gravierend. Gerade bei Szenarien, die die Dimension alltäglicher Geschäftsrisiken sprengen, scheinen Kooperation und ein Informationsaustausch zwischen Staat und Privatwirtschaft, eine sogenannte *Public Private Partnership*, von beidseitigem Nutzen. Private Unternehmen haben auf strategischer Ebene unter Umständen Informationslücken, die der Staat füllen könnte. Andererseits könnte der Staat vom fachspezifischen Know-how der Unternehmen profitieren.

Nicht immer zeigt die Privatwirtschaft aber Interesse an einer solchen Kooperation, weil sie erstens befürchtet, dass sensible, mit dem Staat ausgetauschte Informationen über vorgefallene Sicherheitsprobleme nicht mit der nötigen Sorgfalt behandelt werden und dem eigenen Ruf schaden könnten; weil zweitens viele in der Schweiz ansässige Firmen den Grossteil ihrer Geschäfte im Ausland abwickeln; und weil drittens die Privatwirtschaft CIIP primär aus einer betriebswirtschaftlichen Perspektive betrachtet, darunter also in erster Linie ein *business continuity*-Thema versteht und nicht ein sicherheitspolitisches. Der Staat ist also vor die grosse Herausforderung gestellt, die Privatwirtschaft davon zu überzeugen, dass CIIP auch über eine sicherheitspolitische Dimension verfügt, welche die Unternehmen zu ihrem eigenen Nutzen in ihren Risikoanalysen und Notfallplänen berücksichtigen sollten.

Auch auf staatlicher Ebene sind die Herausforderungen gross. In der Schweiz beschäftigen sich auf Bundesebene eine Vielzahl von Verwaltungsstellen mit CIIP, so dass nicht immer auf den ersten Blick ersichtlich ist, welcher Akteur sich mit welchen Aspekten beschäftigt. Verantwortlichkeiten überlappen sich

6 Informatikstrategieorgan Bund ISB. *Verletzliche Informationsgesellschaft. Herausforderung Informationssicherheit*. Bern: Oktober 2002, S. 9.

7 Metzger, Jan. The Concept of Critical Infrastructure Protection (CIP). In: Bailes, Alyson J.K. /Frommelt, Isabel (Hrsg.). *Business and Security: Public-Private Sector Relationships in a New Security Environment*. Oxford: Oxford University Press, 2004, S. 197–209.

und Unklarheiten über die jeweiligen Zuständigkeiten entstehen. Diese Tatsache stellt hohe Ansprüche an die involvierten Akteure und macht eine Koordination nicht nur zwischen öffentlichem und privatem Sektor, sondern auch innerhalb der Bundesverwaltung unabdingbar. Ziel dieses Artikels ist es deshalb, verschiedene Blickwinkel einer CIIP-Politik zu identifizieren und die sich daraus ergebenden Schwierigkeiten für den Schutz kritischer Informationsinfrastrukturen aufzuzeigen. Folgenden zentralen Fragen wird nachgegangen: *Welche Akteure spielen in der schweizerischen CIIP-Politik auf Bundesebene die Hauptrolle? Aus welchen Blickwinkeln wird das Thema «Schutz kritischer Informationsinfrastrukturen» von den zentralen Akteuren in der Schweiz thematisiert? Welche Folgen haben diese unterschiedlichen Wahrnehmungen für die Zusammenarbeit der Akteure? Wo liegen zur Zeit die grössten Herausforderungen für die Schweizer CIIP-Politik?*

Im Folgenden wird zunächst in einem historischen Überblick dargestellt, wie CIIP im letzten Jahrzehnt in der Schweiz auf die politische Agenda gekommen ist. Dabei liegt der Schwerpunkt auf Strategiepapieren, Initiativen und Massnahmen im Bereich CIIP. Aus dieser Übersicht werden die zentralen Akteure auf Bundesebene abgeleitet und einzeln vorgestellt. Es zeigt sich, dass – bedingt durch die unterschiedlichen Grundaufträge und Aufgaben – diese Akteure CIIP mit unterschiedlichen Konzepten und Motivationen angehen. Daraus lassen sich *vier thematische Blickwinkel* auf das Thema CIIP ableiten: eine (IT-)technische Sicht, eine betriebswirtschaftliche Perspektive, die Sicht von Strafverfolgungsorganen und eine sicherheitspolitische Perspektive. Auch wenn diese Sichtweisen in der realen Welt nicht strikt schematisch zur Anwendung kommen, können divergierende Ansichten zu Schwierigkeiten bei der Politikformulierung führen, weil keine Übereinstimmung über die Problematik beziehungsweise über das, «was wann wie geschützt werden muss», besteht.[8] Die Existenz dieser unterschiedlichen Blickwinkel kann zu Verständigungsproblemen und Interessenkonflikten unter den Akteuren bei der Suche nach effizienten Instrumenten und gemeinsamen Lösungen führen. Dies ist insbesondere bei der Zusammenarbeit zwischen Staat und Privatwirtschaft der Fall. In einer Tabelle werden diese Akteure dann den vier thematischen CIIP-Blickwinkeln zugeordnet. Die dadurch gewonnenen Erkenntnisse fliessen schliesslich in die Analyse der schweizerischen CIIP-Politik ein.

Der Artikel beruht auf Internetrecherchen und öffentlich zugänglichen Publikationen und Informationen. Zudem wurden im Februar 2005 Fragebögen an

8 Dunn, Myriam. Sicherheit im Informationszeitalter. Critical Information Infrastructure Protection (CIIP) als gemeinsame Herausforderung für Politik und Wirtschaft. In: *digma – Zeitschrift für Datenrecht und Informationssicherheit* 4 (2004), Heft 2, S. 66–69.

die zentralen Stellen beim Bund verschickt. Darin wurden zu den Aspekten Definition, Risiken und Gefahren, Zuständigkeit im Krisenfall, Kooperation und Handlungsbedarf Fragen gestellt.[9]

1 Die Entwicklung der CIIP-Politik in der Schweiz: 1997–2004

In der Schweiz werden insbesondere folgende Infrastrukturen als besonders kritisch angesehen: Regierung und öffentliche Verwaltung, Notfall- und Rettungswesen, (Tele-) Kommunikation, Energieversorgung, Finanz- und Versicherungswesen, Industrie und Gewerbe, Medien, Gesundheitswesen, Transport und Logistik und Wasserversorgung.[10] Zu den kritischen *Informationsinfrastrukturen* werden gemäss Experten beim Bund spezifisch gezählt: Telefon, Fax, Internet über Festnetz, Mobilnetz, Satelliten (GPS etc.), Kommunikationsnetze der SBB und der Elektrizitätswirtschaft, elektronische Medien, Kurzwellenfunk BERNRADIO, Funknetze der BORS (Behörden und Organisation für Rettungs- und Sicherheitswesen).

Zu den zahlreichen Risiken und Gefahren, welchen kritische Infrastrukturen ausgesetzt sind, gehören «höhere Gewalt», also Naturkatastrophen, zivilisatorische Katastrophen (z.B. Staudammbruch, AKW-GAU) oder Personalausfall durch Streik oder Epidemie; sodann organisatorische Mängel technischer oder personeller Natur, menschliches Fehlverhalten (aktiv oder passiv), technische Störungen, Abhängigkeiten und Versorgungsengpässe, (Cyber)Terrorismus oder sogenannte *Information Operations*[11], um nur einige Beispiele zu nennen. Aber auch vor Gefahren durch die eigenen Mitarbeiter für die Informationsinfrastruk-

9 Von den Bundesstellen Informatikstrategieorgan Bund (ISB), Melde- und Analysestelle Informationssicherung (Melani), Nationale Koordinationsstelle zur Bekämpfung der Internet Kriminalität (KOBIK), Bundesamt für Kommunikation (Bakom), Bundesamt für Wirtschaftliche Landesversorgung/ICT-Infrastruktur, Bundesamt für Verteidigung, Bevölkerungsschutz und Sport/Konzeptstudie Information Operations (KS IO), Armasuisse und dem Zentrum für internationale Sicherheitspolitik (ZiSP) konnten die erhaltenen Antworten ausgewertet und in die Analyse miteinbezogen werden.

10 InfoSurance/Wirtschaftliche Landesversorgung/Informatikstrategieorgan Bund. *Sektorspezifische Risikoanalysen – Methodischer Leitfaden* (2002).

11 Dem Begriff *Information Operations* (bzw. *Information Warfare*) wurden zunächst in den USA vornehmlich militärische Gesichtspunkte zugeordnet. Mittlerweile sind darunter sämtliche Massnahmen zu verstehen, die darauf abzielen, durch Einwirken auf gegnerische Informationssysteme (aktive Massnahmen) bei gleichzeitigem Schutz eigener Systeme die Informationsüberlegenheit zu erhalten (passive Maßnahmen) und – soweit militärisch relevant – die eigene nationale Militärstrategie durchzusetzen.

12 Unter *Social Engineering* versteht man das Erlangen vertraulicher Informationen durch Annäherung an Geheimnisträger mittels sozialer Kontakte. Die auch von Nachrichtendiensten und Privatdetektiven angewandete Methode wird heute meist mit Computerkriminalität verbunden, also der Beschaffung von Zugangsdaten für fremde Computer und Datennetze. http://de.wikipedia.org/wiki/Social_Engineering.

turen, dem sogenannten *Social Engineering*[12], müssen sich der Staat und die Unternehmen – unabhängig von ihrer Grösse – schützen.

In den letzten Jahren wurde auch in der Schweiz erkannt, dass CIIP eine Aufgabe ist, die die vereinten Kräfte von Regierungsbehörden und privater Akteure erfordert. Ein wichtiger erster Schritt bei der Thematisierung der Risiken und Chancen der neuen Informations- und Kommunikationstechnologien in der Schweiz war die *Strategische Führungsübung 1997 (SFU 97)*. Im durchgespielten Übungszenario wurde die schweizerische Informationsinfrastruktur verschiedenen elektronischen Attacken ausgesetzt. Als Folge der SFU 97 wurde dem Bundesrat als dringliche Massnahme vorgeschlagen, einen *Sonderstab Informationssicherheit* für die Krisenbewältigung auf Stufe Bund zu schaffen.[13] Im Juni 2001 wurde die Nachfolgeübung *INFORMO* zum Thema «Krisen, ausgelöst durch Störungen in der Informationsinfrastruktur» von der Strategischen Führungsausbildung der Bundeskanzlei, durchgeführt. An dieser Übung wurde erstmals die Funktionsweise des *Sonderstabes Information Assurance* (Sonderstab Informationssicherung, Sonia) getestet, der sich aus Vertretern der Bundesverwaltung und der Wirtschaft zusammensetzt. Die Übung zeigte, dass ein Bedürfnis für ein solches Fachorgan besteht, das in Krisensituationen die fachliche Beratung der Entscheidungsträger von Bund und Wirtschaft sicherstellen sollte.[14]

Der im August 1998 veröffentlichte Bericht der *Studienkommission für strategische Fragen* («Bericht Brunner»*)* thematisierte ebenfalls «Störungen im Informatikbereich.»[15] Darin wurde die Abhängigkeit von Staat und Wirtschaft von den Informationstechnologien thematisiert und folgendes festgestellt: «Die Infrastruktur der Informatik kann aber mit Leichtigkeit gestört oder gar zerstört werden. [...] Solche Störungen setzen sich über Grenzen und nationale Souveränität hinweg.»[16] Die Kommission sah diese Problematik als gemeinsame Aufgabe von Behörden und Privatwirtschaft und empfahl, «Entscheidungsträger auf allen Ebenen auf dieses Risiko aufmerksam zu machen. Zu prüfen ist die Errichtung eines nationalen Alarmsystems, allenfalls auch eine Initiative zur Förderung der Forschung und der Zusammenarbeit im Kampf gegen absichtliche Störungen von Informatiknetzen.»[17] Die wenige Jahre später gegründete *Melde- und Analysestelle Informationssicherung (Melani)* nimmt sich inzwischen einem Grossteil dieser damals angesprochenen Herausforderungen an.

13 Aus der Einleitung zu INFORMO 2001, *Krisen, ausgelöst durch Störungen in der Informationsinfrastruktur. Dokument 1999–2001, Ergebnisse und Statements.* Bundeskanzlei: Strategische Führungsausbildung (SFA).

14 Ebd.

15 *Der Bericht der Studienkommission für strategische Fragen (Bericht Brunner)*. NFP 42 Working Paper No. 5. August 1998, S. A-13.

16 Ebd., S. A-13.

17 Ebd., S. A-14.

Die Strategie des Bundesrates für eine Informationsgesellschaft Schweiz wurde am 18. Februar 1998 verabschiedet. Die Umsetzung der darin verankerten Grundsätze und Massnahmen erfolgte seither dezentral in den zuständigen Ämtern.[18] Im Juni 2002 verlängerte der Bundesrat das Mandat der *Koordinationsgruppe Informationsgesellschaft* (KIG)[19] bis Ende 2005. Der *interdepartementale Ausschuss Informationsgesellschaft* (IDA IG) unter dem Vorsitz des *Bundesamtes für Kommunikation* (Bakom) wird die Leitung und Koordination dieser Arbeiten innehaben.

Mit dem Bundesratsbeschluss vom 1. Juli 1998 wurde die KIG beauftragt, ein Konzept für den Bereich *Information Assurance* zu erstellen. Im Mai 2000 wurde ein erstes Konzept vorgelegt, in dem der im November 1999 gegründeten unabhängigen Stiftung *InfoSurance* die Schlüsselrolle im Rahmen der Zusammenarbeit zwischen Staat und Wirtschaft zugewiesen wurde.[20] Zwei Jahre später übernahm das *Informatikstrategieorgan des Bundes* (ISB) die Verantwortung bei der Umsetzung des Konzeptes *Information Assurance*. Das dabei entwickelte Einsatzkonzept, basierend auf Vorarbeiten der KIG und der Untergruppe «Sicherheit» unter Federführung des *Bundesamtes für Wirtschaftliche Landesversorgung* (BWL), beruhte demnach auf vier Säulen[21] und den Erfahrungen mit dem Millenium-Bug.[22] Dieses *Vier-Säulenmodell* bildet bis heute das Kernstück der schweizerischen Informationssicherung:

18 Die zuständigen Departemente wurden beauftragt, Konzepte und Aktionspläne zu folgenden Massnahmenbereichen zu erarbeiten: Bildungsoffensive (Eidg. Departement des Innern und Eidg. Volkswirtschaftsdepartement); Attraktivitätssteigerung des Wirtschaftsstandortes (Eidg. Volkswirtschaftsdepartement); Elektronischer Geschäftsverkehr (Eidg. Volkswirtschaftsdepartement); Elektronischer Behördenverkehr (Bundeskanzlei); Neue Formen der Kultur (Eidg. Departement des Innern); Sicherheit und Verfügbarkeit (Eidg. Departement des Innern); Wissenschaftliche Begleitung (Eidg. Departement des Innern und Eidg. Volkswirtschaftsdepartement); Recht (KIG-Ausschuss; vorläufig delegiert an die Supportstelle der KIG); Koordination und Kooperation (KIG).

19 Koordinationsstelle Informationsgesellschaft, BAKOM. *6. Bericht der Koordinationsgruppe Informationsgesellschaft (KIG) an den Bundesrat*, Juni 2004, S. 4. Die Web-Seite www.Infosociety.ch ist das Informations- und Kommunikationsorgan der KIG.

20 2. Bericht der Koordinationsgruppe Informationsgesellschaft (KIG) an den Bundesrat vom 16. Mai 2000. http://www.infosociety.ch/site/attachdb/show.asp?id_attach=900, S. 26.

21 4. (und 6.) Bericht der Koordinationsgruppe Informationsgesellschaft (KIG) an den Bundesrat, Juni 2002 und 2004. http://www.infosociety.ch/site/attachdb/show.asp?id_attach=926, S. 48-49. In diesem Bericht heissen die vier Säulen «Prävention», «Frühwarnung», «Schadensbegrenzung in der Krise» und «Bekämpfung der Krisenursache». Neu sind die vier Pfeiler etwas anders benannt und die Akteure haben teilweise gewechselt (so wird die Stiftung InfoSurance zum Beispiel nicht mehr erwähnt). Aktuelle Informationen dazu unter: http://www.efd.admin.ch/d/dok/faktenblaetter/efd-schwerpunkte/5_infosicherheit.htm.

22 Rytz, Ruedi. Schutzwälle für die Informationsgesellschaft. Schweizer System zum Schutz kritischer Infrastrukturen. In: *Neue Zürcher Zeitung*, 6. Februar 2004.

1. *Prävention:* Durch geeignete Massnahmen im technischen, organisatorischen, aber auch menschlichen Bereich (Ausbildung, Information) ist dafür zu sorgen, dass sich möglichst wenige Vorfälle ereignen. Prävention erfolgt einerseits im Rahmen der sektorspezifischen Risikoanalysen, welche von den jeweiligen Betreibern der kritischen Infrastrukturen im Rahmen der wirtschaftlichen Landesversorgung durchgeführt werden (früher InfoSurance). Anderseits hat Melani die Aufgabe, sowohl Bevölkerung und KMU, als auch die Betreiber der kritischen Infrastrukturen vor dem Einsatz riskanter und unreifer Technologien zu warnen und auf Sicherheitslücken aufmerksam zu machen.

2. *Früherkennung*: Durch Melani sollen Gefahren und Bedrohungslagen möglichst früh erkannt werden, so dass Abwehrdispositive bereitgestellt beziehungsweise gewisse mit Risiken behaftete Technologien gemieden werden können.

3. *Krisenmanagement*: Sonia – zusammen mit BWL/ICT-I (ICT-I: Information and Communication Technology Infrastructure) – sorgt als Instrument des strategischen Krisenmanagements dafür, dass die Auswirkungen von Störungen auf Staat, Wirtschaft und Gesellschaft auf ein Minimum beschränkt werden können.

4. *Technische Problembehebung* (Melani und Partner): Die technischen Ursachen für die Störungen müssen eruiert, analysiert und behoben werden.

Auch im *Sicherheitspolitischen Bericht 2000* des Bundesrates wurde die Bedeutung der Sicherheit der Informatik- und Kommunikationsinfrastruktur thematisiert. Es wurde festgehalten, dass der Bundesrat in diesem Bereich die notwendigen Massnahmen trifft, dieses Ziel aber nur in einem koordinierten Vorgehen von Staat, Wirtschaft und Wissenschaft erreichen könne. Ferner sei ein koordiniertes Vorgehen unerlässlich bei der Identifikation kritischer nationaler Infrastrukturen, der Sensibilisierung, der Ausbildung von Experten, der Erfassung der Risikolage, der Früherkennung und Warnung und insbesondere beim Aufbau einer gemeinsamen Sicherheitsinfrastruktur.[23]

Im Bericht des Perspektivstabs der Bundesverwaltung zu «Herausforderungen 2003–2007: Trendentwicklungen und mögliche Zukunftsthemen für die Bundespolitik» wurde die zunehmende Verletzlichkeit der Informationsgesellschaft ebenfalls thematisiert. Als neue Gefahren werden insbesondere *Information Operations* und «das gross angelegte Lahmlegen von kritischen Infrastrukturen

23 Sicherheit durch Kooperation. Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz (SIPOL B 2000) vom 7. Juni 1999 (Sonderdruck). S. 68f.

wie Strom, Telekommunikation oder Eisenbahnnetz» gesehen, die die Wirtschaft empfindlich treffen und die nationale Sicherheit beeinträchtigen würden.[24]

Im Jahr 2004 wurde von der Sektion «Information Operations» des Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) ein Aussprachepapier beim Bundesrat eingereicht für die Schaffung eines departementübergreifenden Koordinationsorgans mit dem Namen *Kobrir (Koordinationsorgan Bund zum Schutz vor Risiken der Informationsrevolution)* – mit dem Ziel, die Koordination der Aktivitäten der verschiedenen Akteure sowie die Definition einer gemeinsamen und einheitlichen Vorgehensstrategie zu ermöglichen. Kobrir würde (vorerst) auf die Organisationen des Bundes beschränkt.

Dieser knappe Überblick über die Thematisierung und die Initiativen bezüglich CIIP in der schweizerischen Politik zeigt deutlich, dass sich von Anfang an unterschiedliche Akteure mit der Thematik befasst haben. Im nachfolgenden Kapitel werden nun zum einen die Hauptakteure der schweizerischen CIIP-Politik identifiziert; zum anderen wird ein umfassender Überblick über deren Aufgaben und Verantwortlichkeiten gegeben.

2 Die zentralen Akteure in der Schweiz im Bereich CIIP

Bundesrat

Der Bundesrat erachtet die Anwendung von Informations- und Kommunikationstechnologien (IKT) als Chance, sieht aber auch die damit verbundenen Risiken, zum Beispiel im Bereich von Verletzungen des Persönlichkeitsschutzes oder von Grundrechten. Die IKT sollen aus Sicht des Bundesrates dazu dienen, Wissen und Innovation zur Steigerung der Lebensqualität, der Effizienz, des Wachstums, der Wettbewerbfähigkeit und Beschäftigung in der Schweiz zu nutzen.

In der «Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz» vom 18. Februar 1998 wird unter anderem auch die Sicherheit und Verfügbarkeit von Informationen thematisiert. Mit einem adäquaten Informationsmanagement sollen der Zugang zu qualitativ hochstehenden Informationen, die Sicherheit in der Datenübermittlung und -speicherung sowie neue, verlässliche Aufbewahrungsmechanismen langfristig gewährleistet werden. Zudem sei sicherzustellen, dass die Informationen auch in ausserordentlichen Lagen und zur Bewältigung derselben genutzt werden können. «Dies bedingt neue Formen der Zusammenarbeit zwischen den Institutionen, welche Informationen produzieren, verteilen, sammeln oder archivieren.»[25]

24 Schweizerische Bundeskanzlei (Hg.). Bericht des Perspektivstabs der Bundesverwaltung. *Herausforderungen 2003–2007. Trendentwicklungen und mögliche Zukunftsthemen für die Bundespolitik*. 20. November 2002, S. 92.

25 Schweizerischer Bundesrat. *Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz*, 18. Februar 1998. http://www.infosociety.ch/site/default.asp?dossiers=106.

Zuständig für die Massnahmen im Bereich Sicherheit, Vertrauen und Datenschutz sind das Eidgenössische Finanzdepartement (EFD), die Bundeskanzlei (BK) und der Eidgenössische Datenschutzbeauftragte (EDSB). Das EFD hat die Federführung in den Bereichen Informatiksicherheit und Informationsmanagement.[26]

Für den Bundesrat sind also bei CIIP insbesondere die Aspekte von Datenschutz und das Prosperieren der Informationsgesellschaft und damit einhergehend auch der gesamten Wirtschaft (mit e-Business usw.) von zentraler Bedeutung.

Bundeskanzlei (BK): Strategische Führungsausbildung (SFA)

Die Bundeskanzlei ist die allgemeine Stabsstelle des Bundesrates.[27] Zur Bundeskanzlei gehört auch der Fachdienst *Strategische Führungsausbildung*. Dieser entwickelt Ausbildungssegmente für den Bundesrat und die Stäbe der Departemente zum Umgang mit neuartigen Krisen, insbesondere Krisenmanagement und Strategiegestaltung. Wie bereits in Kapitel 1 ausgeführt war die *Strategische Führungsübung 1997 (SFU 97)* dem Thema Risiken und Chancen der neuen Informations- und Kommunikationstechnologien gewidmet. Die Nachfolgeübung

26 Ebd., S. 4. Nicht spezifisch für den Bereich Schutz kritischer Infrastrukturen, aber zentral bei der Organisation der sicherheitspolitischen Führung des Bundesrates sind folgende Akteure und Aktivitäten zudem zu erwähnen: Der Sicherheitsausschuss (SiA) ist ein Ausschuss des Bundesrates mit dem Ziel, die Führungsfähigkeit des Bundesrates zu stärken. Er bereitet die Beratungen und Entscheide des Bundesrates in sicherheitspolitischen Fragen zeitgerecht vor. Er setzt sich zusammen aus den Vorstehern von EDA, EJPD und VBS und Vorsitz wechselt in der Regel jährlich. Vgl. Schweizerischer Bundesrat. Weisungen über die Organisation der sicherheitspolitischen Führung des Bundesrates vom 3. November 1999, S. 158. http://www.admin.ch/ch/d/ff/2000/228.pdf.

Werden in Krisensituationen Entscheide des Gesamtbundesrates notwendig, ermöglicht der Stab Bundesrat der Bundeskanzlei (BK) ein stark gestrafftes Mitberichtsverfahren. In wenigen Stunden kann damit ein Bundesratsbeschluss vorbereitet und zum Entscheid gebracht werden.

Die Lenkungsgruppe Sicherheit (LGSi) ist ein vorbereitendes Stabsorgan des Sicherheitsausschusses und diesem unterstellt. Sie verfolgt laufend die Lage und mögliche Entwicklungen in allen sicherheitsrelevanten Belangen im In- und Ausland aufgrund von Informationen und Beurteilungen aus den einzelnen Departementen und dem Lage- und Früherkennungsbüro. Zudem erarbeitet sie Szenarien, Strategien und Optionen zuhanden des SiA und führt die Liste der ständigen Nachrichtenbedürfnisse des Bundesrates. Schliesslich ist geplant, die beiden Gremien SiA und LGSi durch einen kleinen permanenten Krisenstab (Kernstab) zu ergänzen. Der Bundesrat sieht zudem vor, ab Mai 2005 die Kantone einzuladen, eine ständige Vertretung in die LGSi zu entsenden. Vgl. Pressemitteilungen 23. Dezember 2004. VBS Information. Bundesrat verstärkt die sicherheitspolitische Führung.

27 http://www.admin.ch/ch/d/bk/info/broschuere/bregov.html. Zur Bundeskanzlei gehört der Eidgenössische Datenschutzbeauftragte (EDSB). Zur Aufklärung der Bürger publiziert der EDSB auf seiner Homepage praktische Hinweise zum sicheren Umgang mit PC und Internet: http://www.edsb.ch/d/themen/sicherheit/index.htm.

INFORMO[28] im Jahre 2001 befasste sich ebenfalls mit Störungen in der Informationsinfrastruktur. Dabei wurden zahlreiche offene Punkte bezüglich des Sonderstabes Informationssicherheit artikuliert und danach ein Strategiepapier mit Empfehlungen erarbeitet.[29] Um die in INFORMO aufgeworfenen Fragen und Probleme im Bereich *Information Assurance* weiter diskutieren zu können, wurde im Mai 2002 von der SFA in Zusammenarbeit mit *InfoSurance* die Folgeveranstaltung *InformOrena* durchgeführt, in der sich wiederum Vertreter aus Verwaltung, Armee, Wirtschaft und Wissenschaft mit verschiedenen Aspekten der Informationssicherheit befassten, unter anderem mit Früherkennung und Frühwarnung; Kooperation und Kommunikation zwischen Bund, Kantonen und der Wirtschaft; Vertrauensbildung, internationaler Vernetzung, Information Operations und Führung im operationellen Bereich.

Die Bundeskanzlei erfüllt demnach eine wichtige Aufgabe für das Einüben einer optimalen Zusammenarbeit in so zentralen Bereichen wie Führung, Kommunikation und Krisenmanagement zwischen den verschiedenen Bundesstellen, der Wirtschaft und anderen nationalen und internationalen Akteuren.

Sonderstab Information Assurance (Sonia)

Die Aufgabe von Sonia ist es, die obersten Führungsorgane von Politik und Wirtschaft in Krisen, die durch schwerwiegende Störungen der IKT ausgelöst werden, zu unterstützen. Den Vorsitz führt der oder die Delegierte für Informatikstrategie.[30]

Sollte trotz umfassender Prävention eine Störung in den IKT dazu führen, dass kritische (Informations)Infrastrukturen beeinträchtigt werden, so ist es die Aufgabe und im Interesse des jeweiligen Sektors, dass die Auswirkungen der Störung möglichst begrenzt und die Funktionstüchtigkeit so rasch wie möglich wieder hergestellt werden können. Durch die heutigen grossen Interdependenzen ist eine Koordination mit anderen Sektoren und unter Umständen mit der Regierung für ein erfolgreiches Krisenmanagement erforderlich. Diese Aufgabe fällt Sonia zu, die den Bundesrat und die Wirtschaftsführungen berät und so als deren Bindeglied funktioniert, ohne selbst Entscheidungsträger zu sein.[31]

28 Auswertung INFORMO 2001. Bericht des Projektleiters. Oktober 2001.

29 Mey, Hansjürg. *Strategie zur Gewährleistung der Informationssicherheit (SGIS)*. Bericht der Strategiegruppe INFORMO. Version 17. Januar 2002.

30 Bundesinformatikverordnung vom 26. September 2003, Abschnitt 3, Artikel 10.

31 ISB. *Verletzliche Informationsgesellschaft.* 2002, S. 28f. Nach dem Konzept sollen unter anderem Vertreter des ISB, des BIT, des VBS, des BWL, des Bakom und die Informatiksicherheitsbeauftragten der Departemente (ISBD) vertreten sein. Vgl. Bundeskanzlei/Strategische Führungsausbildung. *Auswertung INFORMO 2001: Gesamtüberblick über die Hauptprobleme und Kernfragen*. Bericht des Projektleiters. Professor Laurent F. Carrel. Version 16. Oktober 2001, S. 18. http://www.admin.ch/ch/d/bk/sfa/downloads/1_hauptprobleme.pdf.

Von besonderer Bedeutung für das Funktionieren von Sonia sind die sektorspezifischen Teams des ICT-Infrastrukturbereichs der Wirtschaftlichen Landesversorgung. Im Krisenfall delegieren diese Teams (oder Koordinationszentren; bis jetzt sind die Sektoren Energie, Telekommunikation, Transport und Verwaltung etabliert, weitere werden dazukommen[32]) Vertreter an den Sonderstab und stellen damit den Kontakt zur Wirtschaft sicher. Daneben stehen Sonia auch die verschiedenen Amtsdirektoren und Fachspezialisten des Bundes zur Verfügung.[33]

Informatikstrategieorgan Bund (ISB)

Das ISB ist dem Generalsekretariat des EFD unterstellt und erarbeitet die Strategie, die Programme und die allgemeinen Standards für die Informatik in der Bundesverwaltung. Zudem ist das ISB auch das Stabsorgan des Informatikrates Bund (IRB)[34]. Gemäss der aktuellen BinfV sind alle Verwaltungseinheiten verpflichtet, dem ISB Ereignisse, welche die Sicherheit von schützenswerten IKT-Mitteln und Daten (Schutzobjekten) betreffen, zu melden und ihm über den Stand der Umsetzung der Sicherheitsmassnahmen zu berichten. Das ISB wiederum orientiert den IRB, der die strategische Gesamtverantwortung für die Informations- und Kommunikationstechnologien in der Bundesverwaltung trägt.[35]

Nicht nur innerhalb der Verwaltung, sondern auch in bezug auf eine landesweite CIIP-Politik spielt das ISB eine zentrale Rolle. Für die Umsetzung des erwähnten Vier-Säulenmodells «Einsatzkonzept Information Assurance Schweiz» hat das ISB die Verantwortung übernommen. Dazu gehört insbesondere der Aufbau und die Aufgabendefinition des Sonderstabes Sonia und der Melde- und Analysestelle Melani. Das ISB versteht Informationssicherung als Staatsaufgabe, kann aber nur erfolgreich sein, wenn auch die Wirtschaft aktiv mitmacht. Eine zentrale Rolle spielt das Informatikstrategieorgan beim Informationsaustausch zwischen den verschiedenen Akteuren. Das ISB hat einen umfassenden Ansatz beziehungsweise Blickwinkel und deckt als Strategieorgan technische, betriebs-

32 Informationen von Vertreter ISB.

33 ISB, *Verletzliche Informationsgesellschaft*, S. 29.

34 Der Informatikrat des Bundes (IRB) trägt die strategische Gesamtverantwortung für die Informations- und Kommunikationstechnik in der Bundesverwaltung. Als eine der Aufgaben des IRB wird auch die Sicherstellung der Betreibung einer Frühwarnungs- und Analysestelle zum Schutz kritischer Infrastrukturen aufgeführt. Das Stabsorgan des IRB ist das ISB, welches organisatorisch dem Generalsekretariat des EFD angegliedert ist (http://www.informatik.admin.ch). Gemäss der aktuellen BinfV sind alle Verwaltungseinheiten verpflichtet, Ereignisse, welche die Sicherheit von schützenswerten IKT-Mitteln und Daten (Schutzobjekten) betreffen, dem ISB zu melden und über den Stand der Umsetzung der Sicherheitsmassnahmen zu berichten. Das ISB wiederum orientiert den IRB, der die strategische Gesamtverantwortung für die Informations- und Kommunikationstechnologien in der Bundesverwaltung trägt. Vgl. BinfV vom 26. September 2003, Abschnitt 3, Artikel 9.

35 Vgl. BinfV vom 26. September 2003, Abschnitt 3, Artikel 9.

wirtschaftliche, organisatorische, gesetzliche und sicherheitspolitische Aspekte von CIIP ab. Es legt auch wert auf Massnahmen in den Bereichen Arbeitsabläufe, Organisationsanweisungen, Schulung und Ausbildung.[36]

Melde- und Analysestelle Informationssicherung (Melani)

Melani arbeitet in einem Kooperationsmodell mit Partnern zusammen, die im Bereich Computer- und Internetsicherheit sowie dem Schutz der schweizerischen kritischen Infrastrukturen tätig sind. Unter der Leitung des ISB – zusammen mit dem Dienst für Analyse und Prävention des Bundesamtes für Polizei (Fedpol) und dem Computer Emergency Response Team (CERT) der Stiftung Switch[37] – ist Melani seit 1. Oktober 2004 operativ und seit dem 1. Dezember 2004 auf dem Internet präsent. Während sich das ISB neben der administrativen Leitung von Melani vor allem auf die Prävention konzentriert und das Bundesamt für Polizei das nachrichtendienstliche Lagezentrum betreibt, kommt dem *Switch-CERT* die Bedeutung des technischen Support- und Kompetenzzentrums vor allem im Bereich der IT-Betriebssysteme zu.[38]

Melani wird die folgenden Leistungen im Rahmen des Vier-Säulenmodells erbringen: Früherkennung und – zusammen mit Partnern – Bekämpfung der Ursachen von Krisen. Früherkennung ist gleichzeitig eine technische und nachrichtendienstliche Aufgabe. Eine weitere Aufgabe von Melani ist das Lagezentrum des Sonderstabes Sonia zur Analyse der Gefahrensituation. Sonia wird im Krisenfall benachrichtigt und aktiv.[39]

36 ISB, *Verletzliche Informationsgesellschaft*, 2002, S. 4–6.

37 Seit 1987 steht SWITCH – eine privatrechtliche Stiftung des Bundes und der acht Universitätskantone – im Dienste der vernetzten Schweizer Wissenschaft, vertritt die Schweizer Interessen in zahlreichen Gremien und trägt damit in einer Schlüsselrolle wesentlich zur Entwicklung und zum Betrieb des Schweizer Internets bei. Das *Computer Emergency Response Team* (CERT) der Abteilung Sicherheit der Switch bietet ihren Kunden (Universitäten, Fachhochschulen) seit 1995 Unterstützung bei Vorfällen im Bereich der Informationssicherheit und Beratung in sicherheitsrelevanten Fragen an. Switch-CERT vertritt die Bedürfnisse seiner Kunden gegenüber den Internet Service Providern (ISP), wie zum Beispiel die Rückverfolgung von Angriffen auf verschiedenen Netzwerken. Switch unterstützt zudem Melani mit CERT-Dienstleistungen. Der Fokus von Switch-CERT liegt demnach im technischen Bereich von IT-Sicherheit (http://www.switch.ch/de und http://www.melani.admin.ch/melani/organisation/index.html?lang=de).

38 http://www.switch.ch/de.

39 Zur Erfüllung seiner Aufgaben ist für Melani die kontinuierliche Beobachtung von Angriffsverfahren, technischen Entwicklungen sowie den damit verbundenen Trends, das Verfolgen der Diskussionen in Mailinglisten, auf Webseiten, in Fachjournalen, aber auch die entsprechenden politischen und gesetzgeberischen Entwicklungen im In- und Ausland unabdingbar. Dazu kommt die enge Zusammenarbeit mit anderen CERTs, Nachrichtendiensten, Herstellern und Anwendern von Computertechnologie und der Austausch mit den wichtigsten Informatikverantwortlichen aus Wirtschaft und Verwaltung. Schliesslich gilt es, die technischen Probleme zu analysieren und adäquate Lösungen und Strategien vorzuschlagen. Vgl. Rytz, *Schutzwälle für die Informationsgesellschaft*.

Zudem bietet Melani privaten Computer- und Internetbenutzern sowie Schweizer Unternehmen Informationen zum Schutz des Computers, Meldungen zu aktuellen Gefahren und Risiken und die (anonyme) Meldemöglichkeit von Vorfällen – wie zum Beispiel Datenzerstörung, *Hacking*[40], *Phishing*[41], *Hoaxes*[42] usw. Im Ereignisfall wird auch eine Beratung bei der Strafverfolgung angeboten. Zudem gibt es das Melani-Net, das sich an ausgesuchte Betreiber von nationalen kritischen Infrastrukturen richtet und Analysen zur Früherkennung von Attacken sowie die Koordination von Massnahmen bei Vorfällen anbietet. Die Wirksamkeit von Melani-Net wird stark vom Vertrauen abhängen, das ihm private Infrastrukturbetreiber entgegenbringen.[43] Melani verfolgt also einen umfassenden Ansatz und ist dank seiner Verlinkung mit Fedpol, Kobik und Switch-CERT ein potenter Ansprechpartner für alle Akteure, die sich mit CIIP befassen.[44]

Nationale Koordinationsstelle zur Bekämpfung der Internet Kriminalität (Kobik)

Zur Bekämpfung der Internetkriminalität auf Kantons- und Bundesebene wurde im Januar 2003 Kobik[45] ins Leben gerufen[46]; Kobik, das zum Fedpol gehört, ist die zentrale Anlaufstelle für Personen, die verdächtige Internet-Inhalte melden möchten. Diese Meldungen werden dann nach einer ersten Prüfung den zuständigen Strafverfolgungsbehörden im In- und Ausland weitergeleitet. Kobik

40 *Hacking* bedeutet das unberechtigte Eindringen in Netze oder andere Computer bzw. die Konten anderer Benutzer.

41 Das Wort *Phishing* setzt sich aus den englischen Wörtern *Password*, *Harvesting* und *Fishing* zusammen. Mittels *Phishing* versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Die Betrüger nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen E-Mails mit gefälschten Absenderadressen zustellen.

42 E-Mails mit Meldungen über neue und angeblich besonders gefährliche Viren sind fast immer Falschmeldungen oder sogenannte *Hoaxes* (engl. für Falschmeldung, Scherz). *Hoaxes* sind stets nach dem gleichen Muster aufgebaut. Sie warnen vor einem neuen, überaus gefährlichen Virus, der nicht einmal mit Hilfe einer aktuellen Antiviren-Software bekämpft werden kann. Zudem wird darauf hingewiesen, dass diese Meldung von einem renommierten Unternehmen aus der IT-Branche stammt und an möglichst viele Bekannte weitergeleitet werden soll.

43 http://www.melani.admin.ch.

44 Für den Kreis der grösseren Kunden, der zur Zeit 18 Unternehmen und Organisationen umfasst, konnten bereits Fälle bearbeitet werden. Im laufenden Jahr werden sich weitere Partner dem Kreis anschliessen. Die Palette der zu ihren Gunsten angebotenen Dienstleistungen wird mit zunehmender Erfahrung erweitert werden. (Stand April 2005). http://www.efd.admin.ch/d/dok/faktenblaetter/efd-schwerpunkte/5_infosicherheit.htm.

45 Auch unter dem englischen Namen Cyco, *Federal Cybercrime Coordination Unit*, bekannt.

46 Aufgrund der Vorschläge der interkantonalen Arbeitsgruppe zur Bekämpfung des Missbrauchs der Informations- und Kommunikationstechnik (Bemik) vom Januar 2001.

hält auch selbst im Internet Ausschau nach verdächtigen und möglicherweise illegalen Inhalten und führt Analysen im Bereich Internetkriminalität durch.[47] Die Koordinationsstelle ist um einen optimalen Informationsaustausch zwischen den Kantonen und eine enge Zusammenarbeit mit dem Privatsektor, den Strafverfolgungsbehörden und den Nachrichtendiensten bemüht und arbeitet eng mit Melani zusammen.[48] Kobik befasst sich also vorwiegend mit juristischen beziehungsweise strafrechtlichen Aspekten von CIIP.

Wirtschaftliche Landesversorgung (WL)

Die WL hat die Aufgabe, die Versorgung des Landes mit lebenswichtigen Gütern und Dienstleistungen für den Fall schwerer Mangellagen sicherzustellen. Die Massnahmen der WL kommen aber erst zum Tragen, wenn das marktwirtschaftliche System massiv gestört wird – wie zum Beispiel durch Pannen oder Sabotage im Bereich der IKT. Die WL ist eine Milizorganisation[49] und unterscheidet zwischen Grundversorgungsbereichen (Ernährung, Energie, Heilmittel) und Infrastrukturbereichen (Transporte, Industrie, IKT-Infrastrukturen, Arbeit).[50]

Aufgabe des vom Bund am 1. August 2000 geschaffenen *Bereich IKT-Infrastrukturen* (ICT-I) ist es, für kritische Wirtschaftsbereiche Notfallstrategien zu erarbeiten sowie Störungen zu verhindern beziehungsweise deren Folgen zu mindern und einen allfälligen Wiederaufbau zu ermöglichen.[51] Gemäss dem Vier-Säulenmodell spielt die WL vor allem bei der Schadensbegrenzung in der Krise eine zentrale Rolle.

ICT-I umfasst sektorspezifische Teams, welche durch Rekrutierung von Milizkadern aufgebaut werden und im Krisenfall Vertreter in den Sonderstab

47 http://www.cybercrime.admin.ch/d/worum.htm.

48 Centre for International Security Policy at the Swiss Federal Department of Foreign Affairs. *CiSP Proceedings. EAPC/PfP Workshop on Critical Infrastructure Protection & Civil Emergency Planning: Dependable Structures, Cybersecurity and Common Standards*. Zurich, 9 – 11 September 2004, S. 128.

49 Der Bundesrat ernennt einen Delegierten für die WL aus der Privatwirtschaft, der dem Eidgenössischen Volkswirtschaftsdepartement (EVD) unterstellt ist und die Organisation im Nebenamt leitet. Zurzeit arbeiten rund 300 Kaderleute aus Wirtschaft und Verwaltung nebenamtlich für die verschiedenen Bereiche der WL. Ausserdem stehen dem Delegierten im Bundesamt für wirtschaftliche Landesversorgung (BWL) rund 35 ständige Mitarbeiterinnen und Mitarbeiter zur Verfügung. http://www.bwl.admin.ch/deutsch/ueberuns-organigramm.asp.

50 http://www.bwl.admin.ch/deutsch/default.asp.

51 Dazu gehört die Planung und Vorbereitung der Mittel und Massnahmen zur Sicherstellung der Verfügbarkeit der Informations- und Kommunikationsinfrastrukturen für den Fall langfristiger Störungen oder Krisenlagen. Da die Handelsbilanz der Schweiz in allen Produktsegmenten des ICT-Sektors negativ ist, besteht eine starke Auslandabhängigkeit. In: Bundesamt für wirtschaftliche Landesversorgung. *Risikoanalyse für die wirtschaftliche Landesversorgung*. November 2001, S. 19.

delegieren. Somit ist für eine effiziente Anbindung der Wirtschaft gesorgt.[52] Die WL ist Teil eines Netzwerkes mit Beteiligten aus Wirtschaft, Wissenschaft und Verwaltung und berücksichtigt (IT-)technische, sicherheitspolitische sowie auch betriebswirtschaftliche Aspekte.[53] Von InfoSurance hat die WL zudem die sektorspezifischen Risikoanalysen übernommen und führt diese weiter.

VBS/Planungsstab: Sektion Information Operations (InfOps)

Im Armeeleitbild zur Armee XXI wird festgehalten, dass die Informationskriegsführung für die Schweiz ein erhebliches Risiko darstelle, weil die Eidgenossenschaft infolge der europaweit höchsten Informatik- und Vernetzungsdichte und der starken internationalen Verflechtung der Wirtschaft von funktionssicheren Datenverbindungen stark abhängig sei. Die komplexen Vernetzungen der unterschiedlichen gesellschaftlichen Bereiche haben demnach eine hohe Verwundbarkeit zur Folge.[54]

Mit dem Ziel, einen gemeinsamen doktrinalen Grundsatz zugunsten der nationalen Sicherheitspolitik zu finden, wurde die *Konzeptstudie Information Operations* (KS IO) unter der Federführung VBS (Planungsstab der Armee) in Zusammenarbeit mit zahlreichen betroffenen Departementen und Hochschulen im Mai 2002 ins Leben gerufen.[55] Bis dahin waren die Aktivitäten auf die klassischen Bereiche wie elektronische Aufklärung, Modernisierung der Übermittlungsmittel oder Datenschverschlüsselung konzentriert.

Auch innerhalb der *Gruppe Rüstung* gibt es eine Fachgruppe, die sich mit Information Operations befasst und KS IO unterstützt. Die behandelten Fachbereiche umfassen Computernetzwerke und -sicherheit, Sicherheitsinfrastruktur und Kryptologie, Risikoanalyse, Forschung und Systemsimulationen. Die Fachgruppe ist bestrebt, technikbezogene Konzepte und Massnahmen im Information Operations Umfeld bei zivilen und militärischen Systemen zu erarbeiten und umzusetzen.[56]

52 ISB, *Verletzliche Informationsgesellschaft*, 2002, S. 29–30.

53 Gegeben durch den gesetzlichen Grundauftrag der WL, gemäss Bundesverfassung Art. 102 und nachgeordnet basierend auf dem Landesversorgungsgesetz (LVG). Informationen von Anton Lagger, Leiter Geschäftsstelle ICT-Infrastruktur des Bundesamtes für wirtschaftliche Landesversorgung.

54 http://www.vbs-ddps.ch/internet/groupgst/de/home/generalstab/armxxi/armeeleitbild.html.

55 Pressemitteilungen, 8. Juli 2003. VBS erarbeitet Studie zum Thema «Information Operations». http://www.admin.ch/cp/d/3f0ac4c1_1@presse1.admin.ch.html. Zwischen Dezember 2000 und Oktober 2001 hat die Untergruppe Operationen des Generalstabes eine Vorstudie durchgeführt.

56 ASUT-Seminar, 12. Juli 2003. Alfred Markwalder: http://www.asut.ch/de/..%5Cupload_files%5Cdownloads%5CPraesentation_Markwalder_d.pdf.

Zusammenfassend lässt sich sagen, dass das VBS in seiner CIIP-Politik einen sicherheitspolitischen Ansatz, gekoppelt mit technischem Knowhow, verfolgt. Die (IT-)technischen Grundlagen liefert dabei vor allem die Armasuisse.

Armasuisse: Zentrum für Wissenschaft und Technologie (W+T-Zentrum)

Das *Command and Control Lab* des W+T-Zentrums der Armasuisse verfügt über ein breites Wissen auf dem Gebiet der Informationsoperationen und deren technologischen Aspekte. Zusammen mit internen und externen Partnern wird ein selektives Forschungsprogramm betrieben, einschliesslich dem Aufbau von operativen Fähigkeiten für die Verteidigung von Computer-Netzwerken.[57] Eine spezielle Fachgruppe Information Operations bearbeitet unter anderem das Teilgebiet «Technik und Sicherheit» für die Konzeptionsstudie Information Operations. Die Forschungstätigkeit der Armasuisse konzentriert sich also auf technische Aspekte, die Schnittstelle zur Sicherheitspolitik ist aber dank des Grundauftrags klar vorhanden.[58]

Bundesamt für Kommunikation (Bakom)

Das Bakom, angesiedelt im Departement für Umwelt, Verkehr, Energie und Kommunikation (Uvek), wurde 1992 als Regulator des Radio- und Fernsehbereichs und zur Schaffung von Voraussetzungen für die Öffnung des Telekommunikationsmarktes geschaffen. Heute ist das Bakom der wichtigste Regulator im Bereich Telekommunikation und IKT in der Schweiz.[59] Gegeben durch seinen Grundauftrag bezüglich elektronischer Kommunikationsinfrastrukturen behandelt das Bakom CIIP insbesondere als ein technisches und betriebswirtschaftliches Thema.

InfoSurance

In der Schweiz hatte die Stiftung InfoSurance eine wichtige Funktion bei der Initiierung von *Public Private Partnerships*.[60] Das nach der Strategischen Führungsübung (SFU 97) gebildete Beziehungsnetzwerk zwischen Wirtschaft, Wissenschaft und Verwaltung führte zur Bildung der Gruppe «Sicherheit Informations-Infrastruktur Schweiz» unter der Leitung der Wirtschaftlichen Lan-

57 Markwalder, Alfred. Information Operations: Wir schlagen Brücken. In: *digma – Zeitschrift für Datenrecht und Informationssicherheit* 4 (2004), Heft 2, S. 50.

58 Information von Vertreter der Armasuisse.

59 Das BAKOM hat zudem den Vorsitz über den Interdepartementalen Ausschuss Informationsgesellschaft (IDA IG), in welchem jedes Departement vertreten ist. Ebenfalls beim BAKOM ist die Koordinationsstelle Informationsgesellschaft angesiedelt, die die Website www.infosociety.ch betreut und die jährlichen KIG Berichte an den Bundesrat zum Stand der Umsetzung seiner Strategie (s. oben) publiziert. http://www.bakom.ch.

60 www.infosurance.ch.

desversorgung. Dank deren Vorarbeiten konnte 1999 die Stiftung InfoSurance von der Privatwirtschaft gegründet werden. Eines der Hauptziele bestand in der Sensibilisierung der Benutzer von Informationstechnologie, der Vernetzung der Akteure und der Initiierung und Durchführung von Risikoanalysen in diversen kritischen Wirtschaftssektoren. Nachdem sich im Jahre 2004 einige Privatfirmen als Geldgeber zurückgezogen hatten, wurden die sektorspezifischen Risikoanalysen an die Wirtschaftliche Landesversorgung/ICT-I übergeben.[61] Inzwischen ist insbesondere Melani darum bemüht, die Vernetzung zwischen dem Staat und den Betreibern von nationalen, kritischen Infrastrukturen zu etablieren und zu intensivieren.

3 Verschiedene Blickwinkel auf CIIP

Die Aufzählung der zentralen CIIP-Akteure auf Bundesebene hat gezeigt, dass je nach Grundauftrag, Aufgabe oder Interesse unterschiedliche Blickwinkel und thematische Schwerpunkte im Vordergrund stehen. Daraus können folgende vier idealtypische Blickwinkel abgeleitet werden, die, grob vereinfacht, wie folgt charakterisiert werden können:

- *Die (IT-)technische Sichtweise:* CIIP wird gleichbedeutend mit Internet- und IT-Sicherheit verstanden. Es wird angenommen, dass Gefahren gegen die Informationsinfrastrukturen ausreichend mit technischen Mitteln wie Anti-Virus-Software, Firewalls, Datenverschlüsselung, der Einhaltung von Standards und so weiter bekämpft werden können. Dieser rein technische Fokus ist zweifellos von zentraler Wichtigkeit, erfasst aber nicht die ganze Problematik von CIIP.

- *Die betriebswirtschaftliche Sichtweise:* CIIP wird mit sicherem E-Business beziehungsweise E-Economy und möglichst permanenter Verfügbarkeit wichtiger Geschäftsprozesse gleichgesetzt. Die Mittel stimmen weitgehend mit denjenigen der technischen Sichtweise überein. Der Fokus ist aber etwas breiter und umfasst auch organisatorische und personelle Faktoren. Die Förderung der Informationsgesellschaft, von Public Private Partnerships, der internationalen Zusammenarbeit und von Standards sind zentrale Komponenten dieser Sichtweise.

- *Die Sichtweise von Strafverfolgungsorganen*: CIIP wird verstanden als Schutz der Gesellschaft vor Internet- und Cyberkriminalität, die eine Vielzahl von unterschiedlichen Straftatbeständen umfasst, die mit Hilfe von IKT begangen werden können. Cyberkriminalität wird mit Hilfe

61 Die jährliche Durchführung der Luzerner Tage für Informationssicherung LUTIS sowie eine breit angelegte Initiative zur Verbesserung der Informationssicherheit in den KMU gehörten ebenfalls zu den Aktivitäten.

von Strafverfolgungskonzepten bekämpft, wobei die Anpassung der nationalen Gesetzgebung und die kantons- und grenzüberschreitende Zusammenarbeit unabdingbar sind.

- *Die sicherheitspolitische Sichtweise:* CIIP wird als Politik verstanden für den ausserordentlichen Fall und somit für Vorkommnisse, die nicht zu den alltäglichen, routinemässigen Vorfällen gehören. Diese Sichtweise umfasst verschiedene Ansätze, da im Prinzip die ganze Gesellschaft als gefährdet angesehen wird. Somit sind Aktivitäten auf der technischen, der gesetzgeberischen, der organisatorischen und der internationalen Ebene notwendig. CIIP wird im sicherheitspolitischen Sinn also nicht als ausschliesslich militärische Aufgabe verstanden. Bei dieser Sichtweise haben insbesondere die Nachrichtendienste in der Prävention und Lageanalyse eine zentrale Aufgabe und bewegen sich dabei an der zivil-militärischen Schnittstelle. Von zentraler Bedeutung ist zudem die interdepartementale Zusammenarbeit und der kooperative Informationsaustausch.[62]

Wie erwähnt sind die (IT-)technische und die betriebswirtschaftliche Sichtweise eng miteinander verknüpft. Dies ist auch auf Bundesebene der Fall: Akteure wie das ISB, Melani, das Bundesamt für wirtschaftliche Landesversorgung mit dem Bereich ICT-I sowie das Bakom befassen sich – nebst der sicherheitspolitischen Sichtweise – damit. Der Fokus auf die (IT)-technische und betriebswirtschaftlichen Aspekte von CIIP stehen auch im Zentrum der Interessen der Privatwirtschaft. Die Sichtweise von Strafverfolgungsorganen nimmt insbesondere Kobik ein.

Bei fast allen Schweizer Bundesstellen ist die sicherheitspolitische Sichtweise ein zentraler Aspekt bei CIIP. Dies gilt insbesondere für den Planungsstab des VBS und dessen Konzeptstudie Information Operations. Das W+T-Zentrum der Armasuisse im VBS befasst sich neben der sicherheitspolitischen insbesondere auch mit (IT-)technischen Aspekten von CIIP. Im Fall einer Krise der IKT spielen insbesondere der Bundesrat und Sonia eine zentrale Rolle. Die Vorbereitung der Akteure auf den Krisenfall ist die Aufgabe der Strategischen Führungsausbildung der BK.

Die folgende Tabelle ordnet die vorgestellten CIIP-Akteure in der Schweiz den vier verschiedenen Blickwinkeln zu. Die Zuordnung kann nicht in jedem Fall eindeutig erfolgen (Kreuze in Klammern) und ist primär als vereinfachender Überblick gedacht.

62 Dunn, Myriam/ Wigert, Isabelle. *The International Critical Information Infrastructure Protection (CIIP) Handbook*. Zürich: Forschungsstelle für Sicherheitspolitik, 2004, S. 22 und Dunn, *Sicherheit im Informationszeitalter*, S. 67f.

Blickwinkel und Schwerpunkte der analysierten Akteure im Bereich CIIP

Sichtweisen / Akteure	(IT-) Technische	Betriebswirtschaftliche	Strafverfolgungsorgane	Sicherheitspolitische
Bundesrat		(X)		X
BK/SFA				X
Sonia (interdepartemental)				X
ISB (EFD)	X	X		X (über Sonia)
Melani (EFD/EJPD/SwitchCERT)	X	X	X	X
Kobik (EJPD)			X	
BWL/ICT-I (EVD)	(X)	X		X
InfOps (VBS)	(X)			X
Armasuisse (VBS)	X			X
Bakom (UVEK)	X	X		(X)
Stiftung InfoSurance	X	X		

Wie aus dieser Tabelle hervorgeht, befassen sich fast alle staatlichen Akteure mit der sicherheitspolitischen Komponente von CIIP. In diesem Punkt unterscheiden sich die Interessen der staatlichen Stellen von denen der Privatwirtschaft. Andererseits sind sowohl der Staat als auch die Privatwirtschaft an der betriebswirtschaftlichen als auch an der (IT)technischen Sichtweise von CIIP interessiert, wobei sich Synergien ergeben könnten. Diese gemeinsamen Interessen könnten für den Austausch von fachspezifischem Know-how genutzt werden.

4 Analyse der Schweizer CIIP-Politik

Bei der Analyse der staatlichen schweizerischen CIIP-Politik fallen vor allem zwei eng miteinander verwobene Ziele der verschiedenen Massnahmen auf:

- Erstens ist der Staat daran interessiert, die neuen IKT zu nutzen, um die Informationsgesellschaft und damit die Wettbewerbsfähigkeit und Wohlfahrt in der Schweiz zu fördern.
- Zweitens ist der Staat bestrebt, die Bevölkerung und die Unternehmen vor den Gefahren und Risiken ebendieser Informationstechnologien zu schützen.

Von einigen Ausnahmen abgesehen kann gesagt werden, dass dieselben Informationsinfrastrukturen, die der Staat aus der Perspektive nationaler Sicherheit schützen will, auch die Basis für die Wettbewerbsfähigkeit und Prosperität der Schweiz bilden. Insofern erstaunt nicht, dass einer der wichtigsten strategischen Akteure in der schweizerischen CIIP-Politik, das ISB, dem Eidgenössischen Finanzdepartement unterstellt ist.

Diese Tatsache erscheint auf den ersten Blick naheliegend, ist aber, wie ein Vergleich mit anderen Staaten zeigt, nicht immer so. Zum Beispiel in Frankreich und in Schweden sind die Vereidigungsministerien in der nationalen CIIP-Politik federführend, während in den USA, Australien und Neuseeland die CIIP-Politik in die allgemeinen Antiterror-Massnahmen – bei denen die Nachrichtendienste eine zentrale Rolle spielen – integriert ist.[63]

Wie in diesem Artikel weiter gezeigt wird, sind innerhalb der Schweizer Regierung verschiedene Initiativen und Strategien im Bereich CIIP im Gang, die der nationalen Sicherheit als ganzes sowie der wirtschaftlichen und gesellschaftlichen Wohlfahrt zugute kommen sollen. Der Bund hat dabei folgende, sich ergänzende, Aktivitäten und Massnahmen im operationellen wie strategischen Bereich gewählt:

- Zu den operationellen Massnahmen kann das Sammeln und Austauschen von Informationen – was insbesondere für die Frühwarnung und Prävention unerlässlich ist, – sowie das Bereitstellen von Angeboten und Dienstleistungen für die CIIP-Akteure gezählt werden. Auf die Schweiz bezogen sind die Aktivitäten von Melani ein sehr gutes Beispiel für operationelle Massnahmen. Ferner können auch die Aktivitäten der BWL/ICT-Infrastruktur und Kobik dazu gezählt werden.
- Zu den strategischen Massnahmen gehört insbesondere das Ziel, das Verhalten bestimmter Akteure durch Sensibilisierung zu beeinflussen. Dies kann sich wiederum in der Schaffung neuer Politiken, Standards

63 Dunn/Wigert, *CIIP Handbook 2004*.

oder (rechtlicher) Rahmenbedingungen äussern. Um die Akteure zur Implementation der gewünschten Massnahmen zu bewegen, kann der Staat auf regulatorische, finanzielle oder auf die Kooperation und Koordination fördernde Mittel zurückgreifen. In der Schweiz sind in diesem Bereich insbesondere das ISB und das Bakom tätig. Die SFA der Bundeskanzlei ist vor allem für die Sensibilisierung der Verantwortlichen beim Bund zuständig. Das VBS ist sowohl strategisch als auch, im Fall einer Krise, operationell tätig.

In der Schweiz wird CIIP trotz seiner sicherheitspolitischen Komponente vor allem als (IT-)technisches Problem aufgefasst, das heisst Hacker werden nicht mit politischen, sondern primär mit kriminellen Absichten in Verbindung gebracht. Auf Bundesebene wird CIIP nicht als Teil der Terrorismus-Problematik behandelt wie zum Beispiel in den USA, obwohl die sicherheitspolitische Sichtweise bei fast allen Bundesstellen vorhanden ist.

Dabei ist klar, dass bei kleinen, «alltäglichen» Gefahren für die Informationsinfrastrukturen wie Viren, Hackerangriffen oder kurzen Systemunterbrüchen in erster Linie die (privaten) Infrastrukturbetreiber selbst um einen adäquaten Schutz bemüht sein müssen. Wie auch in anderen Staaten liegt der Fokus in der Schweiz auf der Eigenverantwortung der einzelnen Unternehmen. Der Staat reguliert nur im Notfall und muss die richtige Balance finden zwischen Sicherheitsstandards und Wirtschaftlichkeit. Handelt es sich hingegen um Gefahren in der Kategorie von Angriffen von Terroristen oder anderen Staaten auf unsere Informationsinfrastrukturen, dann wird ein Handeln seitens des Staates erwartet, da es sich um ein sicherheitspolitisches Problem handelt.

Die Schweiz verfügt über keine umfassende nationale Strategie zum Schutz der kritischen Informationsinfrastrukturen und keine zentrale Stelle, die sich ausschliesslich mit CIIP befasst. Bestehende Kompetenzen und fundiertes Sachwissen werden da genutzt, wo es bereits vorhanden ist – in den dafür spezialisierten Departementen und Stellen. Da CIIP ein so breites Feld ist, werden die unterschiedlichen Teilaspekte traditionell von verschiedenen Organisationen abgedeckt, was sicher sinnvoll ist. Andererseits kann das mitunter zu Unklarheiten führen. Die gemachte Umfrage hat gezeigt, dass auf die gestellte Frage an verschiedene staatliche CIIP-Akteure, wer ihrer Ansicht nach beim Bund die Hauptverantwortung für CIIP trage, so unterschiedliche Antworten wie «der Bundesrat in Zusammenarbeit mit den verschiedenen Departementen», «das ISB mit Sonia und Melani», «diese Frage lässt sich nicht beantworten, da unklare Rollenverteilung», «das Bakom für den Bereich Telecom und das ISB und BIT für die Verwaltung, schweizweit im Bereich IT niemand» oder, «das Bakom, ISB, WL/ICT-I, VBS: BABS und InfOps» gegeben wurden.

Diese Antworten zeigen, dass innerhalb der verschiedenen Organisationen Unsicherheiten bezüglich der Rollen- und Aufgabenverteilung in Bezug auf CIIP

auf Bundesebene bestehen. Demnach konnte sich bis jetzt keine Stelle beim Bund als klarer Hauptakteur im Bereich CIIP etablieren. In Zukunft werden Sonia und Melani wohl verstärkt diese zentrale (Führungs)Rolle im *operationellen Bereich* einnehmen. Zur Zeit kann davon aber noch nicht die Rede sein. Ausschlaggebend wird dabei sein, inwieweit die privaten Infrastrukturbetreiber bereit sind und die Notwendigkeit einsehen, in diesem sensiblen Bereich mit dem Staat zusammenzuarbeiten. Eine wichtige Voraussetzung für eine erfolgreiche Public Private Partnership wird immer sein, dass sie auf Vertrauen und nicht auf Konkurrenz beruht. Das schweizerische Milizsystem ist in dieser Hinsicht gewiss von Vorteil, weil der Austausch zwischen Politik und Wirtschaft seit langem gepflegt wird. Falls es zur Schaffung von Kobrir kommt, wäre dies eine umfassende Plattform für den *strategischen Bereich.*

5 Herausforderungen und Handlungsbedarf

Bei CIP, also dem physischen Schutz kritischer Infrastrukturen und strategisch wichtiger Objekte vor möglichen Gefahren, pflegt die Schweiz eine lange Tradition. Genauso muss es das Ziel des neuen sicherheitspolitischen Bereichs CIIP sein, mögliche Bedrohungen, Verletzlichkeiten und Risiken der Informations- und Kommunikationstechnologien durch umfassende Massnahmen wie Prävention, Frühwarnung und Lagebeurteilung zu reduzieren und die Robustheit der IKT zu erhöhen. Zudem müssen für den Fall einer grösseren Störung Notfallpläne und effektives Krisenmanagement vorhanden sein.

Der systematische Ausbau eines übergreifenden Informations-, Krisenmanagement- und Schutzsystems für die Informationsinfrastrukturen, wie es im sogenannten Vier-Säulenmodell vorgesehen ist, kann aber nur in enger Partnerschaft von Staat und Privatwirtschaft realisiert werden. Aufgrund der Komplexität der Aufgabe und der Vielseitigkeit der Bedrohungen bedarf der Infrastrukturschutz eines holistischen Ansatzes: Dabei müssen die (IT-)technische, die betriebswirtschaftliche und die sicherheitspolitische Sichtweise sowie die Sichtweise von Strafverfolgungsorganen zusammen berücksichtigt werden. Der alleinige Fokus auf die technischen und betriebswirtschaftlichen Risiken – wie es viele Unternehmen zu tun pflegen – lässt mögliche sicherheitspolitische und terroristische Gefahren ausser acht.

Wie in diesem Artikel gezeigt worden ist, haben sich verschiedene Stellen auf Bundesebene mit unterschiedlichen Blickwinkeln und Schwerpunkten dem Schutz der kritischen Informationsinfrastrukturen angenommen. Dabei können durchaus Interessenskonflikte entstehen, wenn es darum geht, zu definieren, was genau und von wem geschützt werden soll. Eine klare Rollenverteilung und Führung sind jedoch insbesondere im Fall einer Krise von zentraler Bedeutung, nicht zuletzt weil der Ausfall der Informations- und Telekommunikationsinfrastrukturen im allgemeinen mit sehr kurzer oder ohne Vorwarnzeit erfolgt. Die Frage nach

dem grössten Handlungsbedarf im Bereich von CIIP beantworteten die meisten Befragten denn auch mit der Notwendigkeit einer klaren Aufgabenverteilung und einer schweizerischen Gesamtstrategie sowie einer verstärkten Kooperation und Koordination zwischen den Akteuren. Ferner wurde das Bedürfnis nach einer klaren Gesetzgebung ebenso wie die notwendige Erarbeitung eines umfassenden Notfallplans und eine verstärkte Sensibilisierung der Öffentlichkeit und der KMUs angemeldet.

Vor allem auch privaten Infrastrukturbetreibern muss bekannt sein, bei wem die Kompetenzen liegen und an welche Bundesstelle sie sich wenden können. Dabei muss auch eine gemeinsame, allen verständliche Sprache gefunden werden. Denn wenn es um die Entscheidung geht, ob es sich im Fall eines grösseren Ereignisses um eine alltägliche Störung der IKT handelt, die von den betroffenen Unternehmen selbst behoben werden kann, oder ob es sich um eine Krise nationalen Ausmasses handelt, welche die Führungskompetenz des Bundes verlangt, ist die Kommunikation zwischen den verschiedenen Akteuren entscheidend. Das Ziel des Bundes muss es sein, dass jeder Akteur darüber unterrichtet ist, wer wann und in welcher Situation welche Aufgaben erfüllt und wer direkter Ansprechpartner ist. Hier könnte ein bundesweites Koordinationsorgan die Lösung bieten.

Diejenigen Bundesstellen, bei denen alle CIIP-Blickwinkel zur Deckung gebracht werden, sollten eine verstärkte Zusammenarbeit ebenso fördern wie einen intensiven Informationsaustausch. Bei vielen Stellen wird dies heute schon der Fall sein, sei es auf formellem oder informellem Wege. Es sollte unter Umständen aber untersucht werden, ob vielleicht Doppelspurigkeiten bestehen, die unnötig sind, oder ob es sich dabei um Redundanzen handelt, die es braucht.

Eine zentrale und spezialisierte Bundesstelle wie die sich im Aufbau befindende Melani, die sich umfassend um die Belange der Sicherheit von Informations- und Kommunikationsinfrastrukturen, insbesondere auch des Internets, kümmert, ist zweifellos von zentraler Bedeutung. Ein grosser Vorteil dieser neu geschaffenen Bundesstelle besteht darin, dass alle vier beschriebenen Blickwinkel auf CIIP berücksichtigt werden. Nur eine solche umfassende Kompetenz- und Ansprechstelle ermöglicht es einem modernen Staat auf den Ebenen der Strategieentwicklung, der Früherkennung von Gefahren und Risiken, des Austauschs von Informationen und letztlich der Koordination bei der Bekämpfung der Krisenursache auch international zu kooperieren.

Die aktive Rolle des Bundes ist nicht nur in der Krise, sondern auch bei der Prävention einer Krise gefragt – und zwar insbesondere im Bereich Sensibilisierung, Früherkennung und bei der Abgabe von Empfehlungen. Ferner müssen der Dialog und die Zusammenarbeit mit sämtlichen involvierten Akteuren auf Bundes- und Kantonsebene sowie den privaten Infrastrukturbetreibern und der Wissenschaft gepflegt und vertrauensbildende Massnahmen gefördert werden.

Auf Bundesebene sollten sich insbesondere auch die zivilen und militärischen Bereiche ergänzen, die sich bei CIIP überschneiden. Deshalb ist auch der Austausch mit geeigneten Stellen im Ausland zentral, vor allem auch mit Nachrichtendiensten, wenn es um Frühwarnung geht. Informationssicherung stellt einen Prozess dar, in welchem der ständige Austausch von Erfahrungen eine zentrale Rolle spielt. CIIP ist am besten dadurch zu erreichen, dass eine Balance zwischen den Bedürfnissen der verschiedenen Akteure nach Sicherheit und ihren eigenen Kapazitäten, diese Bedürfnisse zu erfüllen, gegeben ist.