



Grundlage zum Konzept Melde- und Analysestelle Informationssicherheit (MELANI) sowie für den Sonderstab Information Assurance (SONIA)

Autor: Dr. Ruedi Rytz¹

© Alle Rechte vorbehalten. Ohne ausdrückliche schriftliche Genehmigung des Informatikstrategieorgans Bund ISB ist es nicht gestattet, diesen Text oder Teile daraus in irgendeiner Form durch Fotokopie, Mikrofilm oder ein anderes Verfahren zu vervielfältigen oder zu verbreiten.

Einleitung

Die vom 13. – 15. Juni im Zivilschutzzentrum von Schwarzenburg durchgeführte Übung INFORMO 2001 hatte die Überprüfung des Konzepts für einen Sonderstab Informationssicherheit zum Ziel [1]. Erste Auswertungsberichte liegen vor [2,3] und hinterlassen einen zum Teil widersprüchlichen Eindruck [3]. Breiter Konsens in Wirtschaft und Verwaltung besteht jedoch darin, dass die Schweiz und speziell auch der Sonderstab Informationssicherheit eine gut ausgerüstete und (international) vernetzte Melde- und Analysestelle für Vorfälle im Bereich der Informations- und Kommunikationsinfrastrukturen braucht,² wie dies bereits im Konzept „Information Assurance“ der KIG und dem entsprechenden Bundesratsantrag vom 17. Mai 2000 gefordert wurde [4].

1 MELDE- UND ANALYSESTELLE INFORMATIONSSICHERHEIT (MELANI)

1.1 Ausgangslage

Sinn und Zweck einer Melde- und Analysestelle ist die Früherkennung von Problemen in der Informations- und Kommunikationsinfrastruktur. Gerade der Sonderstab „Information Assurance“ ist als nicht permanente Organisation in besonderem Masse auf so eine Stelle angewiesen. Man muss sich allerdings bewusst sein, dass die Früherkennung in vorliegendem Fall ein schwieriges Problem darstellt. Einerseits sind die Vorwarnzeiten kurz bis sehr kurz, andererseits lassen sich – im Gegensatz zu Geiselnahmen oder zur Radioakti-

¹ Der Autor verdankt A. Lagger und Dr. U. Haudenschild vom Bundesamt für wirtschaftliche Landesversorgung, Belpstrasse 53, 3003 Bern, wertvolle Hinweise und Ratschläge zur vorliegenden Arbeit, sowie den Abschnitt „Die Rolle des Milizamts ICT-I beim Aufbau der CCs“. Wichtige Anregungen – vor allem im Bereich der Frühwarnung – stammen von A. Hardmeier, Nationale Alarmzentrale, 8044 Zürich, welche an dieser Stelle ebenfalls verdankt werden.

² Solche Vorfälle werden sich in aller Regel durch Störungen und Funktionsausfälle in den kritischen Sektoren manifestieren.

vität – kaum Grenzwerte festlegen, wann eine Krisensituation³ erreicht ist. Zudem kann zur Zeit kaum auf Erfahrungen mit typischen Bedrohungslagen zurückgegriffen werden. Dem Problem von kurzen Vorwarnzeiten, unklaren Grenzwerten und Bedrohungslagen versucht man im militärischen Umfeld mit Nachrichtendiensten zu begegnen. Das ist im Bereich der „Information Assurance“ grundsätzlich nicht anders, auch wenn es im Bereich der Informations- und Kommunikationsinfrastruktur weniger um die staatshoheitliche Nachrichtenbeschaffung geht, als vielmehr um das auf gegenseitigem Vertrauen zwischen Verwaltung und Wirtschaft basierende freiwillige Melden von Vorfällen an eine zentrale Stelle, welche die eingehenden Daten analysiert und zu beidseitigem Nutzen aufarbeitet. Dieser Gedanke wird auch mit dem Namen Melde- und Analysestelle Informationssicherheit (MELANI) zum Ausdruck gebracht.⁴ Dass so eine Partnerschaft (sogar im internationalen Kontext) durchaus geeignet ist, ein gemeinsames Problem im Technologiesektor zu bewältigen, hat das „Y2K-Projekt“ gezeigt [5].

1.2 Lösungsansatz

In der „Information Assurance“ Landschaft der Schweiz braucht es also eine gut ausgerüstete und permanent (7 x 24 Stunden) besetzte Melde- und Analysestelle, welche Nachrichten im Bereich der Informations- und Kommunikationsinfrastruktur sammelt, triagiert und in geeigneter Weise an ihre Kunden kommuniziert. Ein bedeutender Kunde, wenn auch bestimmt nicht der einzige, ist der Sonderstab Information Assurance. Dieser nutzt MELANI zu seinem Aufgebot beim Erreichen gewisser Grenzwerte sowie als eine seiner wichtigsten Nachrichtenquellen während des Einsatzes.

Aus den Diskussionen an INFORMO, dem Konzept des Sonderstabs Informationssicherheit [1] sowie aus weiteren Quellen, haben wir folgende Liste von Aufgaben, Produkten und Eigenschaften von MELANI zusammengestellt, welche noch zu erweitern, zu konsolidieren und mit den Partnern in Verwaltung und Wirtschaft abzusprechen ist:⁵

a) Aufgaben

- Sammeln und bewerten von Vorfällen aus dem operativen IT-Betrieb der Bundesverwaltung, sowie aus den Kantonen und Gemeinden.
- Sammeln und bewerten von Vorfällen aus dem operativen IT-Betrieb von Unternehmen.
- Nachrichtenbeschaffung und Bewertung aus öffentlich zugänglichen Quellen (z.B. Medien, Internet, CERT-Advisories).
- Einbezug nachrichtendienstlicher Quellen (z.B. EDA, BAP, SND, OPAL).
- Pflege von Kontakten zu vergleichbaren Stellen im Ausland,⁶ sowie zu technischen Analysestellen (z.B. CERTs).

³ Unter Krisensituation wollen wir eine Lage verstehen, die ein grosses Potential zur Eskalation erkennen lässt.

⁴ Das Pendant zu MELANI wäre SONIA (Sonderstab Information Assurance). Die Namensgebung beruht auf einer Idee von D. Bircher und M. Holenstein, Ernst Basler + Partner, Zollikon (ZH).

⁵ Ein entsprechender Auftrag wurde der Firma Ernst Basler + Partner, Zollikon (ZH) übertragen.

⁶ Als Beispiel kämen das US-amerikanische NIPC (National Infrastructure Protection Center) oder das sich im Aufbau befindliche nationale Frühwarnsystem der Bundesrepublik Deutschland in Frage.

b) Produkte

- Frühwarnung, respektive Früherkennung von Vorfällen im Zusammenhang mit Informations- und Kommunikationsinfrastrukturen. Es wäre zu prüfen, ob bei unmittelbar drohender Gefahr und unter bestimmten Voraussetzungen, z.B. so lange die zuständigen Organe des Bundes nicht handeln können, MELANI in eigener Kompetenz Behörden und Bevölkerung informieren könnte.
- Alarmierung des Sonderstabs und Nachrichtenquelle im Einsatzfall (evtl. zur Verfügung Stellung von geeigneten „Werkzeugen“ für die Stabsarbeit).
- Bereitstellung von Erkenntnissen und Informationen für ein breites Publikum aus Verwaltung, Wirtschaft und Forschung.⁷
- Unterhalt und Betrieb von Datenbanken mit relevanten Ereignissen. Die graphische Aufbereitung dieser Daten wäre wünschenswert. (Welches Ereignis hat wann und wo stattgefunden? Welche Gegenmassnahmen wurden allenfalls bereits ergriffen und welchen Erfolg haben diese gezeitigt?)

c) Eigenschaften

- MELANI muss neutral sein und sowohl in der Verwaltung als auch in der Wirtschaft als verlässlicher Partner anerkannt sein.
- Der Sonderstab und evtl. auch andere Kunden sollten über geschützte und wenn nötig redundante Kommunikationswege mit MELANI verbunden sein.
- Sie kann auf sichere auch gegen äussere Einflüsse (z.B. NEMP, Mikrowellenkanone) geschützte Anlagen zurückgreifen.

Ad a) Der Erfolg der Melde- und Analysestelle wird entscheidend von der Menge und vor allem von der Qualität der eingehenden Meldungen abhängen. Die Bundesverwaltung mit ihrer umfangreichen zivilen und militärischen Informations- und Kommunikationsinfrastruktur gepaart mit der Tatsache, dass staatlich betriebene Infrastrukturen seit jeher eine besondere Anziehung auf Angreifer ausüben, bietet sich in fast idealer Weise als Informationslieferant an. Zu diesem Zweck sind sowohl im zivilen als auch im militärischen Teil der Bundesverwaltung Intrusion Detection Systems (IDS) aufzubauen und daraus gewonnene Erkenntnisse, z.B. über versuchte oder erfolgreiche Einbrüche ins Netzwerk, an MELANI weiterzuleiten. Ebenfalls zu melden sind Vorfälle mit Computerviren, Würmern, Trojanern aber auch Fälle von menschlichem und technischen Versagen,⁸ welche die Informationssicherheit der Bundesverwaltung betreffen.

⁷ Die überwiegende Anzahl eingehender Meldungen (schätzungsweise weit über 99.99%) wird nicht zum Aufgebot des Sonderstabs führen, was aber nicht heisst, dass solche Meldungen wertlos sind. Im Gegenteil: Man sollte versuchen, diese auf geeignete Art aufbereitet und ausgewertet, interessierten Kreisen zur Verfügung zu stellen.

⁸ Während Fälle von menschlichem Versagen in ihren Auswirkungen wohl meist lokal beschränkt bleiben, kann die Kenntnis von technischem Versagen bestimmter Anlagen oder Computersysteme entscheidend dazu beitragen, Krisen abzuwenden. Ein Beispiel ist der totale Zusammenbruch des Mobiltelefonnetzes der Swisscom Ende Juli 2001, welcher auf einem Softwarefehler beruhte, der der Firma Alcatel Tage im Voraus bekannt war. Mit zunehmender „digitaler Monokultur“ im Internet wird dies in Zukunft weiter an Bedeutung gewinnen.

Anmerkung: Einen vergleichbaren Weg beschreitet übrigens auch die US-amerikanische Verwaltung, welche den zivilen Teil ihres „Intrusion Detection Systems“ mit FIDNet (Federal Intrusion Detection Network) und den entsprechenden militärischen Zweig mit JTF-CND (Joint Task Force-Computer Network Defense) bezeichnet [6]. Die weitere Verarbeitung der Ergebnisse aus FIDNet und JTF-CND ist allerdings ziemlich umständlich und dürfte sich in der Praxis wohl nicht bewähren.

Wenn man davon ausgeht, dass nicht nur die Informationssicherheit der Verwaltung zur Diskussion steht und man unter Information Assurance in der Schweiz ein Gemeinschaftswerk von Verwaltung und Wirtschaft versteht, dann müsste auch die Privatwirtschaft bereit sein, ihre Beobachtungen an MELANI weiterzuleiten. Neben dem Vertrauen auf die Verschwiegenheit dieser Stelle (siehe unten), wird die Bereitschaft der Privaten bei MELANI mitzutun ganz entscheidend davon abhängen, ob diese auch von den Produkten der Melde- und Analysestelle profitieren kann. Gute „Verkaufsargumente“ könnten die Breite des zur Verfügung gestellten Datenmaterials (In- und Ausland) sein, wie es für einzelne Unternehmungen wohl nur schwierig aufzubringen sein dürfte, sowie dessen professionelle Aufarbeitung und Darstellung. Wichtig ist, dass dahingehende Abklärungen bei Exponenten aus der Wirtschaft (Grossfirmen, Dächverbänden) gemacht werden. Ein guter Gradmesser für das Interesse der Wirtschaft an einer solchen Melde- und Analysestelle wäre vermutlich ihre Bereitschaft zur finanziellen Beteiligung.⁹ Andererseits könnte man auch argumentieren, dass die Risiken mittlerweile sicherheitspolitisch relevante Dimensionen annehmen und es somit die Aufgabe des Staates sein könnte, MELANI allenfalls auch im Alleingang zu realisieren. Dies hätte aber einen entscheidenden Einfluss auf das Organisationsmodell. MELANI könnte in diesem Fall vermutlich (bei entsprechenden personellen Aufstokungen) von bereits existierenden Nachrichtendiensten betrieben werden.

Ad b) Sicher ein wichtiges Produkt der Melde- und Analysestelle ist die Alarmierung des Sonderstabs Informationssicherheit. Welche „Trigger“ diese auslösen sollen, ist eine der zentralen und sogleich eine der schwierigsten Fragen. Zu deren Beantwortung müssen unter anderem (vielleicht in Zusammenarbeit mit Hochschulen) ein paar Szenarien¹⁰ ausgearbeitet werden, bei denen der Sonderstab aufzubieten wäre. Zusätzlich sollten Überlegungen angestellt werden, welche Massnahmen zur Krisenbewältigung in Frage kämen. Sind zum Beispiel breit angelegte Abschaltungen der IP-Netze realistisch? Interessant könnte auch die Skizzierung eines „worst-case“ Szenarios sein. Es ist klar, dass solche Studien Stückwerk bleiben müssen. Vielleicht werden sich aber mit der Zeit und den Erfahrungen aus dem Betrieb von MELANI, die Probleme systematisieren und beispielsweise in Klassen einteilen lassen. Auch brennende Fragen, wie das Erkennen von Krisenschwellen oder das Aufzeigen von Eskalationsmechanismen, müssen so angegangen werden. Gerade aus diesen Gründen ist es wichtig, dass MELANI durch fest angestellte IT-Spezialisten ein möglichst hohes Mass an Kontinuität gewährleisten kann. Schliesslich wird man in so einem jungen Gebiet auch aus Fehlern lernen können. Anfängliche Fehlalarme müssen dabei in Kauf genommen und anschliessend entsprechend begründet und kommuniziert werden.

⁹ In der Bundesrepublik Deutschland scheitert der Aufbau eines CERTs für die Wirtschaft bis heute an deren Wille zur finanziellen Beteiligung.

¹⁰ Ein entsprechender Auftrag wurde an Prof. Bernhard Hämmerli und Pius Ziegler an die Hochschule für Technik und Architektur HTA nach Luzern vergeben.

MELANI müsste als stehende Organisation, Mittel zur Unterstützung der Stabsarbeit zur Verfügung stellen. Denkbar sind CMS-Systeme (Content Management Systems) aber auch eine Palette von Kommunikationsmitteln, angefangen von Telefon, Fax, allenfalls Schnurlostelefon, Internet, Intranet, VULPUS und andere. Eine gute und kommentierte Zusammenstellung findet sich in Ref. [7]. Zur Führungsunterstützung gehören ebenfalls der Betrieb von Ereignisdatenbanken sowie die graphische Aufbereitung der Daten, was sich in der Operation MILLENNIUM TRANSIT gut bewährt hat [8]. Analoge Produkte können von MELANI auch für weitere Kunden aus Verwaltung und Wirtschaft angeboten werden unabhängig davon, ob der Sonderstab im Einsatz ist.

Ad c) Es ist selbstverständlich, dass den einzelnen Firmen, die ja direkte Konkurrenten sein können, durch solche Meldungen keinerlei Wettbewerbsnachteile entstehen dürfen. Zum Schutz ihrer Identität sind daher die Berichte von geeigneten Stellen zu anonymisieren. Ganz allgemein wird es nötig sein, sich über die Klassifizierung von Daten Gedanken zu machen. MELANI muss in dieser Beziehung eine von allen beteiligten Parteien akzeptierbare Politik verfolgen. Dies wird insbesondere für Daten aus den nachrichtendienstlichen Quellen relevant werden.

Die Forderung nach geschützten Anlagen und Kommunikationswegen mag im ersten Moment erstaunen, wenn man bedenkt, dass man es selbst bei dem von US-amerikanischen Experten an die Wand gemalten Schreckgespenst des „Electronic Pearl Harbor“ [6] oder dem vom früheren CIA-Chef John Deutch prognostizierten „Cyber War“ [9] nicht mit Angriffen zu tun hat, bei welchen die physische Zerstörung von Einrichtungen im Vordergrund steht. Bedenkt man jedoch die zentrale Rolle, die diese Melde- und Analysestelle für die Informationssicherheit in der Schweiz und speziell auch für den Sonderstab spielt – sie ist sowohl das Instrument zur Erkennung der Krise als auch der zentrale Informationslieferant während seines Einsatzes – und stellt man diese den verhältnismässig einfachen Mitteln gegenüber, die es erlauben, die ICT-Infrastruktur in einem ungeschützten Gebäude zu zerstören [10], so wird einem der Schutzbedarf rasch klar. Hinzu kommt, dass der Wert von MELANI ganz entscheidend von der Anzahl (und Qualität) der Quellen abhängt. Je mehr Informationen zur Verfügung stehen, desto einfacher lässt sich die Situation überblicken und in einen grösseren Zusammenhang stellen. Unter anderem deshalb, aber auch aus rein ökonomischen Gründen, sollte in der Schweiz der Aufbau einer *einzig* solchen Anlage ins Auge gefasst werden, die auch den andern Organisationen im Rahmen des Konzepts „Information Assurance“ (z.B. den IO/IW) sowie der Wirtschaft zur Verfügung steht. Durch die Konzentration auf einen einzigen Standort steigt jedoch nicht nur die Attraktivität für potentielle Angreifer, sondern auch das Schadenspotential bei Naturkatastrophen und Zivilisationsumfällen. Solche Achillesfersen müssen entsprechend geschützt sein.¹¹

1.3 Probleme

Neben den offensichtlichen Vorteilen des oben skizzierten Lösungsansatzes, wie z.B.

¹¹ Keine Lösung wäre es, MELANI nur im Fall konkreter Bedrohungen oder im Einsatzfall des Sonderstabs in geschützte Anlagen zu verlegen. Solche Änderungen der Abläufe sind problematisch und sollten in jedem Fall vermieden werden.

- breite Palette der Informationsquellen
- Partnerschaft von Verwaltung und Wirtschaft auch in der Früherkennung
- Vermeidung von Doppelspurigkeiten dank des Aufbaus einer einzigen Anlage

bedürfen doch einige Punkte einer genaueren Überprüfung. Einer der (objektiv gesehen) grössten Vorteile, nämlich der Einbezug der verschiedensten Quellen, könnte sich unter Umständen in der Praxis als ein grosser Nachteil erweisen. Dieser Fall würde dann eintreten, wenn sich die Informationslieferanten gegenseitig nicht hundertprozentiges Vertrauen schenken. Vertraut zum Beispiel der Strategische Nachrichtendienst nicht auf den verantwortungsvollen Umgang mit seinen Meldungen, könnte sich dieser veranlasst sehen, entweder überhaupt keine Meldungen weiterzuleiten oder dann nur noch solche von geringerer Brisanz. Genau gleich würde sich die Situation auch auf der Seite der Wirtschaft darstellen. Einer klaren Regelung wer von wem, was erfahren darf oder sogar muss, wird eine zentrale Bedeutung zukommen. Ganz ähnlich sieht es auch mit der angestrebten internationalen Vernetzung aus und der Klärung der Frage, ob diese nicht im Widerspruch zu nationalstaatlichen Interessen steht. Der „Y2K-Bug“ hat zwar gezeigt, dass gemeinsame Bedrohungslagen oder Problemstellungen die Bereitschaft zur internationalen Zusammenarbeit fördern. Doch kam es offenbar auch in diesem Fall zur Unterdrückung von Informationsflüssen [8].

Wie bereits angesprochen, dürften sich auch aus der Optik der beteiligten und teilweise miteinander konkurrierenden Unternehmen ähnliche Probleme ergeben, welche sich vermutlich nur auf der Basis des gegenseitigen Vertrauens lösen lassen werden. Dies wird in jedem Fall bei der Vergabe des Aufbaus von MELANI prominent zu berücksichtigen sein. Natürlich könnte man versuchen, die Wirtschaft, z.B. mit Hilfe eines Informationssicherheits-Gesetzes, zur Herausgabe relevanter Informationen zu bewegen. Diese Versuche dürften sich aber als nicht sachdienlich erweisen und wären auch kaum durchsetzbar, da es es doch relativ einfach ist, brisante Informationen zum Beispiel mit dem Hinweis darauf, dass man den ganzen Umfang des Problems falsch eingeschätzt habe, so lange zurückzuhalten, bis sie allgemein publik und damit für MELANI wertlos werden. Ob die Wirtschaft bereit sein wird, freiwillig Vorfälle an MELANI zu rapportieren, dürfte in hohem Mass davon abhängen, wie wertvoll diese, die von ihr erbrachten Leistungen einstuft.

1.4 Organisationsmodell

Schema 1 zeigt einen möglichen organisatorischen Aufbau von MELANI. Auf der untersten Ebene stehen die IT-Betriebe der Wirtschaft, respektive der BVerw, welche Informationen (z.B. erfolgreiche oder versuchte Einbruchversuche ins Netzwerk, Datendiebstähle, Virenvorfälle u.a.) an den Monitor melden. Die Punkte rechts vom Kasten „IT-Betriebe BVerw“ deuten an, dass sich die Liste der Informationslieferanten beliebig erweitern lässt. Beispiele sind zahlreiche Quellen im WWW, Mailinglisten, Online Magazine, Virenzentren (Symantec, Trend Micro, McAfee), Computer Emergency Response Teams (CERTs)¹² und andere mehr. Der Monitor bewertet die eingehenden Meldungen, triagierte diese und meldet diejenigen von besonderer Brisanz an die Alarmstelle, an welcher ebenfalls Infor-

¹² Bei CERTs muss man sich bewusst sein, dass diese als „Response Teams“ aus verständlichen Gründen häufig erst dann informieren, wenn entsprechende „patches“ vorliegen.

mationen aus verschiedenen nachrichtendienstlichen und anderen Quellen zusammenlaufen. Je nach der Beschaffenheit der Daten und der noch notwendigen Aufarbeitung, respektive Verifizierung lassen sich weitere Quellen entweder am Monitor oder direkt an der Alarmstelle aufhängen. Schliesslich entscheidet ein Pikett, das neben einem guten ICT-Sachverständnis, vor allem ein „Gefühl“ für das Eskalationspotential einer Lage, sowie für die Abhängigkeiten der verschiedenen kritischen Sektoren hat, über die Aufbietung des Stabschefs, welcher dann (allenfalls nach Rücksprache mit verschiedenen Stabsmitgliedern) über die Einberufung des Sonderstabs entscheidet. Der Monitor lässt seine Erkenntnisse entweder direkt (z.B. übers WWW) oder über eine Organisation wie InfoSurance der Wirtschaft zu gute kommen.¹³

Während die verschiedenen Nachrichtendienste (EDA, BAP, SND) bereits existieren, müsste der Monitor neu aufgebaut werden. Die dazu einzusetzenden personellen Mittel hängen neben seinen Aufgaben (siehe unten) stark von der Art und Menge des zu sichtenen Datenmaterials ab. Eine gute Koordination und Absprache mit den Nachrichtendiensten scheint daher unverzichtbar. Aufgaben des Monitors, respektive seiner Mitarbeiter sind:

- Monitoring, Analyse und Triage des Datenmaterials aus den IT-Betrieben von Wirtschaft und Verwaltung.
- Jeweils ein Mitarbeiter nimmt den Pikettdienst an der Alarmstelle wahr.
- Je nach Aufgabenteilung mit den Nachrichtendiensten u.U. die aktive Datenbeschaffung.
- Pflege und Unterhalt einer Auswertungs- und Analysedatenbank. (Was haben wir in der Vergangenheit falsch beurteilt? Was für Lehren können wir daraus ziehen?)
- Sie nutzen ihr Wissen und ihre Erfahrung zur Ausarbeitung von Szenarien, kritischen Pfaden und möglichen Lageberichten.
- Sie unterhalten einen Internetdienst, z.B. in Form eines regelmässig nachgeführten „bulletin boards“ als „point of reference“ für Vorfälle in der Informations- und Kommunikationsinfrastruktur der Schweiz.
- Bereitstellung von Mitteln zur Führungsunterstützung im Einsatzfall von SONIA, sowie deren periodische Prüfung auf Funktionstüchtigkeit.

Zur Erledigung dieser Aufgaben ist ein Kontaktnetz zu allen wichtigen Kunden und Partnerorganisationen von MELANI im In- und Ausland aufzubauen. Beispiele sind: Der Sonderstab Information Assurance, das Milizamt ICT-I, die Stiftung InfoSurance, das Informatikstrategieorgan Bund ISB, die Hochschulen und weitere. Die genaue Anzahl der benötigten Stellen ist Gegenstand weiterer Abklärungen. Sie dürfte in der Grössenordnung von 12 – 15 Mitarbeitern liegen. Nicht vergessen sollte man allerdings, dass die eigentliche „Monitoringstelle“ permanent, d.h. 7 x 24 Stunden, mit ca. 2 Leuten zu besetzen ist. Diese relativ monotone und dennoch anspruchsvolle „screening“ Arbeit in geschützten Anlagen dürfte zu Verschleiss- und Ermüdungserscheinungen führen. Um die Attraktivität der Arbeitsplätze nicht zu gefährden, sind diese Dienste zeitlich einzuschränken (z.B. auf 40%

¹³ Wenn immer möglich soll die Kommunikation zwischen den aufgeführten Stellen über physisch sichere Kommunikationswege erfolgen. Die Authentizität und möglicherweise die Vertraulichkeit sollen mit geeigneten Mitteln (z.B. PGP) gewährleistet werden.

der Arbeitszeit). Solche Überlegungen könnten die Anzahl der zu besetzenden Stellen noch erhöhen.

Vielleicht könnte der Monitor durch militärisch ein-, respektive umgeteilte Milizionäre verstärkt werden. Die dazu notwendigen rechtlichen Grundlagen müssten durch eine Verordnung analog VEMAC SR 732.345 geschaffen werden.¹⁴

Nach diesen Ausführungen zur Melde- und Analysestelle wollen wir uns im folgenden Abschnitt dem vorliegenden „Konzept für einen Sonderstab Informationssicherheit“ zuwenden und Möglichkeiten seiner Komplettierung und Einbettung ins Konzept „Information Assurance“ aufzeigen.

2 SONDERSTAB INFORMATION ASSURANCE (SONIA)

2.1 Auftrag und Kompetenzen

Um die Tauglichkeit des vorliegenden Konzepts (vgl. Ref. [1]) diskutieren zu können, ist es absolut zwingend, sich zuerst über die Aufgaben und Produkte des Sonderstabs im klaren zu sein. Nur wenn man genau weiss, was man mit SONIA erreichen und welche Situationen man abdecken will, kann man die Zweckmässigkeit der eingesetzten Mittel sowie seine Zusammensetzung beurteilen. Obwohl die Frage nach den Aufgaben und Produkten des Sonderstabs zentral ist, erweist sich dessen Beantwortung als nicht ganz einfach, wie man an den verschiedenen diesbezüglichen Voten im Rahmen von INFORMO 2001 gesehen hat.¹⁵ Auch der Gesetzgeber, welcher durch die Bundesinformatikverordnung (BinfV; Art. 7 Abs. 3) die Rechtsgrundlage für SONIA geschaffen hat, äussert sich weder im Gesetzestext noch in den Erläuterungen zu Verordnung und Weisungen über die Informatik und Telekommunikation in der Bundesverwaltung vom 15. Februar 2000 über Einsatzzweck und Aufgaben von SONIA. Das Konzept Information Assurance der KIG bleibt in diesem Punkt – mit einer Ausnahme (siehe unten) – ebenfalls wenig konkret. Nach geltendem Organisationsrecht des RVOG, auf welchem sich auch die BinfV abstützt, haben Stabsorganisationen vorbereitende Funktionen. Dazu gehören Lagebeurteilungen, die Erarbeitung von Lösungsvorschlägen zu Händen des Bundesrats, sowie die interne Koordination (siehe auch Ref. [11]). Unter zusätzlicher Berücksichtigung des Leitgedankens vom partnerschaftlichen Miteinander zwischen Verwaltung und Wirtschaft, hat man dem Sonderstab in der Konzeptstudie die folgenden Aufgaben zgedacht [1]:

1. Er berät den Bundesrat im Falle schwerwiegender Ereignisse im Bereich der Informationssicherheit und stellt diesem sowohl Entscheidungsgrundlagen als auch Lösungsvorschläge zur Verfügung.

¹⁴ Hier könnten sich allerdings folgende Probleme ergeben: (a) Im Krisenfall werden so eingeteilte Fachspezialisten ebenfalls in ihren Unternehmen gebraucht, was zu Interessenkonflikten führen könnte. (b) Die Milizionäre erhalten während ihrer Tätigkeit für MELANI Kenntnis über sensitive Daten von Firmen (auch von Konkurrenten!) und Nachrichtendiensten, was Unternehmen dazu veranlassen könnte, mit ihren Meldungen Zurückhaltung zu üben.

¹⁵ Wichtige Anhaltspunkte zur Beantwortung dieser Frage erwarten wir uns noch von den an der HTA ausgearbeiteten Szenarien, welche Ende November 2001 vorliegen sollten.

2. Er beurteilt laufend die Lage zum Krisenverlauf und kommuniziert diese situationsgerecht an interessierte Stellen. Zentral ist die Information der Bevölkerung unter anderem mit dem Ziel, das Vertrauen in die Führung der Behörden herzustellen.
3. Er kann im Sinne der operativen Krisenbewältigung für die Bundesverwaltung Massnahmen anordnen.
4. Er koordiniert die Anstrengungen der Wirtschaft (kritische Sektoren), der Bundesverwaltung sowie der Kantone und Gemeinden zur Überwindung der Krise.

Ad 1) Diese Aufgaben entsprechen Sinn und Zweck von Stabsorganen, wie in Artikel 55 des RVOG festgesetzt; sie werden bereits im Konzept Information Assurance der KIG vorgeschlagen und sind soweit unumstritten.

Ad 2) Krisen, gleich welcher Art und Prägung, können bei unsachgemässer und ungeschickter Informationspolitik rasch zu einem erheblichen und irreparablen Vertrauensverlust in die betroffenen Institutionen führen. Positive (Absturz der SR 111 bei Halifax, 1998) wie negative (Unfall bei der damaligen Sandoz SA, Schweizerhalle, 1986) Beispiele sind uns noch bestens präsent. Bei einem Sonderstab der Bundesverwaltung ist diesem Thema grösste Bedeutung beizumessen, da in diesem Fall die Glaubwürdigkeit der Verwaltung und letztlich auch der Schweiz auf dem Spiel steht. Daher sind die Mitteilungen des Sonderstabs durch die Kommunikations- und IT-Fachspezialisten gemeinsam zu verfassen und auf die Bedürfnisse des Zielpublikums abzustimmen. Medienmitteilungen sollen generell über die Bundeskanzlei kommuniziert werden.

Ad 3) Ein Sonderstab Information Assurance der Bundesverwaltung muss dazu da sein, Krisen in der BVerw, welche durch Störungen in der Informations- und Kommunikationsinfrastruktur herbeigeführt werden, auch zu bewältigen. Krisenbewältigung ist typischerweise eine operative Aufgabe, welche von den Entscheidungsträgern operativer Einheiten auf Direktionsstufe wahrgenommen werden muss. Bei der Besetzung des Stabs mit Mitgliedern aus der BVerw, ist darauf zu achten, dass diese die Umsetzung der beschlossenen Massnahmen „Kraft ihres Amtes“ verfügen können. Dies erhöht nicht nur die Akzeptanz der getroffenen Entscheide, sondern macht auch den Erlass einer weiteren Verordnung zur Festlegung der Kompetenzen der Stabsmitglieder (vorerst einmal derjenigen aus der BVerw) unnötig [12].¹⁶ Im Sinne der Doktrin konzentrierter Arbeitsstrukturen und Straffung der Abläufe, sind diesen Entscheidungsträgern, Fachspezialisten aus der Bundesverwaltung beizuordnen. Diese können aus dem Informatikstrategieorgan sowie aus den entsprechenden Verwaltungseinheiten, z.B. dem BIT, rekrutiert werden. In einzelnen Departementen könnte es vorteilhaft sein, die entsprechenden ISBDs ebenfalls anzubieten. Welche Departemente und Ämter im Sonderstab vertreten sein müssen, ist zur Zeit Gegenstand weiterer Abklärungen.¹⁷

Ad 4) Während die Punkte 1 – 3 weitgehend klar und bis auf Detailfragen als Aufgaben, respektive Produkte des Sonderstabs unumstritten sind, gab der vierte Punkt immer wieder Anlass zu Diskussionen und Missverständnissen. Das Mitwirken der Privatwirtschaft in einem Sonderstab der Bundesverwaltung beruht auf der Einsicht, dass wegen der Vernetzung der verschiedenen (kritischen) Sektoren untereinander und dieser mit der BVerw, ein

¹⁶ Die Besetzung des Stabs müsste in Informatikweisungen des Bundesrats und des IRB festgeschrieben werden.

¹⁷ Dieser Frage wird vom ISB und von Ernst Basler + Partner im Zuge der Überarbeitung des Konzepts zum Sonderstab Informationssicherheit nachgegangen.

staatlicher Alleingang nicht zweckmässig ist. Auf die Möglichkeit des Beizugs „geeigneter Stellen ausserhalb der Bundesverwaltung“ wird denn auch explizit in der rechtlichen Grundlage für den Sonderstab Information Assurance (BinfV, Art. 7 Abs. 3) hingewiesen. Weitere Einzelheiten sind auch hier nicht geregelt; Aufgaben und Befugnisse bleiben ungeklärt. Im Sinne der bereits unter Punkt 3 erwähnten Doktrin der konzentrierten Arbeitsstrukturen und Arbeitsabläufe sollte ein Sonderstab auf Grund seiner Zusammensetzung in der Lage sein, für eine rasche Koordination der vertretenen Parteien zu sorgen. Was allgemein unter „Koordination“ und im speziellen unter „Koordination zwischen Wirtschaft und Verwaltung“ verstanden wird hängt unter anderem auch vom Erfahrungsschatz des jeweiligen Gesprächspartners ab, wie wir in zahlreichen Diskussionen feststellen konnten. Zwei (Extrem)fälle können unterschieden werden:

1. **Aktive Koordination:** Auf Grund der Lagebeurteilung beschliesst der Sonderstab (wenn angezeigt nach Rücksprache mit den politischen Entscheidungsträgern) Massnahmen, welche von den entsprechenden operativen Einheiten in den Sektoren zwingend umzusetzen sind. Beispiele der aktiven Koordination sind die VEOR (Verordnung über die Einsatzorganisation bei erhöhter Radioaktivität; SR 732.32) und die SoGE (Verordnung über den Sonderstab Geiselnahme und Erpressung; SR 172.213.80).
2. **Passive Koordination:** Der Sonderstab beschränkt sich in seiner Arbeit primär auf die Lagebeurteilung, auf Grund welcher die einzelnen Wirtschaftssektoren selbständig Massnahmen veranlassen können. Informationen über bevorstehende und bereits erfolgte Massnahmen sowie über deren Erfolg, respektive Misserfolg werden zwischen den Sektoren via Sonderstab ausgetauscht, worauf die Massnahmen angepasst und verfeinert werden können. Der Sonderstab versteht sich somit als Lagezentrum und Informationsdrehscheibe in der Krise. Hier könnte die Organisation MILLENNIUM TRANSIT als Beispiel genannt werden.

Welche Form der Koordination ist nun für SONIA richtig? Die Beantwortung dieser Frage entscheidet sowohl über die Zusammensetzung des Sonderstabs als auch über das noch zu schaffende gesetzliche Regelwerk. Wie (fast) immer haben beide Varianten sowohl Vor- als auch Nachteile, die gegeneinander abgewogen werden müssen. Trotzdem konnte sich das ISB relativ leicht für das zweite Modell, also für die passive Koordination, entscheiden. Diese Wahl werden wir im nachfolgenden Abschnitt begründen und uns dann der Beschreibung eines möglichen Organisationsmodells für SONIA zuwenden.

2.2 Lagezentrum in der Krise

Eine Krise, welche durch Störungen in der Kommunikations- und Informationsinfrastruktur hervorgerufen wird, ist in vieler Hinsicht anders als „herkömmliche“ Krisen. Sie ist anders bei der Früherkennung, tritt (meist) anders in Erscheinung und verlangt zu deren Überwindung ebenfalls ein anderes Zusammenspiel zwischen den Partnern aus Verwaltung und Wirtschaft. Nehmen wir als Beispiel die radioaktive Verseuchung, welche durch einen Unfall in einem KKW ausgelöst wird. Ein solches Ereignis lässt sich auf Grund bekannter Messgrössen und Messvorschriften rasch erkennen und lokalisieren. Ist der Verursacher gefunden, so kann der weitere Verlauf der Geschehnisse mittels bekannter Modelle (Naturgesetze) wenn auch nicht exakt bestimmt, so doch erahnt werden, worauf sich entspre-

chende Massnahmen einleiten lassen. Menschenleben sind von Anbeginn potentiell bedroht und sowohl staatliche als auch private Stellen in etwa gleich betroffen, wodurch partikuläre Interessen rasch in den Hintergrund rücken. Für Fälle, in denen solche Szenarien die Regel und nicht die Ausnahme bilden, müssen Strukturen aufgebaut werden, welche durch *aktive Koordination* der Mittel befähigt sind, die Krise zu überwinden; der Führungsanspruch des Staates ist gemeinhin akzeptiert. Im Gegensatz dazu gelten für Krisen, welche durch Störungen in der Kommunikations- und Informationsinfrastruktur ausgelöst werden, andere Gesetzmässigkeiten. Sie lassen sich – wenigstens zur Zeit – nur schwer messen und erkennen. Sie werden sich durch sekundäre Merkmale, wie zum Beispiel den Ausfall von Zugverbindungen, den Unterbruch der Wasserversorgung oder den Verkehrszusammenbruch in einer Grossstadt zu erkennen geben. Ursache und Wirkung sind nicht unbedingt kausal verknüpft und folgen keinen Naturgesetzen. Schliesslich werden nicht alle Wirtschaftssektoren gleich stark betroffen sein und sogar im gleichen Sektor werden sich Unterschiede feststellen lassen (z.B. Swisscom ist stärker betroffen als Sunrise oder Orange). Wenn wir mit SONIA auf so eine Krise verhältnismässig und situationsgerecht reagieren und gleichzeitig der enormen Komplexität Rechnung tragen wollen, so dürften sich dazu zentralistische Ansätze wie im VEOR schlecht eignen.¹⁸ Das dazu notwendige Wissen kann kaum an einer einzigen Stelle (in einem Sonderstab) vereinigt werden; ganz zu schweigen von der immensen Vielfalt an operativen Aufgaben, die sich in so einem Umfeld ergeben. Die Lösung dieser Probleme muss in der Vernetzung von kleineren wohl definierten Einheiten mit eigenen Befugnissen und Kompetenzen bestehen. Bevor wir zur Beschreibung eines solchen Modells kommen, möchten wir in den nächsten zwei Abschnitten noch ein paar weitere Gründe anführen, weshalb für SONIA eine Lösung mit aktiver Koordination der Mittel nicht im Vordergrund stehen kann.

Eine aktive Koordination bedingt die Vereinigung der Entscheidkompetenz im Sonderstab. Während sich dies für die Bundesverwaltung durch Delegation der entsprechenden Amtsdirektoren bewerkstelligen lässt, wird es schwierig sein, analoges in der Wirtschaft durch Delegation von CEOs zu erreichen. In der Krise werden gerade solche Leute ihren Aufgaben im Unternehmen nachkommen wollen und sich nur ungern an einem Sonderstab der Bundesverwaltung beteiligen. Als Alternative wird gelegentlich die Entsendung von Vertrauenspersonen mit entsprechenden Vollmachten genannt. Auch diese Variante vermag einer kritischen Überprüfung nicht Stand zu halten. Erstens haben Beispiele in der Vergangenheit gezeigt, dass CEOs ihre Entscheidkompetenzen in einer Krise nicht delegieren und zweitens würde die Aufnahme auch nur eines Vertreters aus jeder relevanten Unternehmung die Grösse des Sonderstabs derart anschwellen lassen, dass eine effiziente Entscheidungsfindung verunmöglicht würde. Diese Zahl durch „Branchenvertreter“ aus den entsprechenden Verbänden reduzieren zu wollen, scheitert allein daran, dass solche Leute *per se* keine operativen Aufgaben wahrnehmen können.

¹⁸ Vielleicht etwas plakativ aber sicher nicht unzutreffend kann man feststellen, dass sich zentralistische Lösungen (wie z.B. im VEOR) besonders dann eignen, wenn die Problemstellung verhältnismässig einfach ist und das Schadenspotential *a priori* als hoch eingestuft werden muss. Natürlich wäre es im Sinne der Vereinheitlichung der verschiedenen Einsatzorganisationen auch verführerisch, für alle Sonderstäbe den Ansatz mit aktiver Koordination zu beschreiben. Es könnte argumentiert werden, dass man so auch für schwere Krisen gewappnet sei und sich allfällige Interessenkonflikte, welche die Problemlösung behindern, rasch lösen liessen. Man sollte sich aber bewusst sein, dass jede vorgeschlagene Einsatzorganisation erstens praktisch umsetzbar und zweitens effizient sein muss, so dass ein ausgewogenes Verhältnis zwischen Massnahmen und Risiko besteht. Auch für Sonderstäbe sollten die klassischen Grundsätze, Methoden und Verfahren des Risikomanagements gelten (siehe dazu auch Ref. [13]).

Neben diesen zum Teil logistischen Unzulänglichkeiten würde der Versuch der aktiven Koordination durch den Sonderstab, welche durch Verabschiedung verbindlicher Massnahmen zu geschehen hätte, auch juristische Probleme aufwerfen; insbesondere die Frage nach der Haftung bei Fehlentscheiden. Massgebend wäre Art. 3 Abs. 1 des Verantwortlichkeitsgesetzes (VG; SR 170.32). Nach dieser Bestimmung haftet der Bund für Schäden, die Beamte in Ausübung der amtlichen Tätigkeit Dritten widerrechtlich zufügen, ohne Rücksicht auf das Verschulden des Beamten (strenge Kausalhaftung). Fehlinformation oder unzuweckmässige Empfehlungen durch die zuständigen Bundesbehörden können im Einzelfall durchaus als Widerrechtlichkeit im Sinne des VG in Betracht kommen; sie sind daher zumindest im Grundsatz zur Auslösung nach oben unbegrenzter Schadenersatzforderungen gegen den Bund geeignet. Das gleiche gilt, wenn trotz entsprechender Verpflichtung (also bei Garantenstellung des Bundes) eine Information oder Empfehlung unterlassen wird (siehe auch Ref. [12]). Im Fall der VEOR, bei dessen Einsatzfall man davon ausgeht, dass Bevölkerung und Umwelt durch erhöhte Radioaktivität bedroht sind (vgl. VEOR; Art.1 Abs. 1), sind solche finanziellen Risiken für den Bund vertretbar. Dies ist im Fall von SONIA zumindest zu hinterfragen, vor allem wenn man bedenkt, dass mögliche Massnahmen rasch einmal hunderte von Firmen (mit dem entsprechenden Schadenspotential) betreffen können. Vernünftig scheint es, dass SONIA Grundlagen für die Entscheidungsfindung liefert, die Entscheidung selbst sowie dessen Umsetzung aber dort belässt, wo sie hingehört, nämlich zu den einzelnen IT-Betreibern in der Wirtschaft. Nur diese kennen ihre Infrastruktur hinreichend genug, um angemessene und verantwortungsvolle Massnahmen beschliessen und umzusetzen zu können. Dies entspricht auch der an INFORMO 2001 vorherrschenden Meinung, dass dem Bund weder in der Datenverarbeitung noch in der Telekommunikation rechtlich umfassende Kompetenzen zustünden und dieser auch fachlich nicht alleine sachverständig sei. Weder rechtlich noch fachlich bestehe somit eine Basis, um einen Führungsanspruch des Bundes bezüglich der Informationssicherheit zu begründen [11].

2.3 Organisationsmodell

Wir schlagen das in Schema 2 dargestellte Modell vor: Die Melde- und Analysestelle Informationssicherheit (MELANI) ist durch einen Kasten dargestellt. Sie wird ihre Arbeiten – vor allem im Bereich der Nachrichtenbeschaffung und Auswertung – auch in der Krise weiterführen, was der Doktrin der unveränderten Arbeitsabläufe beim Übergang von der Normal- zur Krisensituation entspricht. Im Einsatzfall von SONIA ist eine Erhöhung der Kadenz der Lagebeurteilungen denkbar. Dies sollte durch geeignete Massnahmen (z.B. Ausschöpfung von Überkapazitäten, längeren Dienstzeiten, Streichung von Ferientagen) relativ kurzfristig erreicht werden können. Kämen Milizionäre zum Einsatz, sieht man sich mit dem Problem konfrontiert, dass diese ebenfalls an ihren angestammten Arbeitsplätzen gebraucht werden, was zu Interessenkonflikten führen könnte. Noch abzuklären ist, ob bei unmittelbar drohender Gefahr und unter ganz bestimmten Voraussetzungen, z.B. so lange die zuständigen Organe des Bundes nicht handeln können, MELANI in eigener Kompetenz Behörden und Bevölkerung informieren könnte (gestrichelter Pfeil).

Die Schnittstelle zwischen MELANI und Sonderstab ist seine Lagezelle („Lageoffizier“), welche die Informationen entgegennimmt und in eine auf die Bedürfnisse des Sonderstabs zugeschnittene Form bringt. Die Lageinformation wird durch Nachrichten aus den Sekto-

ren, welche über die Delegierten der Coordination Centers (DCC) und die Amtsdirektoren (AD) eintreffen, kontinuierlich ergänzt. Erfahrungen aus der Operation MILLENNIUM TRANSIT sowie aus INFORMO 2001 haben gezeigt, dass eine einzelne Person mit diesen Aufgaben rasch überfordert ist, so dass die Lagezelle mit einer angemessenen Anzahl von Leuten (drei oder mehr) zu besetzen sein wird.

Die Infozelle arbeitet eng mit der Lagezelle zusammen und erstellt situationsgerechte an den jeweiligen Verteiler (Bundesrat, Behörden, Bundeskanzlei) angepasste Mitteilungen. Durch Absprache mit den Stabsmitgliedern stellt die Infozelle sicher, dass keine widersprüchlichen Signale ausgesendet werden. Dies ist besonders wichtig, wenn die Nachrichten für die Bevölkerung bestimmt sind, damit keine unnötigen Ängste geschürt werden. Als weitere vertrauensfördernde Massnahme wird die Information der Bevölkerung durch die Bundeskanzlei vorgenommen. Die Kommunikation mit dem Bundesrat (z.B. das Stellen der Anträge sowie die Entgegennahme von Aufträgen) soll durch den Delegierten für die Informatikstrategie des Bundes (in seiner Funktion als Chef Sonderstab Information Assurance) wahrgenommen werden.

Die mit AD (Amtsdirektoren) und FS (Fachspezialisten) bezeichneten Kästchen bilden den Block der Stabsmitglieder aus der Bundesverwaltung, welcher für die Krisenbewältigung innerhalb der BVerw zuständig ist. Ebenfalls in diese Kategorie fallen die Verbindungspersonen zum Milizamt ICT-I sowie zu den Information Operations der Armee (im Schema 2 nicht explizit aufgeführt). Die im Konzept des Sonderstabs vorgeschlagenen Eskalationsstufen (Sonderstab < Milizamt ICT-I < IO/IW) sind noch einmal zu überdenken. Beispiele aus der Vergangenheit belegen nämlich, dass die Grenzen zwischen „zivilen“ und „militärischen“ Operationen im Bereich der Informations- und Kommunikationsinfrastruktur nicht klar zu ziehen sind. Wir verweisen auf die Hackerangriffe gegen Banken mit vermuteten Milosevic-Konten während des Kosovokrieges oder auf die Attacken chinesischer Computerspezialisten gegen amerikanische Webseiten im Anschluss an die Kollision eines chinesischen Militärjets mit einem U.S. Spionageflugzeug am 1. April 2001. Dies würde in besonderem Masse gelten, falls die Vorstudie „Information Operations“ des Generalstabs zum Schluss kommen sollte, dass IO/IW auch für die Schweiz im Sinne der „US Joint Doctrine for Information Operations“ zu interpretieren sei, wo nicht nur der Schutz der eigenen, sondern auch die gezielte Beeinträchtigung der gegnerischen Informationsinfrastruktur angestrebt wird. Vor allem solche offensiven Aktionen können auf die heimische Wirtschaft zurückfallen und sind daher mit dieser vorgängig abzusprechen. Durch seine Organisationsstruktur bietet SONIA auch hierfür beste Voraussetzungen. Noch abzuklären ist die Rolle der Bundespolizei. Im Gegensatz zu MELANI und den IO/IW der Armee ist der Sonderstab keine stehende Organisation, sondern ein (Informationsaustausch-) und Lagezentrum *in* der Krise. Strafverfolgung von Computerkriminalität hingegen ist eine permanente Aufgabe des Staats und daher vorzugsweise an MELANI anzusiedeln.¹⁹

¹⁹ Ein weiteres Argument, die Strafverfolgung an MELANI aufzuhängen, ergibt sich daraus, dass das BAP als Informationslieferant von MELANI vorgesehen ist und die einschlägigen Beziehungen somit schon etabliert sind. Zudem werden Logfiles und andere Mittel der Spurensicherung ebenfalls an der Melde- und Analysestelle anfallen. Selbstverständlich gilt auch hier, dass dem verantwortungsvollen Umgang mit den Daten aus der Wirtschaft grösste Bedeutung zukommt. Insbesondere dürfen keine Daten über Opfer ohne Einverständnis publik gemacht werden. Dass dies funktionieren kann, beweist das US-amerikanische NIPC (National Infrastructure Protection Center), welches am FBI angesiedelt ist. Dazu ihr Direktor Ronald Dick: „As to our growing sensitivity to the needs of the private sector – unless someone in the private sector says d-

Die mit DCC bezeichneten Kästchen stehen für die Delegierten der Coordination Centers. Sie stellen die passive Koordination der Massnahmen der Wirtschaft und der Bundesverwaltung sicher. Die entsprechenden Coordination Centers (CCs) sind jeweils für jeden der kritischen Sektoren unter Mitarbeit von InfoSurance und der Wirtschaftlichen Landesversorgung separat aufzubauen. In ihnen sollen die „Key Players“ der Sektoren – also z.B. Swisscom, Sunrise und Orange im Bereich Telekommunikation – aber auch andere interessierte Unternehmungen Einsitz nehmen. Pro CC sind dem Chef Sonderstab zwei Delegierte zu melden, welche in SONIA als Verbindungspersonen („Verbindungsoffiziere“) zwischen CC und Sonderstab mittun. Sie sollen sowohl vertiefte Kenntnisse ihres Sektors als auch der jeweiligen IT-Infrastruktur aufweisen, wie die Firmenvertreter in den CCs selbst. Auf die gleiche Art wie die CCs mit ihren DCCs im Sonderstab in Kontakt stehen, sollen diese auch mit ihren IT-Spezialisten und dem Management ihrer Unternehmungen Informationen über die Geschehnisse austauschen. Dadurch wird sichergestellt, dass sich auch die eigentlichen Entscheidungsträger in der Wirtschaft („Wirtschaftskapitäne“) rasch und effizient ein Bild von der Situation machen können. Die CCs bilden somit die Informationsdrehscheiben zwischen Sonderstab und den einzelnen Firmen, welche auf Grund der Lagebeurteilung Massnahmen beschliessen und umsetzen. Sie können sich so konstituieren, wie es für den jeweiligen Sektor angemessen scheint; dabei ist es sinnvoll bereits vorhandene Strukturen (z.B. firmeneigene IT-Sicherheitsabteilungen, Dachverbände usw.) miteinzubeziehen und untereinander zu vernetzen. Somit können die CCs mit relativ einfachen Mitteln aufgebaut werden und je nach Bedürfnis wachsen oder allenfalls weitere Aufgaben im Umfeld der Information Assurance wahrnehmen. Ein möglicher Startpunkt wäre eine Datenbank, durch welche die Mitglieder auf sichere (vertrauliche und authentifizierte) Art Informationen und Erfahrungen miteinander austauschen können. Dies gerade im Bereich der Planung vorsorglicher Massnahmen für Notfälle („Contingency Planning“) wünschenswert. Denn im Fall einer Krise ist es wichtig, dass ein gewisser Konsens, zum Beispiel über die Art und Weise wie gewisse Lagen zu beschreiben und zu verstehen sind, vorhanden ist; nur so wird kohärentes und rasches Handeln überhaupt erst möglich. Deshalb sollte diese „unité de pensée“ bis hinauf zum Sonderstab durchgängig vorhanden sein. Die Coordination Centers werden den im Konzept für einen Sonderstab Informationssicherheit vorgeschlagenen „erweiterten Sonderstab“ oder „Expertenpool“ vollumfänglich ersetzen (siehe Ref. [1]).²⁰

Im nachfolgenden Abschnitt beschreiben die Experten des Milizamts ICT-I des Bundesamts für Wirtschaftliche Landesversorgung ihren Beitrag zum Aufbau der Coordination Centers.

rectly to us that it's OK to talk about an attack, we won't talk about the company. We'll generalize the attack description so the reporting company is unrecognizable. It does no one any good for the FBI to be out there reminding people that certain entities were victims of a DDoS attack. We can make the same points on television or in a presentation to the public describing the vulnerability and what we did together with the private sector to solve it...Historically, when the FBI has talked about incidents or issued press releases, we normally talked about the victims. We don't do that anymore.“

²⁰ Die Bundesvertreter im „erweiterten Sonderstab“ sollen – wenn nötig – direkt in den Sonderstab integriert werden. Im Vordergrund stehen hier die ISBDs oder ISBOs (vor allem des EFD und des Querschnittleistungserbringers BIT). Noch offen ist der Einbezug der Kantone und Gemeinden, die bis anhin ebenfalls dem „erweiterten Sonderstab“ zugeordnet waren. Ein Modell wie dasjenige der CCs könnte Vorbildcharakter haben.

3 ROLLE DES MILIZAMTS ICT-I BEIM AUFBAU DER CCs²¹

Die Wirtschaftliche Landesversorgung hat den verfassungs- und gesetzmässigen Auftrag, die Versorgung des Landes mit lebenswichtigen Gütern und Dienstleistungen für den Fall schwerer Mangellagen, denen die Wirtschaft nicht selbst zu begegnen vermag, sicherzustellen (Art. 102 BV). Zu den lebenswichtigen Gütern und Dienstleistungen zählen nach Art. 2 Landesversorgungsgesetz auch Dienstleistungen wie diejenigen des Transport- und Fernmeldewesens.

Aufgrund ihres Auftrags kommt der Landesversorgung im Hinblick auf die ICT-Infrastrukturen eine doppelte Verantwortung zu. Einerseits muss sichergestellt werden, dass bei Störungen, ausgelöst durch Krisen in der ICT-Infrastruktur, Produktion und Verteilung der lebenswichtigen Güter - Nahrungsmittel, Energie, medizinische Güter usw. - aufrecht erhalten werden kann, andererseits gilt es, in Zusammenarbeit mit den entsprechenden Fachstellen, mit geeigneten Massnahmen die für die Versorgung des Landes nötigen Informations- und Kommunikationsinfrastrukturen im Hinblick auf langfristige Störungen aufrecht zu erhalten.

Die Wirtschaftliche Landesversorgung ist eine Milizorganisation. Sie besteht aus einem vollamtlichen Stab (35 Etatstellen) und fünf Bereichen (Ernährung, Industrie, Transporte, ICT-Infrastrukturen und Arbeit), welche je über ein eigenständiges Milizkader (total ca. 350 Personen) verfügen. Aufgrund der Organisationsverordnung sind die Bereiche in der Lage, Personen aus Wirtschaft, Wissenschaft und Verwaltung zu rekrutieren, welche mehrere Tage im Jahr zu ihren Gunsten im Einsatz stehen (Ausbildung, Übung, Lageanalyse, Massnahmenplanung usw.). Damit bestehen in vielen, im Hinblick auf die ICT-Infrastrukturen sensiblen Bereichen Fachgruppen (Abteilungen und Sektionen), die im Hinblick auf die neuen Aufgaben im ICT-Bereich als Bindeglieder zwischen Wirtschaft und Staat zuhanden des Sonderstabs als CCs eingesetzt werden können.

In der bestehenden Organisation verfügt die Landesversorgung im Bereich Industrie u.a. über eine Abteilung Energie, eine Sektion Chemie & Pharmazeutika und eine Sektion Trinkwasserversorgung, über einen eigenständigen Bereich Transporte (See- und Lufttransporte, Strassen- und Schienentransporte, Rheinschifffahrt) sowie über einen Bereich Ernährung, welche gegenüber dem Sonderstab als CCs eingesetzt, und deren Chefs als Vertreter in den Sonderstab delegiert werden können. So verfügt z.B. der Chef der Abteilung Energie mit den Sektionen Mineralöle, Elektrizität, Gas und Holz über einen Pool an Wirtschaftsvertretern, die einerseits in der Lage sind, die Situation in den verschiedenen Branchen jederzeit kompetent zu beurteilen, andererseits dafür Gewähr bieten, dass Massnahmen des Bundes im Notfall von der Wirtschaft mitgetragen und in der Branche umgesetzt werden können.

Im Rahmen des neuen Bereichs ICT-Infrastrukturen werden einerseits die Teilbereiche Datenproduktion, Übermittlung und Speicherung aufgebaut, andererseits in sensiblen Gebieten, welche in der bestehenden Organisation der Landesversorgung nicht vertreten

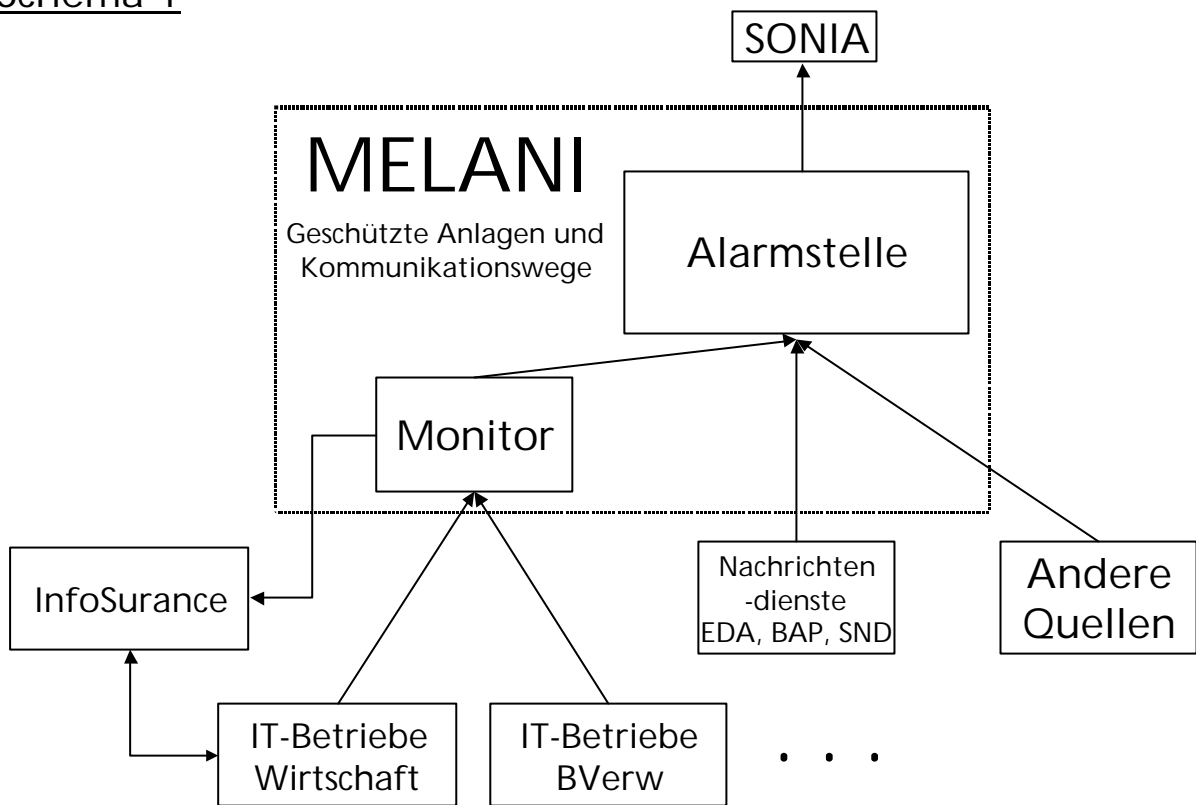
²¹ Beitrag von Dr. U. Haudenschild, Bundesamt für wirtschaftliche Landesversorgung, Belpstrasse 53, 3003 Bern.

sind, neue Fachbereiche (Finanz- und Versicherungswesen, Medien, öffentliche Dienste) geschaffen. Diese können wiederum als CCs eingesetzt und deren Chefs in den Sonderstab delegiert werden, wobei beabsichtigt ist, dass die entsprechenden Stellen in Zukunft in Absprache mit dem ISB und unter Berücksichtigung der Interessen beider Organe besetzt werden sollen.

4 LITERATUR

- [1] *Konzept für einen Sonderstab Informationssicherheit Version 1.0 (vertraulich)* Informatikstrategieorgan Bund ISB und Ernst Basler + Partner, Bern und Zollikon **März 2001**
- [2] *Sonderstab Informationssicherheit – Auswertung der Übung INFORMO 2001*, Ernst Basler + Partner, Zollikon **Juni 2001**
- [3] Wildhaber, E. *Bericht der Gruppe Evaluation Strategische Führungsausbildung SFA*, Bern **Juni 2001**
- [4] *Konzept „Information Assurance“* Koordinationsgruppe Informationsgesellschaft KIG, Bern **Mai 2000**
- [5] *Y2K: Starting the Century Right* Report of the International Y2K Cooperation Center, Washington **February 2000**
- [6] *National Plan for Information Systems Protection Version 1* The White House, Washington **2000**
- [7] *Lagezentrum Schweiz – Schlussbericht der Operation MILLENNIUM TRANSIT* s.15ff, Generalstab, Bern **Mai 2000**
- [8] Vernez, G. *Persönliche Kommunikation* Generalstab UG Op, Bern **August 2001**
- [9] Hutter, R. *Angriffe auf Informationstechnik und Infrastrukturen – Realität oder Science Fiction* Aus Politik und Zeitgeschichte, B41 – 42, s. 31 **2001**
- [10] *Beitrag: Die Mikrowellenkanone* Menschen, Technik, Wissenschaft MTW, Schweizer Fernsehen DRS **Juni 2001**
- [11] Carrel, Laurent F. *Kernprobleme und Kernfragen aus INFORMO 2001 (interne Fassung für die Projektleitung)* Bern **August 2001**
- [12] *Prüfung der Verordnung Sonderstab Informationssicherheit* Rechtsdienst des Eidgenössischen Finanzdepartements GS-EFD **Juli 2001**
- [13] Oppliger, R. *Informatiksicherheit = Verstehen und Beherrschen von Risiken* digma, Heft 3, **2001**

Schema 1



ISB/SEC



Schema 2

