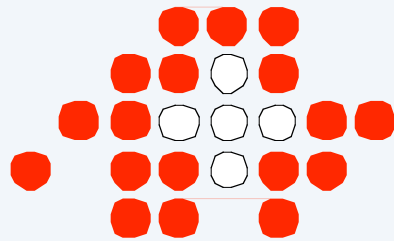


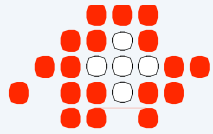


# C(I)IP – Critical (Information) Infrastructure Protection

Dr. Ruedi Rytz  
Informatikstrategieorgan Bund ISB  
Friedheimweg 14  
CH-3003 Bern  
Telefon +41-(0)31-323-4507  
Fax +41-(0)31-322-4566  
[ruedi.rytz@isb.admin.ch](mailto:ruedi.rytz@isb.admin.ch)



Informatikstrategieorgan Bund ISB  
Unité de stratégie informatique de la Confédération USIC  
Organo strategia informatica della Confederazione C  
Organ da strategia informatica da la confederaziun

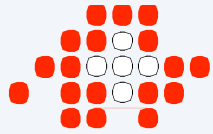


# Kritische Infrastrukturen

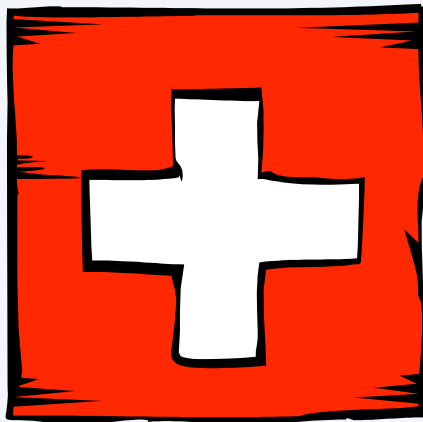
Systeme, die für das **Funktionieren der Gesellschaft kritisch** sind:

- Energieversorgung
- Telekommunikation
- Finanz- und Versicherungswesen
- Transport und Logistik
- Notfall- und Rettungswesen
- Gesundheitswesen (inkl. Wasserversorgung)
- Regierung und öffentliche Verwaltungen





# Partnerschaft: Verwaltung und Wirtschaft



Staatsaufgabe: Art. 2 "Zweck"  
der Bundesverfassung



Mitarbeit der Wirtschaft  
(PPP: Public Private  
Partnership)



## CIP: Mittel gestern . . .

### **Strategisch**

- Prävention (Ausbildung, Sensibilisierung)
- Sicherheitspolitik (Internationale Netzwerke)
- Nachrichtendienste

### **Operativ**

- Polizei
- Zivilschutz
- Armee
- Wirtschaftliche Landesversorgung (WL)



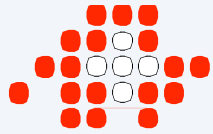
## . . . und heute

- Haben sich über **Jahrzehnte bewährt** und **bleiben** weitgehend **dieselben**
- Müssen **dort verstärkt** werden, wo die kritischen Infrastrukturen durch **neue Abhängigkeiten bedroht sind**
- **Neue Abhängigkeiten** werden durch den breiten Einsatz von **Informations- und Kommunikationsinfrastrukturen** geschaffen



## Fallbeispiele

1. **Wasserversorgung** Queensland, Australien (April 2000)
2. **Schweizerische Bundesbahnen SBB**,  
Betriebszentrum Basel (Juni 2001)
3. **Kernkraftwerk** in Ohio, USA (Januar 2003)
4. **Blackout** USA/Kanada (August 2003)



## CIIP in der Schweiz: 4 Säulen

pre-  
vent

- **Prävention** durch Informationsaustausch, Kontaktnetz, Unterstützung beim Aufbau von Strukturen (**InfoSurance**)

de-  
tect

- **Früherkennung**, Lagezentrum, Benachrichtigung von Sonderstab und betroffenen Kreisen (professionelle Melde- und Analysestelle **MELANI**)

re-  
act

- **Verminderung der Auswirkungen** von Krisen (Sonderstab zur Führungsunterstützung **SONIA**)
- **Bekämpfung der Ursachen** von Krisen (**MELANI** und betroffene **Fachstellen**)



## MELANI – MELde- und ANalysestelle Informationssicherung

- **Lagezentrum** (für Behörden, SONIA, usw.)
- **Früherkennung** von Gefahren und Bedrohungen
- **Koordination der Massnahmen** bei Vorfällen
- **Alarmierung** und Aufbietung **des SONIA**, falls nötig
- **Kompetenzzentrum** (für CIIP)
- Entwicklung von **Strategien**



# Organisation: Funktionale Anforderungen

- **CERT-Funktion:** Meldestelle und Supportzentrum für technische Störungen
- **Nachrichtendienstliche Funktion:** Sammel- und Analysestelle für betriebliche Vorfälle und kriminelle Aktivitäten
- **Fachfunktion:** Auswertung von Ereignissen zwecks
  - Strategie
  - Vorgaben (für die Bundesverwaltung)
  - Empfehlungen
  - Ausbildung



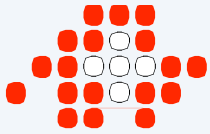
## Organisation: Kooperationsmodell

- **Modell mit Partnern**, die schon heute analoge Aufgaben erledigen.
- Dadurch ergeben sich:
  - **Einsparungen** im Vergleich zum Alleingang
  - Positive Auswirkungen auf weitere Projekte bei den Partnern (z.B. durch **Wissenstransfer**)
  - Möglichkeiten zum **raschen** und **effizienten Aufbau**

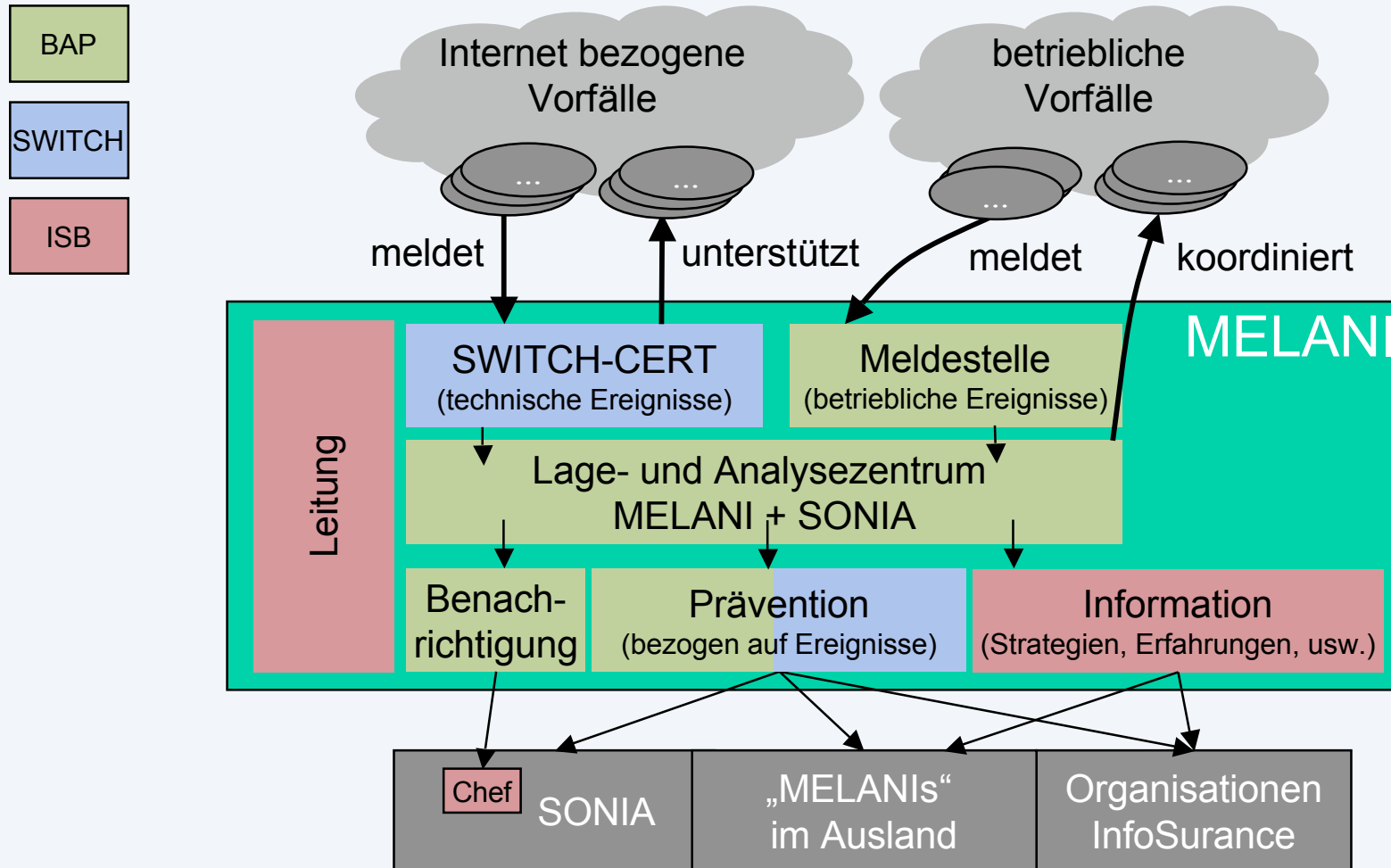


## Organisation: Partner

- **CERT-Funktion:** SWITCH
- **Nachrichtendienstliche Funktion:** Dienst Analyse & Prävention (Koordinationsstelle zur Bekämpfung der Internetkriminalität)
- **Fachfunktion:** Informatikstrategieorgan Bund (ISB) & Partner
- **Führung:** Informatikstrategieorgan Bund (ISB)



# Betriebsmodell





# Informationsquellen

## 1. Netzwerk:

- **Vergleichbare Stellen im Ausland**
- Computer Emergency Response Teams **CERTs**
- **Nachrichtendienste**
- **InfoSurance** und **WL \_ Risikoanalysen**

## 2. Kundenkreise:

- Ausgewählte **Betreiber kritischer Infrastrukturen**
- **KMU** und **Bürger**



# Kundenkreise <sup>1/2</sup>

Kundenkreis	Geschlossen		Offen
	SWITCH-CERT	MELANI	MELANI
Mitglieder	ausgewählte Betreiber kritischer Infrastrukturen		KMU Bürger
Anzahl (#1 _ #2)	30 _ 60		unbeschränkt
Vertrauen	starkes Vertrauensverhältnis		unpersönlich
Aufbau des Vertrauens	InfoSurance ( <i>Round Tables</i> )  Wirtschaftliche Landesversorgung (Mitglieder der Coordination Centers _ SONIA)		Medien, WWW  KMU: Förderung durch Organisationen (Verbände, InfoSurance)



## Kundenkreise <sup>2/2</sup>

Kundenkreis	Geschlossen		Offen
	SWITCH-CERT	MELANI	MELANI
Kontakt	<p><b>cert@melani.</b> admin.ch</p> <p>www.melani. admin.ch</p> <p>0844 800 511</p>	<p><b>incident@melani.</b> admin.ch</p> <p>www.melani. admin.ch</p> <p>0844 800 512</p>	<p>www.melani. admin.ch</p>

**Anmerkung:** Diese Angaben dienen der Illustration und sind nicht endgültig



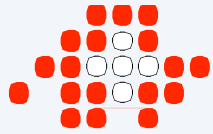
## Dienstleistungen für den *geschlossenen* Kundenkreis

- **Tagesgeschäft**
  - **Selektive Weiterleitung** von Warnungen, Mahnungen und Verletzlichkeiten
  - **Stärkung des Vertrauens**
- **Im Ereignisfall**
  - **Help Desk** und **Koordination der Massnahmen**
  - **Situationsanalyse** und **Erfahrungsaustausch**
  - **Beratung** bei der **Strafverfolgung**



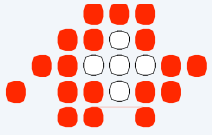
# Dienstleistungen für den *offenen* Kundenkreis

- **Tagesgeschäft**
  - Bekanntgabe von Warnungen, Mahnungen und Verwundbarkeiten in „**angemessener Form**“
  - Publikation von Material zur **Vorbeugung von Vorfällen**
- **Im Ereignisfall**
  - **Hinweise** zur Problemlösung (über WWW)
  - Beratung bei der **Strafverfolgung**



# MELANI wird nicht alle Probleme lösen können...





...aber wir sind auf dem richtigen Weg.

