UNIVERSITÄT MANNHEIM

What is an Early Warning System?

Felix C. Freiling
University of Mannheim
Germany

First European Workshop on Internet Early Warning and Network Intelligence (EWNI)
Hamburg, January 27, 2010

Disclaimer

- This is the definitive answer!

- German perspective
- Academic view

To the roots ...

Bundesministerium
des Innern

Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI)

www.bmi.bund.de

Goal 8 of NPSI

- Build a national status and analysis centre
  - "nationales Lage- und Analysezentrum"
- Set up a network of sensors for IT security incidents
  - "Sensornetz für IT-Sicherheitsvorfälle"

Goal 9 of NPSI

- Inform about current threats and risks
  - "Informationen über aktuelle Bedrohungen und Risiken bereitstellen"
- Implement an alarm and warning system
  - „Alarmierungs- und Warnsystem einrichten"

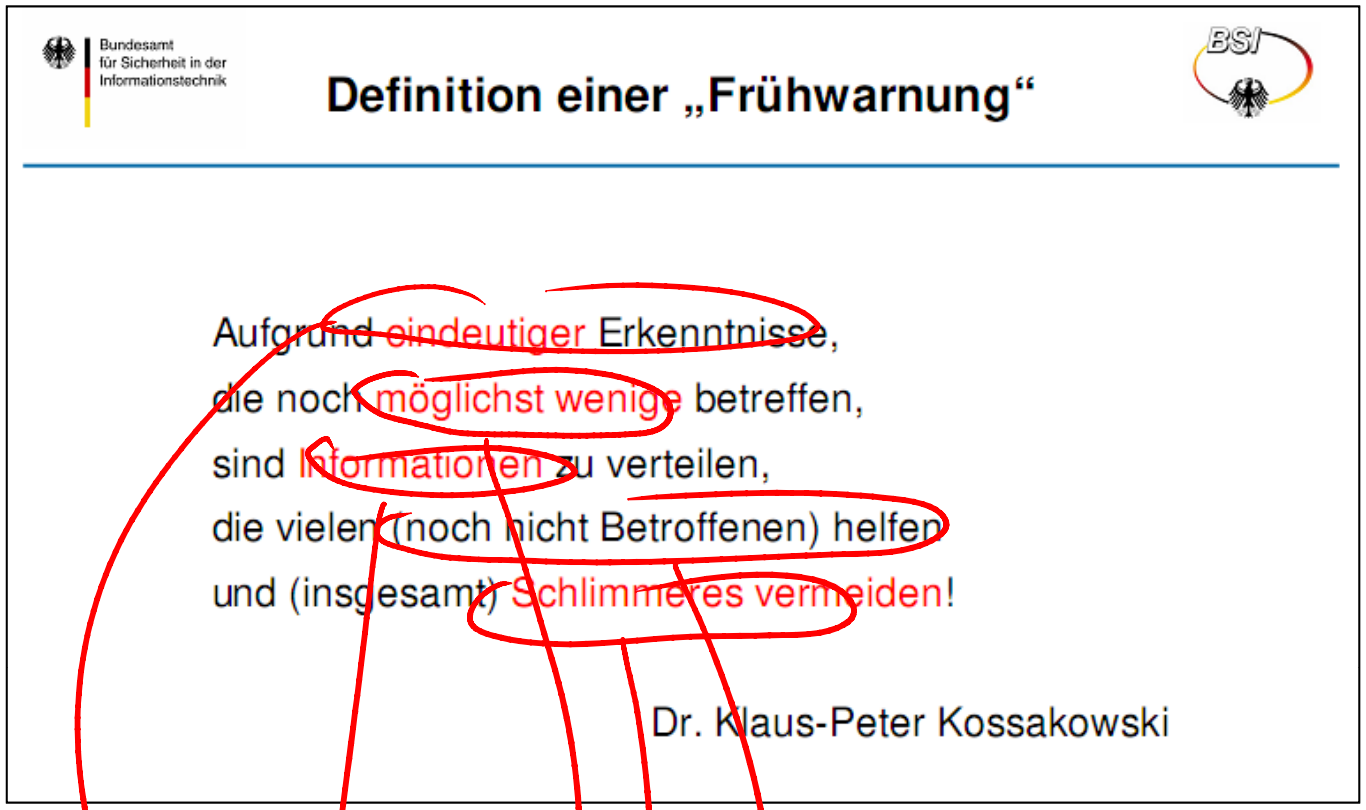
Does NPSI define EWS?

Definition?

Mit dem nationalen IT-Krisenmanagement des Bundes wird auch ein Alarmierungs- und Warnsystem eingerichtet, mit dem bei akuten Angriffen auf oder schwerwiegenden Störungen in Informationsinfrastrukturen alle potenziell Betroffenen schnell und umfassend informiert werden können. So werden rechtzeitige Gegenmaßnahmen ermöglicht und Schäden in größerem Ausmaß vermieden.

Source: NPSI, p. 15

1. in case of imminent attacks or failures
2. in information infrastructures
3. fully inform
4. all potential victims
5. to prevent even larger damage



1. conclusive evidence
2. affecting a small set of people
3. distribute information
4. to a yet non-affected larger set of people
5. to prevent even larger damage

Source: Ennen, BSI, 2006

Formalization

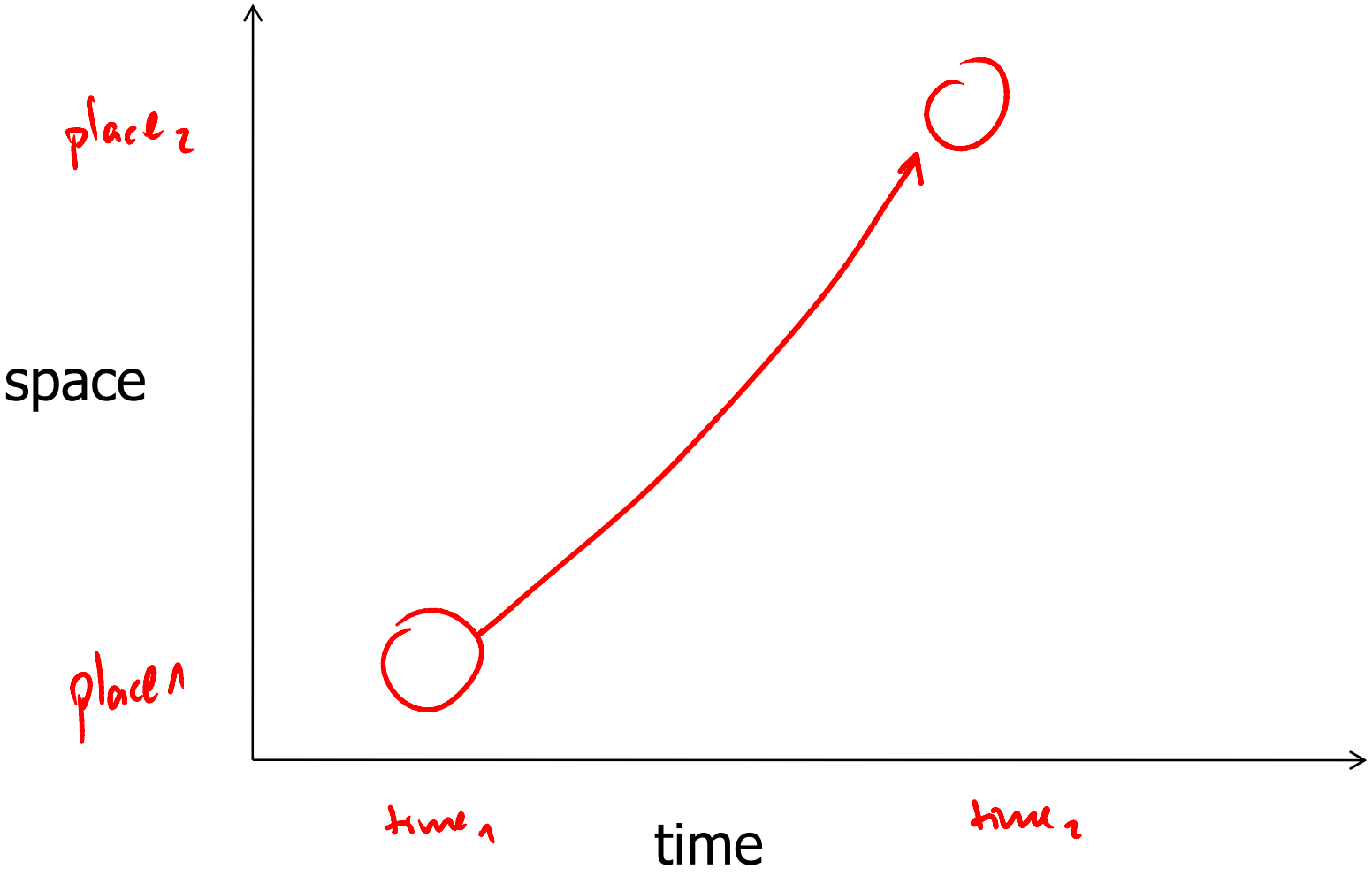
Information, Space and Time

- (At least) two different places in cyber**space**
  - $place_1$ and $place_2$
  - Or distinct sets of people
- (At least) two instances in **time**
  - $time_1$ and $time_2$
  - "early"

$time_1 < time_2$

- Transfer **useful information** for prevention of damage
  - "warn"

Syntax: Space and Time



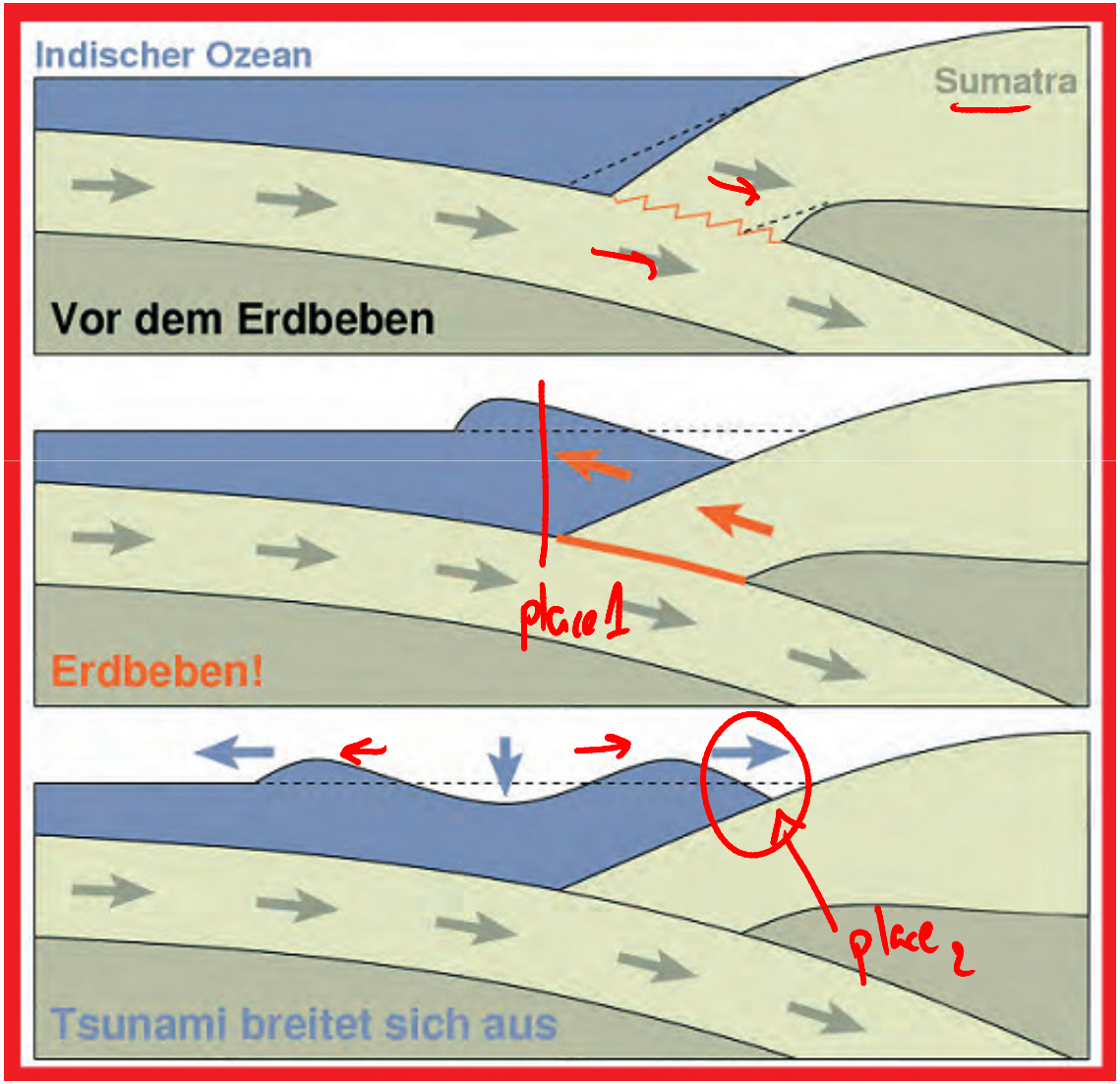
Semantics: Useful Information

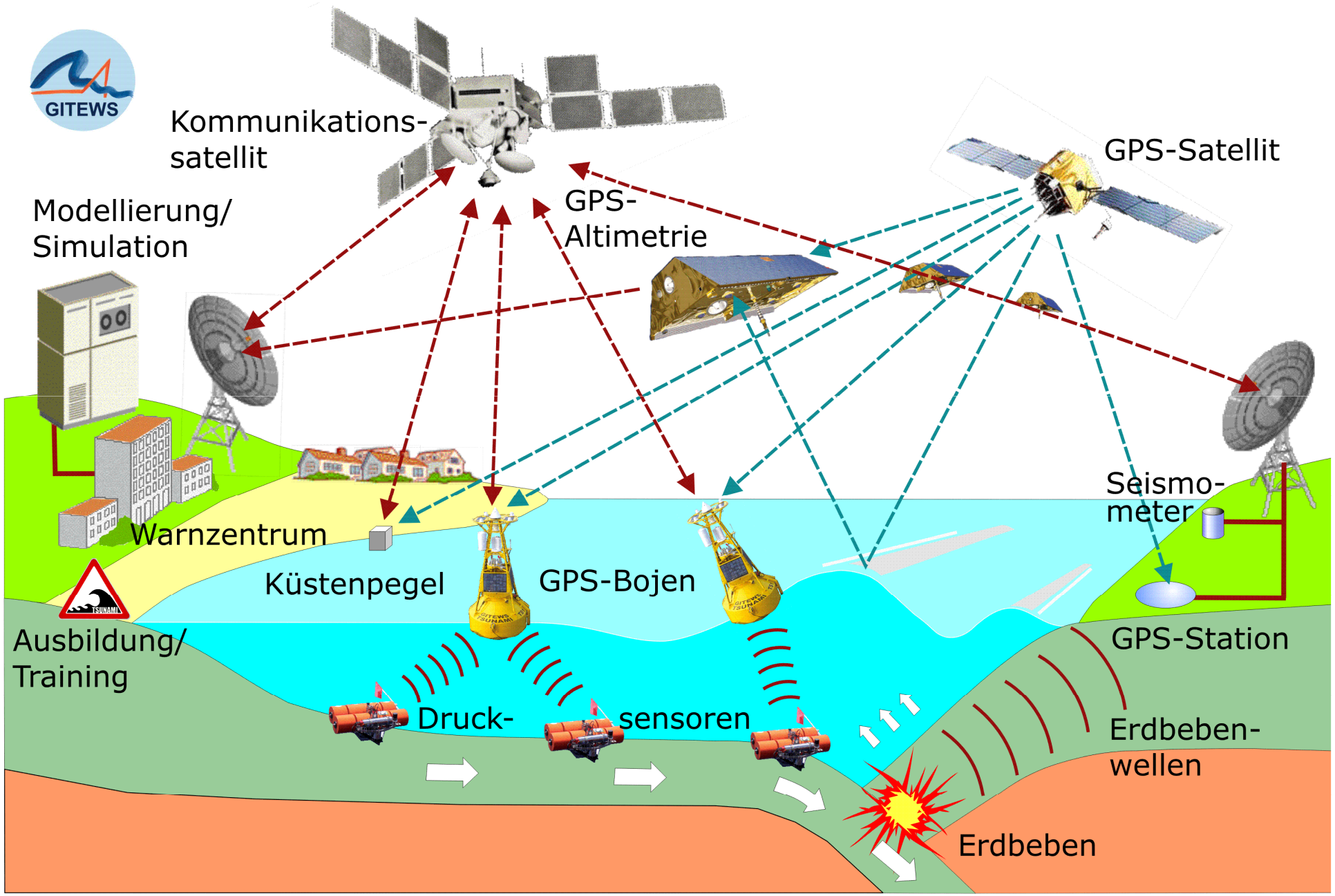
- Information that is useful to prevent further damage at $place_2$
- Information must be available *early enough*:
  - $time_2$ must be before effect of activity at $place_1$ reaches $place_2$
  - hard to formalize, depends on circumstances

Other “early warning systems”


GITEWS: Homepage - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://www.gitews.de/
early warning system
GITEWS: Homepage
GITEWS
Deutsch-Indonesisches Tsunami Frühwarnsystem
Homepage | Presse & Medien | Kalender | Kontakt | Partner | International | Internes | Sitemap | Suche | Impressum
26.01.2010 :: English :: Druckversion
Site:
Konzept
Seismologie
Ozeaninstrumentierung
GPS-Technologien
Warnzentrum
Modellierung
Ausbildung/Training
Informationsmaterial zum Herunterladen
Fertig

GI-TEWS


Indischer Ozean
Sumatra
Vor dem Erdbeben
Erdbeben!
Tsunami breitet sich aus

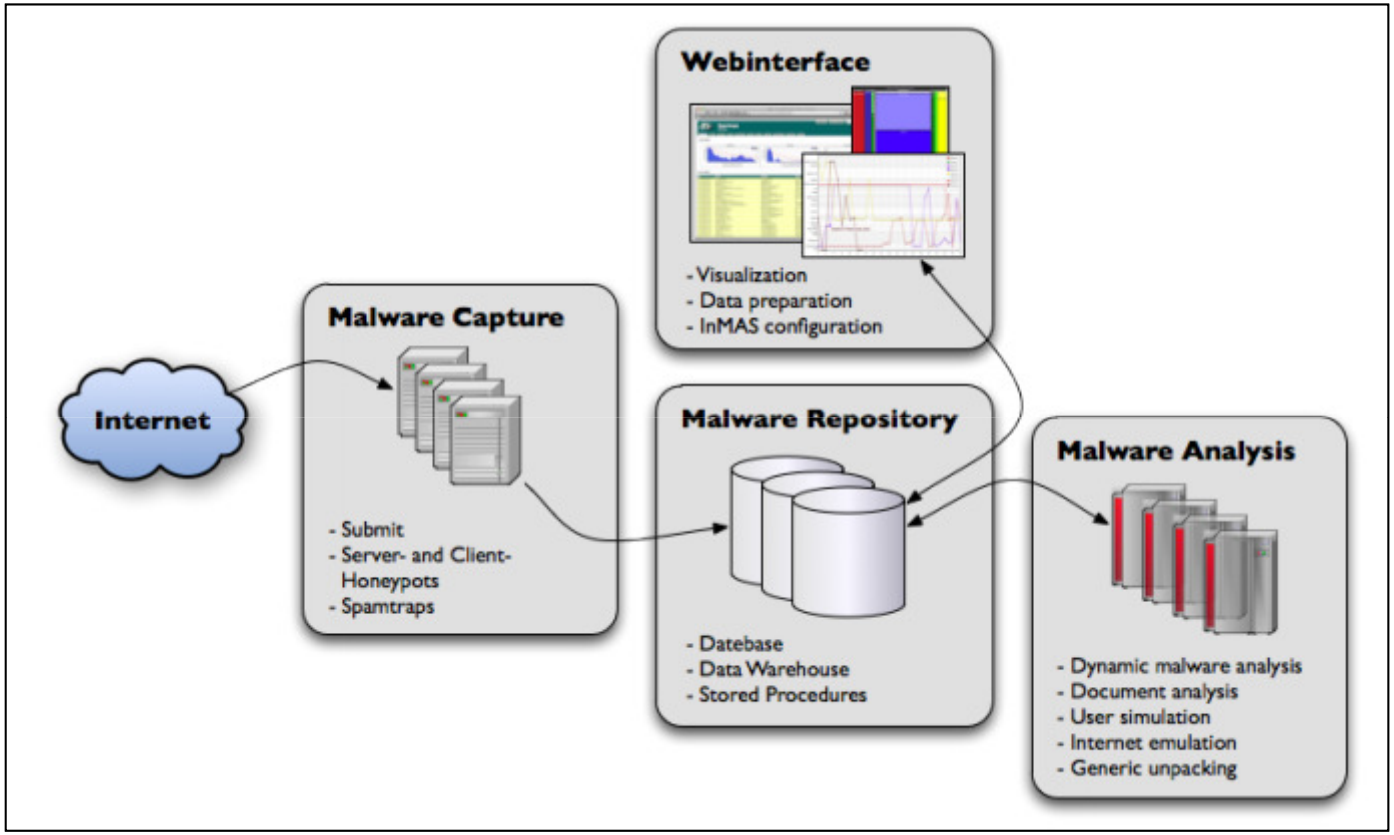

GITEWS
Kommunikations-
satellit
GPS-Satellit
Modellierung/
Simulation
GPS-
Altimetrie
Seismo-
meter
Warnzentrum
Küstenpegel
GPS-Bojen
Ausbildung/
Training
GPS-Station
Druck-
sensoren
Erdbeben-
wellen
Erdbeben

Resulting Projects from NPSI

InMAS

- Funded by BSI
- Built by University of Mannheim, Germany

- Focus on Malware
  - Honeypots, client-side honeypots

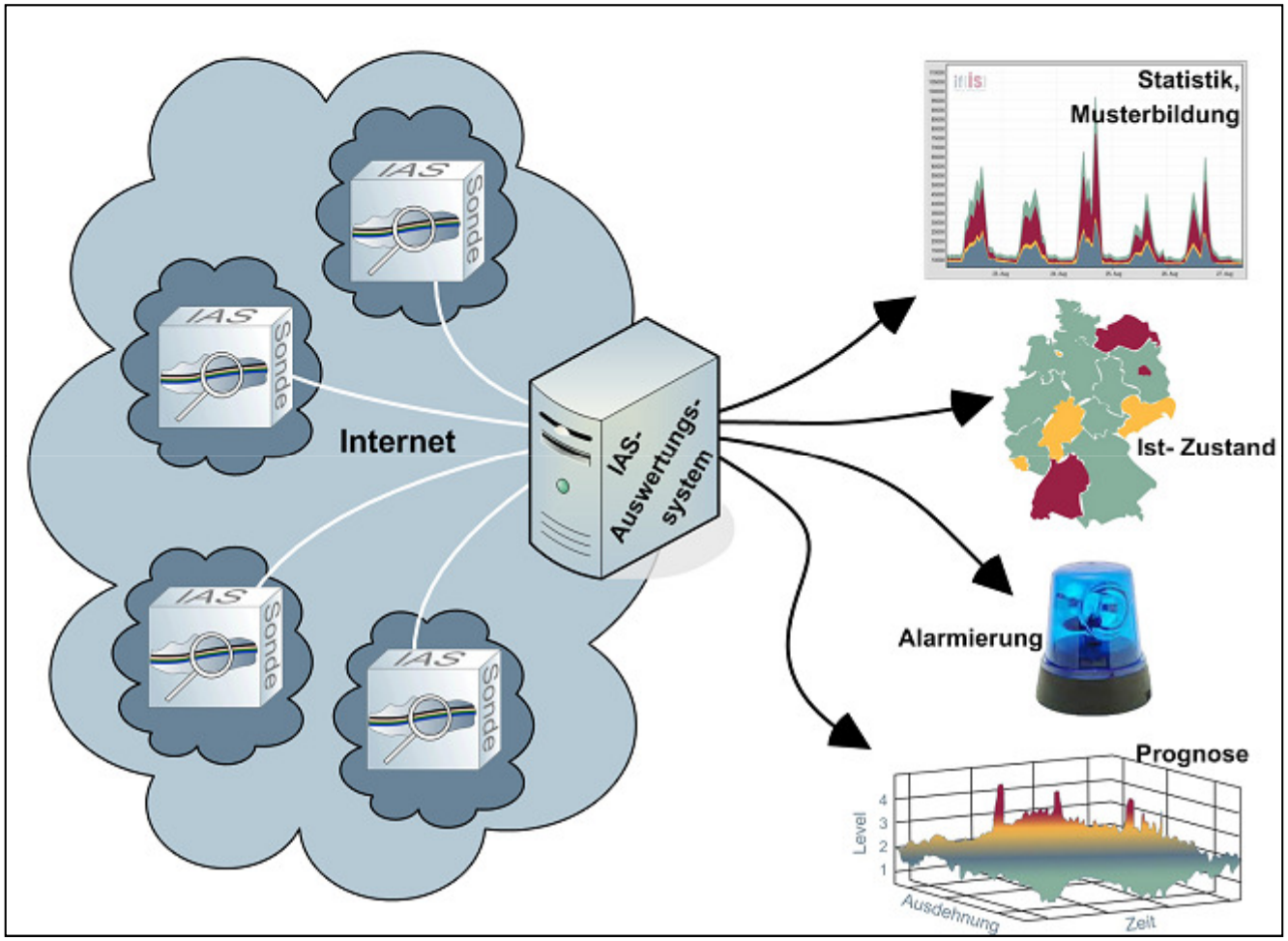


Source: InMAS paper by Engelberth et al., EWNI 2010

IAS

- Funded by BSI
- Built by "Institut für Internet-Sicherheit" of Gelsenkirchen University of Applied Sciences, Germany

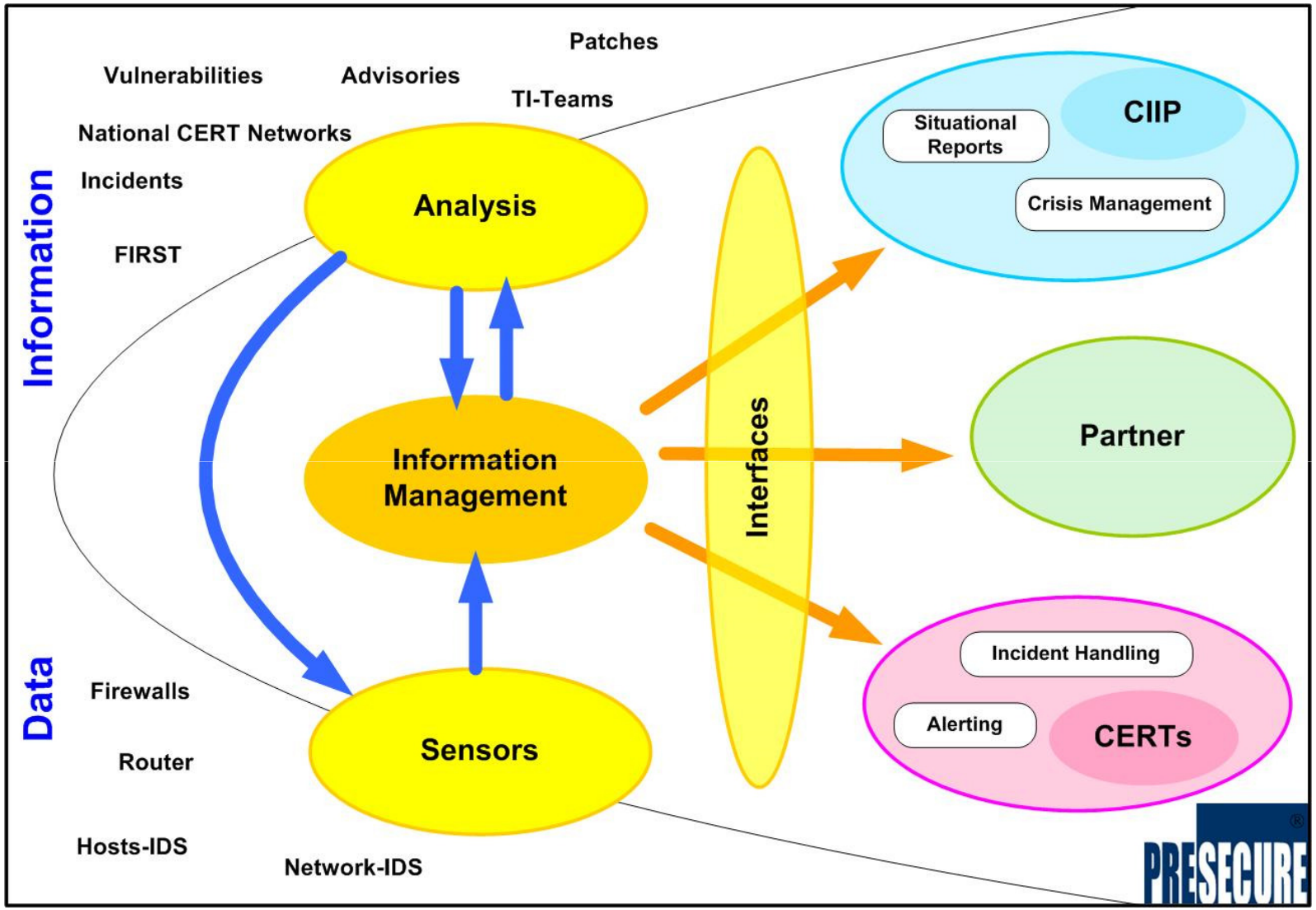
- Gathers statistics on network traffic
  - Packets, flags, etc.



Source: http://www.internet-sicherheit.de

CarmentiS

- Funded/built by BSI and several German CERTs
- Platform for cooperative information management of CERTs
- Now being integrated with IAS and InMAS



Source: http://carmentis.org

Checking the definition

	CarmentiS	IAS	InMAS
$place_1$ and $place_2$	✓	✓	?
$time_1$ and $time_2$	✓	✓	?
useful information	?	?	✓

Open problems

Attack Spreading Prediction

- How and when do attacks at $place_1$ affect $place_2$?
- Work on spreading of autonomous malware exists
  - Spread models based on epidemical models, e.g. Zou, Gao, Gong, Towsley in ACM CCS 2003.
- No work exists on spreading of other types of malware
  - Modeling is hard, especially if adversary adapts

Generalization of Measurements

- Estimate probability that statements measured in $place_1$ are true in $place_2$
  - How many sensors do we need to infer anything of interest?
- Apply techniques from empirical social sciences
  - Distribute sensors in a random fashion
  - First work at University of Mannheim (as part of InMAS research)

Information Overload

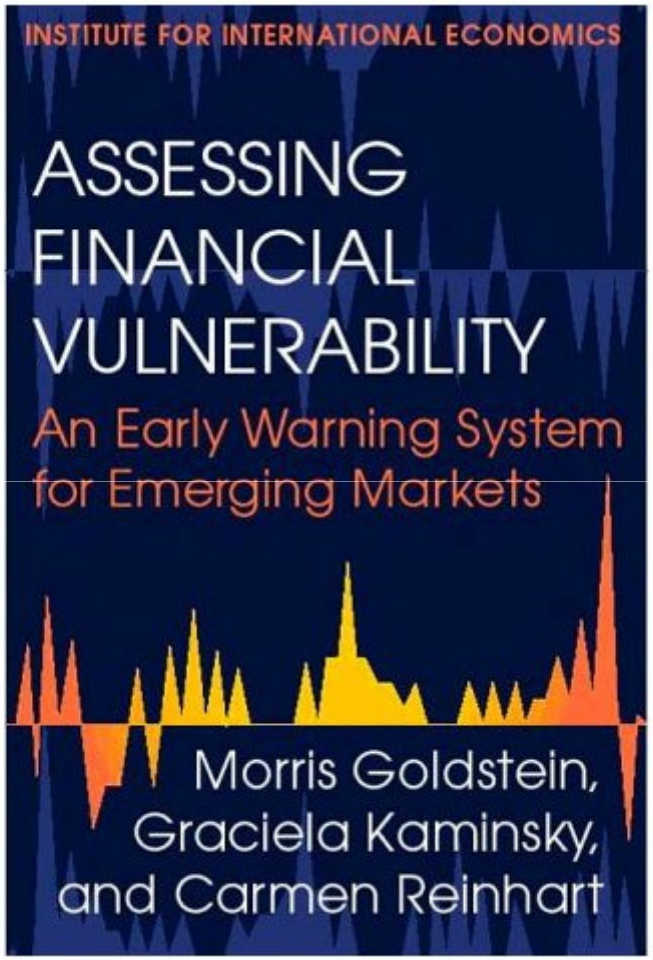
- Focus on data that is useful
- Additional definitory aspect: EWS does **only** disseminate useful information


password

Contact

Prof. Dr. Felix Freiling
Universität Mannheim
Lehrstuhl für Praktische Informatik 1
68131 Mannheim
Germany

https://pi1.informatik.uni-mannheim.de


INSTITUTE FOR INTERNATIONAL ECONOMICS
ASSESSING FINANCIAL VULNERABILITY
An Early Warning System for Emerging Markets
Morris Goldstein, Graciela Kaminsky, and Carmen Reinhart

More Definitions

- Grobauer, Mehlau, Sander: Carmentis: A co-operative approach towards situation awareness and early warning for the Internet. Proc. IMF 2006, pp. 55-66.
- Biskup, Hämmerli, Meier, Schmerl, Tölle, Vogel: Working Group – Early Warning System. In: Dagstuhl Perspectives Workshop: Network Attack Detection and Defense. Dagstuhl Seminar Proceedings, Vol. 08102, 2008.