CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

acris

WG 2 – Chapter 3: Voluntary Information Sharing

Prof. Dr Bernhard M. Hämmerli bmheammerli@acris.ch
Bernhard.Haemmerli@SATW.ch

Why we are benefitting from Voluntary Information Sharing?

Chapter 3: Voluntary Information Sharing

NIS-P Group Member: Expertise, Group Work, Comments: This means all of you

With thanks to Nils Gaute Prestmo for the Griffin Cyber Land description and Karin Mulvihill for her restructuring and translation to native English

Editorial Board:

John M. SALOMON, Financial Services ISAC, FS-ISAC, (Continental Europe)

Aristotelis TZAFALIAS, Research Project Officer, DG Connect, European Commission

Lionel DUPRE, NIS Expert, ENISA

Karin Mulvihill, IRM Expert, BNY Mellon

WG 2 Chair: Dr. Waldemar GRUDZIEN, Director, Association of German Banks)

WG 2 Rapporteur: Prof. Dr. Bernhard M. Hämmerli Acris GmbH

“Just a Twitter distribution of a new attack reduces losses of a given attack by 40% in a rural area of Kenya”

There are no other means to communicate…

Serah Francis Kenya

Master in Information Security, Mgt. at Gjøvik University, Norway
Currently, doing research on ICT and IT-Security Strategy and implementation in Kenya.
serah.francis@hig.no

APT Prevention

- Awareness
- Advanced Solutions on technical level like cyber fusion centre with big data analytics
- **Information Sharing**

Structure of Chapter 3

1. Management Summary
2. 10 Recommendation / 3 Issues for Policy Makers

3. Chapter Body

References / Other Relevant Documents / Sharing Schemas

State-of-Play:

Final: Last opportunity to bring in your wishes … but before June 3.

Body of Chapter 3 “Voluntary Information Sharing”

1. Introduction
2. Information Sharing Characterisation
3. Key Considerations
4. Content Types
5. Risks
6. Strategies
7. SMEs

Appendix

8. The EU baseline scenario - Griffin Cyber Land
9. Additional factors surrounding information sharing
10. References

One for all, all for one: we are all connected!

Picture http://thefutureshapers.com/the-next-wave-of-innovation-means-being-interconnected/

Models of Sharing: Example Germany

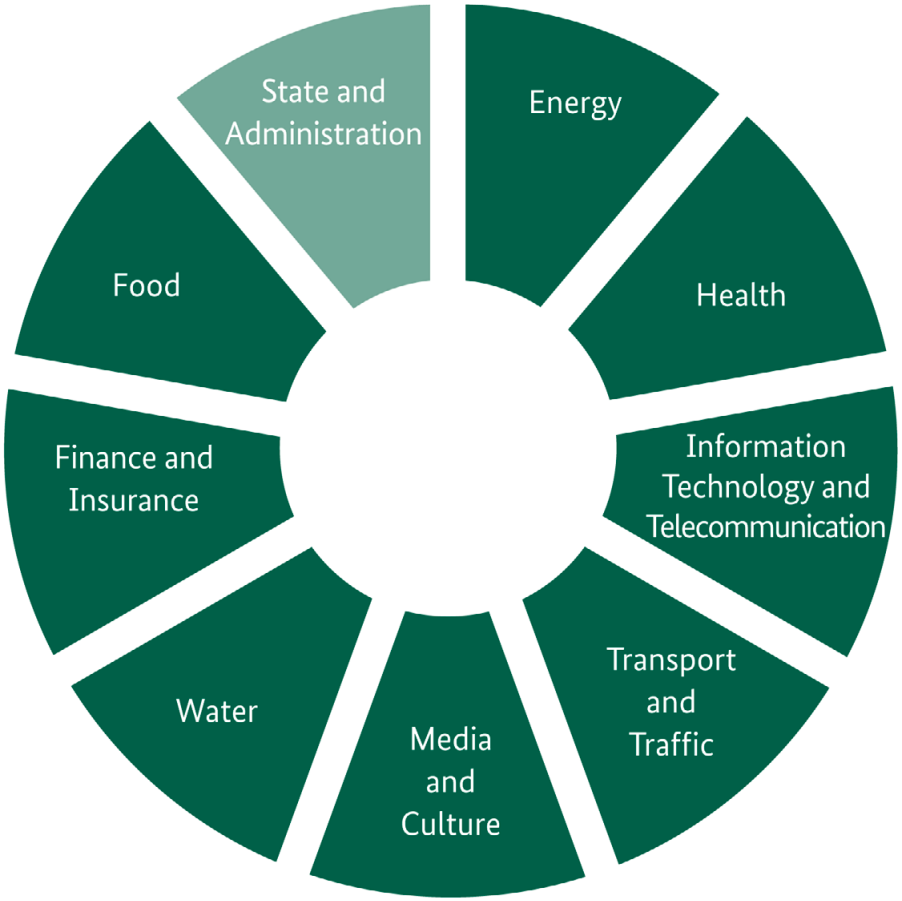


Fig. 1: The sectors of critical infrastructure in Germany

Sectorial approach: More mutual trust
Inter-sector (one Member States)
Between Member States
International sector-wise
International cross sectors

Inter-Sector Sharing

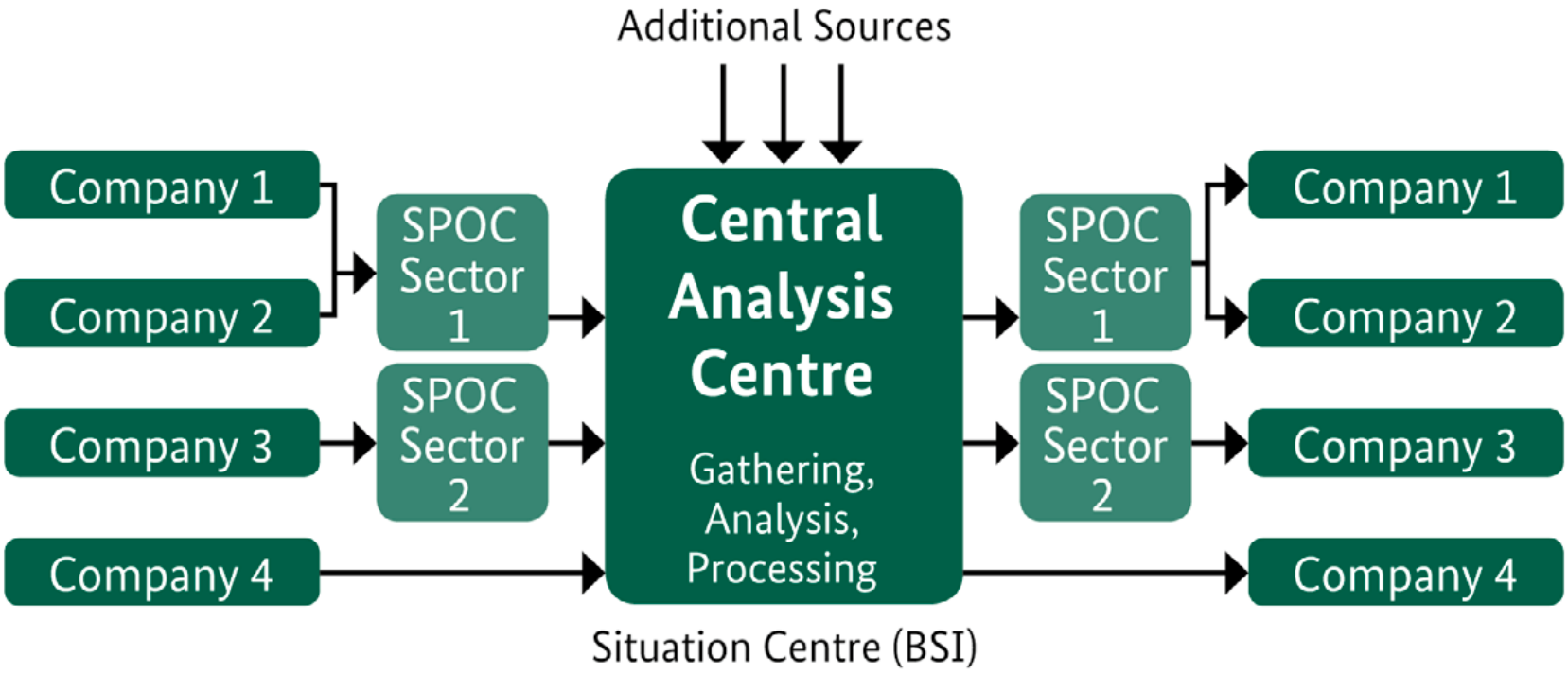


Fig. 2:
Communication structure of the operative-technical cooperation in the UP KRITIS

Committees for strategic-conceptual collaboration within UP KRITIS

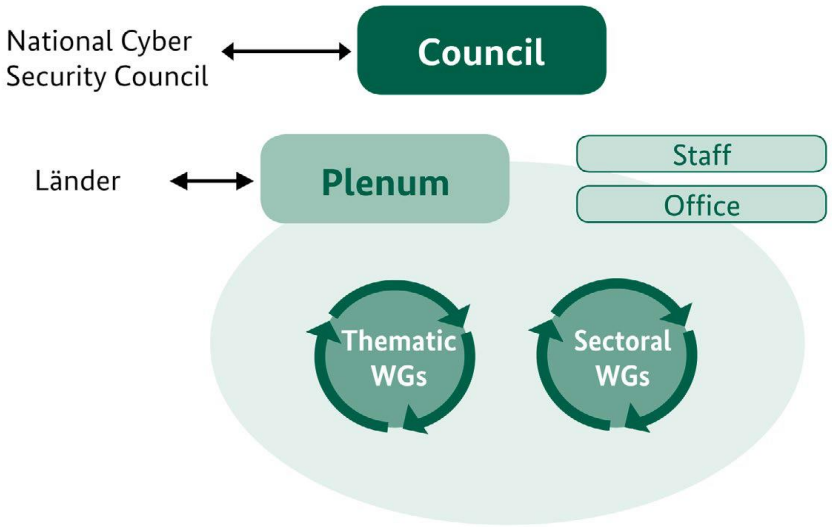


Fig. 3:
new organisational structure of the UP KRITIS

The core components of the organisational structure are working groups for the exchange of expertise between specialists; the cross-sectoral plenum and a council established at a high level (see Fig. 3). A planning staff and the office support these committees

Shared Content related to Sharing Level

Operational

- Reputation sharing products & services
- Audit of info shared
- Assets at risk
- Vuln. in ICS
- Metrics on severity
- Scale of indicators for incidents e.g. continuous
- Mediation e.g. human intervention
- Technical response: what didn't work?
- Counter measures – how to solve the incident? Patches,..
- Accounting logs+alerts

Tactical

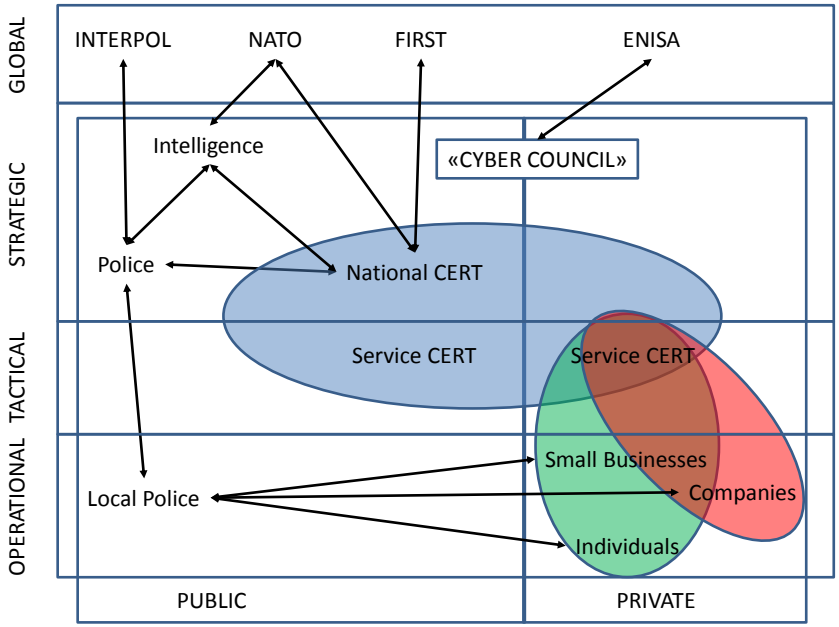
- Success stories, near misses
- Tactics, Techniques, Procedures, Operational Policies, Processes, Agreements
- Importance of incidents
- Validation of partners
- Investments in tools
- Informal interpretation by people «I can see»
- Common formats for data sharing
- Best practices, risks of sharing
- Knowledge of infected clients/customers
- SCADA events
- Technical response: what didn't work?
- Threat awareness
- CERTS Community
- Trust of data

Strategic

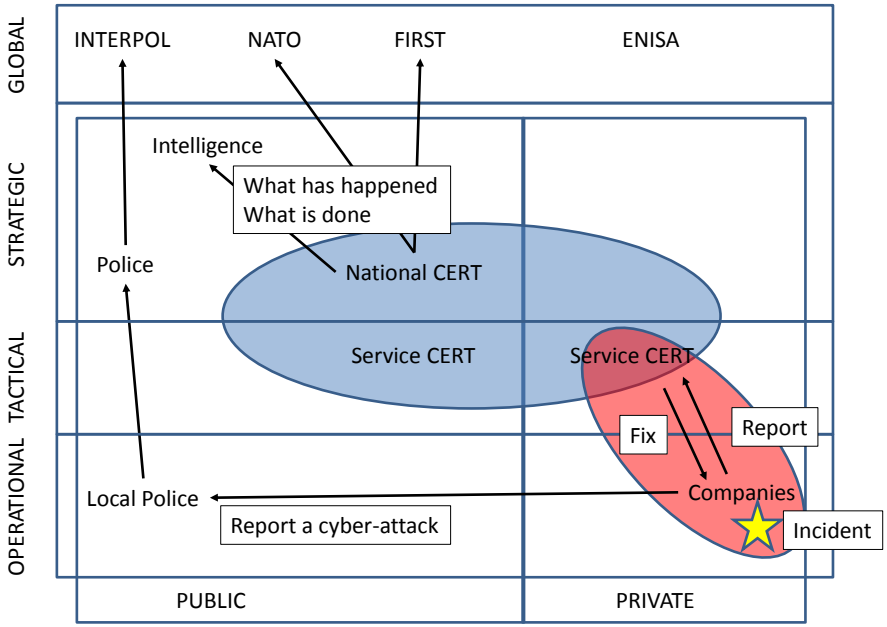
- Supply chain sharing
- Consumer consent
- Mgmt SProv
- Purposes for sharing
- ROI/incentives
- Metrics about shared info
- Strategic Framework
- Training re info&data
- Lessons learnt
- Barriers of sharing too much
- Cost of sharing /severity
- Trustworthiness, credibility of info/source
- Threat analysis = impact on IT biz
- Data breach notification
- Threat intelligence
- Strategy for privacy and data protection
- Issues of reput-ational risks

Example “Griffin Cyber Security Strategy” in Action

GRIFFIN CYBER SECURITY STRATEGY – INFORMATION SHARING



GRIFFIN CYBER SECURITY STRATEGY – INCIDENT HANDLING



Recommendations I

Recommendation 1: Define and Position the Information Sharing Arrangement
There are so many option: Take informed decision on the arrangement

Recommendation 2: On Sharing between Sharing Arrangements:

Option for mutual benefit

Recommendation 3: Creating widely accepted Standards
➔ specific to the level of sharing

Recommendation 4: Supplier crises support

need for detailed and stringent service level agreements with suppliers with clearly delineated support models for crisis situations

Recommendations II

Recommendation 5:

Foster realistic and down to earth trust in Sharing Arrangements

Trust is the base on which information sharing is built. To foster trust personal interaction is always key: E.g. periodic exercises and training for expertise sharing

Recommendation 6: Create an ontology and landscape of information sharing

Today, the diversity of arrangements in information sharing is not sufficiently addressed … Research is needed

Recommendation 7: Common Approach for certain Tasks

Subsidiarity is a well-desired goal of all activities in Europe.

he common interest within Europe and a strong position towards global suppliers needs some coordination, helpdesk or reference-function on EU level. A framework with rules and support of all MS should be elaborated and put into action.

Recommendations III

Recommendation 8: Create Legal Security for Information Sharing Personnel

Make in-depth legal studies to learn about challenges and limits to information sharing stemming from the law. Use-cases should be elaborated and applied to train information sharing personnel.

Recommendation 9: Provide Citizen and SME Best Practice and Victim Support

An often reoccurring incident should be well described, easy to find and foreseen with a solution in electronic form (blog / Database). Today everyone has its secret source …

Recommendation 10:

Leverage Existing Experience from all Level of Information Sharing

Running information Sharing is a separate task and differs from

“Security and Incident Information Sharing”

Issues for Policies

Policy Issue 1: Close the Biggest Gaps

Usually, information sharing is instituted for the benefit of the sharing partners, and not for the benefit of larger communities and non-specialised user groups.

Policy Issue 2: Strengthen Security by clear ownership Definition of Vulnerabilities

Who is the owner of vulnerability and threat information, and who has to act upon it if they have information about vulnerabilities in their possession?

Policy Issue 3: Firm screening & verification of shared information from untrusted sources

If we do this
Security in EU
will boost like a rocket …

Concluding remarks

The brief overview does not replace the in-depth understanding of the complex and very broad surroundings of information sharing.

The dialogue between expertise, science and policy is necessary to make information sharing support a more secure European cyber future.

http://xn80aqafcrtq.cc/img/2/7/8/278486.jpg

Overview on the nine discussion groups

WG 1: Group 1-4

- **G1: Managing risks in an organisation**
  Animator: Rob Kloots

- **G2: Why we need verification and audit**
  Animator: Ian Morton
  Rapporteur: Ralph Eckmaier

- **G3: Internal Audit / External Audit**
  Animator: Pryesh Prasad

- **G3: External Certification**
  Animator: Guillermo Manent

WG 2: Group 5-7

- **G5: How to illustrate use cases/scenarios**
  Animator: Waldemar Grudzien
  Rapporteur: Rossella Mattioli

- **G6: Possible legal bases to justify voluntary information sharing efforts**
  Animator: Ulrich Sledeslachts
  Rapporteur: Rainer Whyphol

- **G7: Examples of existing technical solutions & security controls**
  Animator: Steve Purser
  Rapporteur: Karin Mulvihill

WG 3: Group 8-10

- **G8: Strategic Research and Innovation Agenda in NIS**
  Animator: Fabio Martinelli
  Rapporteur: Paul Riesco

- **G9: Cybersecurity Education & Training (E&T)**
  Animator: Maritta Heisel

- **G10: Responsible Disclosure Policy**
  Animator: Leva Kupce

Why is it important to contribute by now?

Information Sharing:

Speak about by sharing your view opinions and information **NOW**

Reporting the outcome of the nine discussion groups

The only sustainable results are documented results

Please 2-3 pages for each session of text

Thank you!

Further Questions?

Prof. Dr. Bernhard M. Hämmerli
+41 79 541 7787 / bmhaemmerli@acris.ch