Examining the feasibility of an European Information Sharing and Alert System (EISAS)

Criteria to identify European Critical Infrastructures in the ICT Sector

Brussels, 05th February 2008

Agenda

- **History of the study**: why did we do it?
- **Some definitions**: what do we mean?
- **Methodology**: how did we proceed?
- **Results**: what did we find out?
- **Next steps**: how can be followed up?
- Finalise the study

Formal Background

http://ec.europa.eu/i2010

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, [...]
COM(2006) 251

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"

{SEC(2006) aaa}

http://ec.europa.eu/information_society/doc/com2006251.pdf

ToR concerning the Request from the Commission
Version 1.1

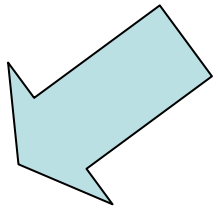
Examining the feasibility of a EU-wide information sharing and alert system

Background

In its COM(2006) 251, the Commission emphasises that public authorities, in Member States and at EU-level, have a key role to play in properly informing users to enable them to contribute to their own safety and security. "In order to improve the European capability to respond to network security threats" means "to facilitate effective responses to existing and emerging threats to electronic networks" should be explored. This need is being matched by the Commission's request to ENISA *"to examine the feasibility of a European information sharing and alert system"* (Section 3.2.2). In so doing, the Commission highlights the role of ENISA in fostering a culture of security in Europe.

Scope and Objectives

One of the main objectives of fostering a culture of security is **raising awareness on NIS issues** and providing appropriate and timely information on threats, risks and alerts as well as on good practices. To this end, the primary responsibility of MS in carrying out these activities to improve national capabilities to respond to NIS threats according to their national NIS and related policies is acknowledged. However, better cooperation among MS might add value to those single initiatives. Against this background, the aspect of promoting the exchange of information and lessons learnt among MS could help achieve the overall goal (enhancing NIS in the EU). The task is primarily targeting at citizens and SMEs (but network operators and service providers should not be excluded at this point in time).
The expected result is a recommendation whether and if so, how an EU-wide system could be realized by combining existing MS' systems.



Motivation

NIS information for citizens and SMEs is important

There is already a lot going on in the Member States, but ...

... what?

... who?

... where?

... are there gaps?

... how?

... where are the gaps?

BÜRGERCERT

CASES LUXEMBOURG

CASES contact network

[...]

WAARSCHUWINGSDIENST.NL

ITsafe

BSI für Bürger

And finally: what can the EU do?

Objectives

- **Goal**: raising awareness on NIS issues
- **Target group**: citizens and SMEs
- **Base**: existing systems

Terms & Definitions

- Feasibility Study(!)
- Information Sharing & Alerting(?)
- NIS Security related Information (Good Practice & Recent Developments)

Methodology of the study

- **Analyse** the current “state of affairs”
- **Develop** possible scenario(s)
- **Determine** the most feasible scenario
- **Determine** the added value

Start: 09/2006

End: 10/2007

Support by a group of Experts

- Nominated by the EU Member States (NLO network) and the Permanent Stakeholder Group (PSG)
- Expertise in running Information Sharing Systems
- Contribute to the study

15 Experts from the Member States & Switzerland

Analyse the current “state of affairs” (I)

13 Annex B – Inventory of existing systems

Name, Country	Web page	Maintainer	Language	Type	Model
ARAKIS, PL	http://www.arakis.pl	CERT Polska/NASK	Polish English	Real time	Governmental Commercial Research
ARGOS, NL	http://www.few.vu.nl/~porto/argos/	Vrije Universiteit Amsterdam	n/a	Real time (Software)	Research
ATLAS, US	http://atlas.arbor.net	ARBOR	English	Dynamic Real time	Commercial
Bichos, ES	http://www.rediris.es/cert/proyectos/bichos/	UNAM-CERT CAIS-RPN	Spanish	Real time	Research
BSI fuer buerger, GE	http://www.bsi-fuer-buerger.de/	BSI	German	Static	Public
Buerger cert, GE	http://www.buerger-cert.de	Mcert	German	Dynamic	Public
CAIDA, US	http://www.caida.org	Cooperative Association for Internet Data Analysis	English	Software	Public
CarmentiS, GE	http://www.cert-verbund.de/carmentis/index.html	CERT-Verbund	German	Real time	Research
CASES.lu, LU	http://www.cases.public.lu/	Ministère de l'Économie et du Commerce extérieur	French	Static Dynamic	Governmental
CERT-EE, EE	http://www.cert.ee	CERT EE	Estonian English	Static Dynamic Real time	Governmental
CERT-FI, FI	http://www.cert.fi	Finnish Communications Regulatory Authority	Finnish	Dynamic Real time	Governmental
CERT-PT, PT	http://www.cert.pt/	CERT PT - Lino Santos	Portuguese	Static	Governmental

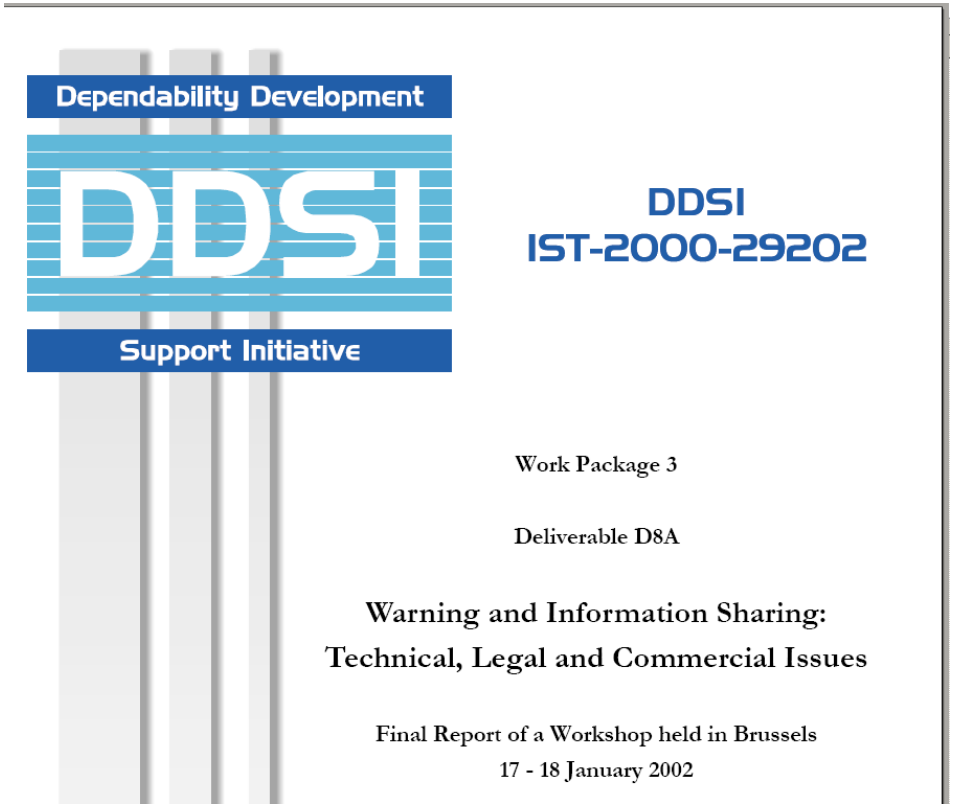
Analyse the current “state of affairs” (II)

14 Annex C – Inventory of existing sources of information

Name	Weblink	Topics	Info Provider	Distribution	Language
Adobe	http://www.adobe.com/cfusion/entitlement/index.cfm?e=szalert	Vulnerabilities	Commercial / Vendor	Mailing list	English
Antivirus	http://antivirus.about.com/	Viruses	Commercial / Vendor	Website	English
Apache	http://httpd.apache.org	Vulnerabilities	Commercial / Vendor	Website	English
Apache	http://httpd.apache.org/lists.html#http-announce	Vulnerabilities	Non-Commercial	Mailing list	English
Apache	http://www.apacheweek.com/features/security-13	Vulnerabilities	Commercial / Vendor	Website	English
Apple	http://docs.info.apple.com/article.html?artnum=61798	Vulnerabilities	Commercial / Vendor	Website	English
Apple	http://lists.apple.com/mailman/listinfo/security-announce	Vulnerabilities	Commercial / Vendor	Mailing list	English
Apple – Product Security	http://www.apple.com/support/security/	Notifications	Commercial / Vendor	Website	English
Arkoon	http://www.arkoon.net/FR/veillearkoon.php	Vulnerabilities	Commercial / Vendor	Website	French, English
AusCERT	http://www.auscert.org.au/	Vulnerabilities	CERT Academic	Website	English
BEA	http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/index.jsp	Vulnerabilities	Commercial / Vendor	Website	English
BELNET CERT	http://cert.belnet.be	Vulnerabilities	CERT	Website	English
BugTraq	http://www.securityfocus.com/archive	Vulnerabilities	Commercial /	Mailing list	English

First version by ad-hoc WG “CERT Services” 2006

Analyse the current “state of affairs” (III)



Lessons learned in the past

Analyse the current “state of affairs” (IV)

Lessons learned in the past

Discussion Workshop in Brussels

enisa European Network and Information Security Agency

EISAS validation workshop

Time Frame:	Monday, 16.04.2007, 10:30 – 16:45
Meeting Minutes:	ENISA
Logistics:	(Breaks to be scheduled short-term)
Meeting Venues:	Sofitel Hotel in Brussels

Proposed agenda:
(EN = ENISA, EG = Expert Group Members)

10:30	EN	Introduction
	EN	Briefing: i2010, COM(2006)251, EC request
11:00	EG	Presentation of existing systems: AT, CH, EE, FI, FR, LT, NL, PL, PT, UK
13:00	all	Lunch
14:00	EN	Presentation of inventories
	EN	Presentation of EG input
	EG	"Top-down" through the inventories - systems/software to cover - systems for base - systems for sources
	EG	Assessment of inventories
15:00	EN	Presentation of different scenarios

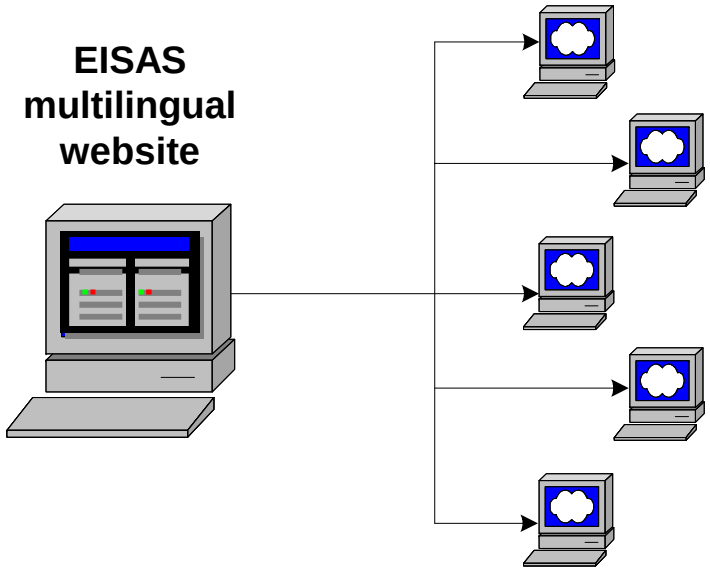
Expert Group + invitation to EU MS (via NLOs)

NIS Information for Home-Users & SMEs
Basic Principles (excerpt)

- Use **Native Tongue** to address
- Use **understandable** language (No “Tech Talk”)
- Provide **comfortable** distribution channels
- Deliver as **close** to the user as possible (Trust)
- Avoid **Information Overflow**

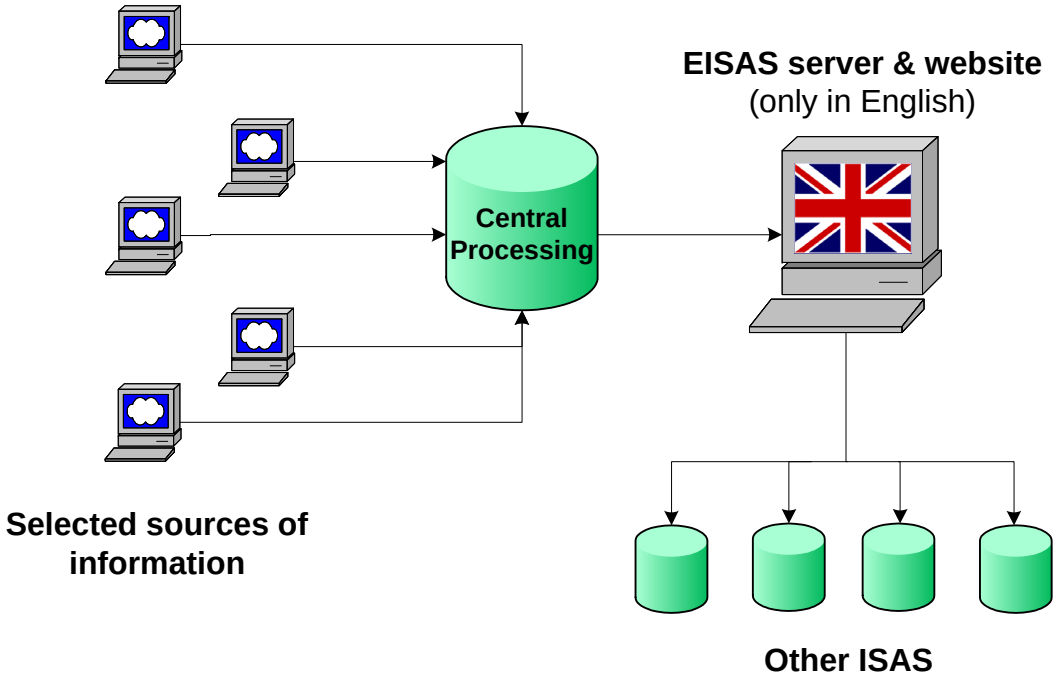
- **Do not compete with existing initiatives**

Thinking “results first” (I): EISAS **could** be ...



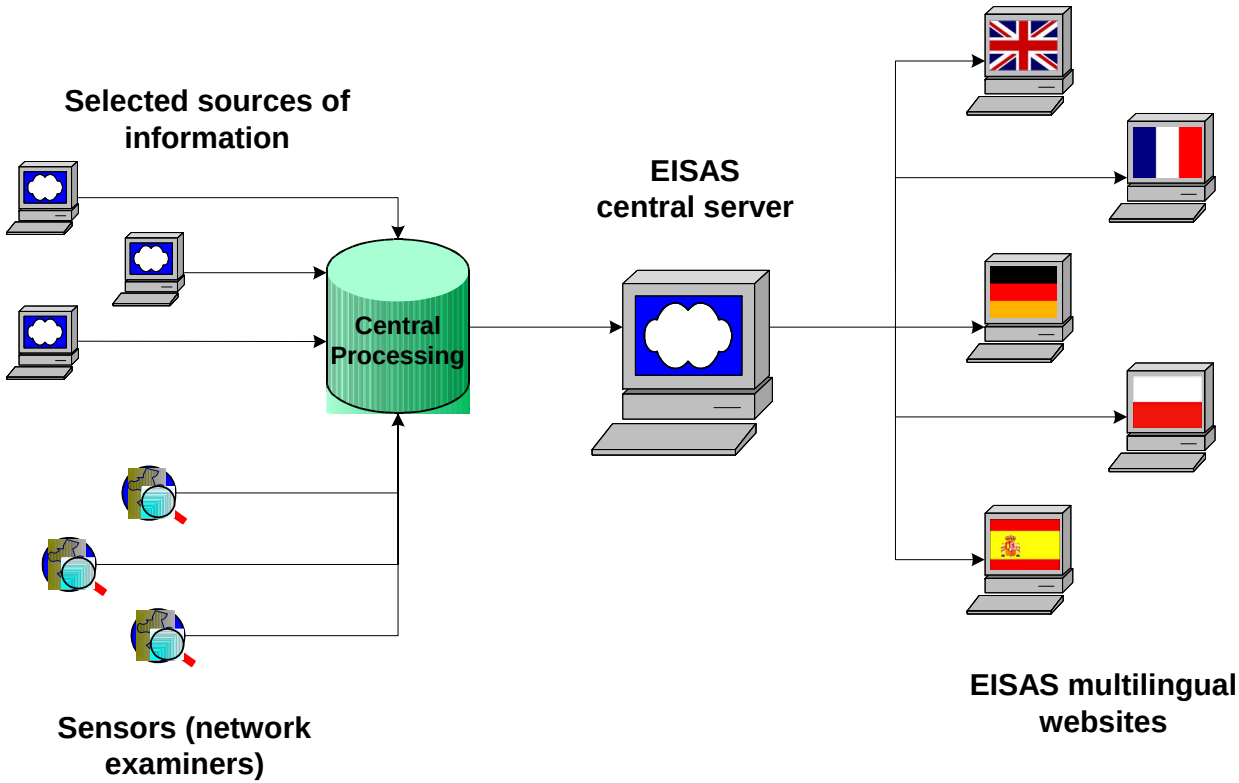
... a Europe-wide link portal

Thinking “results first” (II): EISAS could be ...



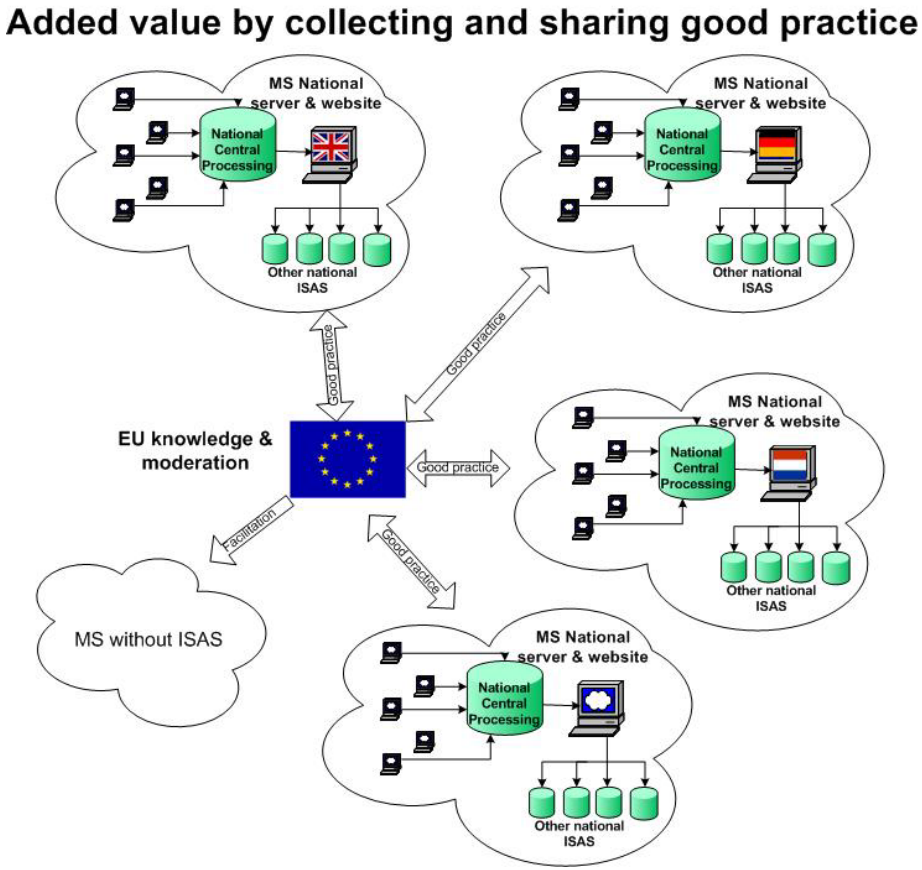
... a limited Europe-wide information gathering and sharing system

Thinking “results first” (III): EISAS could be ...



... a centralised, fully fledged Europe-wide system

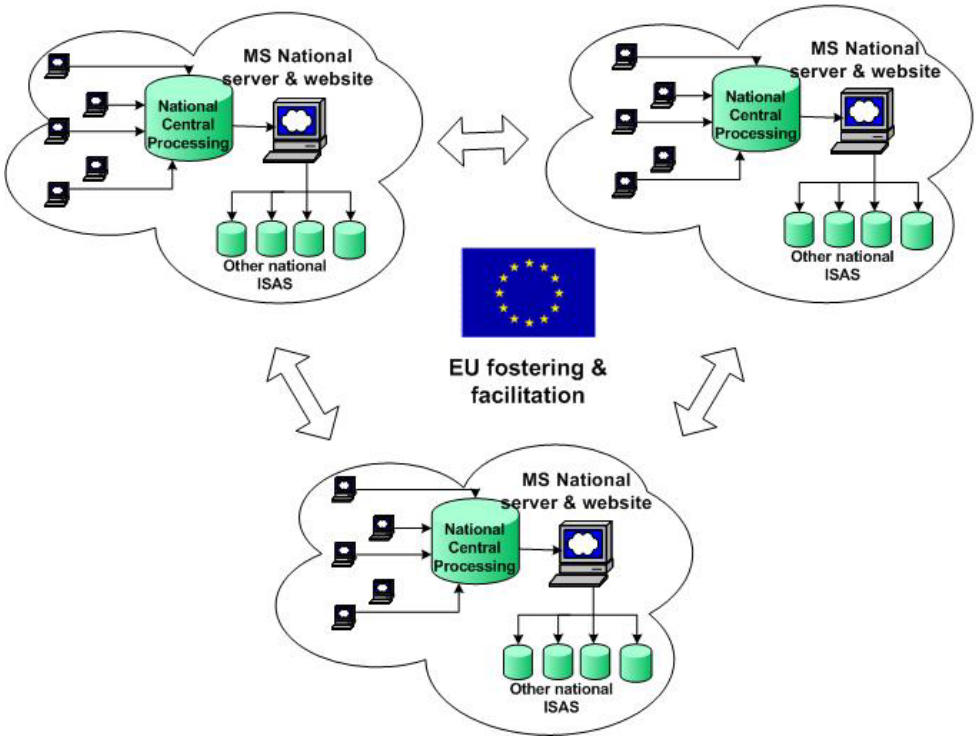
But: Following the analysis (I) EISAS **should** provide



to support national systems!

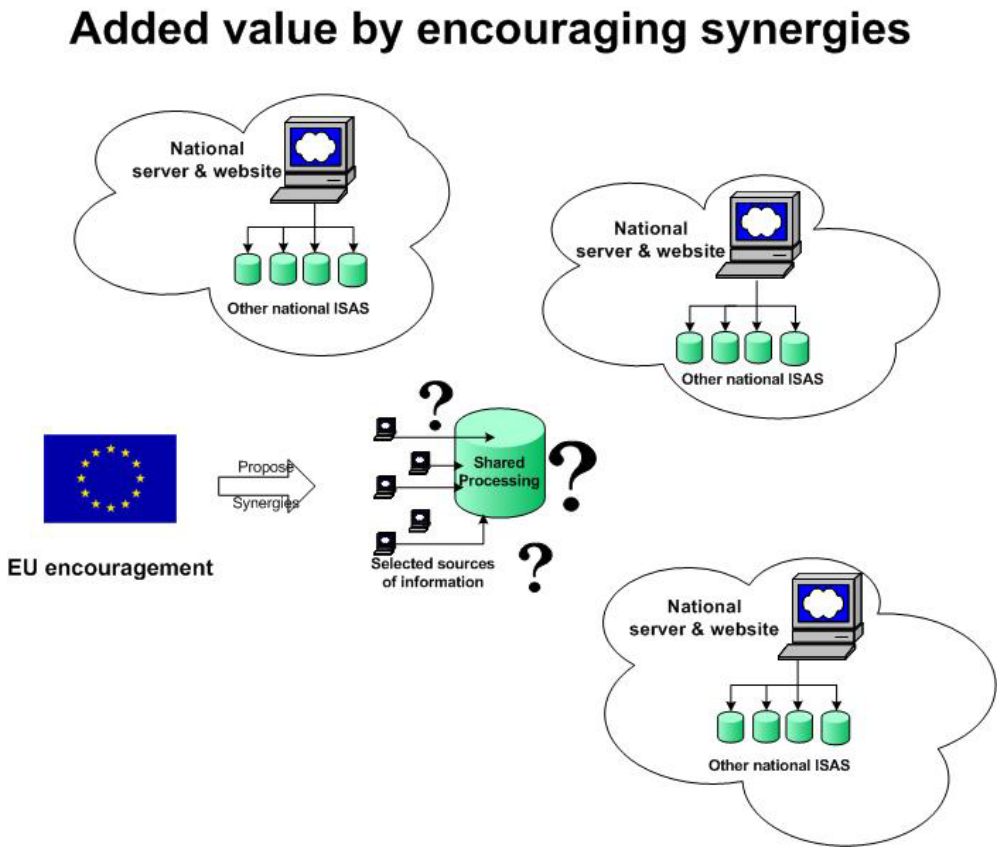
Following the analysis (II) EISAS **should** provide

Added value by fostering dialogue



among the Member States and existing initiatives

Following the analysis (III) EISAS **should** provide



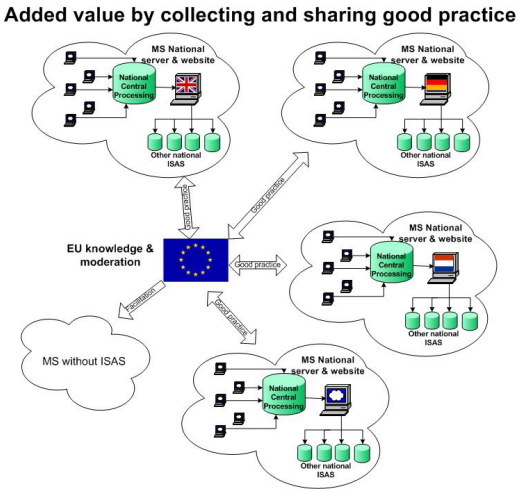
for example to avoid double work

Proposal for next steps

Discussion involving all stakeholders, ...

... involving the Member States, ...

... involve European experts and ...



... further develop scenarios and initiate a proof of concept.

Finalise the study

DONE

Questions, comments, compliments, threats?

Marco Thorbruegge

Senior Expert CERT

Marco.Thorbruegge@enisa.europa.eu

Thank YOU!