

Response
readiness

What R the new CERTs?

Why this Question?

1988 Creation of CERT as
Computer Emergency
Response Team

2003 Creation of US-CERT
as Computer Emergency
Readiness Team

A Brief History of CERTs

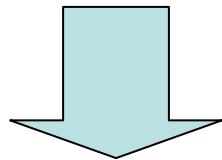
- 1988: Creation of CERTs
- 1990: Creation of FIRST (11 members, mainly from Academic and Defense)
- Early 90's: Development of Academic CERTs
- Late 90's: Development of Business CERTs as well as National CERTs
- Early 2000's: Development of Government CERTs

Some Examples of Government CERTs

- CERTA - France
- CERT-Bund – Germany
- CERT-FI – Finland
- GOVCERT.NL – The Netherlands
- SITIC – Sweden
- UNIRAS – UK
- US-CERT – USA
- CCIRC - Canada
- ArCERT – Argentina
- NIRT – Japan
- (KrCERT/CC) - Korea
- (CNCERT/CC) - China

Usual Issues

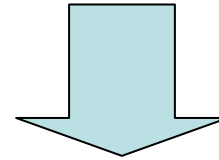
- Incident Handling
- Response
Coordination
- Technical Analysis
- Information Exchange



Response

Government Issues

- Protection of Critical
Infrastructure
- Early Warning and
Alerts
- Contingency Plans



Readiness

CERTA

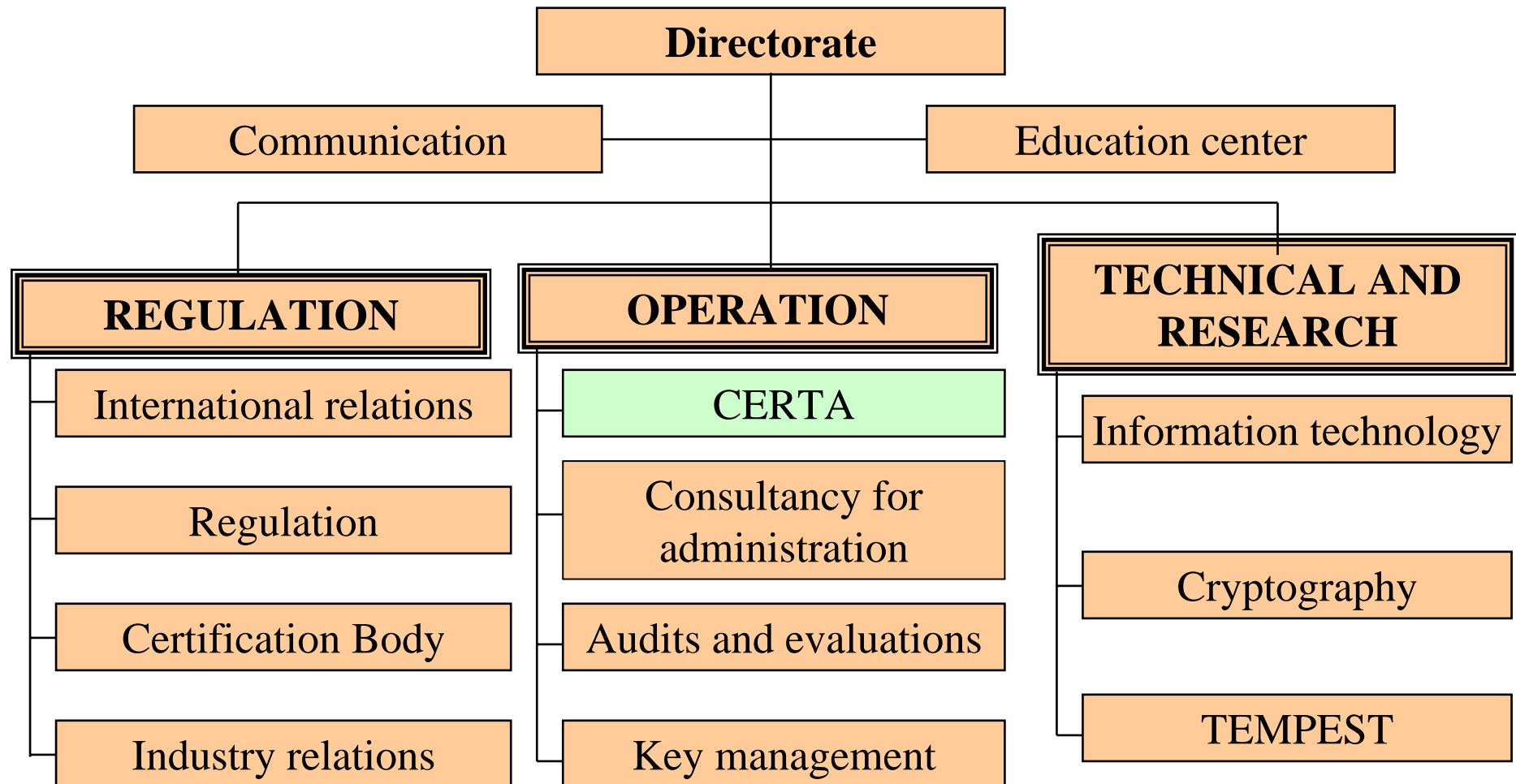


Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE

Centre d'Expertise gouvernemental
de Réponse et de Traitement des
Attaques informatiques

French governmental CERT (Computer Emergency **R**esponse Team)



French governmental CERT

(1/4)

- Creation of the the CERTA : Decision of "Comité Interministériel pour la Société de l'Information" (CISI) on January 19th 1999:
- « ***To strengthen State networks against attacks***
- *In order to strengthen and to co-ordinate the struggle against intrusion into governmental computer systems, the government decide to create an assistance and warning team, whose missions are to watch and to answer issue related to computer attacks. »*

French governmental CERT

(2/4)

- CERTA missions :
 - Keeping up with technological innovations (software and hardware vulnerabilities);
 - Solving computer incidents within the French government information system;
 - Creating and maintaining a trust network within the French government services.

French governmental CERT

(3/4)

- CERTA publishes 5 kinds of documents :
 - AVIS (Advisories) give a brief description of a vulnerability, its consequences and means of protection (usually a vendor patch);
 - ALERTES (Alerts) are advisories where no patch have been published yet and require a fast decision to be taken;
 - NOTES D'INFORMATION (Information Notes) are a detailed explanation of a security topic;
 - RECOMMANDATIONS (Recommendations) are dedicated to organisational measures.
 - BULLETINS D'ACTUALITE (Weekly Report) give a picture of recent activity seen by CERTA

International cooperation

CERTA has relations with :

- TF-CSIRT (European Task Force for the cooperation of CSIRTs)
- FIRST (Forum of Incident Response and Security Teams)
- European governmental CERTS

The French ITSOC

- French Name = COSSI (Centre Opérationnel pour la Sécurité des Systèmes d'Information)
- International Name = ITSOC (IT Security Operation Center)



Readiness

IT Security Operational Centre

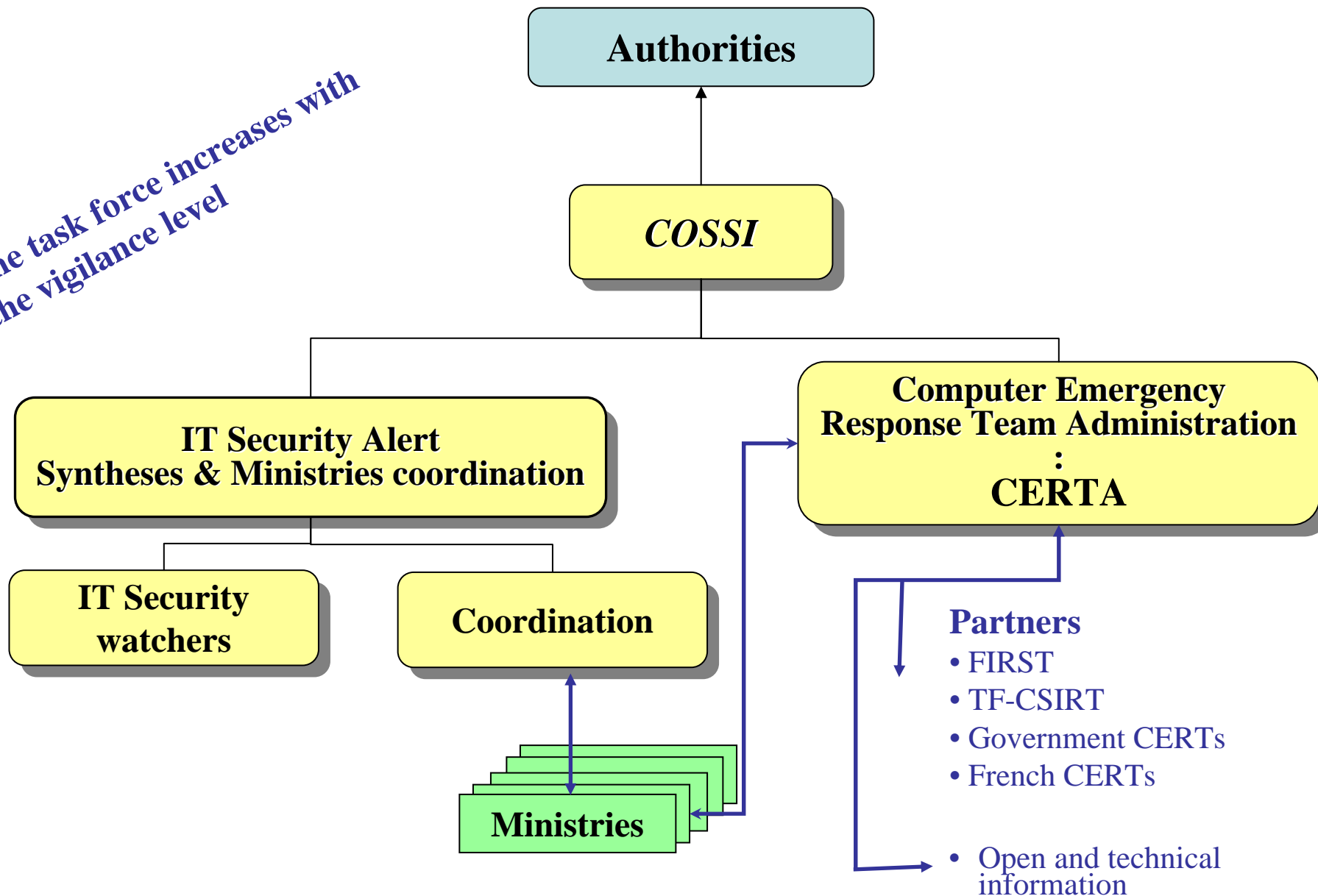
•Main tasks : the ITSOC, the IT security permanent operational centre, has been set to cooperate the governmental plans against cyber malware - VIGIPIRATE (IT Security aspects) and PIRANET.

ITSOC main tasks

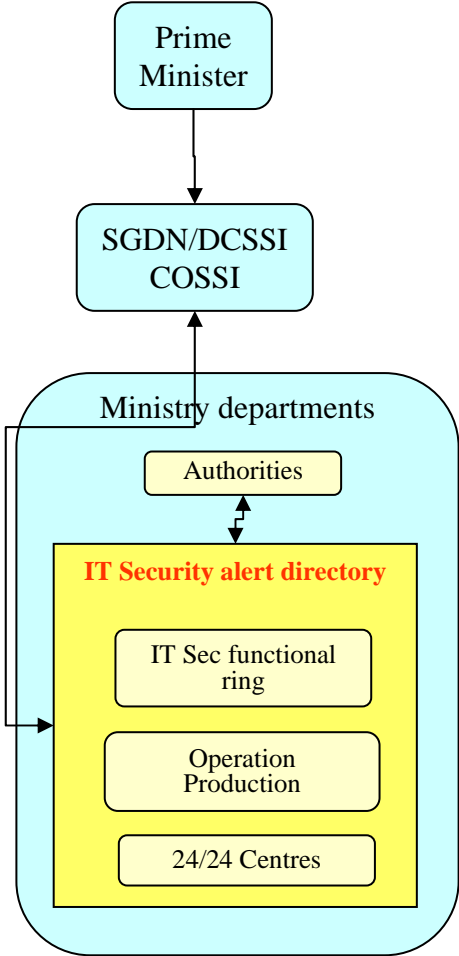

- Technical tasks : technical expertise to prevent and solve incidents
 - Generic measures in order to increase overall security level
 - Specific technical measures against attacks
- Coordination tasks
 - Lead official actions for effective reactions
- Communication tasks : IT Security synthesises for authorities
 - Quick actions / decisions to be taken
 - General information for public audience
 - Specific information for authorities

Information flows

The task force increases with the vigilance level



IT Security alert and crisis organisation

Actors	Steps	VIGIPIRATE IT Sec	PIRANET
	Triggers	Vigilance level 	Pre-alert / Alert
	<ul style="list-style-type: none"> •Threats / incidents / vulnerabilities analysis •Relevant IT Security measures selection 	Functional IT Security group of measures regarding the vigilance level	Generic measures and specific mechanisms
	Implementation of IT Sec. measures including ministry adaptations	Implementation of the IT Sec measures.	Implementation of the IT Sec. and the adapted measures and mechanisms

Main points :

- Ministries Guidelines / Actors key actions cards
- Ministerial & inter-ministerial alert directories

Questions?

David CROCHEMORE

E-Mail: David.Crochemore@certa.ssi.gouv.fr

CERTA: certa-svp@certa.ssi.gouv.fr

Tel: +33 1 71 75 84 50