

# Baseline capabilities of national/governmental CERTs

ANDREA DUFKOVA

CERT relations

European Network and Information Security Agency

<NIS Summer School, Hersonissos, Crete>

# Outline

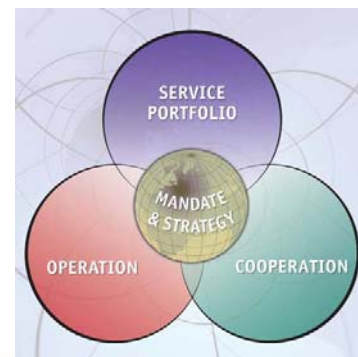
- Introduction to CERTs
- CERTs work, duty, responsibilities...
- Our work in 2011



## ENISA and CERTs...

### ENISA supports the Member States and their CERTs by

1. Provide help with the setting-up, training and exercising of the teams
2. Definition of “baseline capabilities” for new and established teams
3. Help CERTs to enhance their capabilities by providing good practice guides in:
  - Setting-up and operating CERTs
  - Training, exercising and piloting of projects
  - Basic services like incident management
  - Enhancing cross-border cooperation



# 1. Provide help with the setting-up, training and exercising of the teams

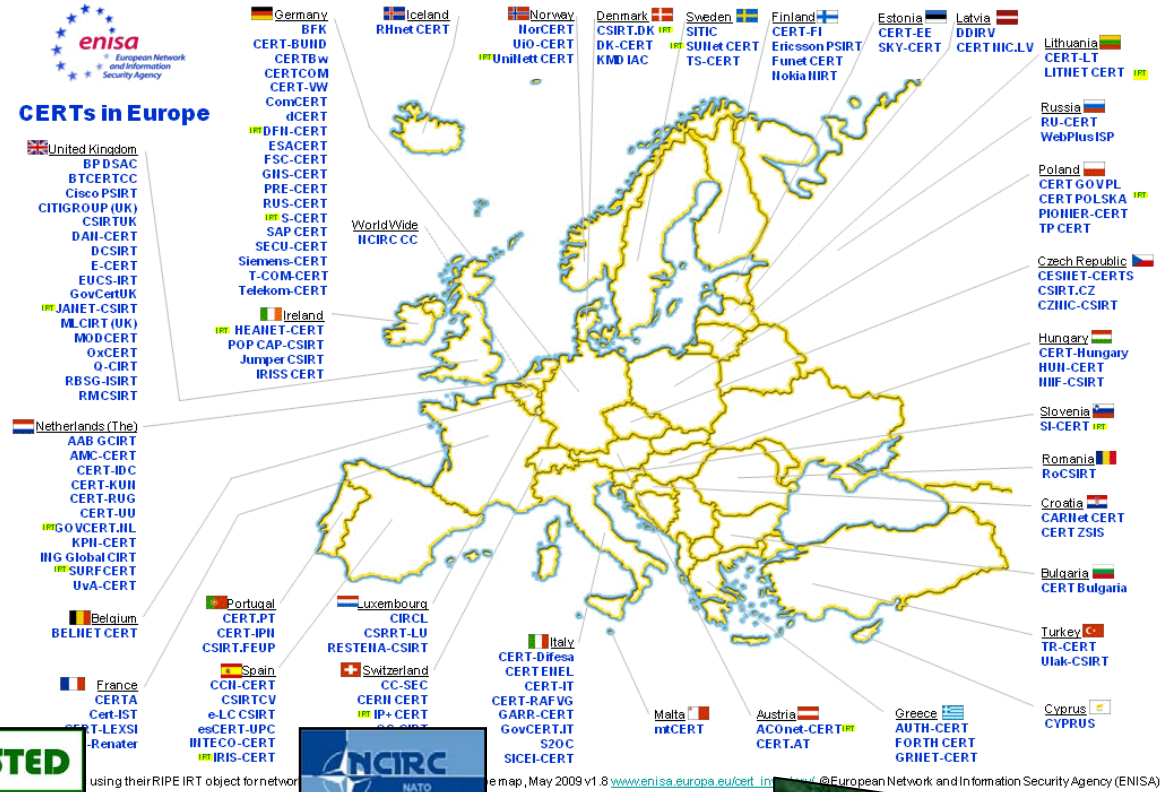
## ➤ ENISA CERT INVENTORY MAP (more than 160 teams listed!)

### ➤ INFO:






- TRUSTED INTRODUCER
- FIRST
- (TF-CSIRT)

### ➤ Cross-border cooperation among teams exists, but can be improved


- *GET INTRODUCED!*
- *DESERVE TRUST!*
- *PROFIT FROM THE COOPERATION!*



## 2. Help CERTs to enhance their capabilities by providing good practice guides

<p>2005: Stocktaking</p>  	<p>2006: Setting up &amp; Cooperation</p>  	<p>2007: Support Operation Quality Assurance</p> 	<p>2008: CERT Exercises</p> 	<p>2009: CERT Exercises Pilots &amp; CERT Baseline Capabilities</p> 
--	---	--	--	---

**2010:**  
**CERT Baseline Capabilities – Policy Recommendations & Incident Management Guide**

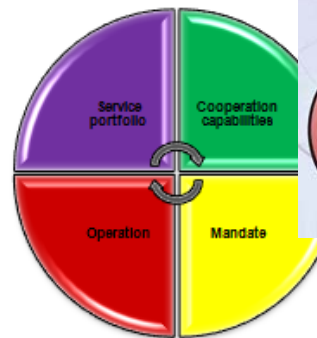
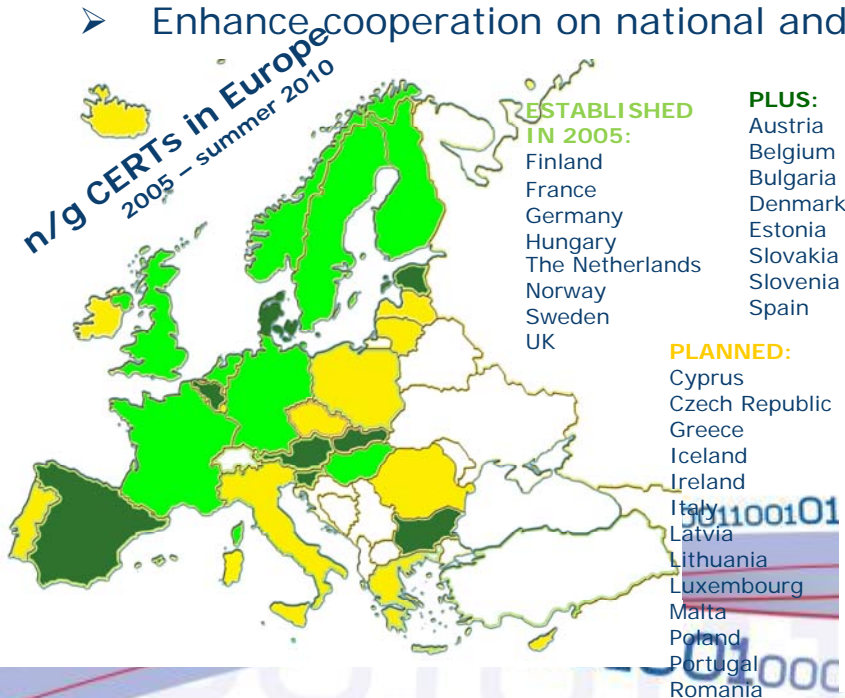



<http://www.enisa.europa.eu/act/cert/support>

# 3. Definition of "baseline capabilities" for new and established teams

## The objectives are:

- Definition and further development of a set of baseline capabilities for national / governmental CERTs in the Member States
- Establish national / governmental CERTs in every Member State
- Offer or support activities to help teams to reach (and go beyond) the baseline
- Enhance cooperation on national and European level



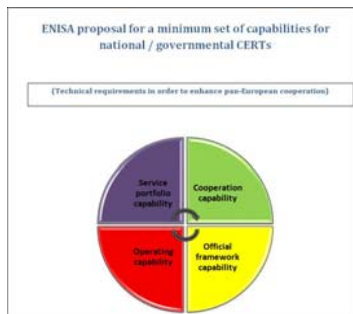

# Reinforcing national / governmental CERTs (Our mission)

National / governmental CERTs play a major role in protection of CIIP in the Member States (EC CIIP communication)

A “well functioning” national / governmental CERT in each Member State is mandatory (EC CIIP communication)

These documents constitute a very first attempt to define a minimum set of capabilities that a Computer Emergency Response Team (CERT) in charge of protecting critical information infrastructure (CIIP) in the Member States should possess to take part and contribute to a sustainable cross-border information sharing and cooperation.

## Operational recommendations



2009



## Policy recommendations



2010



## Compliance?

2012











# Outlook 2011: Situation awareness for CERTs and EISAS

The objectives are:


- Stock taking of available situation awareness mechanisms to define the “state of the art” of “early warning” (proactive detection of incidents) for NIS.
- Analysis of results - the benefits and shortcomings will be assessed and potential further developments identified.
- European Information Sharing and Alerting system
  - Continuous and ongoing work on the development of EISAS basic
  - New capability targeting end users and SMEs





# Want to know more?

<http://www.enisa.europa.eu/act/cert>



The screenshot shows the ENISA website page for CERT. At the top, there is a navigation bar with links for Site Map, Accessibility, Contact, and Legal Notice, along with a search box. Below this is a secondary navigation bar with links for Home, About ENISA, Our Activities, Publications, Press & Media, and Events. The main content area is titled 'CERT' and includes a sidebar with links for Overview, Support, Other work, Events, and About us. The main text describes CERTs as key tools for Critical Information Infrastructure Protection (CIIP) and lists ENISA's work in the field of CERTs / CSIRTs. It includes a section 'What is it all about?' and 'What do i find here?'. The 'What do i find here?' section lists three categories: Overview, Support for CERTs / CSIRTs, and Other related work from ENISA. On the right side, there is a 'videos' section with a video thumbnail and a 'related sites' section with logos for APCERT, CERT, FIRST, NCIIRC, NATO CIRC, TERENA, and TRUSTED Introducer.

**CERT**  
— filed under: [Training](#), [Information Sharing](#), [Incident Response](#), [Good Practice](#), [CERT](#), [Cooperation](#), [Exercises](#), [Incident Reporting](#), [CIIP](#)

**ENISA's work in the field of CERTs / CSIRTs**

**What is it all about?**

**CERT (Computer Emergency Response Team)**

Computer Emergency Response Teams (CERTs, aka CSIRTs) are the key tool for Critical Information Infrastructure Protection (CIIP). Every single country that is connected to the internet must have capabilities at hand to effectively and efficient respond to information security incidents. But CERTs must do much more: they must act as primary security service providers for government and citizens, act as awareness raisers and educators.



Not every country connected to the internet disposes of CERT capabilities. And the level of maturity among those who do vary dramatically. It is ENISA's mission to as much as we can clear out the "white spots" on the CERT worldmap and to minimise the gaps by facilitating setting-up, training and exercising of CERTs.

**What do i find here?**

These pages contain information about ENISA's work in the field of CERTs / CSIRTs, together with a lot of background information, useful supporting material and recommendations for further reading.

- **Overview**  
Find out more about CERTs and CSIRTs, who they are, what they do and where they are located. [More...](#)
- **Support for CERTs / CSIRTs**  
Find a lot of useful material from ENISA to support the EU Member States and other stakeholders with establishing and running CERTs / CSIRTs. [More...](#)
- **Other related work from ENISA**

**videos**



View or download the CERT Exercise video

**related sites**

-  **APCERT**  
Asian Pacific CERT
-  **CERT**  
CERT Coordination Centre
-  **FIRST**  
FIRST
-  **NCIIRC**  
NATO CIRC
-  **NATO CIRC**
-  **TERENA**  
Terena TF-CSIRT
-  **TRUSTED**  
Introducer

