# 22nd TF-CSIRT Meeting

## Building National CERT of the Czech Republic

20 - 21 September 2007

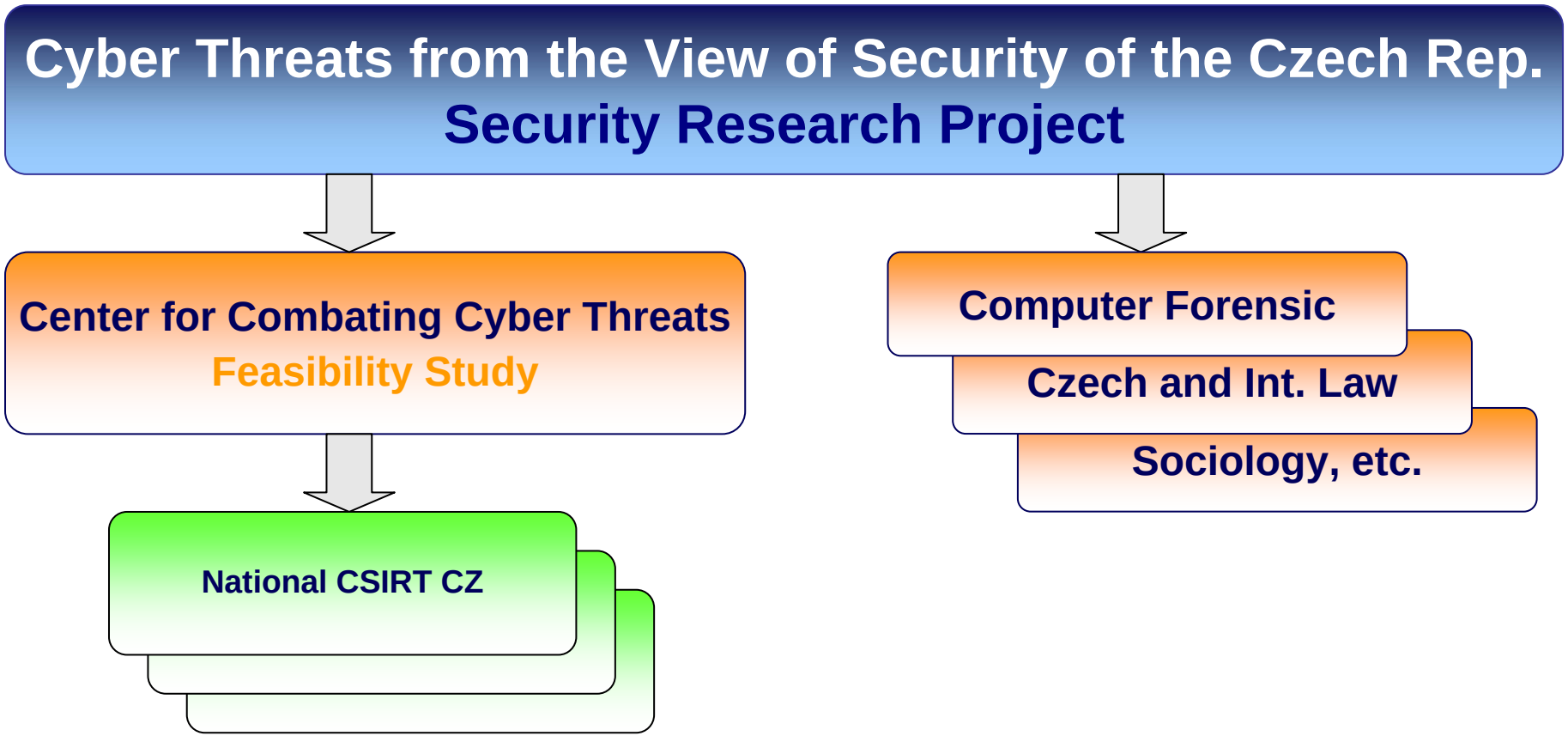
Porto

# Introduction

- Participants
  - Andrea Kropáčová (CESNET-CERTS), know-how
  - Robert Malý (NESS), start up, professional services
  - Martin Kult (NESS), start up, professional services
  - Václav Jirovský (MFF UK), leader of the project

- Project “Cyber threats from the view of the security of the Czech Republic”
  - Sponsor of the project is the Ministry of Interior
  - Active within 2007 - 2010
  - Project “*Building National CSIRT of The Czech Republic”*

# Czech Activities in Cyber Security

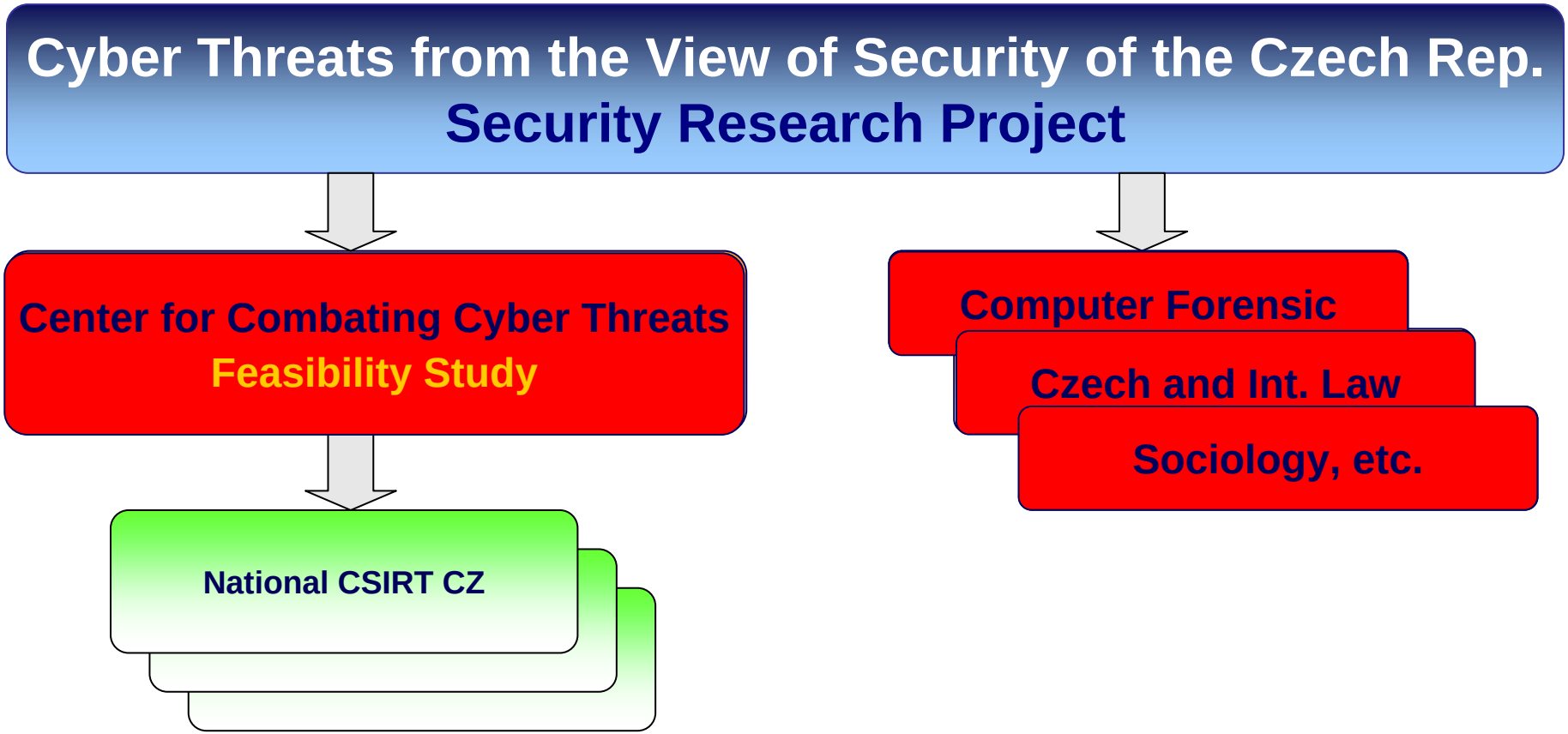


# Security Research Project

## The participants in this project:

- Faculty of Mathematics and Physics of Charles University in Prague
- Faculty of Law of Charles University in Prague
- Faculty of Electrical Engineering of the Czech Technical University in Prague
- Institute of Sociology of the Academy of Sciences of the Czech Republic
- CESNET
- NESS Czech

# Czech Activities in Cyber Security



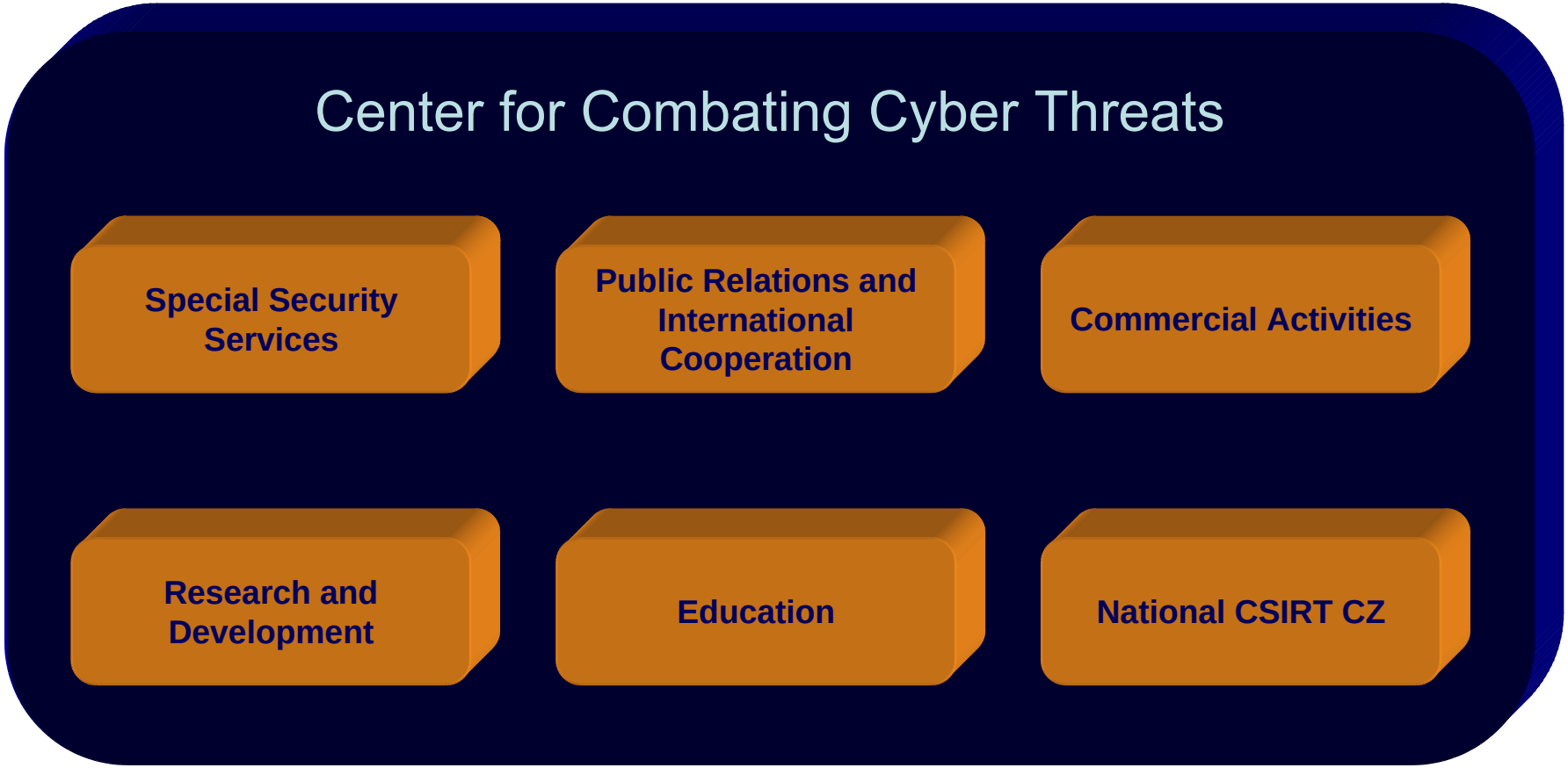
# Center for Combating Cyber Threats

- Agency established and controlled by the Czech government
- Support security research and development projects
- Responsible for Cyber Security in the Czech Republic
- Joins the public sphere and the academic world

# Center for Combating Cyber Threats – Major Goals

- concentrating highly qualified personnel and technical resources
- establishing the point of contact for dealing with similar foreign institutions
- facilitating conditions for long term projects that cannot be carried out by other means
- creating financial resources sufficient to contract the most specialized experts

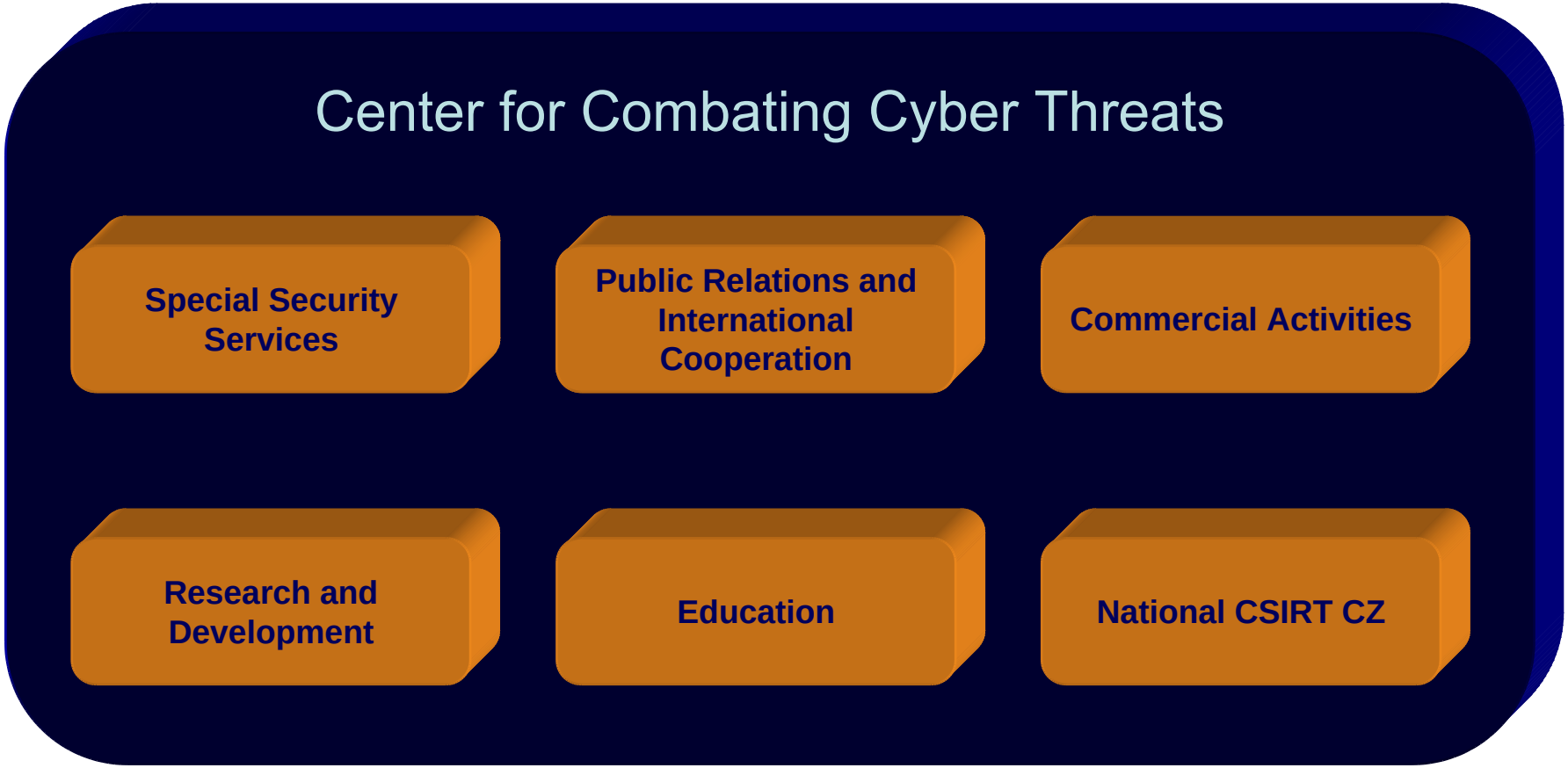
# Center for Combating Cyber Threats



# Division I
# **Special security services**

- Focuses on forensic analyses
- Gathers evidence for the courts and other entities
- Analyzes the impact of security incidents
  - Gives recommendations to state agencies and network administrators
  - Etc.

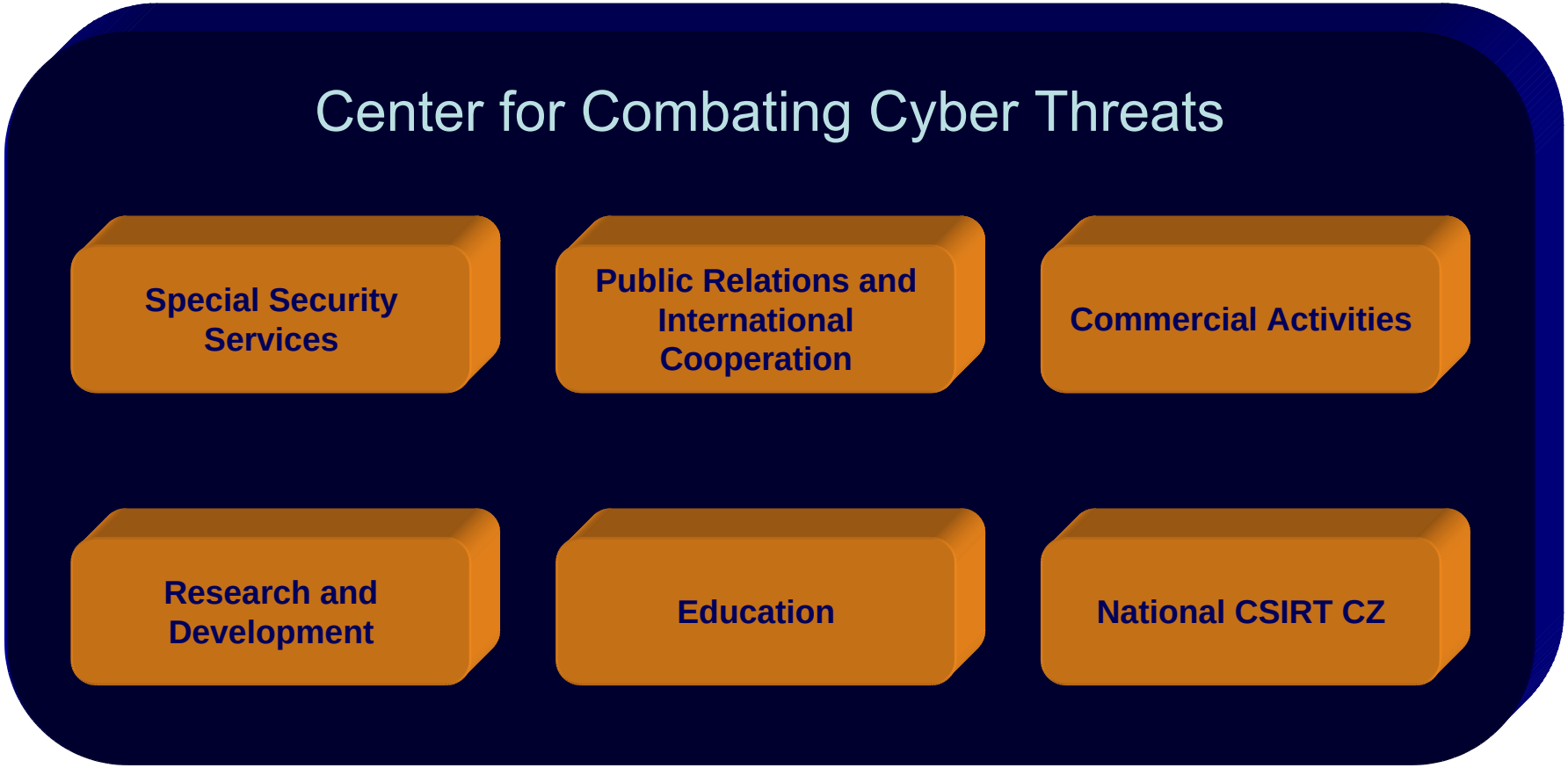
# Center for Combating Cyber Threats



# Division II
# **Public Relations and International Cooperation**

- Public relations activities
- Promoting the image of the Center
- Point of Contact for cooperation with foreign institutions

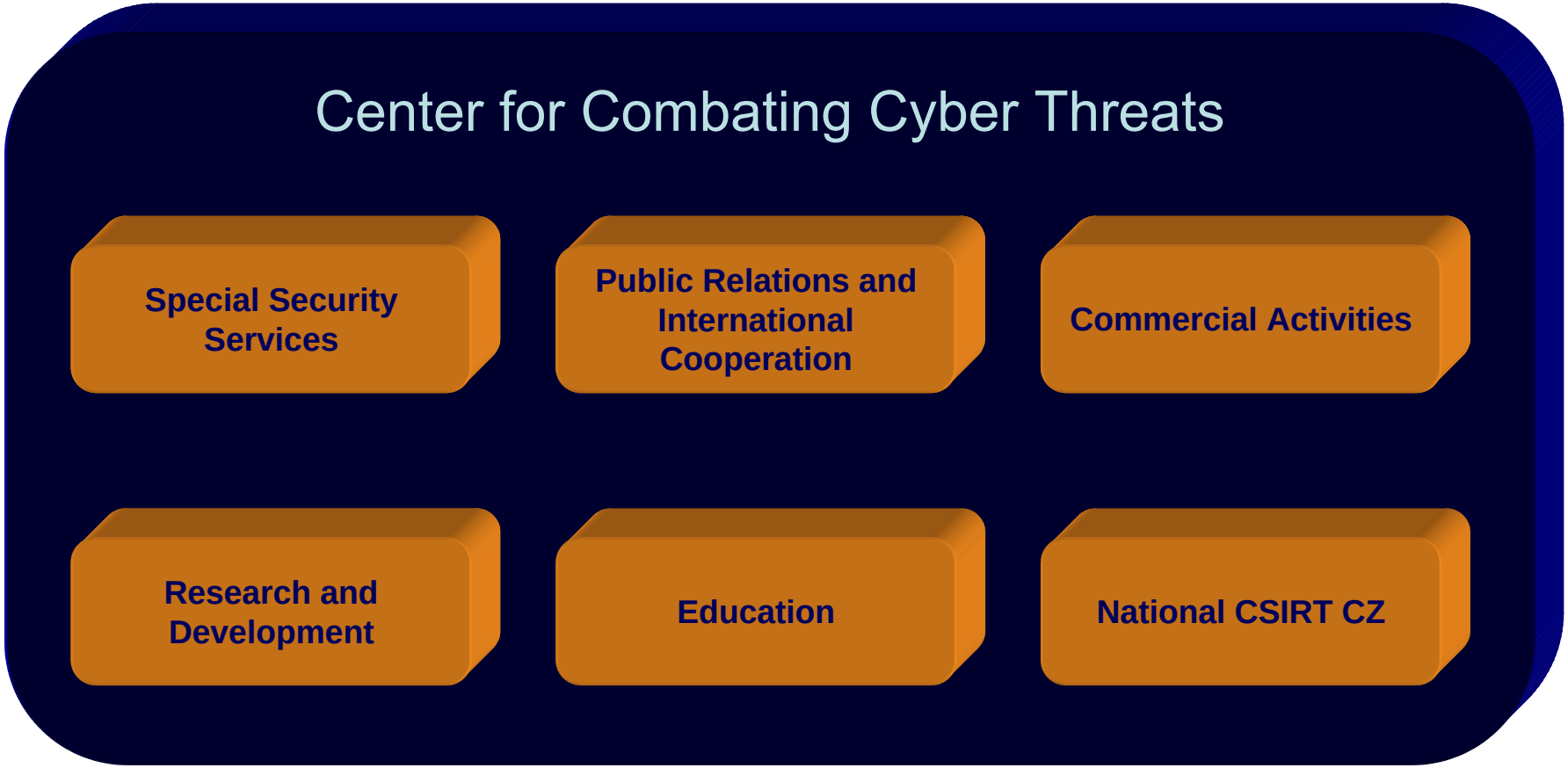
# Center for Combating Cyber Threats



# Divison III
# **Commercial activities**

- Supplements other activities of the Center
- Public Private Partnership activities
  - Certification of IT products
  - Security testing
- Etc.

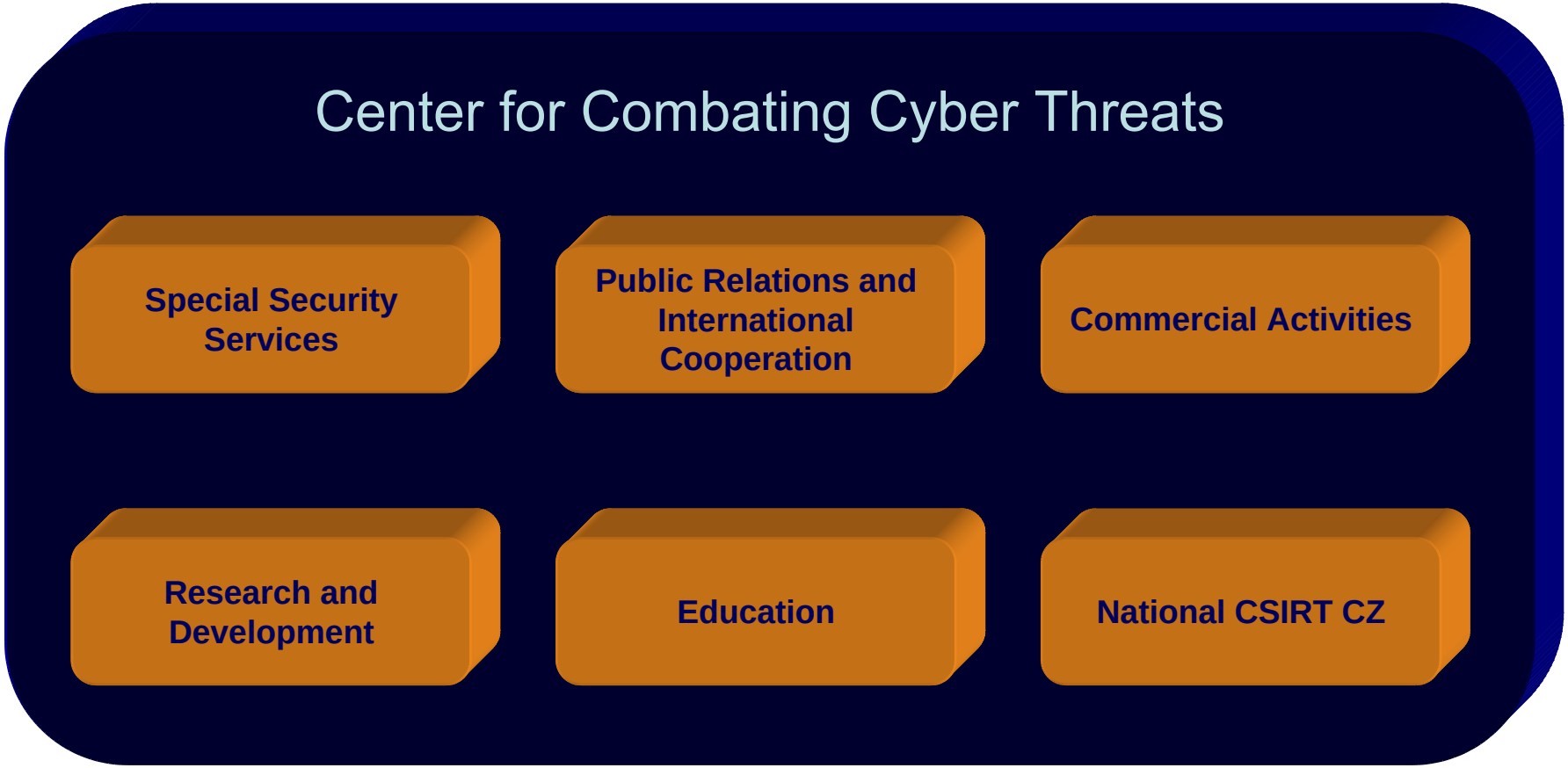
# Center for Combating Cyber Threats



# Division IV
# **Research and Development**

- Consultations
- Research Reports
- Technological and research/development resources
  - Special SW for security purposes
  - Exploration of methodology and development of tools
  - Steganography, investigation of *data mining* methods, etc.

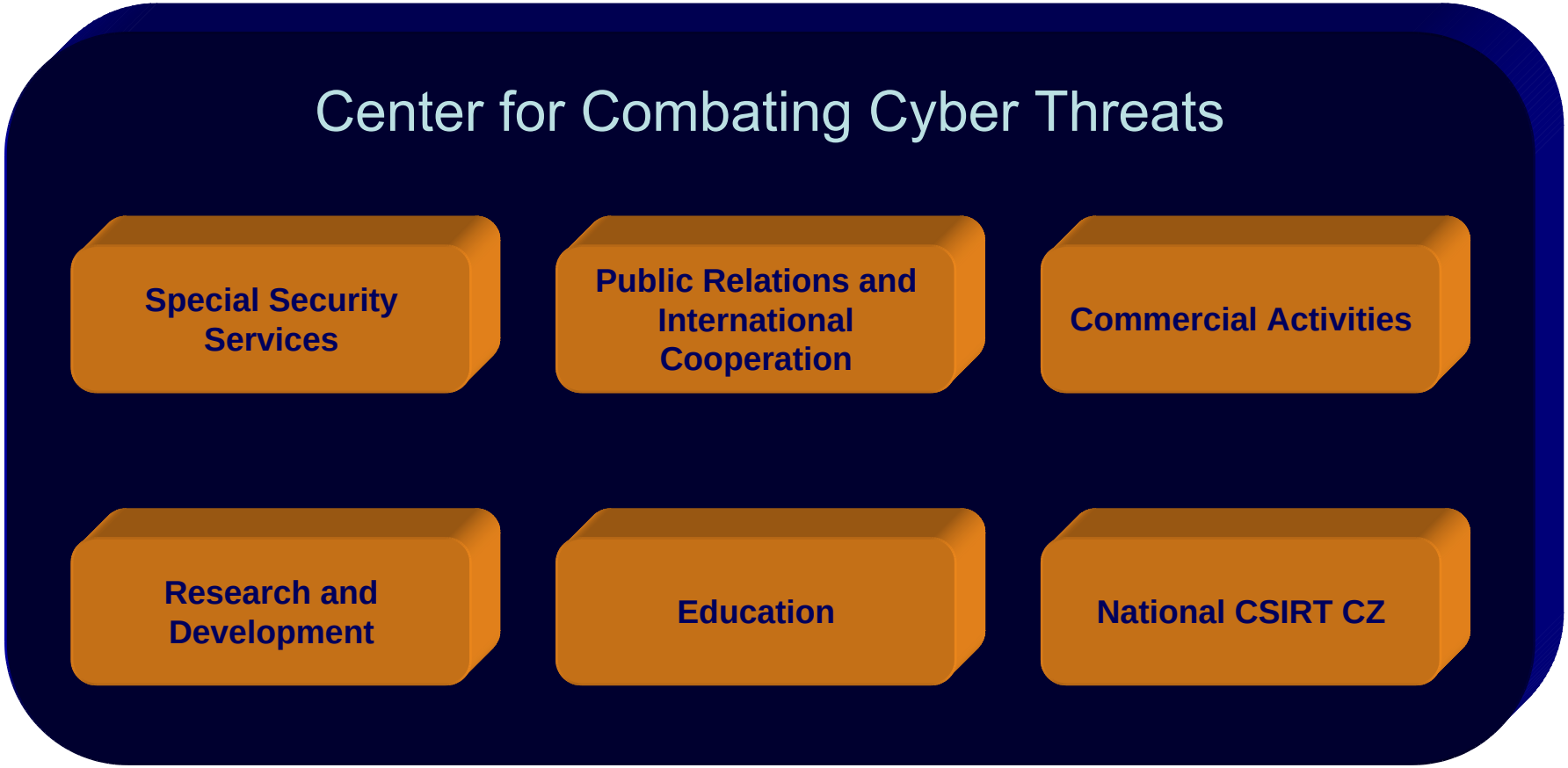
# Center for Combating Cyber Threats



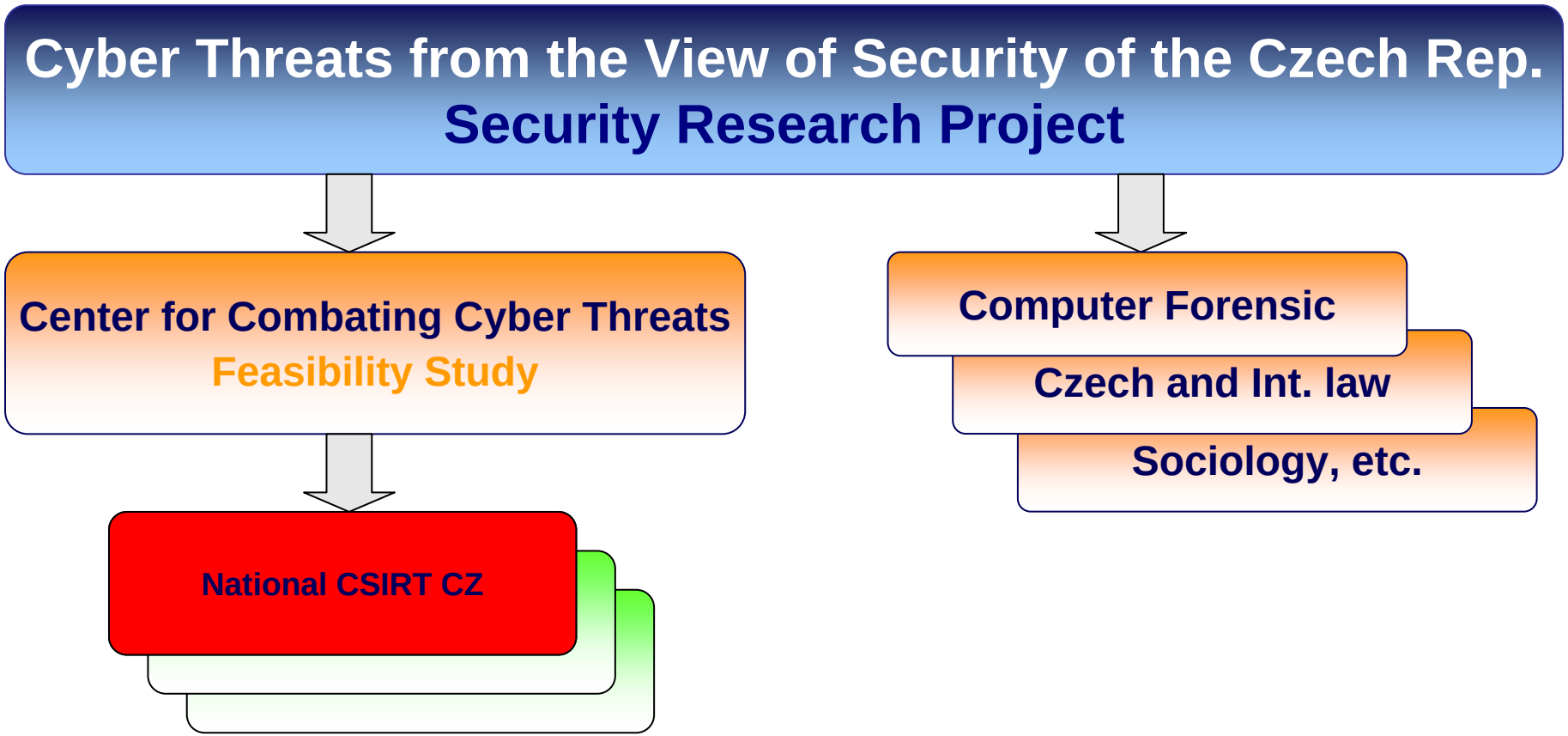
# Division V
# **Education**

- Prepares educational material
- Conducts courses
- Provides education via e-learning
- The main users are
  - Ministries
  - Courts
  - Prosecutors
  - Police
  - Etc.

# Center for Combating Cyber Threats



# Czech activities in Cyber Security



# History ...

- 1999 – The Millenium bug (Y2K) initiated first moves toward Cyber Security
- 2001 – The Ministry of Interior – conception of national security
  - First attempt to set up National CSIRT
- Jan 2002 – The Ministry of Informatics was established
- Oct 2006 – Call for proposals “Cyber Threats from the view of security of the Czech Rep.”, by Ministry of Interior
- Jan 2007 – The Call won by the Consortium of Universities, CESNET and NESS
- Jan 2007 – The Ministry of Informatics revocated, The Ministry of Interior take over its role
- Feb 2007 – Memorandum about National CERT of The Czech Republic (Relsie), by Ministry of Informatics
- May 2007 – Project “Cyber Threats” starts

# ISPs in The Czech Republic

- There is about 2000 ISPs in the Czech Republic
- Major ISPs (about 25):
  - Telefónica O2
  - Contactel
  - Bohemia-Net
  - CESNET
  - GTS
  - Nextra CZ
  - UPC

# How do we start?

- Csirt.cz domain registered
- Web building – www.csirt.cz
- Memorandum of understanding between the Project and Czech ISPs
- Join or surrender – clear message to Czech ISPs, volunteer to cooperate on takeoff before you are forced to follow established law
- Cooperation with TF-CSIRT, FIRST...

# Milestones

- Autumn 2007:
  - Signing of Memorandum of Understanding with Czech ISPs
  - Building working group formed by Czech ISP's representatives
  - Apply procedures, policies and tools from CESNET-CERTS
- The pilot project
  - starts on 1st January 2008
  - 2008 – gathering data and experiences about providing National CSIRT
  - 2008 – 2010 – accreditation, FIRST membership
  - Etc.

# Services in 2008

- We need your help
  - We would appreciate copy of reports concerning incidents from Czech networks  to abuse@csirt.cz
- We will provide
  - Incident handling for the networks in CR – initial phase provided by the CESNET-CERTS
  - Serious security incidents reported to the government with recommendation of the appropriate actions
  - Certification of ISP's security teams
  - Workshops and tutoring:
    - For members of “National CERT Team of The CR”
    - For ISP's administrators
    - For everyone who is interested :-)

**Thank you for your attention.**

**Any questions?**