Cyber Cooperation and Exercises

NLO Meeting, 04 March 2015, Athens

Outline

- Overview of ENISA Activities on Cyber Crisis Cooperation and Exercises (C3E)

- Overview of Cyber Europe 2014
  - CE2014 Phase I: technical-level
  - CE2014 Phase II: operational-level
  - CE2014 Phase III: strategic-level

Cyber Crisis Cooperation and Exercises at ENISA

EU Cyber Exercises

- **Cyber Europe 2010**:
  - Europe's first ever EU cyber security exercise
  - Exploratory objectives – no private sector involved
  - Communication and cross border information exchanges
- **Cyber Atlantic 2011:**
  - First attempt for EU-US exercise on cyber
  - Exploratory objectives on transatlantic cooperation
- **Cyber Europe 2012:**
  - Involved MS, private sector and EU institutions.
  - Testing the **EU Standard Operational Procedures (EU-SOPs**)
- **EuroSOPEx 2012**:
  - Small scale (5-7 countries) focused cyber exercises
  - Focused tests of the **EU-SOPs** for Cyber Crisis Cooperation
- **Cyber Europe 2014:**
  - Involved MS, private sector and EU institutions.
  - Testing the **EU Standard Operational Procedures (EU-SOPs**)

2nd Pan - European Cyber Exercise

Studies on cyber crisis cooperation

- Good practice guide on **National Contingency Plans** (2012)
  - Practices, structures and procedures for effective national-level contingency planning

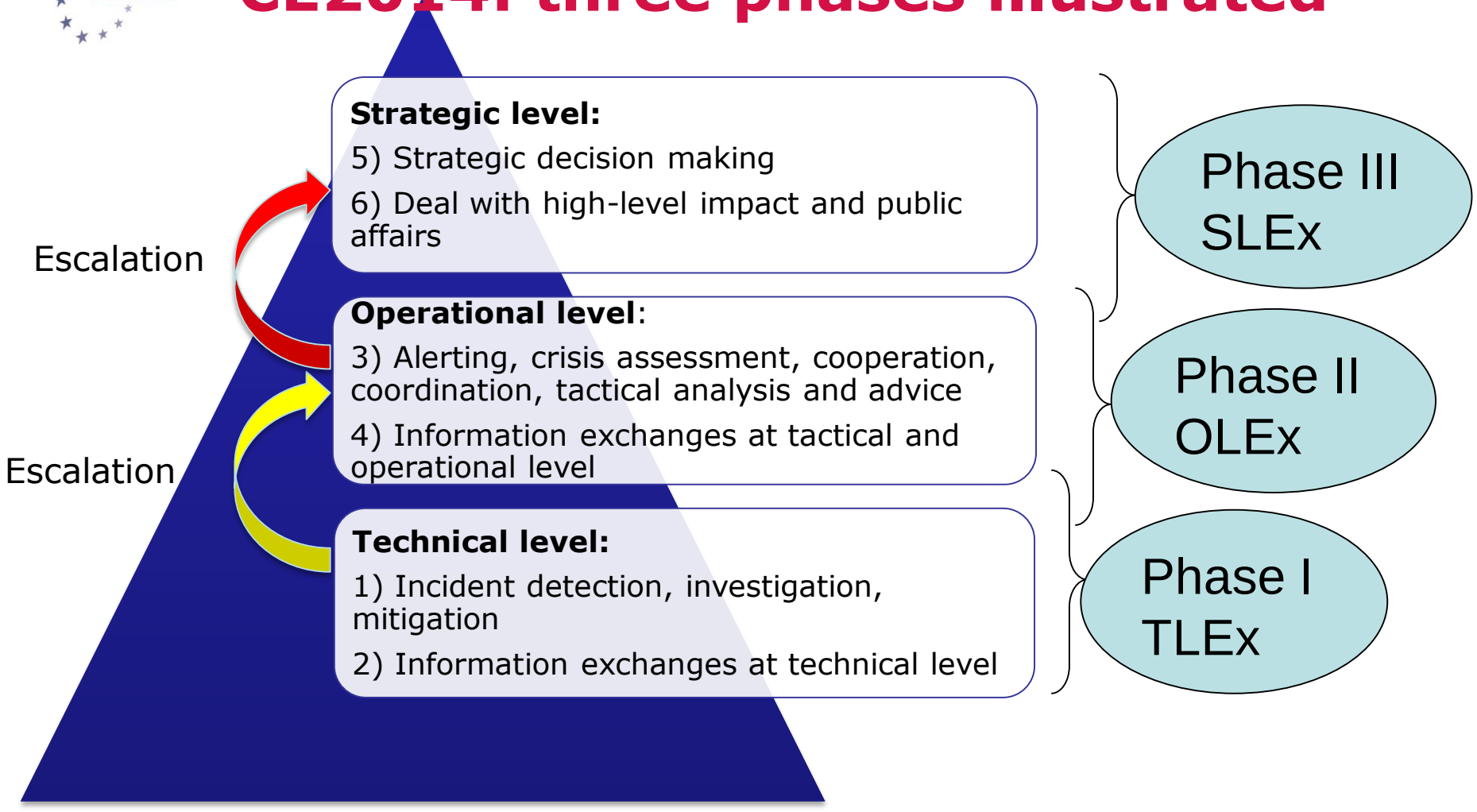
- **International Conference on Cyber Crisis Management** (2012 and 2013)
  - Will be organised again in **2016**
- Study on **Cyber crisis management: a theoretical view** (2014)
- Study on **EU Structures and Frameworks for Crisis Management** (2015)

Overview of Cyber Europe 2014

Cyber Europe 2014: objectives

1. Test cross-country cooperation procedures EU-SOPs (EU-level)
2. Test national-level capabilities (national-level)
3. Explore cooperation between private-public and private-private players
4. Explore the escalation and de-escalation processes (technical-operational-strategic)
5. Explore the public affairs issues

CE2014: three phases illustrated



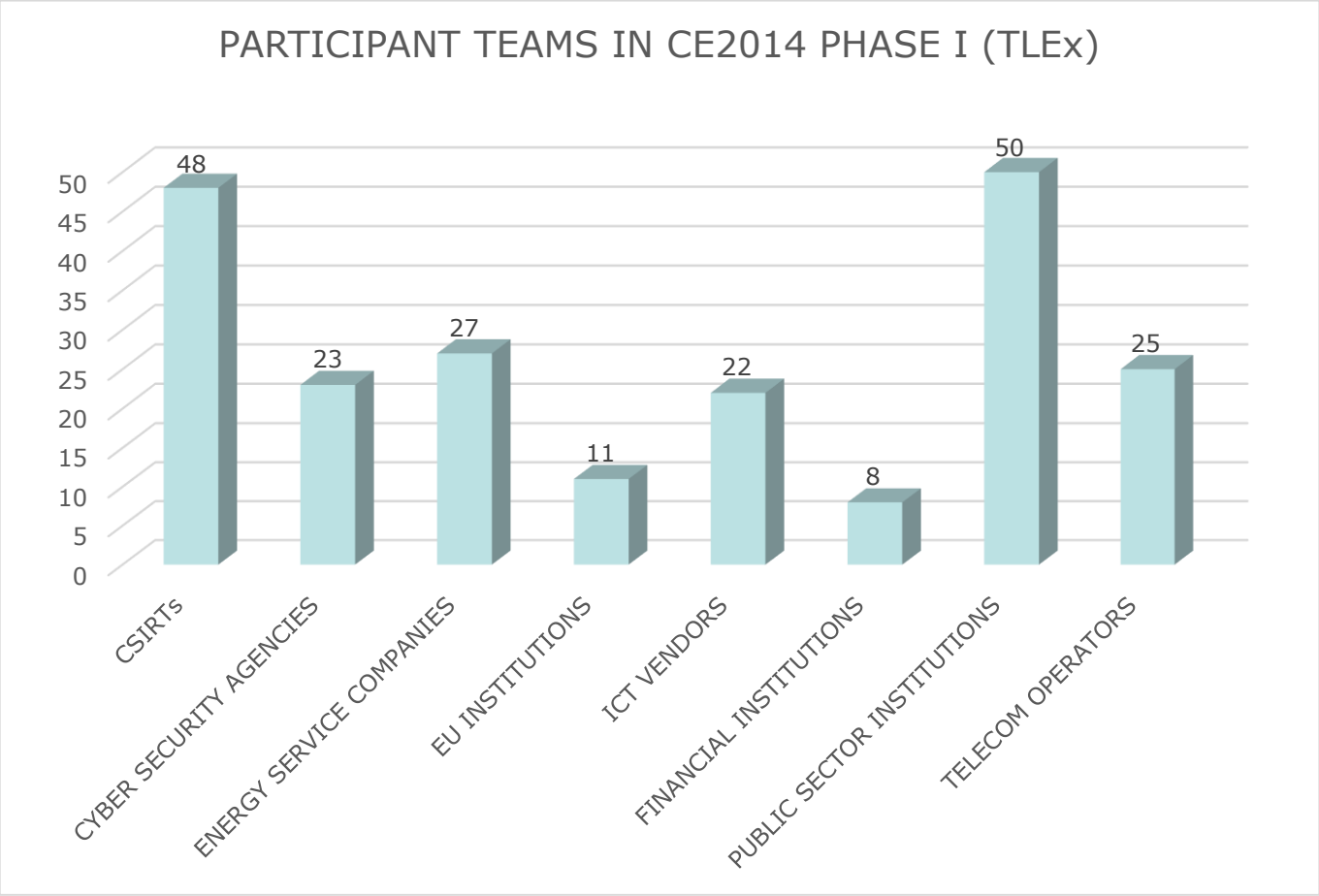
CE2014: three phases

- CE2014 Phase I - TLEx: Technical-level Exercise √
  - 28-30 Apr 2014 (49 hours continuously)
  - Technical cybersecurity exercise
- CE2014 Phase II -OLEx: Operational-level Exercise √
  - 30 Oct 2014
  - Distributed operational-level exercise – EU-SOP cooperation
- CE2014 Phase III -SLEx: Strategic-level Exercise √
  - 24-25 Feb 2015: Workshop and table-top
  - Consultation with decision-making level stakeholders in EU

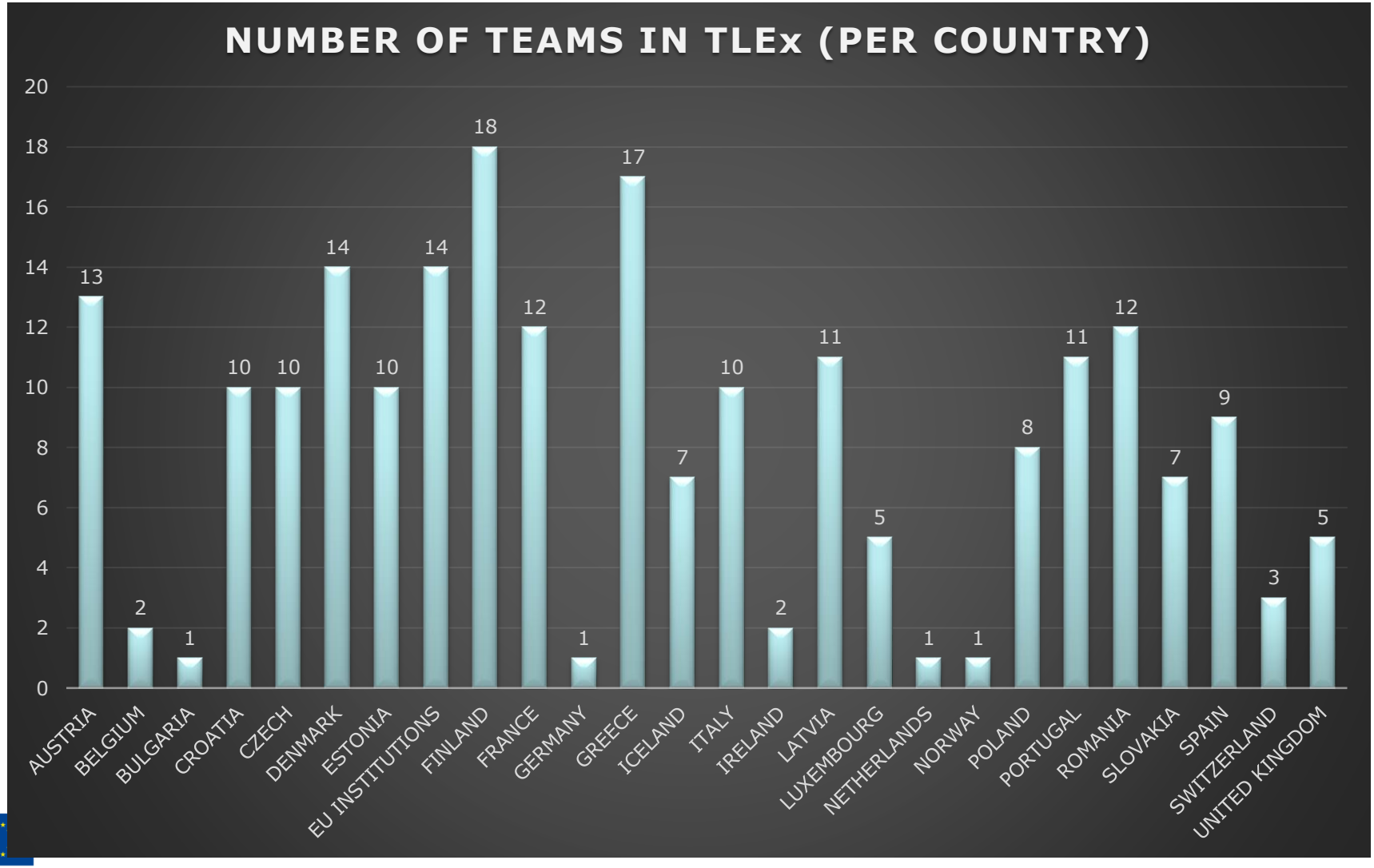
CE2014 PHASE I TLEx

CE2014-TLEx: Participants

Total participants (individuals)	**675**
Teams (organisations)	**214**



Participating Teams per country

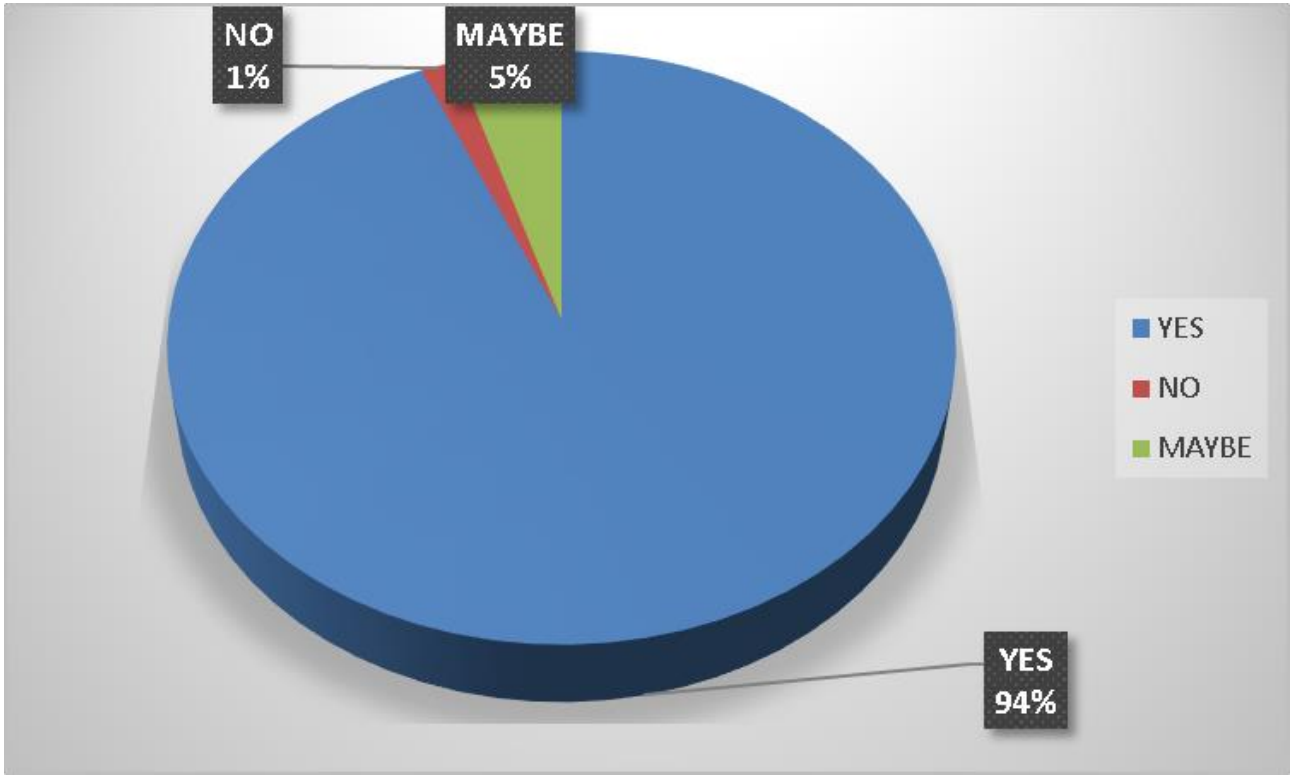


CE2014: Events and Incidents

- Three types of Events and 15 types of Incidents
  - All over Europe
- Types of Events exercised
  - Spreading of malware
  - Analysing cyber espionage campaigns
  - Denial of Service operations
  - Attacks against critical infrastructures

CE2014 TLEx Future

- Would you like the future Cyber Europe exercises to continue having Technical-level incidents?



CE2014 PHASE II OLEx

OLEx (10hour Exercise @ 30 Oct)

TOTAL TEAMS	269
PLAYERS	187
MONITORS	42
MODERATORS	32

TEAMS PER SECTOR	
CSA/CSIRT	121
ISP/TELECOM OPERATOR	41
MINISTRY/E-GOVERNMENT	61
ENERGY COMPANY	50

PLAYER TEAMS PER SECTOR	187
CSA/CSIRT	63
ISP/TELECOM OPERATOR	37
MINISTRY/E-GOVERNMENT	39
ENERGY COMPANY	48

841 individual participants!

CE2014 Video

http://www.youtube.com/watch?v=0AsizcOYAu0

High-level observations from OLEx

- Cooperation at national level went generally very well – a lot of opportunities
- EU-SOPs worked well – can be improved
  - Many lessons learned
- Many exchanges at EU level (within the SOPs)
  - We have no view on the private-private communications
- The crisis got escalated
  - Last EU SOP teleconference mentioned that political level response is needed
- Media responses were good
  - Limited view on this
- The CEP worked efficiently all day
  - Only very few minor issues!

CE2014: Phase III - TLEx

Setup and Participation

- A centralised, moderated, discussion-based exercise
  - Moderators: FR and UK
  - Included presentations from countries and EU institutions
- 58 participants in total (including EU)
  - Public sector only
- 20 Countries played:
  - AT, BE, BG, CZ, DE, DK, EE, ES, FI, FR, IE, IT, LV, NL, PL, PO, RO, SK, SE, UK
- 3 Countries observed:
  - CH, GR, LU
- 9 Countries missing:
  - HR, CY, HU, LI, MT, NO, SL, IS, Lichtenstein

Preliminary observations

- A great opportunity for participants to understand the EU-level Political-level Crisis Management
  - IPCR, Solidarity Clause, Integrated Situational Awareness
  - The boundaries and linkages of our community during an escalated crisis became more apparent
- Perception and interpretation of key terms varies
  - crisis, cyber crisis, escalation etc.
- Multilateral cooperation is still not widely used/acknowledged
  - Bilateral and regional cooperation prevail
- A common operational picture is thought to be useful
  - But the way to develop it is still not widely agreed
- The role of ENISA was discussed
  - Support the cooperation networks and processes
  - Incentivise trust and multilateral cooperation
  - Help building crisis preparedness capacities

Next steps

- CE2014 Final Evaluation Workshop (May 2015)
  - After action report covering all phases of CE2014
  - Follow up on recommendations (e.g., EU-SOPs improvement)
  - Alignment with the NIS Directive (when approved by Council)

- Support the organisation of focused exercises
  - ENISA Cyber Exercise Platform (CEP): exercise playground
  - Member states will be invited to

- Kick off the planning of CE2016 (May 2015)

Questions?

Cyber Crisis Cooperation and Exercises

ENISA

Contact email:

c3e@enisa.europa.eu

CE2014 video

http://www.youtube.com/watch?v=0AsizcOYAu0