2088_03 EU-CoE CyberEast
Project Launching Event

19–20 September 2019, Brussels, Belgium
Organized by the European Commission and C-PRO

Further development of international and public/private cooperation

Why we need Cyber Security

- Providing an open, reliable and secure cyberspace for activities and social interactions (including human rights); BECAUSE the economies and all national systems largely depend on application of information and communication technologies;
- The rise in the use of the IT systems increases the risk of abuse and emergence of new more sophisticated types of cybercrime, which makes the cybercrime one of the more serious threats to national security;

Improving Cyber Security by

- Strengthening the operational capacity, coordination and cooperation among the relevant institutions involved in the combat against cybercrime;
- Establishing an integrated, multidisciplinary approach to secure closer cooperation and coordination between the defense department, institutions involved in the combat against crime, private sector, and other relevant stakeholders;
- Strengthening the national capacities for prevention and protection against cyber attacks, as well as implementing a campaign to raise cyber attack awareness;
- Establishing common **standards**, training, and education of all institutions involved in the development of cyber security.

Interagency cooperation

- **Regular meetings**

- Usually there is a lack of opportunities for deferent entity to meet. There should be a focus on national-level meetings. Cooperation between conference and meeting organizers should be encouraged and meetings should be coordinated as much as possible.
  - **24/7 model for cybercrime**
- It's recognize the importance of a 24/7 model, however the cases where 24/7 availability is really needed are in practice very rare. The emergency cases be dealt with on an ad hoc basis.
  - **Mitigation**
- For mitigation of cybercrime, it is recommended that national law is made clearer. 'Gentlemen's agreements' between CERTs and ISPs have also proved to be valuable. Hosting providers should try to introduce an 'acceptable use policy'.
  - **Education**
- It is recommended that judges, prosecutors, etc., be given specialized education and training on cybercrime matters. It is extremely important that these people are well educated on this topic as they have a decisive role in the investigation and prosecution of cybercrime.
  - **Formal vs. informal cooperation**
- A more mature form of cooperation is clearly needed, arising from both formal and informal networking models, as both models have their advantages.

Interagency cooperation

- **Trust**

- In the end, collaboration and informal cooperation between teams is based on trust between members of teams. It is important that those people know each other and that they meet face to face. Both teams should make an effort to overcome the distance.
  - **Requests for assistance**
- It is important for LEAs to know that they can count on the expertise of a CERT team for assistance in handling certain cases; however, the mandatory handling of criminal cases could damage the agility of the CERT community, which is one of the most valuable assets of CERT teams. It is not recommended to make the response to a request for assistance mandatory by law.
  - **Data protection**
- It is recommended that data protection authorities be asked for permission to handle IP addresses and bank account numbers.
  - **Reporting of cybercrime**
- Generally speaking, all crime should be reported to LEAs. Hence, it is strongly recommended that all cybercrime be reported to the appropriate LEA.
  - **Starting cooperation**
- All entities responsible for cybercrime are different organizations with different roles and priorities, it can be difficult to initiate cooperation. It is very important, though, to make start on this collaboration, even if it is only minor at first.

Activities to streamline and facilitate

- Designing cooperation protocol
- Designing and performing regular and ad-hoc data exchange between all entities
- Designing and propose legislative changes obliging institutions to report incidents
- Establish National register of authorized contact points for information security
- Establish Directory of ICT experts and their competencies
- Coordination meetings and networking with security community
- Organizing Workshops, Exercises and Trainings

- Platform for cooperation

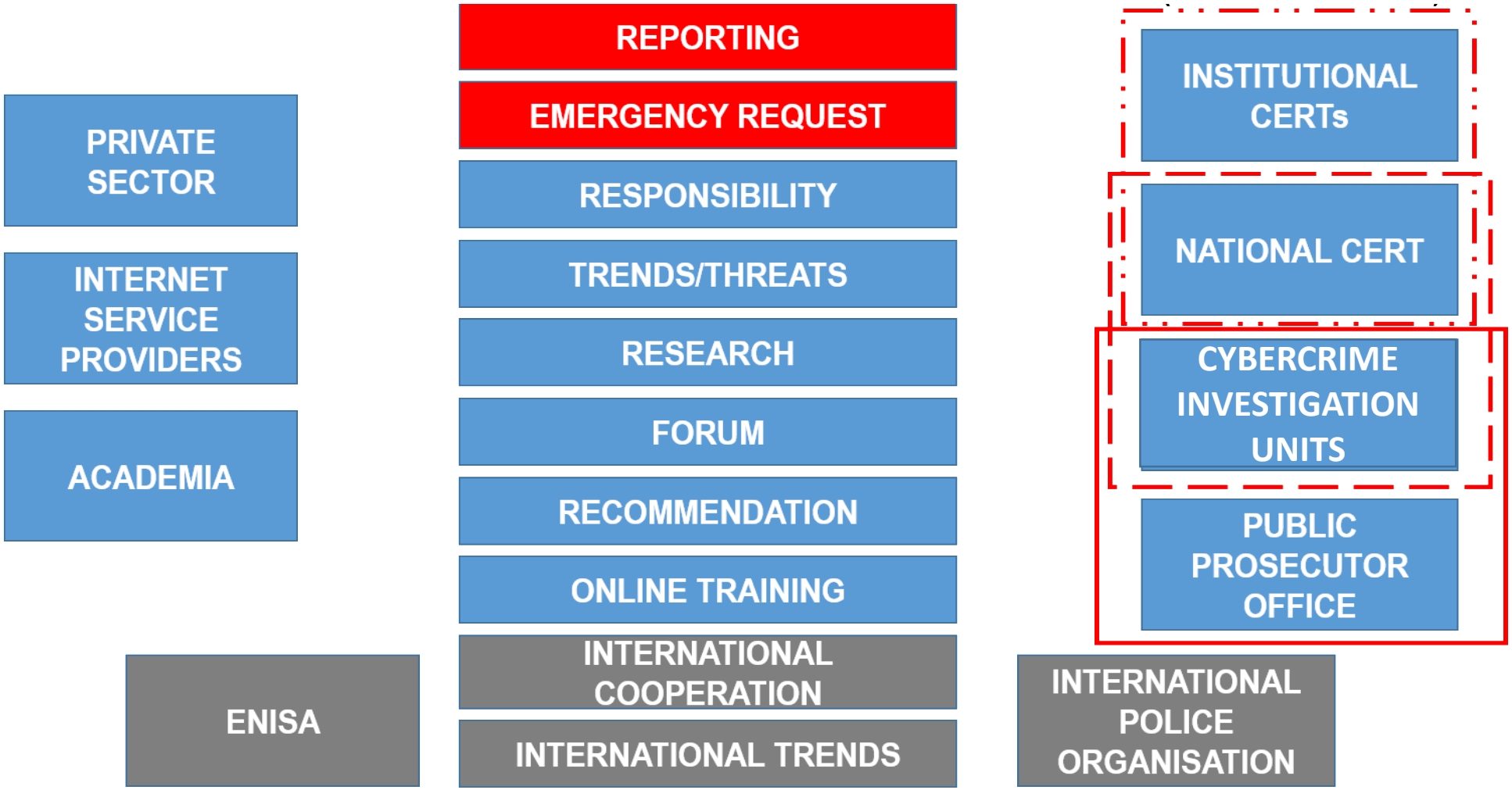
Responsible Institutions and Responsibilities

- Public sector, including the law enforcement,
- Private sector, including the ISPs, and
- Academia.

- Handling computer incidents,
- Giving support for handling the computer incidents,
- Acting as a hub for information exchange,
- Reporting to the national cyber crime unit,
- Preparing and publishing researches and providing recommendations,
- Leading the main role in the international cooperation with the other CERTs,
- Following the recommendations from ENISA
- Using and analyzing the newly published security challenges from ENISA.

- Giving a legal framework in which the case could be investigated and prosecuted,
- Investigating the computer incidents,
- Supporting the entity which system is bridged in handling the incidents,
- Collecting the relevant evidence and making analyses,
- Supporting the National CERT in handling the computer incidents,
- Contributing to the researches and analyses of the incidents,
- International cooperation with the other police services and international police organizations,
- Providing information about the newly identified trends and potential attacks.

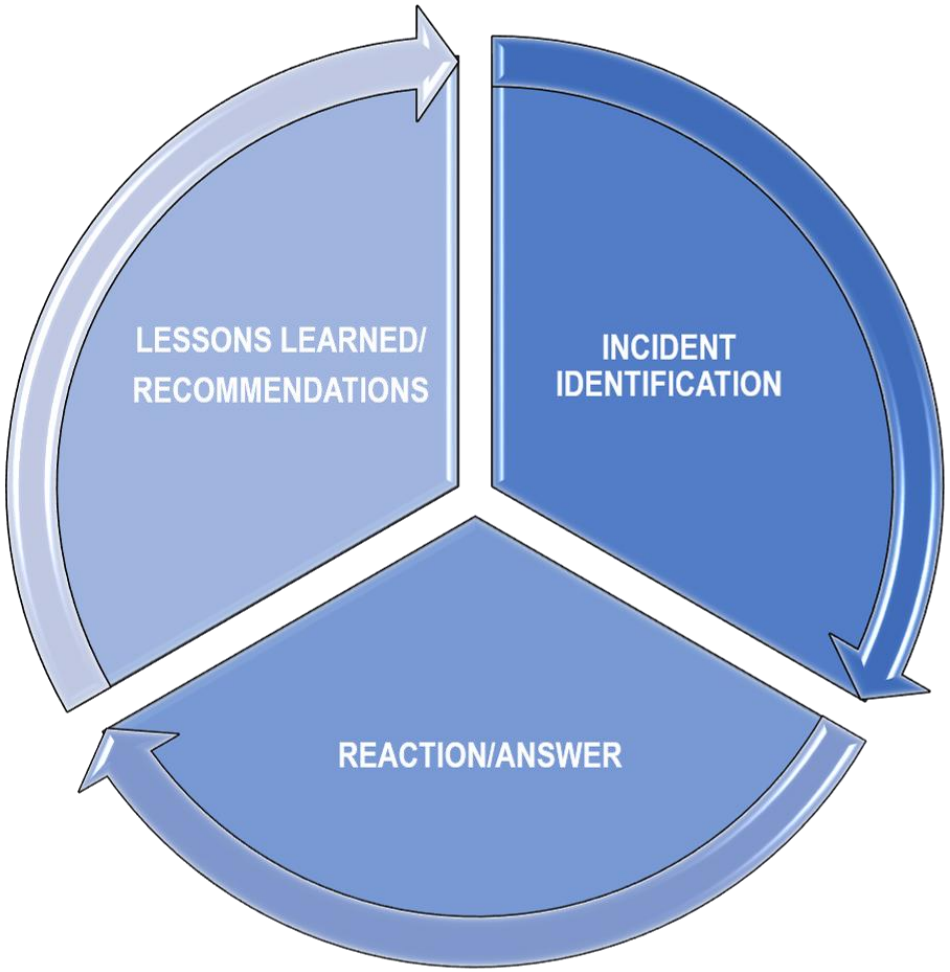
“Platform” for Sharing information



REACTION/ANSWER PROCESS

There are different models for responding the computer incident. The model proposed consists three main steps:

- Exact identification of the situation and understanding,
- Concrete reaction, and
- Recommendation.



Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Questions