Crime prevention policy	
EU- priority	CSE/CAM Child Sexual Exploitation/Child Abuse Materials
Country	SPAIN
Year	2018

1. Overview of the field

Definition of Cybercrime

Cybercrime consists of criminal acts that are committed online by using electronic communications networks and information systems. In this case, include child sexual abuse materials and child sexual exploitation of a person below the age of 18, as well as to the production of images of such abuse and the sharing of those images online.

Assessment of trends and developments

Peer-to-peer (P2P) networks and anonymised access like Darknet networks remain the main environment to access child abuse material and the principal means for non-commercial distribution. Also, live-streaming of child sexual abuse concerns a lot because of the profit-driven abuse of children overseas. This criminal activity has a close relation with the sexual tourism from european citizens to Asian Region aimed at getting Child Sexual Abuse Materials.

Recent overview of statistics and research

Technological innovation continues to shape the serious and organised crime in Europe. Criminal actors in the EU display a high degree of creativity in exploiting new technologies in order to have an impact on virtually all types of serious and organised crime.
Innovation in technology enable the prosecution of CSE crimes because of the anonimity given by some private networks and the privacy obteined by using encripted aplication to share CSAM.

2. Crime strategy and coordination

Objectives of the crime strategy

The goals of the CSE crime strategy is focused on victim identification, online markets and for a linked to serious CSE offending, travelling Child Sexual Offenders (TCSO), Child Sexual Abuse materials involving Companies hosting services and the organisation of a victim identification taskforce at Europol.

Role of prevention in the crime strategy on state/regional/local level

Role of prevention is mainly oriented to fight against the different means of committing this crimes and the identification of the victims in cooperation with Europol and Interpol.

Implementation of the policy (which level is responsible for the implementation and how is the implementation coordinated?)

Lines of the implementation are the responsibility of the Spanish Home Office.

Stakeholders (working groups, specialised agencies, partners, etc)

Spain works in coordination with the most important Law Enforcement Agencies and is coordinated with Europol and Interpol as member on their specialized working groups.
On the other hand, Spanish LEAs has relationships with a lot of NGOs who collaborate actively in the prevention and prosecution of CSE crimes.

Participation in European/ international networks, working groups, etc.

Spain co-drives the CSE EMPACT Group in Europol. At the same time, Spain is represented in the expert group of CSE in Interpol.
In order to enhance the fight against this sort of crimes and the implementation of new methods of prevention, these officers are involved in some Projects with important stakeholder in the Cybersecurity.

3. Good practices

Overview of recent good practices, prevention programs, etc.

There are some operative action programs in order to prevent the download of CSAM through P2P networks, the coordination of undercover operations in anonymous fora and the development of a good practices in this investigation.

In addition, it remains important victim identification activities as one of the most relevant actions in the CSE crimes.