Crime Prevention Politics

EU- priority	Cybercrime Child Sexual Exploitation Credit Card Fraud Crimes depending on ITCs
Country	SPAIN
Year	2018

1. Summary

Cybercrime Definition –Computer Crimes.

There is no definition or specific type of "cybercrime" in the Spanish legislation, however, it can be understood as all those punishable actions that have the use of new technologies in common, either as a means (child pornography, hate crimes...), object (hacking, phishing, spamming) or protected legal right.
The Spanish Penal Code typifies a list of unlawful actions related to computer crimes that threaten different protected legal rights.

Assessment of trends and developments

The Spanish authorities listed the following main trends with regard to current cybercrime:

- sexual exploitation of children on the Internet;
- online fraud (Payment fraud);
- cyber attacks.
- online criminal markets
- the convergence of cybercrime and cyberterrorism.
- cross-cutting cime factors, mainly social engieering techniques and cryptocurrencies.

The National Police is fully aware of this ever-increasing and unstoppable demand and the great importance that citizen collaboration and fluent relationships with different groups of people have in terms of crime **prevention**. Therefore, it counts on a Central Unit solely dedicated to Community Policing in order to meet every social need countrywide and to adapt policing to this changing society.

Through the implementation of different preventive activities aimed at citizens, the Central Unit of Community Policing fosters commitment and collaboration of groups for their own safety and thus they take their share of responsibility.

Through citizen relations and the establishment of a solid bidirectional communication channel, it is possible to get to know first-hand the problems and proposals of the citizens regarding security matters. This allows the institution to develop a faster and more effective response when applying various strategies, programmes and safety plans related to those issues that concern our society the most.

Recent overview of statistic and research data

The State Prosecutor's Office and the Public Prosecution Service prepare annual reports compiling statistical data on prosecutions and on all types of criminal activity respectively. The 2018 report were also published recently.

Ministry of Interior has published recently the “Study about Cybercrime in Spain 2018” with all the statistics reported for Spanish LEAs

When it comes to the **Director Plan** (in school centres), some of the preventive activities carried out during the 2017-2018 school were meetings, talks and presentations addressed to the Educational Community. The total amount of talks given about "Internet Risks" was 14,862.

In reference to the **Elder Security Plan**, there have been 1898 preventive activities during 2017 aimed at people over 65 in order to make them know the criminal reality that is affecting them when it comes to Cybercrime. They have been provided with tools of self-protection and a direct contact with a police expert.

With regard to **Hate Crimes**, it is the so-called "hate doctrine" that many criminal groups spread through the Internet and social networks. This phenomenon of "cyberhate" applies to any use of information and communication technologies (internet, mobile devices, etc.) to spread anti-Semitic, xenophobic, homophobic, racist, intolerant messages or information, etc. The National Police -through the talks and meetings of the delegates- works to help and inform, in the event of a criminal offence is taking place, and about how to denounce all these antisocial behaviours.

Within the scope of the **Safe Tourism Plan**, the preventive activities carried out during 2017 were 8150, aimed at the different professional services directly or indirectly related to tourism (frauds related to apartment rentals during vacations, identity theft –phishing–, etc.)

Through the **Citizen Groups Programme** –in charge of the protection and safety of potentially vulnerable groups and minorities to become victims of crimes– 14,889 activities have been carried out focused on prevention.

Among all these, the activities related to cybersecurity and prevention of breaches committed making use of new technologies play an important role, and there is a growing demand and interest of citizens in this regard.

Other national priorities besides child sexual exploitation, payment card fraud and cyber-dependent crimes?

- online criminal markets

- the convergence of cybercrime and cyberterrorism.

- cross-cutting crime factors, mainly social engieering techniques and cryptocurrencies.

2. Strategy and Crime Coordination

Objectives of the crime strategy

The guiding principle of the National Cybersecurity Strategy is ensuring the appropriate coordination and cooperation among all the public authorities and also involving the private sector and citizens when necessary. The investment in prevention is growing in order to reduce the possibility of the citizens to become a victim of any kind of crime.

Role of Prevention in Crime Strategy country-/region-/localwide

The prevention is a fundamental pillar. There are many initiatives and good practices in terms of awareness-raising campaigns within schools, training of practitioners and mass media campaings:

- Giving a coordinated and efficient answer to issues related to the security of both minors (schools and their environments) and the rest of groups of Spanish population (the elderly, tourists, vulnerable groups of people, etc.)
- Fostering the awareness of the society about police resources for crime prevention and victims’ protection.
- Enhance the trust of society in the National Police and the development of proactive behaviours to reveal the situations and crimes of which they may be victims.
- Participate in the training and education of citizen groups, as well as making them conscious of the risks associated to the use of new technologies by promoting the organization of activities, talks and lectures given by police experts.
- Designing permanent coordination instruments and mechanisms throughout the national territory, between police experts and the community.
- Improve the police response when interacting with people and the groups of population who ask for their intervention.
- Collaborating with other public institutions with responsibilities in this area.
- The information that comes from the problems of security reported by different citizen groups –once analysed and properly treated– constitutes one of the fundamental tools used to implement crime prevention plans or programmes.

Implementation of the Politics (What level is responsible for the implementation and how is it coordinated?)

Spain has a robust National Cybersecurity Strategy adopted in December 2013 by its National Security Council. The National Cybersecurity Council, which is a political body with a broad and flexible composition, bears responsibility for the implementation of the National Cybersecurity Strategy, therefore It is the responsible for this issue.

Coordination and cooperation is specifically needed taking into account the complexity of the task, both in terms of the number of actors involved in acting against cybercrime and of the way in which competences are shared, especially among law enforcement authorities (LEAs) and different coordinating bodies.

The National Centre for the Protection of Infrastructure and Cybersecurity (CNPIC) as a part of the State Secretariat for Security of the Ministry of the Interior is responsible for the coordination in cybersecurity matters. It maintains close relations with public administration at central and regional level and private companies that manage and own infrastructure. It consists of members of the LEAs. To anticipate and respond to cyber attacks, CNPIC has teamed up with INCIBE to form the Computer Emergency Response Team (CERTSI) which deals specifically with cybersecurity of critical infrastructure, and provides a response in the event of a cyber attack on critical infrastructure. CERTSI is in charge of dealing with cyber attacks against companies, the academic network and citizens, and has direct contact with critical infrastructure operators for this reason. As a part of the CNPIC, the Cybernetics Coordination Office (Oficina de Coordinación Cibernética - OCC) serves as the Ministry of the Interior's point of contact for all issues related to cybersecurity. The OCC provides the link between Spain's LEAs and the Computer Emergency Response Team (CERTSI) as a part of INCIBE.

From operational perspective Spain has two different LEAs acting in the field of preventing and combating cybercrime, there is a national system in place enabling operational information to be uploaded onto a general platform (CITCO) by both actors, the National Police and the Guardia Civil. When hits are detected there is a special Protocol to resolve the issue.

The General Direction of National Police has named this Unit (**Central Unit for Community Policing**) responsible for the implementation, development and coordination of the *Prevention Plans* in National Police countrywide. In every province, a police expert responsible for the *Prevention Plans* coordination in their area has been also designated. These experts are the permanent points of contact who provide the Spanish society with technical advice or specialised police support when it comes to prevention and security.

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

Coordination and cooperation is specifically needed taking into account the complexity of the task, both in terms of the number of actors involved in acting against cybercrime and of the way in which competences are shared, especially among law enforcement authorities (LEAs) and different coordinating bodies.
Spain has a complex system of different CERTs in both the public and private sector. Although they co-exist in parallel, each institution is able to manage cyber events effectively, with technical and tactical contributions to investigations.
The work of the National Institute of Cybersecurity (INCIBE) should be specifically praised with regard to its role in improving the level of IT security in industry and among the public, with activities in the field of prevention and awareness-raising.

Spain has developed public-private partnership in the IT sector with various actors. The policy is to target the big private operators and set up a good partnership with them. However, reporting mechanisms need to be strengthened and to cover cooperation with the small operators as well.

In order to improve cybersecurity in the preventive aspect, and taking into account the good results brought by the implementation of prevention plans, working groups with public and private companies and institutions have been created in order to focus on the following areas: teaching, research, health and telecommunications.

In order to improve prevention and provide as many citizens as possible with security advice, the Central Unit of Community Policing (National Police) is formed by different working groups –with public and private companies and institutions dedicated to cybersecurity, protection of people with disabilities, etc. These groups create campaigns and informative and contents adapted to each group through joint prevention strategies.

Participation in European or International Networks, work groups, etc.

The National Police and Guardia Civil are represented in the most important agencies, institutions and networks –in the country, in Europe and internationally– related to the activity of the Law Enforcement Agencies, such as EUROPOL (J-CAT, EMPACT CSE, EMPACT PCF, EMPACT CAIS, EUCTF, ECTEG, Virtual Currencies Working Group, iTOM), INTERPOL (Digital Forensics Expert Group, Americas Working Group, Working Group on Darkweb and Cryptocurrencies), CEPOL, ENISA and Council of Europe (TC-Y)

Additionally, the National Police leads and coordinates the Spanish delegation of “Law Enforcement Working Party”, depending on what there are many groups of experts -in different areas related to security-. Guardia Civil also takes part in LEWP.

3. Good Practice

Review of Recent Good Practice, Prevention Programmes, etc.

The National Police has organised the total amount of 56,715 prevention activities during 2017 (meetings, talks and lectures, mass-media interventions and further activities).

The UAM (Autonomous University of Madrid) - Over two years, the UAM's ICFS managed an EU-funded project aimed at strengthening public-private cooperation on fighting cybercrime. In particular, it sought to link up academia, LEAs and private companies through the creation of a cybersecurity centre of excellence.

Guardia Civil is working to develop both forensic and investigative tools, a notable instance being its work with the universities, which has led to the development of the 'Quijote' programme for searching for child pornography in P2P networks, and various forensic tools that allow identification of internet users who download child pornography files.

Guardia Civil has “Naviga seguro” (surf securely) programme, which is a tool targeting children and minors. The programme has been worked out in cooperation with the Walt Disney company and presents some basic rules on safe Internet surfing illustrated by some Disney film characters.