# Awareness of Relevant National Authorities

Overview of key national authorities related to cybercrime reporting in the EU.

The roles and responsibilities of these authorities and how they coordinate with EU-level bodies.

# Authority Profiles: Introduction to Key National Cybercrime Authorities

In the European Union, each member state has established authorities dedicated to handling cybercrime. These include national cybercrime units within law enforcement agencies, cybersecurity centers, and sometimes special branches within national security agencies. For example, the UK's National Cyber Security Centre (NCSC) plays a pivotal role in cyber threat assessment and response. Other countries have similar institutions, each with a specific mandate for cybercrime prevention, investigation, and response.

Let's delve into more examples of national authorities in various EU member states dedicated to cybercrime reporting and response:

**Germany:** The German Federal Criminal Police Office (Bundeskriminalamt, BKA) has a specialized department for combating cybercrime. This unit focuses on cyberattacks against critical infrastructure, cyber espionage, and other serious cyber offenses.

**France:** France's National Gendarmerie hosts a specialized cybercrime unit known as the Cybercrime Fighting Center (C3N). This unit plays a key role in investigating cybercrimes, digital forensics, and collaborating with international partners.

**Spain:** In Spain, the National Police Corps operates the Technological Investigation Brigade (BIT), focused on tackling various forms of cybercrime, including online fraud, cyber terrorism, and child exploitation on the internet.

**Italy:** The Postal and Communications Police (Polizia Postale e delle Comunicazioni) is Italy's primary agency for handling cybercrime. Their responsibilities include dealing with online fraud, copyright infringement, and cyberbullying.

**Netherlands**: The Netherlands has the High Tech Crime Unit (HTCU) within its National Police, which specializes in combating complex and high-impact cybercrimes, including cyberattacks on government institutions and large corporations.

**Sweden:** The Swedish Police Authority includes a division for IT-related crimes, focusing on cybercrimes such as online fraud, hacking, and illegal online content.

# How do these bodies function and interact with EU-level organizations

National cybercrime units in EU member states engage in a multi-faceted relationship with European organizations such as Europol's European Cybercrime Centre (EC3) and Eurojust. This collaboration is essential due to the inherently international scope of cybercrime, which often transcends national boundaries.

**1. Europol's European Cybercrime Centre (EC3):** EC3 plays a crucial role in enhancing the capabilities of member states to combat cybercrime. It offers:

a. Strategic Support: EC3 provides analyses of cybercrime trends, helping national authorities adapt to evolving threats.
b. Operational Assistance: It coordinates cross-border investigations and offers technical expertise in complex cases.
c. Capacity Building: EC3 conducts training and exercises to improve the skills of national law enforcement officers.
d. Forensic Support: It aids in digital forensics, crucial for gathering evidence in cybercrime investigations.

**2. Eurojust:** Eurojust's role complements that of EC3 by focusing on the judicial aspect of tackling cybercrime:

a. Judicial Coordination: Eurojust facilitates cooperation between the judicial authorities of different member states, helping to navigate the varying legal systems.
b. Legal Assistance: It provides guidance on legal questions, ensuring adherence to international laws and treaties.
c. Joint Investigation Teams: Eurojust supports the formation and operation of Joint Investigation Teams (JITs), enabling coordinated investigations and prosecutions across member states.

**3. Information Sharing:** Both EC3 and Eurojust serve as hubs for information exchange. They collect, analyze, and disseminate data on cybercrimes and cyber threats, fostering an environment of shared intelligence.

**4. Joint Operations:** National authorities often collaborate with EC3 and Eurojust in joint operations. These operations can target cybercriminal networks, dismantle illegal online marketplaces, and respond to large-scale cyberattacks.

**5. Policy Development:** National bodies work with these EU organizations to influence and shape cybersecurity policies and strategies. Their insights and experiences are vital in formulating effective, continent-wide cyber defense mechanisms.

**This project was funded by the European Union's Internal Security Fund - Police Programme under Grant Agreement No 101038738**