# Setting the scene on cybercrime: trends and new challenges

5 July 2019

The level of digitalisation in our societies is increasing every day and so, unfortunately, is cybercrime. This situation requires law enforcement and prosecution practitioners to constantly adapt their expertise, tools and practices to effectively and efficiently respond to this change. Today, Europol and Eurojust published a **joint report** identifying and categorising the current developments and common challenges in combating cybercrime, which fall into five different areas:

1. **Loss of data**: electronic data is the key to successful investigations in all the cybercrime areas, but the possibilities to obtain such data have been significantly limited.
2. **Loss of location**: recent trends have led to a situation in which law enforcement may no longer establish the physical location of the perpetrator, the criminal infrastructure or electronic evidence.
3. **Challenges associated with national legal frameworks**: the differences in domestic legal frameworks in EU Member States often prove to be serious impediments to international cybercrime investigations.
4. **Obstacles to international cooperation**: in an international context, no common legal framework exists for the expedited sharing of evidence (as does exist for the preservation of evidence). There is also a clear need for a better mechanism for cross-border communication and the swift exchange of information.
5. **Challenges of public-private partnerships**: cooperation with the private sector is vital for combating cybercrime, yet no standardised rules of engagement are in place, and investigations can thus be hampered.

**Borderless crime calls for international measures**

All these challenges are of special relevance to combat cybercrime, but affect other crime areas as well.

The very nature of cyberspace means that cybercrime is borderless. Consequently, international measures are required to address the current challenges. Significant progress has been made since the publication of the last report in 2017. Key components of this progress include enhanced cooperation between all parties involved and providing platforms and networks dedicated to sharing knowledge and best practice, such as the European Judicial Cybercrime Network (EJCN) and the Joint Cybercrime Action Taskforce (J-CAT).