Ransomware: the EU perspective

CATHRIN BAUER-BULST
RANSOMWARE: THE EU PERSPECTIVE

Ransomware is not only a major threat in the cyber realm, it also brings together most of the challenges faced by police and justice when conducting cyber investigations. The international nature of ransomware, the complexity of the criminal business models, the variety of malevolent actors involved, and the high level of technicity in every phase of ransomware attacks impose an encompassing approach to increase deterrence.

First, we need to adapt international rules to the evolving reality. The second additional protocol to the Budapest Convention sets common principles to fight cyber-attacks, beyond the EU, and the e-evidence legislative package will allow a swift access to digital evidence irrelevant of data storage location. Further reflection is needed on how to enhance the intelligence picture on malevolent cyber activities, notably through better reporting of cybercrime.

The Commission is also committed to reinforce coordination and cooperation mechanisms, to facilitate exchange of information, to enhance public-private cooperation and develop partnerships with cybersecurity actors and other relevant stakeholders, and finally, to ensure that police and judicial authorities have the relevant capacity, including tools and skills, to fight ransomware.