Council of the
European Union

Brussels, 16 September 2021
(OR. en)

11719/21

LIMITE

COSI 170
ENFOPOL 320
CYBER 235
JAI 987

NOTE

From:	Presidency
To:	Delegations
Subject:	Enhancing the role of law enforcement in cybersecurity

Cybersecurity can be defined in slightly differing ways[1] but it is oftentimes regarded as the overall protection of networks, government or otherwise, from malicious attacks and cyber threats to safeguard critical information. Cybercrime can be defined as actions by criminals trying to exploit human- or security-related weaknesses in the cyberspace to steal money or data including passwords and personal data. A general perception is often also that a crime needs to have taken place before law enforcement can take up its role to investigate the crime with an online dimension as well as to provide the digital forensics expertise in order to bring those responsible to justice.

[1] The Cybersecurity Act (Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013) defines cybersecurity as "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats".

Law enforcement carries out a variety of tasks ranging from determining whether a cybersecurity incident has a criminal nature to conducting the investigation of cybercrime cases and reaching out to the victims of such cases to advise them and ensure their collaboration. It is clear, however, that this role can and should be even more expansive especially in the current setting where polycriminality and holistic threats against the internal security of individual Member States or the EU as a whole are often difficult to pull apart and their origins or objectives often tricky to identify. This links to the discussion on hybrid threats and comprehensive security: before we attribute attacks, it would be even more beneficial to allocate roles to different actors so that each could play a part in countering and addressing these threats with the aim of them never even materialising.

In this context, it would be useful to link law enforcement to a more integrated approach to cybersecurity - and to ensure that law enforcement is not forgotten when cybersecurity strategies are prepared and relevant roles allocated. Law enforcement is an expert on accessing and safeguarding data and evidence, which is often at the very centre of malicious attacks, whether on critical networks or personal computers, and it could contribute towards not only investigating but also effectively countering and preventing these attacks. Law enforcement is well versed in the constantly evolving modus operandi and specific techniques of cyber criminals but also in analysing trends and threats when it comes to the overall criminal patterns as well as the particularities of specific types of crime, including cybercrime and many forms of cyber-facilitated crime.

There are various ongoing developments that concern the relationship between law enforcement and cybersecurity, such as the negotiations on the Directive on measures for high common level of cybersecurity across the Union (the NIS 2 proposal)[2] as well as the recent Commission Recommendation on a Joint Cyber Unit[3].

---

[2] COM(2020) 823 final. On 16 December 2020, the Commission issued the NIS 2 proposal as one of the actions foreseen in the EU's Cybersecurity strategy for the digital decade. On the basis of article 114 TFEU, it aims to further improve the resilience and incident response capacities of public and private entities, competent authorities and the Union as a whole. The proposal significantly broadens the scope of the current Directive; among others, it strengthens the security requirements imposed and streamlines reporting obligations, contains provisions addressing information sharing and cooperation on cyber crisis management at national and Union level, provides for regulation of databases of domain registration data.

[3] https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit

It is important to note that the NIS 2 proposal is handled by the Horizontal Working Party on Cyber Issues (HWPCI). This COSI discussion is intended to contemplate on relevant policy and practical aspects to the internal security communities and their activities to allow for a better understanding of the proposal's wider implications. It is thus not the intention to discuss the legal provisions of the NIS 2 proposal since the negotiations are handled at the HWPCI.

Encryption

Encryption and specifically the need to strike a balance between the commercial, legal and societal interests concerning secure means of electronic communications, and the need for law enforcement to access the data it needs for relevant criminal investigations, is a main topic in the JHA context.

As stated in the Council Resolution on encryption adopted on 14 December 2020, encryption is a central vehicle for fundamental rights in the online context. While encryption increases the privacy of users, it can have an impact on the exercise of online powers of law enforcement and judicial authorities to detect, investigate and prosecute criminals. It is clear that this complex question can only be addressed through a transparent dialogue between various actors. This is all the more important with the deployment of new technologies such as the roll-out of 5G standards and the increasingly wide-spread use of end-to-end encrypted electronic communication applications.

In the recently adopted EU Strategy to tackle Organised Crime[4], the Commission underlined the importance of ensuring lawful access to encrypted information, while maintaining the effectiveness of encryption to protect fundamental rights, including freedom of expression, privacy and data protection. In line with this, the Commission will suggest a way forward in 2022 to address the issue of lawful and targeted access to encrypted information in the context of criminal investigations and prosecutions.

Encryption is an important element also in the field of cybersecurity. For example, the NIS 2 proposal lists key elements that all companies must address or implement as part of the measures they take, including incident response, supply chain security, encryption and vulnerability disclosure. If introduced, cybersecurity and cyber resilience of the companies in the scope of the proposal, including the whole digital infrastructure, will be increased, however the data in their possession or hosted/administered by them could also become increasingly inaccessible to law enforcement, due to strengthened mandatory encryption.

---

4 8085/21

At the same time, the proposal states[5] that the use of end-to-end encryption should be reconciled with the Member States' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law. Furthermore, it goes on to outline that solutions for lawful access to information in end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime. Thus it remains vital to discuss law enforcement access to data from all relevant angles and in line with all the legislative changes that may have an impact on this ability in the future.

Access to WHOIS data

Another topic that is crucial for law enforcement and that has come up also in the NIS 2 proposal and the ensuing negotiations is access to WHOIS data. The main issue in this context is establishing and ensuring the necessary legal basis to access WHOIS data swiftly as well as sufficiently addressing those issues that are crucial for allowing and ensuring law enforcement access in a timely manner.

It is indeed important to assess ways in which law enforcement and other public authorities' access to WHOIS data, at scale and in the appropriate timeframes, could be restored. Relevant authorities could be clearly referenced as legitimate access seekers to better respond to, as well as prevent, major incidents. Providing simple, secure, needs-based access to this (previously freely available) information as speedily as possible needs to be in any case realised taking into consideration fundamental rights including data protection requirements.

5 The NIS 2 proposal, recital 54

Cooperation between Computer Security Incident Response Teams (CSIRTs) and law enforcement authorities

ENISA[6] has recently analysed in more detail the relationship between three communities relevant in this context, namely CSIRTs, law enforcement and judiciary. According to the report, among the three communities different approaches and different levels of cooperation exist. While operational cooperation, especially in daily interactions and informal communication, seems to be well established, more structured cooperation would be useful in order to achieve a less fragmented information flow between the communities. In addition, there is an even bigger gap in the interaction between CSIRTs and the judiciary than in the cooperation established between law enforcement and the judiciary.

The report identifies some critical areas for cooperation. CSIRTs and law enforcement authorities need to cooperate to decrease the risk of evidence being compromised or destroyed, and they can also usefully cooperate during the analysis of evidence. CSIRTs play an important role in informing (potential) victims of cybercrime and in providing them with information on how to report a crime to the police. Several competences are required for incident handling and cybercrime investigation, and while each community has developed its own set of skills and knowledge, the report finds that each could benefit from the competences of the other communities. Furthermore, strengthened cooperation could also help in tackling the issue of underreporting of cyber incidents of a suspected or known criminal nature to the law enforcement authorities.

Law enforcement authorities are not solely involved in the detection and investigation of cybercrimes. A key component of their role is the *preventive aspect* of cybercrime, and it is here that cooperation with other communities, particularly the CSIRT community, becomes apparent, especially to support preventive strategies.

The synergies between law enforcement authorities and NIS-security actors, including notification of law enforcement authorities, is also a topical issue in the NIS 2 negotiations.

---

6 2020 Report ON CSIRT/LE Cooperation. A study of the roles and synergies among selected EU Member States/EFTA countries, January 2021, ENISA.

Europol's role and reporting of suspected cybercrimes

Law enforcement authorities play a vital role in addressing the main gaps identified in the NIS 2 Impact Assessment, specifically in the joint situational awareness and joint crisis response, in case of cyber incidents of a suspected malicious nature.

More specifically, under the Europol Regulation, the European Cybercrime Centre (EC3) has a mandate to provide the operational and technical support to the EU Member States in cases of cyber incidents of a suspected or known malicious nature concerning two or more Member States. EC3 already has extensive expertise and tried and tested full-scale operational and technical capacity, and it can support national competent authorities in response to cyber incidents and cyber crises of a criminal nature, including via the activation of the EU Law Enforcement Emergency Response Protocol (EU LE ERP) for cross-border cyberattacks.

One of perhaps the best ways to enhance the joint situational awareness and to de-conflict the actions during a cyber incident or crisis response could be to involve Europol's EC3 as an observer in the relevant NIS Cooperation Group Work Streams, the CSIRT Network as well as the Cyber Crisis Liaison Organisation Network (EU-CyCLONe). Since Europol has an extensive criminal intelligence database in its use, cyber incident related information could be cross-checked with the view to quickly identify potential links with other ongoing investigations and relevant intelligence. Additionally, after successful action against cyber threat actors, law enforcement authorities can facilitate the proactive checking of victims on the basis of the lawfully seized databases.

Conclusions

As stated at the beginning, there are various ongoing developments that will influence the way in which law enforcement authorities can cooperate with those actors mainly responsible for cybersecurity nationally, as well as the way in which law enforcement authorities can be integrated into any national frameworks. The proposal and negotiations on NIS 2 are only one embodiment of this development but will play an important part.

In any case, it is important to consider not only the law enforcement needs to access electronic data but also to take into consideration the already established strengths that law enforcement has in this area, especially in relation to detecting, investigating, analysing but also preventing cybercrime and cyber-facilitated crime. Establishing a more integrated approach to cybersecurity would enhance this cooperation and allow the different communities to exploit each other's strengths, taking naturally into consideration legal mandates and national specificities.

The existing national coordination processes should be used to their full extent, in order to ensure that law enforcement needs as well as strengths are recognized and taken into account in the framework of horizontal discussions on cybersecurity, such as in the context of the NIS 2 negotiations taking place at the HWPCI.

Questions to the delegations:

What are the most relevant aspects regarding enhancing the role of law enforcement in cybersecurity?

Which are the concrete ways to realise these aspects?

What should be COSI's role in supporting a closer link between law enforcement authorities and cybersecurity?