Council of the
European Union

Brussels, 6 May 2019
(OR. en)

8983/19

LIMITE

CT 45
COSI 97
CATS 67
ENFOPOL 213
TELECOM 202
CYBER 144

NOTE

From:	EU Counter-Terrorism Coordinator
To:	Delegations
Subject:	**Law enforcement and judicial aspects related to 5G**

Introduction

The deployment of 5G[1] within the EU has gained a lot of attention, lately. The purpose of this paper is to highlight the issues which need to be addressed from a **law enforcement and judicial perspective**[2], which so far are not sufficiently covered in the EU context, although Europol has started to work on this and presented to the Law Enforcement Working Party[3].

In its conclusions of March 22nd, the European Council expressed its support for a concerted approach to the security of 5G networks. In its **recommendation**, adopted on March 26th, the Commission sets out a series of operational measures, with a view to **assessing the vulnerabilities of 5G networks, and better managing these risks, both at national level and European level**. According to a tight schedule, national risk assessments should be completed by the end of June 2019. By October 1, a coordinated EU risk assessment will be presented by the Commission with the support of the European Agency for Cybersecurity (ENISA) and lead to the definition of a cybersecurity toolbox (certification requirements, tests, controls, identification of non-secure products) to be used at national level by the Member States.

---

1 The fifth generation of wireless technology 5G is much more than an evolution of 4G standards. It promises a significantly faster and higher transfer rates through improved mobile broadband connections, shorter response times (latency), ultra-reliable connections and a secure internet of things. 5G will become the backbone of a variety of business models such as interconnected and autonomous driving, telemedicine, fully integrated value chain for the industry, smart cities etc. for which the 4G network, focused on improving data for the mobile phone, isn't powerful enough. In the context of the EU's wish to support European technological autonomy and leadership of European companies in emerging technologies, the excellent position of European companies in the 5G market is good news. The 5G market will be a multi-trillion dollar business. There are only 5 companies serving the radio access network space, two of which are European (Ericsson and Nokia), two Chinese (Huawei and ZTE - the Chinese government has made leadership in 5G and other key future technologies a long term strategic priority) and one South Korean (Samsung). There are no US 5G network companies, although they have big players in related businesses such as the 5G chip business (Qualcomm). Hence, from a leadership perspective in new technologies, it's one of the rare future markets where European (and not American) companies are very well positioned for leadership.

2 Similar challenges may also arise for security services. However, this paper focuses only on law enforcement and judicial authorities.

3 See Europol Position Paper on 5G of 10/4/2019, Council doc. 8268/19

In addition to the cyber security aspects which are dealt with in the Commission's recommendation, issues also arise related to 5G from a **law enforcement and judicial perspective** in particular related to lawful interception of communications[4], which would also be important to consider in the EU context. Some tensions can already be identified between law enforcement operational needs and cybersecurity standards. Is there a technology that simultaneously allows lawful interception and provide the highest standards against malicious attacks? It is critical that all these issues be addressed. More generally, it would be important for the EU to discuss and take a **comprehensive approach** on all dimensions of 5G: competitiveness, technological autonomy, cybersecurity, economic and geo-political issues and law enforcement and judicial concerns. 5G requires a very strong coordination of all these aspects at EU and national level. This note aims to bring law enforcement and judicial aspects into the debate.

Many of the challenges for law enforcement and judicial authorities **can be addressed at national, European or international level**. There is an **urgency**: a lot of the standards, product features and legislation are currently being developed. In particular, the EU Electronic Telecommunications Code of 2018 states that national regulatory authorities can make any approvals regarding 5G dependent on the capability of network providers to carry out monitoring of communications.

1. The 5 G related challenges for law enforcement and judicial authorities

1.1. Lawful interception of communications

5G will make it harder for law enforcement and judicial authorities to carry out lawful interception. Due to 5G's high security standards and a fragmented and virtualised architecture, law enforcement and judicial authorities may lose access to valuable data.

[4] Briefly mentioned in the Commission's recommendation: "Directive 2002/21/EC […] provides that competent national regulatory authorities have powers, including the power to issue binding instructions, to ensure compliance with such obligations."

5G will offer very high security standards. Although **end-to-end encryption** is not yet set out as mandatory in the 5G standards, it cannot be ruled out that it will be included in the standardisation process that will be completed in December 2019. End-to-end encryption would make it impossible to access content in electronic communications, even through lawful interception. In addition, **encryption of IMSI number** (it is the individual number of the mobile phone card) would make it impossible for law enforcement and judicial authorities to identify the mobile devices or location of criminals or persons who pose a serious threat, as well as potential victims or persons facing a threat. Without access to the IMSI number, certain lawful interceptions are not possible. Therefore, metadata normally available via interception (such as location, date, time, call duration, calling and contacted party) would be lost to law enforcement and judicial authorities. In addition, 5G will have **strict authentication processes** (in order to identify a user before access is granted) such as **false-base detection** that will make it harder for law enforcement to investigate via lawful interception without being detected (IMSI catchers which are necessary for interception of mobile devices and location of suspects/victims would be detected).

While **encryption** has already been an issue in the current context, **5G risks making it a lot more serious and widespread**: the **scale** of the problem will change enormously as in the future almost all electronic communications might be encrypted (not just Skype, WhatsApp etc. as today). In addition, today the IMSI numbers are not encrypted, which allows identification and localisation of the device and hence access to other **metadata** through interception.

The second reason why 5G is a challenge for law enforcement and judicial authorities revolves around the **fragmented and virtual architecture of 5G**. Up to now, when carrying out a lawful interception, these authorities deal with a limited number of network providers. With 5Gs **network slicing technology**[5], network and service providers may not - unless they are obliged to do so - have a complete copy of the information available, which would make lawful interception impossible.

[5] Several network and service providers may be able to operate on the same physical infrastructure. For example, one company will provide enhanced mobile broadband, cellular phones for example, another one will provide massive machine type communications and a third one will provide low latency communications. Each service provider will use a customized virtual layer of the same physical infrastructure, with different technical specifications. Relevant telecommunication monitoring information may therefore not be available in every network slice.

Another illustration of 5G **fragmented architecture** is the multi-access edge computing (MEC). In order to improve timely response, MEC will allow mobile phone networks to store and process contents in **decentralised clouds** in the vicinity of network users which can directly communicate with each other. Information will **not necessarily be directed via central nodes**, where lawful interception is currently implemented. Here again, data may not always be available anymore. As network functions and components which used to exist physically become virtual or may be moved abroad, existing measures to protect confidentiality of interception measures (protection against access to or even altering target lists by having specifically vetted staff to carry out the measures on the national territory and physical protection measures such as access restrictions) will no longer work. It may be important to consider the requirement that some functions be carried out within the EU territory.

5G's architecture means that in order to monitor communications in the future, one could require the cooperation of numerous network providers both at home and abroad, under different jurisdictions. While law enforcement authorities currently make requests to a single network provider operating from national territory, in the future with 5G, they may have to deal with multiple service and network providers, including from abroad. The cross-border dimension of 5G technology may increase need for international cooperation, which may increase the time between request and implementation of the interception, with a non-negligible risk of losing a complete copy of the technical information. It would be key to oblige service providers that offer services in the EU to be able to fulfil law enforcement requests, even if it means that they have to reach out to their partner companies abroad.

Without lawful interception, less evidence will be available for prosecution and in the trial, hence the judiciary is affected as well.

1.2. Authenticity of the evidence

Given the multitude of actors involved in providing the 5 G networks, it might be more difficult for the judiciary to establish the authenticity of the evidence and to distinguish fake from real evidence.

1.3. Availability of the network from a law enforcement perspective: Mission critical communications

In the cybersecurity context, one specific use of 5G, related to law enforcement, needs mentioning: **mission critical communications (MCC)**. MCC is defined as the ability of delivering communication means where conventional networks cannot meet the required demands, typically a disaster stricken area or public safety incidents where conventional mobile networks collapse, leaving onsite first responders without any means of communication. Global rise in terrorism threat is pushing governments to improve public safety and **timely coordination between law enforcement agencies, fire departments, emergency medical services** etc. Demand for mission critical communications is high and current dedicated networks, such as terrestrial trunked radio (TETRA) are reaching their limits. With its high reliability and low latency, 5G offers great potential to replace those networks, but it needs to be kept safe from cyberattacks and other external interference. For law enforcement services it will be key to ensure **full and permanent availability of the mission critical communications network,** in particular to prevent distributed denial of service (DDoS) attack and other external interference in network functioning. Europol assesses that, currently, terrorist organisations ability to carry out such an attack is quite limited even though they express their willingness to do so. But with more accessible technologies, it cannot be excluded that such an attack happen in the midterm.

2. Way forward - general considerations

The ability of law enforcement and judicial authorities to carry out lawful interception in a 5G environment needs to be maintained and urgent action is needed. At Europol, a meeting of the heads of telecommunications interception units of 16 Member States took place recently, where the law enforcement related interception challenges in the context of 5G were discussed. Europol presented a position paper to the Law Enforcement Working Party on 15 April 2019[6].

2.1 Standardisation

It may not be too late to **influence standard definition**. It will be important to increase the political pressure to take law enforcement concerns into account. The EU could support development of a common approach to strongly support the law enforcement interests in the standardisation process, including to increase pressure on industry and international standardisation bodies.

[6] See Europol Position Paper on 5G Council doc. 8268/19

The International Telecommunication Union (ITU) mandated 3GPP (Third Generation Partnership Project), a worldwide multi-stakeholder collaboration between groups of telecommunications standard associations the members of which are mostly network suppliers and operators, in order to set out 5G standards. ETSI[7] is the European standard association and its members are participating in 3GPP. It seems that the **next and final release (#16) about 5G standards will be issued in December 2019.** Even though some technical specifications have already been frozen in the previous releases, it is still time to express law enforcement concerns. As part of Release 16, lawful interception standards will be further discussed, as well as the possibility of end-to-end encryption.

The challenge with the 3GPP multi-stakeholder format is that it is **driven by industry interests**: the voting rights depend on the financial contributions without veto right of authorities or unanimity principle. The votes of the companies far outweigh the votes of the law enforcement authorities, even if interests could often be aligned. Law enforcement or other relevant authorities of several Member States[8] are represented in the 3GPP sub-group SA3-LI, which looks at issues related to lawful interception. Increased presence of law enforcement authorities in the sub-group would be important. Law enforcement also needs to keep an overall overview over what's happening in the other subgroups and on the growing role of new players other than telecoms (e.g. satellite providers, wireless carriers etc). While legislation can force companies to fulfil other requirements than those set out in the standards, it would be preferable to incorporate the requirements already in the standards as well.

---

7 Within ETSI, public authorities and regulators are a minority and a very few number of them are familiar with security, let alone law enforcement issues: SGDSN (Security and Defence coordination unit directly attached to Prime Minister) and Interior Ministry (FR), Bunderkriminalamt (BKA is the Federal criminal police agency) and Bundesamt für Verfassungsschutz (BfV, security service) (DE), UK national interception authority for law enforcement, national police (NL) or national defence radio establishment (SE). Other national authorities have an expertise in transports and telecommunication (CZ, DK, AT, SK, FI, DE, FR) or send representatives from ministry of economy and finances (ES, NL, DE, FR). At a EU level, the Commission, the EU Broadcasting union, ESA and the European Patent organisation the are participating.

8 DE (BKA), FR, UK, NL, as well as CAN, USA and CH

2.2 Dialogue with operators

Independent of standardisation, a dialogue with operators is needed to encourage them to take law enforcement and judicial concerns into account by designing specific configurations of the network.

2.3 National and potentially EU legislation

Given the industry driven nature of the standard setting, **legislation may also be necessary** to enforce the law enforcement needs.

Given the urgency of legislation and the fact that the EU Electronic Telecommunications Code provides the opportunity to Member States to set the conditions for 5G, national legislation is likely to be the first step in many Member States. Member States could explore to coordinate their actions in this context. From the perspective of the law enforcement authorities carrying out lawful interception, the following elements may be important in the context of national legislation: registration of all providers and obligation for all providers offering services on the territory to extract a complete and decrypted monitoring copy, to structure their network in such a way that location data is always available, to provide cooperation to ensure that technical measures such as IMSI catcher can be implemented.

The **EU could reflect on a common legislative framework** to have a stronger impact vis-à-vis the service providers, to avoid fragmentation / different standards, to require certain functions to be carried out within the EU. This would take time, so it is not an immediate solution.

The EU legislation could also **potentially facilitate cross-border aspects** of lawful/real-time interception within the EU, given that purely national interceptions today may under 5G increasingly have cross-border aspects, given the technology. While this aspect has not been covered in the draft e-evidence legislation, there may be a different urgency and hence need in the future given the future deployment of 5G.

3. Possible next steps in the immediate future

3.1 Continue the working group on 5G at Europol

It is important that heads of telecommunications interception units continue to meet regularly at Europol to exchange on the law enforcement challenges related to 5G and develop suggestions for solutions. Eurojust could be associated to these efforts from the judicial perspective. This working group could also consider to associate, as appropriate, national operators to parts of the discussions as their interests can be aligned with law enforcement agencies and they can prove to be useful allies in standard bodies. It will be important to communicate the outcomes of these discussions to relevant stakeholders in the EU.

3.2 Influence the standard setting in the 3GPP

The Commission could be invited to raise law enforcement and judicial concerns in the various standardisation bodies it participates and engages with. Europol could consider to become a member in ETSI and then the law enforcement subgroup of the 3GPP process to support Member States to defend European law enforcements concerns. Additional Member States law enforcement authorities are also encouraged to participate. The 5G working group at Europol could be in close contact with ETSI to inform about the law enforcement perspective and to learn about what's going on in the other 3GPP sub-groups. How best can the EU involvement and impact be leveraged? How to ensure that law enforcement and judicial concerns are not only heard, but also taken into account?

3.3 Eurojust

Eurojust could be invited to explore issues related to 5 G and authenticity of evidence and possible ways to address them.

3.4 Commission

The Commission could be invited to facilitate further exchanges on this topic and to promote law enforcement concerns with regard to standardisation and in a dialogue with operators to encourage them to design specific configurations of the network equipment which would respond to law enforcement concerns. It could be invited to provide guidelines and explore further measures, including legislation at a later stage to avoid fragmentation. It could also, at a later stage, if Member States so wish, address cross-border real-time interception.

3.5 Integrating law enforcement concerns into the cyber security discussions on 5 G

As the cybersecurity concerns might sometimes be conflicting with law enforcement concerns, it is important that both communities discuss the issues together. At national level, law enforcement and judicial authorities could and often do engage with the responsible authorities for cybersecurity, telecoms, standardisation bodies etc. in order to make sure that law enforcement issues are embedded in national task forces addressing 5G issues. At the EU level, the Heads of the Cyber Security Authorities of Member States will meet regularly after entry into force of the EU's Cyber Security Act. The law enforcement and judicial challenges could be integrated into their discussions on 5G, as cybersecurity choices have an impact on those, too. ENISA, CERT-EU, Europol and Eurojust could work together to promote a coordinated and comprehensive approach of 5G, that addresses both law enforcement, judicial and cybersecurity issues.

3.6 Discussion on the law enforcement and judicial challenges related to 5G at the EU policy level

It will be important that in COSI Member States inform about the legislative and other initiatives they are taking in the context of lawful interceptions. It will also be important for the JHA Council to discuss the matter.