Council of the
European Union

Brussels, 11 April 2019
(OR. en)

8268/19

LIMITE

ENFOPOL 158
COSI 84
CYBER 128

NOTE

From:	Presidency
To:	Law Enforcement Working Party
Subject:	Position paper on 5G by Europol

Delegations will find attached a position paper prepared by Europol on the implications of the upcoming 5G technology for law enforcement in Europe. The document will be presented by Europol at the LEWP meeting on 15 April 2019.

The Hague, 10/04/2019

EDOC# 1038503

Position paper on 5G

1. Background

The “fifth generation” of telecommunication systems, or 5G, is considered to be one of the most critical building blocks of our digital economy and society for the next decades. Described by the European Commission as a ‘game-changer’, 5G is going to enable significantly faster data connections, exceptionally low latency and will be able to handle the increasing number of connected devices. The technology is thus going to form the basis for a number of innovative business models across multiple sectors (i.e. automotive industry, industry 4.0, e-health, logistics, energy, media and entertainment). The expectation is that 5G will have a significant geopolitical impact and is considered a crucial component for Europe to compete in the global market. The European Union has therefore taken significant steps to lead global developments towards this key technology.

2. Objective

The objective of this position paper is to provide background on the issue, to identify the benefits introduced by 5G as well as the potential challenges faced by law enforcement agencies, while at the same time presenting a way forward at both a national and a European level.

3. Developments & Timelines

To ensure early deployment of 5G infrastructure in Europe, the European Commission adopted a 5G Action Plan for Europe in 2016[1]. This plan had as its objective to start launching 5G services in all 28 Member States by the end of 2020 at the latest, followed by a rapid build-up to ensure uninterrupted 5G coverage in urban areas and along main transport paths by 2025. The 5G Action Plan is a strategic initiative which concerns all stakeholders, private and public, small and large, in all Member States, to meet the challenge of making 5G a reality for all citizens and businesses by the end of this decade.

The action plan sets out a clear roadmap for public and private investment on 5G infrastructure in the EU.

[1] https://ec.europa.eu/digital-single-market/en/5g-europe-action-plan

To achieve that, the Commission proposed the following measures:

- Align roadmaps and priorities for a coordinated 5G deployment across all EU Member states, targeting early network introduction by 2018, and moving towards commercial large scale introduction by the end of 2020 at the latest.
- Make provisional spectrum bands available for 5G ahead of the 2019 World Radio Communication Conference (WRC-19), to be complemented by additional bands as quickly as possible, and work towards a recommended approach for the authorisation of the specific 5G spectrum bands above 6GHz.
- Promote early deployment in major urban areas and along major transport paths.
- Promote pan-European multi-stakeholder trials as catalysts to turn technological innovation into full business solutions.
- Facilitate the implementation of an industry-led venture fund in support of 5G-based innovation.
- Unite leading actors in working towards the promotion of global standards.

4. Benefits of 5G

To put the benefits of 5G into perspective, we have to draw a comparison to 4G. The fourth generation of mobile connectivity started to make waves in the late 2000s. 4G made mobile internet speeds up to 500 times faster than 3G and allowed support for HD TV on mobile, high–quality video calls, and fast mobile browsing. The development of 4G was a massive turn for mobile technology, especially for the evolution of smartphones and tablets.

While 4G is now an integrated part of contemporary society, the introduction of 5G will change things once again. With the arrival of the Internet of Things, 4G will not be able to manage the large number of connections that need to connect to the network. Estimations are that there will be more than 20bn connected devices by 2020, all of which will require a connection with great capacity. This is where 5G becomes a crucial piece of the puzzle.

Overall, 5G is widely believed to be smarter, faster and more efficient than 4G. With speeds of up to 100 gigabits per second, 5G is set to be as much as 100 times faster than 4G.

Low latency is a key differentiator between 4G and 5G. Latency is the time that passes from the moment information is sent from a device until the receiver can use it.

To summarise some of the benefits discussed within the 5G context, we are expected to have:

- Higher transmission rates and capacities through enhanced mobile broadband connections
- Shorter response times
- Ultra-reliable connections
- Significant power savings
- Improved security

5. Challenges for Law Enforcement

Despite the many anticipated benefits of 5G, from a law enforcement perspective there are a number of challenges and concerns which we must address together with all the stakeholders involved. The first set of challenges pertains to the potential impact of 5G developments with respect to the ability of law enforcement officials to carry out lawful interception. These challenges pertain to identification and localisation of users as well as to the availability and accessibility of information needed when conducting lawful interception.

5.1. Identification and localisation of users

The IMSI (International Mobile Subscriber Identity) is the individual number of the mobile phone card which is sent in the background during every communication process and which can be used to identify and locate the mobile phone device. In 5G there will be two developments that will complicate the usage of IMSI numbers. The first issue is that due to the encryption of the IMSI, the security authorities are no longer able to locate or identify the mobile devices. The authorities are then also unable to assign a device to a specific person.

The second issue is the development within 5G to make the use of IMSI catchers obsolete. This will be done through a false-base detection, which is a new function within the mobile network that enables both the mobile network of providers and the mobile devices of the users to detect "false" base stations such as the IMSI catcher.

IMSI catchers are indispensable for carrying out lawful surveillance of persons who frequently change their Subscriber Identification Module (SIM) card in order to identify the respective means of communication/SIM card used and then to monitor accordingly. Only then can further police measures (surveillance, arrest) be conducted.

As a result, there is the danger that it would no longer be possible to carry out legally permissible, technical investigation and surveillance measures. One of the most important tactical operational and investigation tools would therefore become obsolete.

5.2. Availability and accessibility of information

5.2.1. Network slicing

The availability and accessibility of information through lawful interception can also be impacted by network slicing. Network slicing is a core feature of 5G. It refers to the slicing of a single mobile radio network into multiple virtual networks. This allows multiple virtual networks to be created on top of a common shared physical infrastructure.

Customisation of the virtual networks takes place to meet the specific needs of applications, services, devices, customers or operators. Network slicing will maximise the flexibility of 5G networks, optimising both the utilisation of the infrastructure and the allocation of resources. This will enable greater energy and cost efficiencies compared to earlier mobile networks.

To carry out lawful interception in the future, law enforcement will therefore require the cooperation of numerous network providers both at home and abroad. Whereas many will be subject to (national) regulation, there is also the potential of ‛private slices’ held by ‛private third parties’ that may not be subjected to such regulation. Either way, the existence of network slicing leads to potential challenges as information is fragmented, and may either not be available or accessible for law enforcement.

5.2.2. Multi-Access Edge Computing (MEC)

Multi-Access Edge Computing (MEC) will allow mobile phone networks to store and process contents in the vicinity of "cellular network participants" in order to achieve faster response times. As a result, terminal devices will in the future be able to communicate directly with each other without having to use the network operator's core network. This direct communication between users leads to consequences in terms of data retrieval for law enforcement.

Communication content and identifiers no longer have to be directed via central nodes, which means information may not be available or accessible for law enforcement.

5.2.3. End-to-end encryption (E2E encryption)

While E2E encryption is not yet set out as obligatory in the 5G standard, the relevant protocols are incorporated in the relevant protocol standard (Release 15). Therefore, there is a chance that E2E encryption will be included in the standard during the upcoming standardisation process (Release 16). An alternative is that terminal manufacturers will (voluntarily) implement this function. Either way, E2E would make it impossible to carry out content analysis of communications within the framework of lawful interception.

5.3. Other challenges

Besides challenges in the area of access to content of communication as well as the identification and localisation of users, there is another challenge impacting law enforcement activity as a result of the virtualisation of physical parts of the network. This is referred to as Network functions virtualisation(NFV).

As a result, existing special staff-related and infrastructural security measures to protect the confidentiality of surveillance measures by the providers, for example spatial security measures, access checks etc., will be nullified. This NFV means criminals can employ or execute attacks to access and even alter telephone numbers (target lists) which are to be monitored. At present there is no know commercial hardware available to prevent these attack scenarios. In addition, functions performed in one country can now be moved abroad: e.g. maintenance of mobile masts, provision of central management services (e.g. customer/user databases), thus making it (adversely) necessary to transfer lists of telephone numbers/persons to be monitored to other countries.

The challenge therefore here, in contrast to the above mentioned challenges, is the confidentiality and the integrity of law enforcement information with respect to lawful interception, in particular the target lists.

5.4. Interest representation

The potential challenges for law enforcement as a result of developments within the area of 5G do not appear to be a priority for developers. Therefore keeping track of 5G developments and ensuring that lawful interception (LI) by design becomes (and stays) part of that evolution will require significant effort.

The primary driver for 5G is commercial interests and innovation. There are high stakes and considerable financial interests involved. Designers and technicians receive full allocation, which means developments are moving fast.

The development of technical standards takes place in the Third Generation Partnership Project (3GPP). This is a worldwide collaboration of seven independent standardisation bodies

From a governmental perspective, a relatively small group of people represents the issue of lawful interception. For some, driving this issue is a secondary task. Therefore, there is an imbalance between 5G development and LI standardisation groups. Whilst we recognise the importance of privacy and security considerations, and support these, the current approach of privacy by design allows little to no room for a balanced consideration of the law enforcement needs in the area of lawful interception to limit criminal abuse of 5G developments.

Law enforcement agencies appear insufficiently aware of the issue and the anticipated impact on LEA operations in and after 2020.

6. Broader security concerns

Whereas the challenges above particularly pertain to law enforcement and its activities, discussions on 5G and security have become a major political topic recently. This is especially the case due to the developments with respect to concerns about Huawei and other Chinese companies. For the comprehensive character of this position paper, this section briefly reflects on that discussion.

Security concerns have been raised against Huawei, China’s leading telecommunications producer, in relation to the construction of 5G mobile networks in Europe. The legal and political environment in which Chinese companies, such as Huawei and ZTE, operate is given as the main concern. Under Chinese law, companies are expected to co-operate with the intelligence services, which has led some countries to conclude these companies are an extension of Chinese intelligence services. The geopolitical impact of the different approaches to Huawei are palpable. Both the United States and Australia have introduced some form of a ban with respect to Huawei equipment. And the US is currently applying pressure for other countries to take a similar approach.

In its conclusions of 22 March, the European Council expressed its support for the European Commission recommending a concerted approach to the security of 5G networks. The European Parliament's Resolution on security threats connected with the rising Chinese technological presence in the Union, voted on 12 March, also calls on the Commission and Member States to take action at Union level.

Recently, the European Commission has recommended a common EU approach to the security of 5G networks. In its recommendation, the Commission provides a number of operational steps and measures to ensure a high level of cybersecurity of 5G networks across the EU. At a national level, the recommendation requires each MS to complete a national risk assessment of 5G network infrastructures by the end of June 2019. Based on this, MS should update existing security requirements for network providers and include conditions for ensuring the security of public networks, especially when granting rights for usage of radio frequencies in 5G bands. EU Member States have the right to exclude companies from their markets for national security reasons, if they do not comply with the country's standards and legal framework.

Exchange of information between MS will occur at an EU level with the support of the Commission (through the NIS cooperation group) and the European Agency for Cybersecurity (ENISA). ENISA will complete a coordinated risk assessment by 1 October 2019. Based on this, MS will agree on a collection of mitigating measures they can implement at the national level.

7. Activities

7.1. Europol

In April 2018, EC3 gathered a limited number of experts to discuss the topic of 5G and its potential impact on LE. At the same time, EC3 drafted a background paper on the issue to start structuring the discussion and the way forward. The topic was also introduced at the Forensic Expert Forum (FEF) in 2018 organised by EC3.

After the inclusion of the topic during the European Police Chiefs Convention (EPCC), the topic gained more momentum and with support of the German BKA, EC3 organised a second meeting with a larger number of experts in February 2019. That meeting and discussion provided valuable input for this position paper as it highlighted not only the potential technical challenges but also the necessity to enhance interest representation at the appropriate venues, such as 3GPP.

7.2. National level

Member states are in different phases with respect to 5G. Many are conducting tests with respect to 5G and some have working groups on the issue. Some MS have representation of law enforcement at 3GPP, but several do not have a representative.

8. Way forward

The way forward requires more attention for the potential concerns raised by the law enforcement community, both at the national as well as at the international level. At the end of 2018, the "Electronic Telecommunications Code" was finalised at the EU level. The new rules are set to go into effect before the end of 2020. The Code states that national regulatory authorities can make any approvals regarding 5G dependent on the capability of network providers to carry out monitoring of communications. National legislative actions is therefore regarded as a priority in order to at least ensure the status quo regarding lawful interception within the framework of the ongoing 5G standardisation process and also with a view to future technological developments.

Yet the need for action extends beyond national borders, especially as the object of such action is to ensure that providers comply or otherwise cooperate in a way with law enforcement to ensure that the potential challenges introduced by 5G can be overcome.

To further the interest of law enforcement with respect to the providers and the developments in the area of 5G, the following actions are necessary:

- stronger representation of law enforcement interests in the international standardisation bodies (in particular 3GPP) by the respective ministries and security authorities,
- representation of law enforcement interests to the EU institutions (e.g. the European Commission, the JHA Council, the Council Presidency and other bodies involved in lawful interception)
- mutual exchange at the level of the European security authorities and also with international co-operation partners such as the USA, CAN and AUS.