POLITIET
KRIPOS

Nasjonal kommunikasjonsmyndighet **NCIS NORWAY**

per e-post

firmapost@nkom.no / avi@nkom.no

Deres referanse:	Vår referanse:	Sted, Dato
		Bryn, 30.08.2019

MERKNADER FRA KRIPOS – HØRING OM FREKVENSER TIL MOBILKOMMUNIKASJON OG 5G

Nasjonal kommunikasjonsmyndighet (Nkom) har i brev av 18. juni 2019 lagt ut "Høring om frekvenser til mobilkommunikasjon og 5G" og bedt om innspill på sentrale problemstillinger knyttet til tildelinger og bruken av frekvensressurser.

Som det fremkommer i høringsnotatet har regjeringen beskrevet overordnede mål for dekning og overføringshastighet for mobil- og bredbåndstjenester i nasjonal plan for elektronisk kommunikasjon. Her nevnes blant annet at innen 2020 så skal 90 prosent av husstandene ha tilbud om minst 100 Mbit/s dekning og at målet på lang sikt er at alle husstander skal ha tilbud om høyhastighetsbredbånd. Blant annet med bakgrunn i ønske om tidlig innføring av 5G i Norge har Nkom allerede gjennomført en auksjon av 700 MHz-båndet, og i løpet av de nærmeste årene har de varslet at store mengder frekvensressurser skal tildeles.

Det sentrale med regjeringens målsetninger er at Norge får god mobildekning der folk bor, jobber og ferdes, noe som følgelig også vil få stor innvirkning på politiets arbeid.

Etter avtale med Nkom er Kripos gitt frist for oversendelse av høringssvar til utløpet av dags dato.

INNLEDNING

Innføringen av 5G medfører ikke bare rene teknologiske endringer, men vil også ha direkte betydning for politiets og påtalemyndighetens mulighet til å nyttiggjøre seg opplysninger fra elektronisk kommunikasjon og sluttbrukerinformasjon i f.eks. etterforsking eller beredskapssituasjoner. For politiet er det svært viktig at slik informasjon kan innhentes, ved f.eks. tvangsmiddelbruk, også etter innføring av 5G.

Post: Pb. 8163 Dep., 0034 Oslo
Besøk: Brynsalléen 6, 0667 Oslo
www.politi.no/kripos

Telefon: (+47) 23 20 80 00
Telefaks: (+47) 23 20 88 80
E-post: kripos@politiet.no

Org. nr: 974 760 827

Etter vår gjennomgang av høringsnotatet er Kripos bekymret for at "tilretteleggingsplikten" etter Lov om elektronisk kommunikasjon (ekomloven) § 2-8[1] ikke vil bli oppfylt. Ekomloven § 2-8 stiller krav om tilrettelegging for lovbestemt tilgang og pålegger tilbyderne å tilrettelegge nett og tjeneste slik at lovbestemt tilgang til informasjon om sluttbruker og elektronisk kommunikasjon sikres.

Det henvises i denne sammenheng også til samtaler i møte mellom Nkom og Kripos dags dato, og til tidligere kommunikasjon om samme tema. Kripos mener det er uheldig at tilretteleggingsplikten ikke er spesifikt nevnt eller tatt med i betingelsene for aktuell tildeling. Kripos etterlyser generelt en mer aktiv forvaltning hva gjelder denne delen av regelverket. Uten en aktiv forvaltning frykter Kripos en uthuling av tilretteleggingsplikten ved at teletilbyderne ut i fra egne behov utvikler/implementerer tjenester og løsninger uten, i tilstrekkelig grad, å oppfylle lovens krav. Da ivaretas heller ikke de samfunnsbehov som ligger til grunn for lovfesting av en slik plikt.

AKTUELLE UTFORDRINGER

Slik Kripos forstår det, vil innføringen av 5G kunne medføre en rekke utfordringer for både kommunikasjonskontroll, trafikkdata og sporing av elektroniske kommunikasjonstjenester. Enkelte av disse utfordringene er oppsummert i to notater fra henholdsvis Europol og EU Counter-Terrorism Coordinator (disse følger vedlagt).

De mest aktuelle utfordringene er kort oppsummert slik;

- **IMSI-nummer blir kryptert**. Det blir da ikke lenger mulig å knytte en bruker til en bestemt enhet. Det betyr at IMSI-catchere blir ubrukelige hvis ikke funksjonalitet for dette blir bygget inn i nettverkene.

- **Network slicing**. Å opprette virtuelle nettverk på «toppen» av det eksisterende nettet, hvor førstnevnte nett støtter bestemte behov er en av kjernefunksjonalitetene 5G gir muligheter for. En stor bedrift eller et stort arrangement kan da f.eks. opprette sin egen «slice». Eieren av "slicen" trenger ikke være tilbyder i tradisjonell forstand og trenger heller ikke befinne seg i Norge. Dette kan medføre at "slicen" ikke blir mulig å avlytte eller at den må avlyttes hos andre enn de tradisjonelle tilbyderne.

- **Multi Egde Computing (MEC)**. Medfører at teletrafikk kan foregå i periferien av nettverket til tilbyderen. Eksempelvis kan to enheter på samme basestasjon kommunisere direkte uten at dette går via kjernenettet til tilbyderen, og vil dermed ikke være mulig å avlytte uten at slik funksjonalitet blir opprettet.

[1] https://lovdata.no/dokument/NL/lov/2003-07-04-83#KAPITTEL_2

Slik Kripos har oppfattet det, er det heller ikke sikkert at 5G-nett vil støtte lokasjonsdata på samme måte som tidligere. Dette vil kunne medføre at lokasjonsdata i forbindelse med avlytting, historiske trafikkdata og opprinnelsesmarkering ikke blir tilgjengelige for politi eller nødetater på samme måte som i dag.

I tilknytting til dette er Kripos også bekymret for at entydig identifikasjon av sluttbrukere for kommunikasjonsanlegg kan bli mer utfordrende, særlig knyttet til e-sim, IOT (internet of things) og lignende tjenester.

Kripos er også urolig for hvilke konsekvenser de fremtidige mulighetene for ende-til-ende kryptering av all trafikk medfører for samfunnets evne til bl.a. kriminalitets-bekjempelse dersom det ikke allerede nå tas høyde for en god tilrettelegging. Med mindre det allerede nå tas høyde for disse forholdene, og relevant funksjonalitet innplasseres, vil i praksis ikke noe innhold være lesbart for politiet. Et slikt resultat vil ikke være forenelig med den lovbestemte tilgang det skal tilrettelegges for.

SITUASJONEN I EUROPA

Flere land i Europa arbeider med tilsvarende problemstillinger for å sikre at tilbyderne også i fremtiden skal levere tjenester som f.eks. gir mulighet for KK. I Tyskland arbeides det f.eks. med en formulering i telelovgivning om at tilbyderne må levere et komplett og dekryptert materiale. Dette vil f.eks. bety at tilbyderne må innrette seg slik at både «slicer» og «MEC» har funksjonalitet for KK. Videre arbeides det med at tilbyderne må tilrettelegge for «implementasjon av tekniske løsninger» - dette for f.eks. å støtte fortsatt bruk av IMSI-catcher-funksjonalitet.

Fordi innføringen av 5G vil ha en betydelig innvirkning på arbeidet for både politi, etterretning og beredskapsetater generelt, har også de nasjonale lederne for Europas politi, inkludert den norske politidirektøren, engasjert seg i problemstillingene knyttet til innføringen av 5G. De har derfor avgitt en felles erklæring omkring sine bekymringer omkring manglende oppmerksomhet rundt de behov som bl.a. politiet har. "Joint Declaration of the European Police Chiefs" følger vedlagt. Kjernen i politisjefenes bekymring er at innføringen av 5G i betydelig grad vil kunne svekke mulighetene for å bruke avlytting som et middel til å sikre Europas borgere. De fremhever bl.a. at avlytting også i fremtiden må kunne fortsette å være et sentralt verktøy for kriminalitetsbekjempelse, særlig internasjonal terrorisme, organisert kriminalitet og nettkriminalitet.

I erklæringen påpekes det videre at alle justeringer som må gjøres i ettertid vil kreve langt større innsats og resultere i høyere investeringskostnader både for tilbydere og myndigheter, og følgelig bør dette hensynstas i tildelingsprosessen når tjenesten utvikles.

KRIPOS VURDERINGER

Tilretteleggingsplikten i ekomloven er ikke valgfri og må hensynstas i hele kjeden av tilbydernes virksomhet. Skiftende teknologi rokker ikke ved plikten. Tilbyderne må tilpasse nye løsninger, ny teknologi og nye tjenester til eksisterende prinsipper for tilrettelegging. Dette må synliggjøres og være klart for tilbyderne allerede fra konkurransetidspunktet, slik at tilrettelegging blir ivaretatt i hele implementeringsprosessen, og ikke – i beste fall - blir fragmentarisk gjennomført på slutten av en lanseringsperiode.

Tilretteleggingsplikten er en sentral del av rammeforutsetningene som tilbyderne må etterleve for å kunne tilby tjenester i Norge. En tilbyder vil ikke kunne sies å ha oppfylt tilretteleggingsplikten etter ekomloven § 2-8 uten at både den grunnleggende evnen til lovbestemt tilgang sikres, og at denne evnen vedlikeholdes og opprettholdes over tid.

I tillegg til at telekommunikasjonsbransjen sikrer landet kommunikasjonstjenester har den etter loven også en plikt til å bidra til vår samfunnssikkerhet. Opplysninger sikret som følge av tilretteleggingsplikten har daglig betydning for den faktiske tryggheten i Norge. Dette gjelder både i tilknytting til etterforsking av straffbare forhold, og for å sikre at nødvendig hjelp kommer frem til de som trenger denne. Når en person i nød ringer til politi, brann eller ambulanse og ber om hjelp, forventer samfunnet at myndighetene har tilrettelagt for at hjelpen kommer frem på best mulig måte. Dersom tilretteleggingsplikten ikke følges, er risikoen stor for at ansvaret ikke kan ivaretas. For samfunnet er det av denne grunn et problem om tilretteleggingsplikten utvannes, enten ved at deler av trafikken defineres ut av plikten (f.eks. gjennom MEC) eller ved at sentral informasjon holdes av enheter som ikke er tilbydere etter ekomloven eller som befinner seg i utlandet (f.eks. gjennom slicer). Vi legger til grunn at den samfunnsøkonomisk beste måten å sikre slik tilrettelegging på, er å stille krav i anbudsrunden og derigjennom påse at lovbestemt tilgang til teledata til både etterforsking og beredskap ivaretas i forbindelse med tildeling.

Kripos vil særlig peke på viktigheten av korrekte lokasjonsdata som en del av bl.a. tilretteleggingsplikten, men også som opprinnelsesmarkering (av nødanrop). Det er viktig at innholdet i de data som oversendes er så nøyaktige som mulig, slik at bl.a. nødetater raskt kan nå den som trenger hjelp. Det er ikke gitt at vedkommende selv er i stand til å meddele sin lokasjon, og her er det viktig at teknologien gir mest mulig korrekt informasjon.

Det at tilbyderne utvikler sine markeder til å omfatte nye tjenester og ny teknologi endrer ikke plikten til å tilrettelegge sine "nett og tjenester". For å kunne utvikle markedene og innføre ny teknologi må tilbyderne derfor også ivareta tilretteleggingsplikten i dette arbeidet, en plikt som åpenbart må være både teknologinøytral og tidsuavhengig.

Tilretteleggingsplikten ble vedtatt for å ivareta viktige samfunnssikkerhetsmessige behov og det er ikke noe som tilsier at disse behovene er endret eller at disse endres i forbindelse med innføring av 5G. Tilretteleggingsplikten er en del av gjeldende rett og som ansvarlig myndighet er Nkom naturlig nok helt sentral i arbeidet med å sikre at bestemmelsen følges.

Med hilsen

Vigleik Antun
ass. sjef

Saksbehandler:
Knut Jostein Sætnan
politiadvokat
Telefon: 992 86 416

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.

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.

EUROPOL

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.

Joint Declaration of the European Police Chiefs

In the field of electronic communications a new generation of mobile communications technology is about to be introduced. The 5th generation of mobile networks (5G) will be gradually introduced in Europe as of 2020 at the latest. Offering significantly greater bandwidths, lower latencies and, at the same time, ultra-reliable connections despite considerable terminal power savings, 5G is no longer a vision for the future but is expected to serve a large number of new business models and will thus become a key digital technology.

However, 5G does not only set new standards in the range of technical services but also in the field of data security. In view of the global importance of the technology in all areas of life, 5G must make tamper-proof communication possible to protect networks and applications (autonomous and interconnected driving, telemedicine, Internet of Things (IoT)). As a result, the development of the technical standards for 5G are even more focused on the "privacy by design" principle ("closing security gaps" even during standardisation) and on an increased use of virtualisation, encryption and anonymization, compared to the previous mobile communication generations.

Therefore, it is obvious that the introduction of 5G will have a considerable impact on the work of law enforcement and intelligence agencies and will significantly impair the capabilities to use lawful interception. In the future, lawful interception will have to remain a central investigation and search tool in all fields of crime fighting, especially international terrorism, organised crime and cybercrime. Considering that the 5G standard will apply all over the world, including in Europe, these challenges require a joint response and co-ordinated action.

In December 2018, the EU legislator enacted the directive (EU) 2018/1972 of the European Parliament and the Council on the European Electronic Communications Code. This directive does not affect the possibility for each member state to take the measures necessary to protect its essential security interests, to maintain public order and security and to investigate and prosecute criminal offences.
At the same time, companies acting at a global level, which exert substantial influence within the standardisation body 3GPP (Third Generation Partnership Project), should take into consideration relevant legal provisions of the Member States during the standardisation process that continues until the end of 2019. Any necessary adjustments made after the finalisation of the standardisation process would require far greater efforts and result in higher investment costs. The same applies to the law enforcement authorities in the member states. They should also articulate their needs during the process, since retroactive requests are far less likely to be successful.

On the occasion of our latest meeting in March 2019, we, the European Police Chiefs, became convinced of the necessity of developing a joint response to the impending massive impacts of 5G. Taking into account the profound changes expected by the spread of digital technology and ever-shorter innovation cycles, we consider it our duty to express our law enforcement needs to ensure these are taken into consideration by our respective national laws. We need clear and technology neutral provisions in order to maintain lawful interception (including the collection of traffic data) as one of our central investigation and search tools.
Specifically, we propose to assess the respective national laws to determine whether they reflect the following needs and to incorporate these needs, if necessary:

1. Legal obligation for electronic communication providers to extract a complete, (near) real-time, and unencrypted surveillance copy;
2. This obligation should apply to all telecommunication providers, independent of their technical structures. There ought to be no difference between the type of communication. Traditional telephone, text messaging, internet-based messenger services, so called over-the-top services (OTT

services) should be included. Even if a provider is not seated in the respective Member State but offers its services there, nothing else should apply in accordance with the lex loci solutionis principle (applying the law applicable in the place of the event/activity).
3. Legal obligation for electronic communication providers and manufacturers of terminal equipment to co-operate in the implementation of lawful technical investigative measures.
4. Legal obligation towards providers to build or structure their service or network in a way that ensures that location information is always available for all electronic communications.

We wish to emphasise that our expression of needs and calls for incorporation of these needs into respective national laws is not about reducing information technology security. This declaration is about introducing procedures secured by technical standards and the rule of law and, as a result, IT security protection. Matters of practical technical implementation and organisation should be primarily left to the providers and manufacturers, but they deserve legal clarity to enhance their ability to assist us in carrying out our law enforcement duties.

Moreover, we recommend intensifying the co-operation of police authorities at and with Europol in the field of lawful interception. For the purpose of enhanced networking and developing uniform methods and technical analysis standards, we kindly request Europol to provide an appropriate platform to join forces to discuss matters that pertain to all of us. Furthermore, we should jointly seek EU-funded technical solutions for secure lawful interception capabilities in Europe.

We welcome the efforts of the EU Counter-Terrorism Coordinator with respect to the document "Law enforcement and judicial aspects related to 5G" (EU document 8983/19) to direct Europe's attention to the impending massive impacts of 5G, giving an outline of further possible courses of action.

We hope that the present declaration contributes to a closer co-operation between the European countries and will convey the urgency of the matter to the political decision-makers in charge of electronic communications, justice and home affairs at national and supranational level, stressing that the principle according to which "the police must be able to do what the police are mandated to do" continues to be valid.