An Impact of Implementation of 5G Technology on Information Security

Dražen Lučić, Petar Mišević
Croatian Chamber of Economy, Zagreb, Croatia
dlucic@hgk.hr
pmisevic@hgk.hr

***Abstract* - The paper deals with a possible impact of implementation of the fifth generation of technology (5G) in mobile telecommunications networks on information security. Information security is one of top concerns among the companies and institutions which are in the process of digital transformation. Internet of Things (IoT), based on 5G, brings a new set of issues, such as: security, safety, privacy and cyber-systems robustness. Therefore, it is outmost important that use of IoT applications in 5G mobile telecommunications networks from start includes protection of critical infrastructure, private and business sensitive information. A possible impact on both information and cybersecurity in the mobile telecommunications networks in Republic of Croatia have been briefly analysed. Some measures are listed and described in order to decrease vulnerabilities and mitigate security and privacy threats under 5G. The role of national regulatory authorities related to information security in the process of implementation of 5G technology have been described in the case of Republic of Croatia.**

Keywords – 5G of Mobile Technology, Information Security, Mobile Telecommunications Network, Internet of Things, Cybersecurity

I. INTRODUCTION

Electronic communications empowered with high speed data connections and high data rates have shaped society and markets. Today we speak about digital/information society, digital transformation and new industrial revolution. Existing wireless communications technology cannot meet all requirements for end-user services in near future (Figure 1). One of the enablers for this tremendous change is the fifth generation of mobile telecommunications networks (5G) [1] due to improvements of e.g. latency and date rate / data throughput.

5G has become challenging and interesting topic not only in technology but in economy and society as well. Internet of Things (IoT) in 5G eco-system requires both new wireless network architecture and innovative end-user services. Contemporary Long Term Evolution (LTE) technology in mobile telecommunications networks (4G) is not sufficient and efficient to meet the demands of multiple device connectivity and a high data date, broader bandwidth, low latency Quality of Service (QoS) and low interference. An emerging and enabling technology, related to 5G, includes, among others: new radio (NR) [2], multiple input-multiple output (MIMO) antennas with beam formation technology [3], very short (millimetre) wave communication technology [4], heterogenous networks (HetNets) [5], low power wide area networks (LPWAN),…

In parallel to this significant technology change in electronic communications there is an another interesting process ongoing. European Union (EU) commission published several documents that strongly influences data processing business as well as information security. In 2016 EU Parliament introduced General Data Protection Regulation (GDPR) [6]. GDPR is a data protection law which came in force in 2018 [7]. This regulation applies to any organisation that controls or processes the data of an EU resident. The regulation has a significant impact on business in all industry sectors, bringing changes for business in terms of both cost and effort. The introduction of new rights for individuals have increased the regulatory burden for both companies and governmental institutions. They reviewed their data protection compliance programs in order to determine next steps and decided on the level of investment required in order to address the changes. e-Privacy regulation, aligned with GDPR rules, has been enforced as well. Therefore, companies need to ensure they have everything necessary in place to comply with the new GDPR, e-Privacy regulation [8] and the Directive on security of network and information systems ("NIS Directive") [9]. This has also a huge impact on electronic communications market regulation in EU with influence on information security and EU single digital market as well.

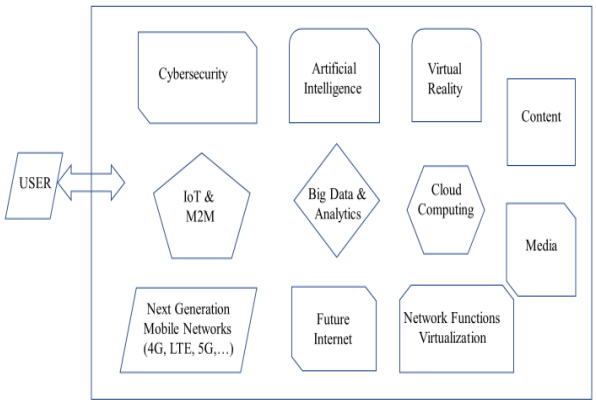

Figure 1. New electronic communications market

II. IMPACT OF 5G ON ELECTRONIC COMMUNICATIONS MARKETS

The global societal challenges related to health, homes, ageing and wellbeing, environment, industrial areas like energy, transport, agriculture, tourism and others, inclusive safety and security are and will be expressed particularly in a "Smart society" (Figure 2). "Smart systems" connecting physical world and information world and providing autonomous mode of operation are recognized as part of the solution. Particularly important is the role of the Internet of Things (IoT) [7, 8]. Basic technology behind such a complex development is Information and Communication Technology (ICT) enabling interaction and collaboration among citizens, services related to city physical and social infrastructure offered to them, and implementation and operation of "Smart systems" for a "Smart city" [9].

The transformation to digital society and digital economy is one of the results of ongoing process of digitalisation and globalisation. The creation of digital single market in EU has provoked that digital economy in EU has become increasingly reliant on the control and processing of personal data. On one side this process creates enormous opportunities for business but on another side could become obstacle or even a huge hurdle in implementation of new technologies. The process is accompanied by a growing public awareness and concern for the importance of information security that also comprises cyber security [10].

Information security is one of the key issues to be addressed by telecommunications network operators during the process of implementation of IoT based on 5G technology and new end-user services based on this technology. It gives the importance of transparency and the risk of personal data breaches. To overcome possible information security problem The implementation of GDPR and full compliance to GDPR, ePrivacy and „NIS Directive" [11] introduce numerous requirements regarding the confidentiality and security of personal data. This process implies also a number of changes that the operators need to implement, particularly in terms of personal data processing and protection.

The problems of security, privacy and personal data protection have appeared with implementation of first IoT based end-user services but they have become a bigger threat with implementation of 5G IoT based end-user services in a "smart society" due to expected boost of new end-services that include a lot of personal data. Another threat is possible vulnerability these end-user services because of their purpose like health, water supply, energy transport, traffic control, etc (Figure 2). Some of new end-user services are not applicable in existing telecommunications network due to satisfactory QoS. Implementation of 5G technology enables QoS that many end-user services required in order to be applicable and wide-spread in a "smart society" thus fulfilling new much stronger and rigid legal requirements on information security.

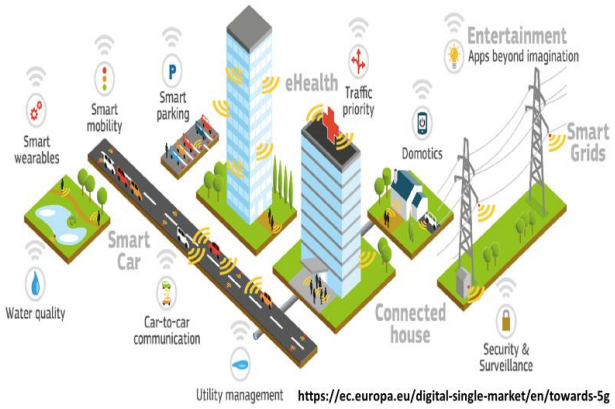

Figure 2. „Smart society" concept in 5G eco-system

III. IMPACT OF IMPLEMENTATION OF 5G TECHNOLOGY ON INFORMATION SECURITY

Electronic communications have gone through a completely different market regulation process, from state monopoly to a competitive market of electronic communications. This transition was governed by statutory regulation. Different approaches have been applied to regulate certain issues in electronic communications, and regulatory objectives have changed in line with technological and market changes. The same process is needed in the future, but at a faster rate. The development of the information and communication technology including networks, services, applications and content is exceptional, as is the research and innovation in this area. This must also be reflected in the governance and regulation of electronic communications, including the 5G technology and IoT in order to be able to adapt to changing environments and prepare solutions for evolved and predicted problems. Different types of problems require different regulation tools, i.e. different solutions for different circumstances. The need for a "smart regulation" that are effective and solution-oriented, ranging from no-regulation (deregulation), self- and co-regulation, to statutory regulation, has been recognized [12]. Such a regulation space and its three dimensions is shown in the Figure 3. These three dimensions are: type of regulation, impact and topic.

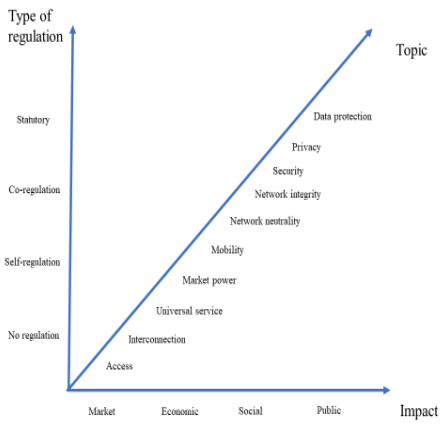

Figure 3. Electronic communications market regulation space

It is obvious that security, privacy and data protection are the most complex topics in the electronic communications market regulation space with a huge both social and public impact. Importance of information security, including cybersecurity, is increased with implementation of 5G technology and IoT end-user services based on 5G in a "Smart society" concept (Figure 4) [13].

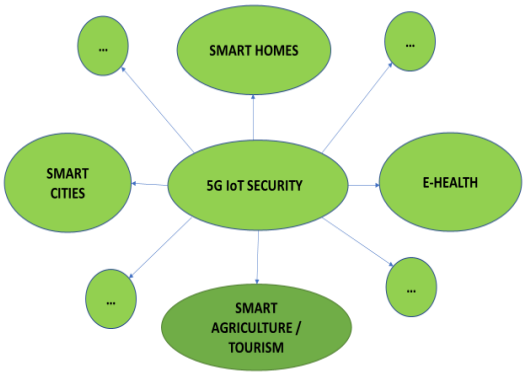

Figure 4. 5G security and „smart society concept"

The Body of European Regulators of Electronic Communications (BEREC) has recognized the importance, as well as complexity of information security challenges by implementation of 5G technology in mobile telecommunications networks [14]. BEREC has issued a report that includes threats but also possible measures in order to cope with a new security challenges in the electronic communications markets where 5G technology is (going to be) implemented [15]. A toolbox for 5G security has been created in order to help and support the mobile telecommunications network operators in fight with upcoming security threats and challenges arose by implementation of 5G technology [16].

European Parliament and European Council have also recognized the importance of information and cyber security in electronic communications markets. They issued "Cybersecurity Act" in 2019. in order to counter fight with continuously increasing risk on both information security and cybersecurity [17]. The act is of the bases for many documents and guidelines prepared by European Union agency for cybersecurity (ENISA) which include, similar like BEREC documents, description of the threats to information/cybersecurity and measures how to cope with new challenges in electronic communications market that are bought by implementation of 5G technology and especially IoT end-user services based on 5G technology [18, 19]. International Telecommunication Union (ITU) also dedicates resources and activities to this topic [20].

IoT is prone to cyber threat environment. Therefore, some significant changes are also expected in the manner how regulation is implemented: from vertical solutions for a specific network or service towards solutions for multiple, in some cases all, networks or services. Many systems and services that combine features from different paradigms require such solutions, for instance using IoT based on 5G technology for sensing and collecting data and cloud computing to store it and execute applications [21]

Research and development of 5G technology based IoT solutions is a global process but implementation is a local process that should take into an account the specific issues and requirements of each state in order to produce benefits for its citizens and promote public interest. One of these specific local requirements is also information security and regulatory framework.

IV. Possible Impact of 5G Technology on Information Security in Electronic Communications Market of Republic of Croatia

The mobile telecommunications network operators in Republic of Croatia have to perform an assessment about possible information security threats, taking in consideration whether all relevant local data protection laws and regulatory obligations have been taken in consideration. The relevant national regulatory authorities (NRA) and state institutions have to check out the outcome of the actions that the operators have undertaken in order to assure required level of information security. In general, most threats and challenges faced by 5G security are the same as those faced by 4G security. However, the security brought by 5G IoT new end-user services, 5G network architecture and implementation of 5G technology to existing mobile telecommunication network need to be considered by each operator. Some examples of these threats and challenges are:

- Access authentication for third party end-user services;
- 3GPP security standards for 5G network architecture like network slicing and Service Based Architecture;
- Secure use of computing resources assets for the applications in "cloud";
- Impact on traditional cryptographic algorithms,

The figure 5 [22] illustrates an overview of threat scenarios from network point of view. There are two types of the threats, outside operator's domain and inside operator's domain

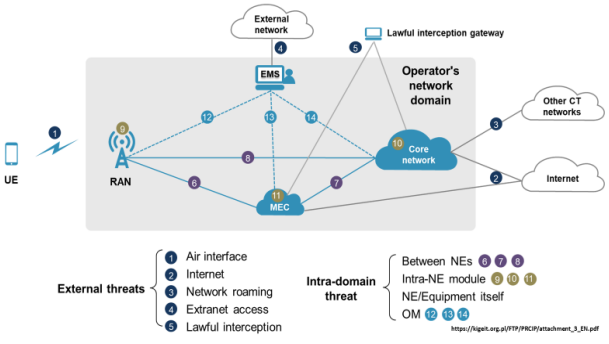

Figure 5. An overview of the threats from 5G network point of view

One of possible responses to those new threats is to increase processing and control. Additional processing power also adds complexity, thus multiplying the number of data points to be aggregated and interpreted when evaluating the best response to any detected event. Any "state of the art" solution will not only need to overcome

the above-mentioned challenges but continually adapt to changes in the usage of technology and evolving threat landscape. Independently which solution will be applied, total cost of ownership for network operator will be increased by full implementation of. These costs could arise to a level that there is no positive business case for an operator to implement a new technical solution or an end-user service which is based on a 5G technology like new IoT end-user services. Furthermore, an additional obstacle in implementation of new technology due to e.g. GDPR could be complexity of administrative procedures that should be undertaken by both operators and end-users in order to fully comply to GDPR requirements, as well as additional costs connected to these procedures.

National risk assessments should identify the typical and most significant threats and their relevance in the case of 5G mobile telecommunications networks. The assessment presented in the Table 1 [22] includes the following high-level categories of information/cyber security threats and threat actors. The main threat actors are:

- Accidental (Acc.) threat actor, e.g. unintended impact or a side effect from an operation not targeting the operation of a mobile telecommunications network;
- An individual "hacker" (Ind.);
- A "hacktivist" group (Hack. group);
- An organized crime group (Crime group);
- An insider within a telecommunication operator or vendor;
- State or state-backed actor.

The main threats are:

- Compromised confidentiality, including espionage;
- Compromised availability
- Compromised integrity of a service.

Relevance rating is from 1 to 5, i.e. very low, low, medium, high and very high respectively.

Table 1. Summary of findings on main threats in electronic communications market in Republic of Croatia

Actors / Threats	Acc.	Ind.	Hack. group	Crime group	Insider	State
Confidentiality	1	2	3	3	4	5
Availability	2	2	2	2	3	4
Integrity	2	2	2	3	3	4

The main threats in electronic communications market in Republic of Croatia don't differ significantly from the main threats in electronic communications markets in other EU or European states. The threat of an intentional cyberattack is high or even very high in a case that main actor behind is a state or a state-backed group. In the case of Croatia a threat of a cyberattack in 5G mobile communication network from individual hacker or a group of hackers is lower than in majority other EU countries due to lack of economic interest of the actors and due to the size of the electronic communications market in Croatia. However, the threat from an insider from the mobile telecommunications networks operators or their vendors is still significantly high and on a similar level to the other EU countries due to regional / pan-European / global networks / Telemach / A1 / T-Mobil).

Hrvatska agencija za mrežne djelatnosti (HAKOM), is Croatian NRA for electronic communications, postal services market and railway services market [23]. The role of HAKOM as the NRA for electronic communications is twofold, the market regulation in collaboration with other regulatory authorities and encouragement of the implementation of 5G technology in existing mobile telecommunications networks. Some policy and regulatory issues fall within the scope of electronic communications, but topics related to privacy, security protection require responsibility across the entire IoT based end-user services value chain. National regulatory authorities for electronic communications having wide experience in all these areas can play significant role in development of trustworthy 5G based IoT end-user services in a "smart society scenario". A close cooperation of HAKOM with Croatian Personal Data Protection Agency (Agencija za zaštitu osobnih podataka – AZOP) [24], as well as with government and market stake holders, is essential prerequisite for a successful implementation of 5G technology.

V. CONCLUSION

Implementation of 5G technology in mobile telecommunication networks enables the operators to increase their competitiveness. In the same time the impact of cyberattacks and other threats to information security grows, especially because the actors increasingly seek to target and disrupt critical infrastructure and systems. Effective multi-stakeholder and public-private cooperation is essential in order to strengthen information/cybersecurity and respond to the large and growing range of information/cyber security threats to the 5G mobile telecommunications networks. The operators of mobile telecommunications network have to connect together all key components of the security infrastructure in a seamless fabric thus enabling a successful implementation of the solutions and innovative IoT end-user services, based on 5G technology. This process could be very expensive for an operator and can jeopardize their business plan and time plan for implementation of the solutions which boost development of digital society, digital economy and single digital market in EU.

The Croatian NRAs for electronic communications (HAKOM), in close cooperation with Croatian personal data protection regulatory authority (AZOP), Croatian government and Croatian market stake holders, has to prepare a broader regulatory perspective for deployment of trustworthy 5G based IoT end-user services. An ultimate common goal is to boost digital economy by deployment and innovative IoT end-user services which are based on

5G technology and in the same time to fully comply to GDPR and ePrivacy directives thus assuring a high level of information security in mobile telecommunications networks.

REFERENCES

[1] 3GPP Specifications Set: 5G
https://www.3gpp.org/dynareport/SpecList.htm?release=Rel-15&tech=4

[2] Ali A. Zaidi, Robert Baldemair, Vincent Moles-Cases, Ning He, Karl Werner, Andreas Cedergren: "OFDM Numerology Design for 5G New Radio to Support IoT, eMBB and MBSFN", IEEE Communications Standards Magazine, June 2018

[3] David Gomez-Barquero, David Navratil, steve Appleby, Matt Stagg: "Ponit-to-Multipoint Communication Enablers for the Fifth Generation of Wireless Systems", IEEE Communications Standrads Magazine, March 2018

[4] Mortzea Hashemi, C. Emre Koksal, Ness B. Shroff: "Out-of.Band Millimeter Wave Beamforming and Communications to Achieve Low Latency and High Energy Efficiency in 5G Systems", IEEE Transactions on communications, vol. 66, no. 2, February 2018

[5] Conor Sexton, Quentin Bodinier, Arman Farhang, Nicola Marchetti, Faouzi Bader, Luiz A. DaSilva: "Enabling Asynchronous Machine-Type D2D Communication Using Multiple Waveforms in 5G", IEEE Internet of Things Journal, 2018

[6] „Protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", REGULATION (EU) 2016/679, 27 April 2016

[7] „Protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA", DIRECTIVE (EU) 2016/680, 27 April 2016

[8] "Regulation of the European Parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (regulation on Privacy and Electronic Communications)

[9] D. Lucic, M. Weber and I. Lovrek, "Electronic Communications as Smart City Enablers", Proceedings 2016 International Conference on Smart Systems and Technologies (SST), pp. 241 – 247, Osijek; Croatia, 2016

[10] M. Weber, D. Lucic and I. Lovrek, "Internet of Things Context of the Smart City", Proceedings 2017 International Conference on Smart Systems and Technologies (SST), pp. 187 – 195, Osijek; Croatia, 2017

[11] "The Directive on Security of network and information systems (NIS Directive)"
https://ec.europa.eu/digital-single-market/en/directive-security-network-and-information-systems-nis-directive

[12] D. Lucic, A. Caric and I. Lovrek, „Standardisation and Regulatory Context of Machine-to-Machine Communication", Proceedings ConTEL 2015 13th International Conference on Telecommunications, pp. 1-7, Graz, Austria, 2015

[13] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, Wei Zhao: "A Survey on Internet of Things: Architecture, Enabling Technologies, Security, Privacy and Applications", IEEE internet of things journal, vol. 4, no. 5, October 2017

[14] Guide to the BEREC 5G Radar and 5G Radar
https://berec.europa.eu/eng/document_register/subject_matter/berec/others/9721-guide-to-the-berec-5g-radar-and-5g-radar

[15] Report on the Impact of 5G on Regulation and the Role of regulation in Enabling the 5G Ecosystem
https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/8910-report-on-the-impact-of-5g-on-regulation-and-the-role-of-regulation-in-enabling-the-5g-ecosystem

[16] The EU Toolbox for 5G Security
https://ec.europa.eu/digital-single-market/en/news/eu-toolbox-5g-security

[17] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act

[18] ENISA Threat Landscape for 5G Networks Report
https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

[19] New Guidelines for Telecom and 5G Networks
https://www.enisa.europa.eu/news/enisa-news/new-guidelines-for-telecom-and-5g-security
https://eur-lex.europa.eu/eli/reg/2019/881/oj

[20] Heung Youl Youm: "5G Security Activities and Future Plan in ITU-T SG17"
https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201807/Documents/Heung_Youl_Youm_Remote.pdf

[21] J. Zhou, Z. Cao, X. Dong, A.V.Vasilakos: "Security and Privacy for Cloud-based IoT: Challenges", IEEE Communications Magazine, vol. 55, no. 1, pp. 26 – 33, January 2017

[22] https://cdn.netzpolitik.org/wp-upload/2019/08/2019-07-02-FinalRiskassessmentguidelinesandtemplateforreporting.pdf

[23] Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM)
https://www.hakom.hr/default.aspx?id=10321

[24] Agencija za zaštitu osobnih Podataka (AZOP) https://azop.hr/naslovna-english/