AUTOMATED M2M COMMUNICATION AS ENHANCER OF CHALLENGES FOR PERSONAL DATA BREACH NOTIFICATION

Frantisek Kasl

Ph.D. student, Masaryk University, Faculty of Law, Institute of Law and Technology Veveri 158/70, 611 80 Brno, CZ
frantisek.kasl@mail.muni.cz

Keywords: ***GDPR, personal data breach notification, automated M2M communication, internet of things, industry 4.0***

Abstract: *The contribution elaborates on one perspective of the author´s dissertation research concerning the challenges to personal data breach notification in the internet of things settings. The focus of the contribution are the potential disruptive effects of the implementation of 5G technologies in the respective NB-IoT and eMTC technology standards. The discussed setting is thereby the evolving automated M2M communication in the industry 4.0, smart city and smart home environments. The attention is limited to the personal data breach notification and communication obligations under Articles 33 and 34 GDPR. The provisions and their interpretations are confronted with this technological development and conclusions are drawn about the limits or challenges that the trend poses in this regard.*

1. Introduction

The world around us is unavoidably becoming increasingly interconnected. The leading enabler of this development is continuous spread of ICT technologies into new contexts and functions.[1] Computational and communication elements are being introduced into broad spectrum of devices and products, which in recent past hardly anyone predicted to have such features.[2] The predicted impact of this technological transition is often likened to the emergence of personal computers or widespread access to the global internet network.[3] The broadly popular label for this multifaceted phenomenon is internet of things, providing in shorthand a reflection of the core aspect of the future environment; introducing connectivity to all categories of products and thereby bringing into much closer contact the physical and the virtual environments surrounding us.

2. Connectivity as the constituting element of the internet of things

There are several key technological prerequisites for widespread transition to the internet of things era. These firstly concern the possibility to economically mass produce ICT elements that can be embedded into the respective products and provide them with the enhanced features.[4] The challenges here concern performance

1 Cf. Baller/Dutta/Lanvin, The Global Information Technology Report 2016: Innovating in the Digital Economy. World Economic Forum, http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf (accessed on 17 December 2019) 2016, p. 7.

2 BEECHAM RESEARCH, M2M Sector Map. Beecham Research Shaping the IoT Future, http://www.beechamresearch.com/download.aspx?id=18 (accessed on 17 December 2019) 2011.

3 THE ECONOMIST, Drastic falls in cost are powering another computer revolution, https://www.economist.com/technology-quarterly/2019/09/12/drastic-falls-in-cost-are-powering-another-computer-revolution (accessed on 17 December 2019) 2019.

4 WORLD ECONOMIC FORUM. Accelerating the Impact of IoT Technologies. Shaping the Future of Technology Governance: IoT, Robotics and Smart Cities. https://www.weforum.org/projects/accelerating-the-impact-of-iot-technologies/ (accessed on 17 December 2019) 2018.

of microprocessors,[5] optimisation of the energy consumption[6] or efficiency of the communication modules.[7] However, the crucial benefits from employing a mesh of such devices rest with the connectivity and corresponding wireless communication technology standards and protocols.

This area of IoT development saw in the previous years the emergence of two major radio technology standards: (a) eMTC (enhanced Machine Type Communication, often included under a broader category of LTE-M (Long-Term Evolution for Machines) and (b) NB-IoT (Narrowband Internet of Things).[8] Both of these were standardized by the 3GPP (3rd Generation Partnership Project),[9] the foremost international standards organisation for mobile communication, ensuring compatibility of telecommunication equipment and devices across major world markets. GSA (Global Mobile Suppliers Association) registered in 2019 over 100 operators who deployed networks supporting these standards.[10]

Each of these standards is designed for a different segment of IoT communication. The NB-IoT provides for low data rate, short range, high density communication that can be employed in high density environment with low cost and low battery consumption.[11] As such, it is focused on indoor coverage and finds employment e.g. by the smart home solutions or home appliance lifecycle management.[12] LTE-M, on the other hand, offers relatively high data rate, is suitable for devices in motion and allows for voice over the network feature, but consequently requires more bandwidth and energy.[13] As such, it provides secure and cost-effective alternative for many applications, which would otherwise require access to Wi-Fi network.[14]

2.1. Limits of the current standards for connectivity of IoT

The above shortly introduced standards enabled the «first generation» of IoT devices, in particular various consumer products that could be incorporated into the smart home environment[15] or basic efficiency increasing devices for business environment.[16] There are, however, limits to the utilisation of these wireless communication standards that hinder more advanced employment of mesh networks, which would enable more

5 Cf. Adegbija/Rogacs/Patel/Gordon-Ross, Microprocessor Optimizations for the Internet of Things: A Survey. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 2018, pp. 7 f.

6 El-Razek/Abedelhalim/Issa, Dynamic power reduction of microprocessors for IoT applications. 28th International Conference on Microelectronics (ICM) 2016.

7 Cf. Purkovic/Hönsch/Meyer, An Energy Efficient Communication Protocol for Low Power, Energy Harvesting Sensor Modules. IEEE Sensors Journal 2019, p. 701.

8 3GPP, Standards for the IoT. https://www.3gpp.org/news-events/1805-iot_r14 (accessed on 17 December 2019) 2016.

9 3GPP, About 3GPP. https://www.3gpp.org/about-3gpp (accessed on 17 December 2019) 2019.

10 GSA, NB-IoT and LTE-MTC Global Ecosystem and Market Status. https://gsacom.com/paper/nb-iot-and-lte-mtc-global-ecosystem-and-market-status/ (accessed on 17 December 2019) 2019.

11 SHARETECHNOTE, NB-IoT. LTE Quick Reference. http://www.sharetechnote.com/html/Handbook_LTE_NB_LTE.html (accessed on 17 December 2019) 2019.

12 GSMA, NB-IoT Commercialisation Case Study: How China Mobile, China Telecom and China Unicom Enable Million More IoT Devices. https://www.gsma.com/iot/wp-content/uploads/2019/08/201902_GSMA_NB-IoT_Commercialisation_CaseStudy.pdf (accessed on 17 December 2019) 2019.

13 Ligero, Differences between NB-IOT and LTE-M. https://accent-systems.com/blog/differences-nb-iot-lte-m/ (accessed on 17 December 2019) 2018.

14 GSMA, LTE-M Commercialisation Case Study: How AT&T and Telstra Connect Million More IoT Devices. https://www.gsma.com/iot/wp-content/uploads/2019/02/201901_GSMA_LTE-M_Commercial_Case_Study-ATT_Telstra.pdf (accessed on 17 December 2019) 2019, p. 6.

15 Soliman/Abiodun/Hamouda/Zhou/Lung, Smart Home: Integrating Internet of Things with Web Services and Cloud Computing. IEEE 5th International Conference on Cloud Computing Technology and Science 2013.

16 Bachlechner et. al., IT-Sicherheit für die Industrie 4.0 Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten Abschlussbericht. http://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-sicherheit-fuer-industrie-4-0.pdf;jsessionid=D0C8D58C4B07532B65334E42E238FFF8?__blob=publicationFile&v=4 (accessed on 17 December 2019) 2016; DIGITAL TRANSFORMATION MONITOR, Germany: Industrie 4.0. European Commission. https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Industrie%204.0.pdf (accessed on 17 December 2019) 2017.

substantial «marginal gains».[17] The solution to this obstacle seems to be the new generation of telecommunication technology standards labelled 5G.

3. Emergence of IoT powered by 5G technology

Currently, many business sectors are abuzz with expectations for the newly emerging 5G technology standard, which was initially specified in the latest 3GPP Release 15 from 2019[18] and expected to be fully established through the upcoming Release 16 in 2020.[19] By many, this technology is seen as the crucial enabler for the boom of IoT and accompanying digital transformation of many enterprise models.[20] The broader commercial employment of 5G technology is expected following the year 2020,[21] however first experiences with this new type of network connection framework are already available from South Korea or Singapore.[22]

The main benefits attributed to this next generation of network technology are greatly increased data rates, significantly lower latency and expected increased capacity of the network as such.[23] Both of the above-mentioned standards for IoT communication were designed to allow future adoption of the networks to support the 5G technology standard.[24] The major shift in IoT that is expected to be brought by the 5G technology is the transition from single-use devices to digitally automated services.[25]

3.1. Network slicing and future role of automated M2M communication

One of the features that should support this development is network slicing, which shall allow to differentiate within a single physical network a multitude of logical networks with unique parameters corresponding to particular communication requirements.[26] This should allow full emergence of the IoT in the predicted complex environments of smart city,[27] smart mobility[28] or supply chains of the industry 4.0.[29] These strongly data driven services shall provide optimisation and individualisation of the user-interaction build on increasingly omnipresent utilisation of AI and automated M2M transfer of data.

These new connectivity capacities are also likely to intensify the use of cloud computing, utilizing the individual IoT devices as mere end-points of the network, which provide input and execute or display output of the

---

17 THE ECONOMIST, The Internet of Things will bring the internet's business model into the rest of the world. https://www.economist.com/technology-quarterly/2019/09/12/the-internet-of-things-will-bring-the-internets-business-model-into-the-rest-of-the-world (accessed on 17 December 2019) 2019.

18 3GPP, Release 15. https://www.3gpp.org/release-15 (accessed on 17 December 2019) 2019.

19 3GPP, Release 16. https://www.3gpp.org/release-16 (accessed on 17 December 2019) 2019.

20 Loozen/Baschnonga, In the next wave of telecoms, are bold decisions your safest bet? EY. https://www.ey.com/en_gl/tmt/in-the-next-wave-of-telecoms-are-bold-decisions-your-safest-bet (accessed on 17 December 2019) 2019.

21 Collela, 5G and IoT: Ushering in a new era. Ericsson. https://www.ericsson.com/en/about-us/company-facts/ericsson-worldwide/india/authored-articles/5g-and-iot-ushering-in-a-new-era (accessed on 17 December 2019) 2017.

22 Alshahab/Paulo, After seven months, here's what South Korea can teach us about 5G. https://www.channelnewsasia.com/news/cnainsider/what-south-korea-first-country-launch-5g-network-can-teach-us-12056726 (accessed on 17 December 2019) 2019.

23 IEEE. 3 Key Benefits of 5G. IEEE Innovation at Work. https://innovationatwork.ieee.org/3-key-benefits-of-5g/ (accessed on 17 December 2019) 2018.

24 QUALCOMM TECHNOLOGIES, Accelerating the mobile ecosystem expansion in the 5G Era with LTE Advanced Pro. https://www.qualcomm.com/media/documents/files/accelerating-the-mobile-ecosystem-expansion-in-the-5g-era-with-lte-advanced-pro.pdf (accessed on 17 December 2019) 2018, p. 6.

25 Kenworthy, The 5G And IoT Revolution Is Coming: Here's What To Expect. Forbes. https://www.forbes.com/sites/forbestechcouncil/2019/11/18/the-5g-iot-revolution-is-coming-heres-what-to-expect/ (accessed on 17 December 2019) 2019.

26 Zhang, An Overview of Network Slicing for 5G. IEEE Wireless Communications 2019, pp. 111 f.

27 Ferdousi, Network Slicing in Smart Cities. http://networks.cs.ucdavis.edu/presentation2018/Sifat-08-17-2018.pdf (accessed on 17 December 2019) 2018.

28 Zhang/Liu/Chu/Long/Aghvami/Leung, Network Slicing Based 5G and Future Mobile Networks: Mobility, Resource Management, and Challenges. IEEE Communications Magazine 2017, pp. 138 f.

29 Kalor/Guillaume/Nielsen/Mueller/Popovski, Network Slicing in Industry 4.0 Applications: Abstraction Methods and End-to-End Analysis. IEEE Transactions on Industrial Informatics 2018, pp. 5419 f.

processes run remotely.[30] This will necessitate a continuous upload of collected data in bulk and subsequent dependence on download of instructions or information from the cloud. It is further likely that functionality as well as convenience requirements will gradually displace manual input gathering through automated collection and M2M communication of the necessary data in order to achieve the sought-after ambient character of the provided services.[31] This as a result may significantly distort the frameworks for data processing and data security, in particular the personal data protection framework.

4. Personal data protection implications and new challenges for the personal data breach notification requirement

The protection of personal data from unauthorized processing is one of the central tenets of the personal data protection framework.[32] It is stressed through multiple provisions, pursuant to the appeal to data minimisation, as well as security, integrity and confidentiality of the processing under the principles of the framework.[33] The challenging issues for this legal setting brought through technological transition towards automated M2M communication within the IoT outlined above shall be exemplified on the particularities facing the notification obligation under Art. 33 and 34 GDPR.

4.1. Personal data breach notification obligation pursuant to Art. 33 and 34 GDPR

The newly introduced requirement for controllers to document and notify occurrences of personal data breach does not in general receive major attention by commentators, however, the provisions hold major promise as instrument enabling smart regulation aimed towards enforcing adoption of appropriate technical and organisational measures for protection of processed personal data and their transfer over communication networks. Despite clear formulation of guiding principles and relevant parameters applicable to personal data protection, concrete benchmarks for adequate measures applicable in a specific case are often difficult to determine, which limits the capacity of the data protection authorities to audit and enforce these requirements.

However, one of the most indicative signals for inadequate measures is the occurrence of personal data breach. The identification and analysis of these situations should obtain major attention by the controller and the data protection authorities, as they on one hand constitute an imminent danger to the rights and interests of the affected data subjects and on the other hand provide a manifestation of a particular weakness in the employed measures that may persist in the controller´s operations, but, importantly, may likely be more widespread and present an easily exploitable vulnerability by other controllers.

4.2. Personal data breach notification obligation in the IoT context

These risks of vulnerabilities reach new threatening levels through the expansion of IoT devices, which often lack adequate security measures due to low priority to these aspects in the design and production stages, despite recent examples of severity, which wide-spread incidents affecting IoT devices may have.[34] This then in

[30] IoT SOLUTIONS WORLD CONGRESS, Advantages of 5G and how will benefit IoT. https://www.iotsworldcongress.com/advantatges-of-5g-and-how-will-benefit-iot/ (accessed on 17 December 2019) 2019.

[31] Cf. Costa, Virtuality and Capabilities in a World of Ambient Intelligence. New Challenges to Privacy and Data Protection. Springer International Publishing, Zurich 2016, pp. 23–24.

[32] De Terwagne, Article 5 Principles relating to processing of personal data. In: Kuner/Bygrave/Docksey/Svantesson/de Terwagne/Kotschy/Kranenborg/Lynskey/Hijmans/Costa de Oliveira. 2018 Draft commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation, OUP 2019), Oxford University Press, http://works.bepress.com/christopher-kuner/1/ (accessed on 17 December 2019) 2019, p. 29.

[33] Cf. Art. 5 para. 1 lit. c and f GDPR.

[34] Krebs, New Mirai Worm Knocks 900K Germans Offline. https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/ (accessed on 17 December 2019) 2016.

effect multiplies the incidents of personal data breaches and increases the damage brought about to the data subjects.[35]

Additional to these extensively documented[36] and broadly recognized[37] challenges in capacity of the IoT environment to effectively prevent the occurrence of personal data breaches and limit their impact, bring the enhanced data transfers facilitated through the implementation of 5G technology further, more intrinsic limits to utilisation of the legal instrument of notification. These are technical, as well as organisational.

The technical challenges relate to the automation of the M2M communication and varying multitude of participating devices. Despite attempts by some major players to seal users into homogeneous networks formed solely by devices of the given producer, it remains likely that most contexts, in particular public environments of the smart city or business networks of small or medium enterprises, will be inhabited by interacting devices from multiple producers with varying communication and security parameters. This shall lead to complex scenarios of compatibility issues, conflicting standards and hidden vulnerabilities.[38] The controller is then left with unique network with many potential weak points. The automated M2M communication shall make overall management of the network traffic and security even more challenging, as it is likely to create new patterns of data transfer, which may be essential for proper functioning of the mesh network, but difficult to assess or curtain from the security perspective.[39] The emergence of new security solutions based on AI heuristic search patterns or device data-flow profiling may offer some counterbalance to these issues,[40] however, extrapolating from the current experience, it is unlikely that many controllers shall in the fast approaching IoT-penetrated future devote significantly more attention and resources to cybersecurity measures and incident detection than done today.[41] As such, IoT powered by 5G technology is likely to bring more security challenges for personal data processing, more frequent and damaging instances of personal data breach, but also less control over the data transferred within the networks of the controllers and serious personal data breaches more likely going undetected.

As such, occurrence of personal data breach indicates failure to comply with regulatory provisions of the personal data protection framework as well as likely damages caused to the affected data subject. These then must be attributable to the accountable controller. The organisational challenges bound to the automated M2M communication within the IoT scenarios like the smart city, relate to the dynamically changing number of devices and liable parties participating on the data transfer or processing. More complex mesh networks and automated services are likely to transform many of the nowadays single-entity business models into layered data-driven networks of service providers known from the online environment. The varying data flows shall create ad hoc role settings under the personal data protection framework, often with multiple joint controllers sharing the personal data and contributing to their processing and protection. Due to the dynamic nature of these relationships is unlikely to always expect a clear and transparent agreement on distribution of accountability, which is likely to also have negative impact on the observance of personal data breach notification obligation. Incentives of the individual entities to report security shortcomings in situations, where attribution

---

35 SYMANTEC, ISTR Internet Security Threat Report, https://www.symantec.com/security-center/threat-report (accessed on 17 December 2019) 2019, p. 20.

36 Cf. Schneier, *Click here to kill everybody*. W.W. Norton & Company, New York 2018.

37 THE ECONOMIST. A connected world will be a playground for hackers. https://www.economist.com/technology-quarterly/2019/09/12/a-connected-world-will-be-a-playground-for-hackers (accessed on 17 December 2019) 2019.

38 Bauwens/Jooris/Giannoulis/Jabandžić/Moerman/De Poorter, Portability, compatibility and reuse of MAC protocols across different IoT radio platforms. Ad Hoc Networks 2019, pp. 144 f.

39 Varga/Plosz/Soos/Hegedus, Security threats and issues in automation IoT. IEEE 13th International Workshop on Factory Communication Systems (WFCS) 2017.

40 Cu, Artificial Intelligence for Cybersecurity: A Review. Faculty Research and Creative Activities Symposium. https://neiudc.neiu.edu/frcas/2019/schedule/49/ (accessed on 17 December 2019) 2019.

41 Cf. Lawrence, A. Gordon/Loeb, Martin P./Lucyshyn, William/Zhou, Lei, Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. Journal of Information Security, Vol. 6, No. 1, https://www.scirp.org/html/3-7800247_52952.htm (accessed on 17 December 2019) 2015.

of the incident to a particular device, and derivatively an individual entity, within the interconnected mesh is difficult to prove, are generally likely to be low.[42]

5. Conclusions

The dawn of IoT era is summoned through recent advances in network communication standards, which should enable the full potential of these meshes of interconnected devices. Alongside the improving ICT capabilities of these devices is the major drive for this development the emerging employment of 5G technology standards, which shall transform the established dominant radio technology standards eMTC (LTE-M) and NB-IoT. This is likely to unlock the potential of new business models providing digitally automated services through increased utilization of automated M2M communication.

As such, this technological development brings about new challenges for applicable regulatory frameworks for data processing and cyber security requirements. Of particular relevance is the adaptability of the personal data protection framework to this emerging environment of continuous data transfers, dynamic role settings and distributed data processing among multitude of devices and entities. The examples of limitation and challenges for this context were presented on the expected applicability issues for the personal data breach notification provisions of Art. 33 and 34 GDPR. These are technical as well as organisational. The former concern mainly the increased likelihood of damaging personal data breaches and limited capacity of controllers and processors to adequately secure and monitor their networks with myriad of IoT devices constantly interacting on autonomous level. The organisational then concern the ad hoc and interchangeable roles of multiple participating entities, who may partially be held accountable for the personal data breach occurrence in the mesh network, however, due to limited capacity for attribution of the incident to particular entity, the individual incentives for compliance with the personal data breach detection and notification obligations are likely to decrease even further from the currently already low level.

6. References

3GPP, Standards for the IoT. https://www.3gpp.org/news-events/1805-iot_r14 (accessed on 17 December 2019) 2016.

3GPP, About 3GPP. https://www.3gpp.org/about-3gpp (accessed on 17 December 2019) 2019.

3GPP, Release 15. https://www.3gpp.org/release-15 (accessed on 17 December 2019) 2019.

3GPP, Release 16. https://www.3gpp.org/release-16 (accessed on 17 December 2019) 2019.

Adegbija, Tosiron/Rogacs, Anita/Patel, Chandrakant/Gordon-Ross, Ann, Microprocessor Optimizations for the Internet of Things: A Survey. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 2018, pp. 7–20, DOI: 10.1109/TCAD.2017.2717782.

Alshahab, Sharifah Fadhilah/Paulo, Derrick A, After seven months, here's what South Korea can teach us about 5G. https://www.channelnewsasia.com/news/cnainsider/what-south-korea-first-country-launch-5g-network-can-teach-us-12056726 (accessed on 17 December 2019) 2019.

Bachlechner et. al., IT-Sicherheit für die Industrie 4.0 Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten Abschlussbericht. http://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-sicherheit-fuer-industrie-4-0.pdf;jsessionid=D0C8D58C4B07532B65334E42E238FFF8?__blob=publicationFile&v=4 (accessed on 17 December 2019) 2016;

Bauwens, Jan/Jooris, Bart/Giannoulis, Spilios/Jabandžić, Irfan/Moerman, Ingrid/De Poorter, Eli, Portability, compatibility and reuse of MAC protocols across different IoT radio platforms. Ad Hoc Networks 2019, Vol. 86, pp. 144–153, DOI: 10.1016/j.adhoc.2018.11.013.

[42] For examples of negative effects of reporting personal data breaches that act as counter-incentives see e.g. Boasiako/O'Connor, The Consequences of Data Breach Disclosure Laws and Disclosed Breaches on Corporate Cash Holdings and Performance. SSRN Electronic Journal 2018, p. 8.

Beecham Research, M2M Sector Map. Beecham Research Shaping the IoT Future, http://www.beechamresearch.com/download.aspx?id=18 (accessed on 17 December 2019) 2011.

Baller, Silja/Dutta, Soumitra/Lanvin, Bruno (Eds.), The Global Information Technology Report 2016: Innovating in the Digital Economy. World Economic Forum, http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf (accessed on 17 December 2019) 2016.

Boasiako, Kwabena Antwi/O'Connor Keefe, Michael, The Consequences of Data Breach Disclosure Laws and Disclosed Breaches on Corporate Cash Holdings and Performance. SSRN Electronic Journal 2018, DOI: 10.2139/ssrn.3191692.

Cu,Tung, Artificial Intelligence for Cybersecurity: A Review. Faculty Research and Creative Activities Symposium. https://neiudc.neiu.edu/frcas/2019/schedule/49/ (accessed on 17 December 2019) 2019.

Collela, Paolo, 5G and IoT: Ushering in a new era. Ericsson. https://www.ericsson.com/en/about-us/company-facts/ericsson-worldwide/india/authored-articles/5g-and-iot-ushering-in-a-new-era (accessed on 17 December 2019) 2017.

Costa, Luiz, Virtuality and Capabilities in a World of Ambient Intelligence. New Challenges to Privacy and Data Protection. Springer International Publishing, Zurich 2016, ISBN: 978-3-319-39197-7.

De Terwagne, Cecile, Article 5 Principles relating to processing of personal data. In: Kuner, Christopher/Bygrave, Lee/Docksey, Christopher/Svantesson, Dan/de Terwagne, Cecile/Kotschy, Waltraut/Kranenborg, Herke/Lynskey, Orla/Hijmans, Hielke/Costa de Oliveira, Piedade. 2018 Draft commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation, OUP 2019), Oxford University Press, http://works.bepress.com/christopher-kuner/1/ (accessed on 17 December 2019) 2019.

Digital Transformation Monitor, Germany: Industrie 4.0. European Commission. https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Industrie%204.0.pdf (accessed on 17 December 2019) 2017.

El-Razek, Mohamed Abd/Abedelhalim, M. B./Issa, Hanady H., Dynamic power reduction of microprocessors for IoT applications. 28th International Conference on Microelectronics (ICM) 2016, pp. 297–300, DOI: 10.1109/ICM.2016.7847874.

Ferdousi, Sifat, Network Slicing in Smart Cities. http://networks.cs.ucdavis.edu/presentation2018/Sifat-08-17-2018.pdf (accessed on 17 December 2019) 2018.

GSA, NB-IoT and LTE-MTC Global Ecosystem and Market Status. https://gsacom.com/paper/nb-iot-and-lte-mtc-global-ecosystem-and-market-status/ (accessed on 17 December 2019) 2019.

GSMA, LTE-M Commercialisation Case Study: How AT&T and Telstra Connect Million More IoT Devices. https://www.gsma.com/iot/wp-content/uploads/2019/02/201901_GSMA_LTE-M_Commercial_Case_Study-ATT_Telstra.pdf (accessed on 17 December 2019) 2019.

GSMA, NB-IoT Commercialisation Case Study: How China Mobile, China Telecom and China Unicom Enable Million More IoT Devices. https://www.gsma.com/iot/wp-content/uploads/2019/08/201902_GSMA_NB-IoT_Commercialisation_CaseStudy.pdf (accessed on 17 December 2019) 2019.

IEEE. 3 Key Benefits of 5G. IEEE Innovation at Work. https://innovationatwork.ieee.org/3-key-benefits-of-5g/ (accessed on 17 December 2019) 2018.

IoT Solutions World Congress, Advantages of 5G and how will benefit IoT. https://www.iotsworldcongress.com/advantatges-of-5g-and-how-will-benefit-iot/ (accessed on 17 December 2019) 2019.

Kalor, Anders/Guillaume, Rene/Nielsen, Jimmy/Mueller, Andreas/Popovski, Petar, Network Slicing in Industry 4.0 Applications: Abstraction Methods and End-to-End Analysis. IEEE Transactions on Industrial Informatics 2018, pp. 5419 – 5427, DOI: 10.1109/TII.2018.2839721.

Kenworthy, Randal, The 5G And IoT Revolution Is Coming: Here's What To Expect. Forbes. https://www.forbes.com/sites/forbestechcouncil/2019/11/18/the-5g-iot-revolution-is-coming-heres-what-to-expect/ (accessed on 17 December 2019) 2019.

Krebs, Brian, New Mirai Worm Knocks 900K Germans Offline. Krebs on Security. https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/ (accessed on 17 December 2019) 2016.

Lawrence, A. Gordon/Loeb, Martin P./Lucyshyn, William/Zhou, Lei, Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. Journal of Information Security, Vol. 6, No. 1, https://www.scirp.org/html/3-7800247_52952.htm (accessed on 17 December 2019) 2015.

Ligero, Raquel, Differences between NB-IOT and LTE-M. Accent Systems. https://accent-systems.com/blog/differences-nb-iot-lte-m/ (accessed on 17 December 2019) 2018.

Loozen, Tom/Baschnonga, Adrian, In the next wave of telecoms, are bold decisions your safest bet? EY. https://www.ey.com/en_gl/tmt/in-the-next-wave-of-telecoms-are-bold-decisions-your-safest-bet (accessed on 17 December 2019) 2019.

Purkovic, Dalibor/Hönsch, Marian/Meyer, Tobias Raphael Maria Karl, An Energy Efficient Communication Protocol for Low Power, Energy Harvesting Sensor Modules. IEEE Sensors Journal 2019, Vol. 19, No. 2, pp. 701–714, DOI: 10.1109/JSEN.2018.2876746.

QUALCOMM TECHNOLOGIES, Accelerating the mobile ecosystem expansion in the 5G Era with LTE Advanced Pro. https://www.qualcomm.com/media/documents/files/accelerating-the-mobile-ecosystem-expansion-in-the-5g-era-with-lte-advanced-pro.pdf (accessed on 17 December 2019) 2018.

ShareTechnote, NB-IoT. LTE Quick Reference. http://www.sharetechnote.com/html/Handbook_LTE_NB_LTE.html (accessed on 17 December 2019) 2019.

Schneier, Bruce, *Click here to kill everybody*. W.W. Norton & Company, New York 2018, ISBN: 978-0-393-60888-5.

Soliman, Moataz/Abiodun, Tobi/Hamouda, Tarek/Zhou, Jiehan/Lung, Chung-Horng, Smart Home: Integrating Internet of Things with Web Services and Cloud Computing. IEEE 5th International Conference on Cloud Computing Technology and Science 2013, pp. 317–320, DOI: 10.1109/CloudCom.2013.155.

SYMANTEC, ISTR Internet Security Threat Report, https://www.symantec.com/security-center/threat-report (accessed on 17 December 2019) 2019.

THE ECONOMIST. A connected world will be a playground for hackers. https://www.economist.com/technology-quarterly/2019/09/12/a-connected-world-will-be-a-playground-for-hackers (accessed on 17 December 2019) 2019, ISSN: 0013-0613.

THE ECONOMIST, Drastic falls in cost are powering another computer revolution, https://www.economist.com/technology-quarterly/2019/09/12/drastic-falls-in-cost-are-powering-another-computer-revolution (accessed on 17 December 2019) 2019, ISSN: 0013-0613.

THE ECONOMIST, The Internet of Things will bring the internet's business model into the rest of the world. https://www.economist.com/technology-quarterly/2019/09/12/the-internet-of-things-will-bring-the-internets-business-model-into-the-rest-of-the-world (accessed on 17 December 2019) 2019, ISSN: 0013-0613.

Varga, Pal/Plosz, Sandor/Soos, Gabor/Hegedus, Csaba, Security threats and issues in automation IoT. IEEE 13th International Workshop on Factory Communication Systems (WFCS) 2017, DOI: 10.1109/WFCS.2017.7991968.

WORLD ECONOMIC FORUM. Accelerating the Impact of IoT Technologies. Shaping the Future of Technology Governance: IoT, Robotics and Smart Cities. https://www.weforum.org/projects/accelerating-the-impact-of-iot-technologies/ (accessed on 17 December 2019) 2018.

Zhang, Shunliang, An Overview of Network Slicing for 5G. IEEE Wireless Communications 2019, Vol. 26, No. 3, pp. 111–117, DOI: 10.1109/MWC.2019.1800234.

Zhang, Haijun/Liu, Na/Chu, Xiaoli/Long, Keping/Aghvami, A./Leung, Victor, Network Slicing Based 5G and Future Mobile Networks: Mobility, Resource Management, and Challenges. IEEE Communications Magazine 2017, Vol. 55, No. 8, pp. 138–145, DOI: 10.1109/MCOM.2017.1600940.