

LITIGATION WITH HUAWEI 5G CORP AND ICT SECURITY

Norbert Malec¹, Marcin Jurgilewicz², Adrianna Czarnecka³

Abstract. Currently, there is an open discussion in the world on the introduction of new technologies to the lives of citizens and the economic sector. Doubts concern the impact of these technologies on the security of the individual and the state. Companies with modern technologies try to cooperate with the government and enter markets with their services. Not all countries undertake such cooperation. The presented text deals with the deliberations on the introduction of the new 5G technology. Its implementation meets the social discussion on social and state security. The implication of modern technology requires changes to the laws of states. The text focuses on studies on a study case concerning Huawei and a dispute with the US government. The discussed example presents the challenges of the authorities and rules enshrined in legal regulations with the functioning of companies introducing 5G to domestic markets. The presented text shows the legal conflict between the Trump government and a company that had to go to legal action. Paper presents analyzes the jurisprudence of the US courts in the dispute between the two above-mentioned entities.

Key words: 5G, state security, new technology, development, law.

JEL Classification: F63, L24

1. Introduction

Public reflections on a new generation of 5G communications technologies started in 2011, based on the prospects for new markets, new usages and advanced technologies which could not be considered during the time frame of development of the 4G/LTE standards (current generation of mobile communications systems) previous generation (4G) (The European Parliament, 2016).

Modern 5G technology arouses great emotions among people. What is new is unknown. Therefore, many conspiracy theories arise on this subject, and when they are used by people propagated in the broadly understood media to unjustifiably discredit specific solutions and spread information chaos, a reaction and logical arguments are required (Ciosek, 2020). Some people believe that the 5G network negatively affects our health, but it can also be used to take control of our minds. This technology and the frequency on which it works is supposed to cause a person to receive encrypted messages and behave in accordance with the information provided. It is supposed to cause a drastic increase in mental illness and even lead to genocide. This is what the opponents of 5G think. On the other hand, the fifth generation of cellular networks is only an improved earlier researched technology that has been

improved slowly for many years (Persona, 2019). The implementation of 5G can also be revolutionary for the economy and our everyday life. The effect is to be the modernization of industry, but also the development of smart cities, agriculture and transport. This network will be necessary in order to support modern devices connected to the mobile network. Increasing the capacity of this network will enable the introduction of the so-called The Internet of Things, i.e. networks of various devices connected to the Internet. Examples include: devices monitoring and controlling the health of patients who are at home, regulating the level of street lighting, building heating or car traffic (Ignar, 2019). An example of use will be its use in the performance of tasks by autonomous devices, e.g. cars which have to collect a lot of information from the environment in order to move safely on the roads. Thanks to the speed of data transfer, a given autonomous device will very quickly obtain more information within a second, which will increase their efficiency and security. In addition, it will be possible to download videos or photos or other files faster. The 5G network may also have an impact on the automotive and transport sectors (Michalski, Jurgilewicz, 2021). The so-called intelligent cars will be able to communicate with each other and with municipal infrastructure objects in order to warn about

Corresponding author:

¹ University of Natural Sciences and Humanities in Siedlce, Poland.

ORCID: <https://orcid.org/0000-0003-0119-2705>

² Rzeszow University of Technology, Poland.

ORCID: <https://orcid.org/0000-0003-2243-2165>

³ Nicolaus Copernicus University in Torun, Poland.

ORCID: <https://orcid.org/0000-0002-1879-4924>

dangers or inform about traffic jams. Such information flow will improve security, and moreover, traffic in the city may be liquidated. Another intention is that there will no longer be routers or Wi-Fi access points in the buildings. This technology is to be advanced enough to even replace Wi-Fi in some situations (Ignar, 2019).

Considering all wireless networks, including the 5G, in terms of state security, the vulnerability of this technology to attacks should be taken into account. Risks to the country's critical infrastructure should also be identified and assessed (Siemiątkowski, et al., 2019). It should be determined what should be the scope of state control over cellular network operators and devices installed in them, so as to ensure effective supervision of competent services for the implementation of defense objectives and the protection of public order in the country. It is a wireless network that is much more vulnerable to attacks than a fiber or cable network. When the last two networks are poorly developed in the country, less secure wireless solutions are used (Krawiec, et al., 2018).

The impact of 5G technology can be divided into: service and business and technological side. From the service and business perspective we can notice a significant increase in mobile video consumption will drive around six times higher traffic volumes per device in North America and Europe after 2020. From the technological perspective we can notice the prospect of economic fibre-like radio access with data rates, the prospect of implementing specific network functions.

Human security was the answer to new threats and challenges (Marszałek-Kawa, and Plecka, 2018). It places a human being in the centre of the debate, analysis, politics and interest. People are important and a State is an instrument of ensuring their welfare. Elementary goods protected in the framework of human security including life and personal safety may be threatened not only by an external aggression but also by internal factor (Szapak, 2015). Considering all wireless networks, including the 5G, in terms of state security, the vulnerability of this technology to attacks should be taken into account. Risks to the country's critical infrastructure should also be identified and assessed. It should be determined what should be the scope of state control over cellular network operators and devices installed in them, so as to ensure effective supervision of competent services for the implementation of defense objectives and the protection of public order in the country. It is a wireless network that is much more vulnerable to attacks than a fiber or cable network. When the last two networks are poorly developed in the country, less secure wireless solutions are used. Wireless public networks are used widely by everyone, including politicians, state officials, government agencies and services, the risk of exposure of sensitive data transmitted via wireless networks cannot be ignored.

5G technology promises extensive remote reading and control capabilities (Internet of Things), which may lead to its use in the management of critical infrastructure. By implementing the 5G technology on a national scale, state services should ensure the necessary actions from the stage of preparation and implementation of outlays to ensure effective state control and the safety of citizens. Detailed analysis and assessment of the security of 5G technology is the responsibility of experts and relevant state services (Szapak, 2015; Jurgilewicz et al., 2020).

2. Research results

This paper examines the around the Huawei legal problems in the United States. The paper makes an attempt to analyze the undertaken efforts by the Chinese corporation to defend its business operations in the US. The authors argue that the corporation can be successful winner in the federal court, therefore the Trump administration act will be void. Worries over Chinese participation in 5G (Jones, 2019) wireless networks stem from assertions that Huawei cellular network instruments might contain backdoors enabling purveyance by the Chinese administration and most important that Chinese regulations compel commercial business to assist the state intelligence agency on the collection of information when warranted. The controversy has led the American authorities to ponder whether Chinese Huawei Corp. and ZTE Corp (ZTE Corp, 2019) might be allowed to participate in 5G deployments.

It should be note that the USA has a right to ban Huawei equipment on its soil only based on Art. XXI of the WTO GATT security exception which allows a party to take action or measures 'which it considers necessary for the protection of its essential security interest The (General Agreement on Tariffs and Trade, 1947).

Huawei has faced various assertions of intellectual property theft and in January of 2019 corporate espionage (Huang v. Huawei Techs. Co.2015), including copying proprietary source code from Cisco Systems instruments, and a worker stealing a robotic arm for smart phone stress testing from a T-Mobile American laboratory. During testimony to the Senate Intelligence Committee in 2018, American intelligence chiefs warned against the Huawei, with FBI director Christopher A. Wray stating that they were concerned about the risks of allowing any corporation or entity that was beholden to foreign administration that don not share our values to gain positions of power inside American telecommunications networks (Salinas, 2018).

On August 13th of 2018 President Trump signed into regulations the National Defense Authorization Act NDAA. Section 889 of the NDAA restricted federal agencies from procuring covered Huawei

Co Ltd telecommunications and video instruments or services; contracting with third parties that use covered Huawei Co Ltd instruments or services; or awarding grants or loans used to procure covered Huawei Co Ltd instruments or services. On 15th May of 2019, president signed executive order 13873 to declare a national emergency under the International Emergency Economic Powers Act EOPA, allowing for restrictions to be imposed on commerce with foreign adversaries that involve information and communications technology. President stated that the American needed to protect itself against foreign adversaries that create and exploited security vulnerabilities in information and communications systems without making specific references to any country or vendor. Also on May 15th of 2019 the American Department of Commerce also added Huawei Co Ltd and various affiliates to its entity list under the Export Administration Regulations by restricting its ability to perform commerce with American commercial business. Department cited that the corporation had been indicted for knowingly and willfully causing the export, reexport, sale and supply, directly and indirectly, of goods, technology and services (banking and other financial services) from the American to Iran and the administration of Iran without obtaining a license from the Department of Treasury's Office of Foreign Assets Control OFAC. In addition The H.R.5515 – John S. McCain NDAA 2019 (McCain, 2019) barred the American federal administration from obtaining instruments from several Chinese dealers, including Huawei and ZTE Corp. On August 7th of 2019, the American Department of Defense DoD, General Services Administration GSA, and National Aeronautics and Space Administration NASA released an interim rule implementing Section 889(a)(1)(A) of the NDAA 2019 prohibits executive agencies from procuring or obtaining, or extending or renewing a contract to procure or obtain, any instruments, system, or service that uses covered telecommunications instruments or services as a substantial or essential component of any system, or as critical technology as part of any system.

The most important legal procedures were undertaken by the American federal prosecutors who have filed criminal charges against Huawei in the Western District of Washington state on January 16th of 2019, and on January 24th of 2019 separate charges in city of New York. The corporation's arraignment in federal court in Brooklyn, NY were based on charges that Huawei (defendant) worked to skirt American sanctions on Iran, in particular that since in or about July of 2007, HUAWEI Corp. repeatedly misrepresented to the American administration and to various victim financial institutions, and their American and Euro zone subsidiaries and branches

and by that violated applicable American regulations, including the ITSR (Amendment to the Iranian Transactions and Sanctions Regulations, 2018).

The 10 counts indictment, returned by a grand jury on January 16th 2019 in the Western District of Washington State charged Huawei corp. with, seven counts of wire fraud, one count of obstruction of justice, and attempted theft of trade secrets conspiracy from Bellevue, Washington based T-Mobile USA. The alleged conduct described in the indictment occurred from 2012 to 2014, and includes an internal Huawei announcement that the corporation was offering bonuses to workers who succeeded in stealing confidential information from other companies. Furthermore it was alleged that Between on or about April 12, 2013, and on or about night 31, 2013, at 26 Bellevue, within the Western District of Washington, and elsewhere, Huawei DEVICE 27 CO., LTD. and Huawei DEVICE USA, INC. attempted to (a) knowingly and without authorization steal, appropriate, take, carry away, and conceal trade secrets belonging to T-Mobile; and by fraud, 2 artifice, and deception obtain trade secrets belonging to T-Mobile; 3 (b) knowingly and without authorization copy, duplicate, sketch, draw, 4 photograph, download, replicate, transmit, deliver, send, communicate, and 5 convey trade secrets belonging to T-Mobile; and 6 (c) knowingly receive, buy, and possess trade secrets belonging to T-Mobile, knowing the same to have been stolen, appropriated, obtained, 7 and converted without authorization;

13 counts indictment brought in the Eastern District of New York state included Conspiracy charge defraud the United States that around July 2007 Huawei allegedly obstructed the operations of the Office of Foreign Assets Control OFAC, an agency that enforces American sanctions laws, with deceitful acts. The alleged acts testimony by a Huawei senior vice president to the American Congress that Huawei's business in Iran did not violate any rules or regulations, including related to sanctions. In or about 2017, I-IDA WEI and Huawei USA became aware of the American administration's criminal investigation of Huawei and its affiliates. In response to the investigation, Huawei and Huawei USA made efforts to move witnesses with knowledge about Huawei Iran-based business to the PRC, and beyond the jurisdiction of the American administration, and to destroy and conceal evidence in the United States of Huawei Iran-based business In or about and between July-2007 and the date of the filing of this Superseding Indictment, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants IIDA WEI and SKY COM, together with others, did knowingly and willfully conspire to defraud the United States by impairing, impeding, obstructing and defeating, through deceitful and dishonest means, the lawful

administration al functions and operations of OFAC, an agency of the United States, in the enforcement of economic sanctions laws and regulations administered by that agency and the issuance by that agency of appropriate licenses relating to the provision of financial services. In furtherance of the conspiracy and to effect its objects, within the Eastern District of New York and elsewhere, the defendants Huawei and SKY COM, together with others, committed and caused to be committed.

Separately the Federal Communications Commission FCC on November 22nd of 2019 American voted to impose new restrictions on subsidies for American telecom commercial business. The ruling was designed to constrain Chinese commercial business, including Huawei and ZTE CORP and to prohibit American carriers from using federal subsidies to buy products from any businesses found on a new FCC blacklist. The American regulators unanimously branded Chinese firms ZTE Corp. and Huawei as threats to national security and blocked them from accessing \$8.5 milliards in federal funds for services and instruments. The FCC determinations meant in fact that banned carriers receiving Universal Service Fund subsidies from using that money to buy instruments from commercial business considered a national security threat it means the Chinese commercial business Huawei and ZT Corp, unfortunately without fair process and without proper support in evidence or regulations. The Chinese corporation claimed later that the Order exceeded the FCC's statutory authority, because nothing in the Universal Service provisions of the Communications Act could authorize the FCC to make national security judgments or to restrict use of Universal Service Funds USF funds based on such judgments. Indeed, the FCC might has no national security expertise neither authority. Finally American Congress might not constitutionally give the FCC such authority, because it was an independent agency not subject to the direction of the office of the American President. The FCC determinations called in addition for carriers receiving USF funds to remove and replace any existing instruments from Huawei and ZTE Corp. they might be using already, and was proposing to establish a reimbursement program to help offset the cost of transitioning to more trusted dealers.

Huawei has sued to invalidate the entire provision, with the most prominent argument that Section 889 was an unconstitutional Bill of Attainder. At the present (as December 10th 2019) all of Section 889 were subject to a legal challenge.

On May 28th of 2019, Huawei Technologies Co., Ltd., and its US-based affiliate, Huawei Technologies USA, Inc. filed a Motion for Summary Judgment, based on the Complaint Huawei filed on March 6th,

of 2019 against the American administration in the American District Court for the Eastern District of Texas, alleging that Section 889 of the NDAA, which restricts administration contractors or agencies from dealing with certain Huawei products or services, violated the American Constitution. According to the complaint, the administration s prohibitions violated the Bill of Attainder and the Due Process clauses of the American Constitution. The prohibition also "violated the separation-of-powers principles enshrined in the Constitution, because Congress was both making the regulations, and attempting to adjudicate and execute it, The regulations lawsuit seeks a permanent injunction against the federal restrictions. Plaintiff Huawei by and through their attorneys, brought this action under the American Constitution and 28 U.S.C. §§ 1331, 2201, and 2202, seeking a declaration that pertinent provisions of section § 889(f)(3)(A), (C) of the NDAA 2019 that defined certain instruments and services produced or provided by Huawei Technologies Co., Ltd. and its subsidiaries and affiliates as "covered telecommunications instruments or services, and consequently restricted the procurement and use of such instruments by executive agencies, federal administration contractors, and federal loan and grant recipients are unconstitutional. Huawei urged a District Judge Amos Mazzant in Sherman, Texas to bylaw that a regulations that prohibits American federal agencies and contractors from buying or using the Huawei instruments was unconstitutional The corporation argument was that it was punished without a hearing or trial by Section 889 of the 2019 National Defense Authorization Act. But it is obvious that in most cases federal judges are usually reluctant to second guess the administration's evaluation of a national security risk. For instance the American court of appeals in Washington Iain 2018 affirmed that Kaspersky Lab, a Russian cybersecurity corporation, wasn't unlawful fully targeted by a similar regulations that excluded it from federal computer systems because of its close relationship with the Russian administration. The court affirmed the district court's dismissal of the NDAA Case for failure to state a claim upon which relief can be granted, as well as its dismissal of the Directive Case for lack of jurisdiction. The attorney for claimant were prepared to challenge a defense spending authorization regulations blocking executive agencies from using Huawei and ZTE's telecom instruments, because the American action was a bill of attainder that singled out a corporation for punishment without trial, procedure that's forbidden by the American constitution provisions. In a petition Huawei asked the court to hold the FCC's order unlawful on the grounds that it fails to offer Huawei required due process protections in labeling Huawei as a national security threat. the FCC in accordance to the plaintiff

also failed to substantiate its arbitrary findings with evidence or sound reasoning or analysis, in violation not only of the American Constitution, but also the Administrative Procedure Act APA, and other regulations. Filed Petition for Review challenged the Order of the FCC both insofar as it barred use of federal USF to purchase products and services from commercial business that the Commission deemed a threat to American national security, and insofar as it arbitrarily and capriciously designated Huawei as such a corporation. It seems that The FCC failed to address multiple legal arguments and material facts presented in comments on the proposed rule. And its cost-benefit analysis considered *only* costs associated with prohibiting the use of USF funds for Huawei and ZTE Corp. products and services – a remarkable deficiency that exposes the Bylaw as simply a vehicle for targeting and burdening these two commercial business, not a genuine attempt to develop a generally-applicable and fair bylaw that would seriously protect telecommunications networks and supply chains. In addition The Bylaw was also unlawfully vague and inconsistent with Due Process. The Order states no standard or criteria whatsoever for identifying a corporation as a genuine threat to the integrity of communications networks or supply chains – again revealing that the FCC goal in the Order was simply to impose restrictions on Huawei and ZTE, and them alone. Furthermore, the Order fails to give Huawei constitutionally required due process before stigmatizing it as a national security threat, such as an opportunity to confront supposed evidence and witnesses, and a fair and neutral hearing process. This was contrary to all American constitutional traditions. Section 889, according to the complaint, also violated the Due Process Clause by selectively depriving Huawei of its liberty – severely curtailing its freedom to do business, stigmatizing it by effectively branding it a tool of the Chinese administration and a risk to American security, and denying it any pre-deprivation legal process to confront the congressional charges against it. And section 889 violated the Vesting Clauses and the resulting separation of powers by legislatively adjudicating Huawei to be “guilty of an alleged connection to the Chinese administration, and by implication a threat to American security, rather than leaving it to the Executive and the courts to make and adjudicate any such charges. It seems that the FCC initial designation of Huawei also lacked either legal or factual support, because it was based only on a fundamental misunderstanding of Chinese regulations, as well on unsound, unreliable, and inadmissible accusations and innuendo, not evidence.

Another legal avenue for the Huawei was filing on December 5th of 2019 a petition with the Fifth Circuit Court in New Orleans challenging the FCC determinations. Firstly, the Huawei declared any sort

of ban on national security grounds constituted foreign policy, rather than telecoms regulation. Secondly, Huawei declared the FCC acted arbitrarily by singling out the corporation and ZTE Corp. without setting out any standards by which those commercial business were being judged. Huawei’s important argument was that singling out the corporation in this way violated its due process rights. The complaint argued that the NDAA deprives Huawei of the liberty to sell to federal agencies, as well as by stigmatizing it and “discouraging other entities across the American from doing business with Huawei. It argued that it was deprived of this liberty without “any pre-deprivation opportunity to be heard, present evidence, or defend itself, in violation of the due process requirement that a legislative deprivation of liberty be imposed in accordance with general rules. Thirdly Huawei declared the FCC compounded that unfairness by not allowing the Huawei to comment on the part of the bylaw that mentioned it specifically, which was announced only after the consultation period suffice to justify such unlawful means. Huawei’s primary argument was that the NDAA was an unconstitutional bill of attainder. Art. I, Section 9 of the American Constitution prohibits “Bills of Attainder, regulations that, under American SC precedent, “legislatively determine guilt and inflict punishment upon an identifiable individual without provision of the protections of a judicial trial. The American SC has established 3 criteria for determining whether a legislative act imposes punishment the historical criterion, which looks at whether the burden inflicted was consistent with the types of burdens that have historically been deemed punishment; the functional criteria examining whether the burden was a means to an end or an end in and of itself by balancing the purpose of the regulation and the burdens imposed; and the motivational criterion, ascertaining whether Congress’s intent was to punish. The most important criterion was the functional test. Finally, Huawei argued that the It can be argued that in the line of American SC determinations NDAA violated the separation of powers because applying legislative rules to enumerated individuals “constitutes the exercise of executive and/or judicial power. For instance in the 1810 SC ruling of the case case of *Fletcher v. Peck*, and two later concurrences 1983 SC ruling in the case of *Immigration and Naturalization Service v. Chadha* and the 1995 SC ruling in the case of *Plaut v. Spendthrift Farm, Inc.* It must be pointed out that by specifically prohibiting the use of Huawei products while leaving up to the secretary of defense the determinations whether other Chinese entities are state controlled, American Congress has made a legislative adjudication that should be made by the judiciary or the executive branch, and has thus deprived the plaintiffs of recourse that might otherwise be available including opportunities for executive consultation and subsequently judicial review.

But it will be seen whether the Federal District Court in the Eastern District of Texas, where the regulations lawsuit was filed, will decide on the unconstitutionality of the Section 889 of the Act.

3. Conclusion

The 5G network enables the emergence of new innovative services that transform sectors such as manufacturing, energy, automotive and health into the IoT era. The implementation of the 5G network is associated with a number of benefits achieved at various levels: starting from the most easily measurable effects, i.e. a step improvement in the performance parameters of telecommunications networks, including a significant improvement in the availability of high-quality services, through the creation of completely new services using 5G technology, to impact on the scale of entire economic and social areas. Second-order benefits are the effects of the use of goods and services addressed directly to society. Four distinct environments can be identified that will be affected by

5G networks: Smart Cities, Out-of-City Areas, Smart Homes and Smart Workplaces.

The term Smart City is not a new concept, but it is still not fully clearly defined yet. According to the definition given in the ETSI TR 103 290 v1.1.1 (2015-04) standard, a city can be defined as smart if investments in human and social capital as well as traditional transport and modern ICT communication infrastructure support economic development and high quality of life with sound management of natural resources by governing with the participation of citizens (Kordonska and Hurnyak, 2018). In particular, the conditions conducive to the development of 5G networks will be created using regulatory policy and investment. Development and implementation of appropriate legal regulations and incentives investment should contribute to the implementation of an effective policy supporting the construction of infrastructure for 5G will contribute to ensuring the sustainable development of the 5G network by preventing it the creation of areas without access to this network (Marszałek-Kawa, and Siemiątkowski, 2020).

References:

- Amendment to the Iranian Transactions and Sanctions Regulations, 31 C.F.R. Part 560 (ITSR) OFAC amended the Iranian Transactions and Sanctions Regulations (ITSR) to implement the President's May 8th, 2018 decision to withdraw from the JCPOA, as outlined in the National Security Presidential Memorandum (NSPM).
- Ciosek, I. (2020). Aggravating Uncertainty – Russian Information Warfare in the West. *Torun International Studies*, 1(13), 57–72. <http://dx.doi.org/10.12775/TIS.2020.005>
- Commission Staff working document (2016). 5G Global Developments in Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.
- Department of Justice Office of Public Affairs Chinese Telecommunications Device Manufacturer and its U.S. (2019). Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction Of Justice January 28.
- Eastern District of Texas on August 14, 2015. *Huang v. Huawei Techs. Co.*, 215-cv-1413-JRG-RSP (E.D. Tex. Aug. 14, 2015).
- ETSI Technical Report (2015). Machine-to-Machine communications (M2M); Impact of Smart City Activity on IoT Environment.
- Fletcher v. Peck, 10 U.S. (6 Cranch) 87 (1810). https://www.wto.org/english/docs_e/legal_e/gatt47_02_e.htm#articleXXI.
- Huang v. Huawei Techs. Co.*, 215-cv-1413-JRG-RSP (E.D. Tex. Aug. 14, 2015).
- Huawei Technologies USA, Inc., and Huawei Technologies Co., Ltd., Plaintiffs, v., in the United States District Court for the Eastern District of Texas Sherman Division.*
- Ignar, M. (2019). Co to jest 5G? Zalety i zagrożenia sieci 5G. *Komputronik*.
- Jones, J. L. (2019). U.S. Marine Corps (Ret.) Recommendations on 5G and National Security February 11.
- Judgment in the case of *Kaspersky Lab, Inc. v. United States Department of Homeland Security*, No. 18-5176 (D.C. Cir. 2018) The D.C. Circuit affirmed the dismissal of the lawsuit.
- Judgment in the case of *Kaspersky Lab, Inc. v. United States Department of Homeland Security*, No. 18-5176 (D.C. Cir. 2018).
- Judgment in the case of *Plaut v. Spendthrift Farm, Inc.*, 514 U.S. 211 (1995).
- Jurgilewicz M. et al. (2020). The implementation of selective passenger screening systems based on data analysis and behavioral profiling in the smart aviation security management – conditions, consequences and controversies, *Journal of Security and Sustainability Issues* Vol. 9(4), June 2020, s. 1145–1155. [https://doi.org/10.9770/jssi.2020.9.4\(2\)](https://doi.org/10.9770/jssi.2020.9.4(2))
- Kordonska, A. and Hurnyak, I. (2018). Efficient use of Common Resources in Conditions of Sustainable Development. *Torun International Studies*, 1(11), 75–87. <http://dx.doi.org/10.12775/TIS.2018.007>
- Krawiec, P., Mongay Batalla, J., Gajewski, M., Sienkiewicz, K., Wiśniewski, P., & Latoszek, W. (2018). National Institute of Telecommunications in the face of challenges for the implementation of 5G networks in Poland. *Telekomunikacja i techniki informacji*.

- Marszałek-Kawa, J and Plecka, D. (eds.) (2019). *The Dictionary of Political Knowledge*. Toruń: Wydawnictwo Adam Marszałek.
- Marszałek-Kawa, J., and Siemiątkowski, P. (2020). The Implementation of the Sustainable Development Goals at the Local Level. The Case of the Districts of Kuyavian-Pomeranian Province. *Baltic Journal of Economic Studies*, 6(2), 1–8. <https://doi.org/10.30525/2256-0742/2020-6-2-1-8>
- Michalski K., & Jurgilewicz M. (2021). *Konflikty technologiczne. Nowa architektura zagrożeń w epoce wielkich wyzwań*, Warszawa, DIFIN.
- Persona, M. (2019). 5 mitów na temat technologii 5G. Na fali nauki.
- Plaintiffs' Motion for Summary Judgment, Huawei Technologies USA, Inc. et al v. US of America, et al, No. 4-19-cv-159-ALM (E.D. Tex. filed May 28, 2019).
- Plaintiffs' Motion for Summary Judgment, Huawei Technologies USA, Inc. et al v. US of America, et al, No. 4-19-cv-159-ALM (E.D. Tex. filed May 28, 2019).
- Salinas, S. (2018). Six top US intelligence chiefs caution against buying Huawei phones. CNBC.
- Siemiątkowski, P., Tomaszewski, P., Jurgilewicz, O., and Poplavska, Z. (2019). Assessment of Basic Elements of the Security System of Local Communities. *Journal of Security and Sustainability Issues*, 9(2), pp. 617–635. [https://doi.org/10.9770/jssi.2019.9.2\(20\)](https://doi.org/10.9770/jssi.2019.9.2(20))
- Szpak, A. (2015). Cities and human security. *Torun International Studies*, 1(8), 119–133. <http://dx.doi.org/10.12775/TIS.2015.011>
- The General Agreement on Tariffs and Trade (GATT 1947), Art. XXI. World Trade Organisation.
- The John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232.