
WSCHODNI ROCZNIK HUMANISTYCZNY
TOM XXII (2025), Nr 4
s. 173-187
doi: 10.36121/mmaluzinas.22.2025.4.173

Martinas Malužinas
ORCID: 0000-0002-2772-9534
(Koszalin University of Technology)

Ewa Maria Włodyka
ORCID: 0000-0002-8229-342X
(Koszalin University of Technology)

Cybersecurity analysis of the mobile application “TikTok” in Poland compared to other countries 2016-2022

Abstract: The purpose of this article is to provide a preliminary analysis of the TikTok app in Poland compared to other countries on smart devices, which has been distributed since 2016 and which reached its peak of 3 billion downloads in 2022. The findings show that the TikTok app requires access to a large amount of sensitive data and permission to use device features such as Wi-Fi, among others, which poses a security risk to users. In the research process, methods adequate for political and administrative sciences were used: comparative method, normative analysis and desk research. It is worth mentioning that quantitative data was also used in the course of the research. The data clearly indicate a higher level of threat in the United States, Germany, Singapore, France and Lithuania, while users of the application in Poland are less threatened.

Keywords: TikTok, IP address, users, China, Poland, international relations

Analiza cyberbezpieczeństwa aplikacji mobilnej „TikTok” w Polsce na tle innych krajów w latach 2016-2022

Streszczenie: Celem niniejszego artykułu jest wstępna analiza aplikacji TikTok w Polsce na tle innych krajów, która jest rozpowszechniana od 2016 roku i osiągnęła szczyt 3 miliardów pobrań w 2022 roku. Wyniki pokazują, że aplikacja TikTok wymaga dostępu do dużej ilości wrażliwych danych oraz uprawnień do korzystania z funkcji urządzenia, takich jak Wi-Fi, co stanowi zagrożenie dla bezpieczeństwa użytkowników. W procesie badawczym wykorzystano metody adekwatne dla nauk politycznych i administracyjnych: metodę porównawczą, analizę normatywną oraz analizę desk research. Warto wspomnieć, że w trakcie badań wykorzystano również dane ilościowe. Dane te jednoznacznie wskazują na wyższy poziom zagrożenia w Sta-

nach Zjednoczonych, Niemczech, Singapurze, Francji i na Litwie, podczas gdy użytkownicy aplikacji w Polsce są mniej narażeni.

Słowa kluczowe: TikTok, adres IP, użytkownicy, Chiny, Polska, stosunki międzynarodowe

Introduction

Contemporary international relations reflect the totality of relations between their state and non-state participants at the political, economic and social levels¹. In turn, social media, which can indirectly influence the aforementioned relations, have become one of the primary forms of communication in the modern world, influencing the socio-political system.

China is a country that seeks to take over from the United States the role of hegemon in the contemporary international system. The object of this article is to preliminarily determine the scale of influence of China's power on Western countries, including Poland, from the perspective of soft resources, while omitting – due to the already large number of publications

– economic and military resources². China's economy and military potential certainly influence the development of other power factors. Economic, as well as military potential, attracts international attention. However, less is said about the soft power factor, which enables the creation of China's foreign policy and public diplomacy through the Internet used³. China's image is improved by propaganda, which takes place not only in the traditional, government-controlled media but also on social media, on the TikTok platform⁴. China is using the service for its own propaganda and is using increasingly sophisticated methods to do so, which are designed to alleviate global concerns about China's rising power and the ongoing changes in EU-PRC relations, which are in the midst of their biggest crisis in decades. China is also regulating its relations with Poland and other Central European countries in the area of cyber security. In doing so, they want to change the image of a state accused of supporting industrial espionage and intellectual property theft using the internet in the region⁵. In doing so, they are making users dependent on them, as well as collecting

¹ B. Molo, E. Cziomer, A. Paterek, *Współczesne stosunki międzynarodowe: wprowadzenie do stosunków międzynarodowych*, Kraków 2014.

² P. Picquart, *Imperium chińskie. Historia i teraźniejszość chińskiej diaspory*, Warszawa 2006; A. Brunet, J. P. Guichard, *Chiny światowym hegemonem. Imperializm Państwa Środka*, Warszawa 2011; A. Hładij, *Międzykontynentalne pazury chińskiego smoka*, 2017, <https://www.space24.pl/międzykontynentalne-pazury-chińskiego-smoka-analiza>. [22.04.2024]; R. Kowal, *Chińska armia pokazała wideo z pociskami DF 16*, 2017, <https://tech.wp.pl/chinska-armia-pokazala-wideo-z-pociskami-df-16-6088523689538177a> [22.04.2024]; R. Czulda, *90-lecie chińskich sił zbrojnych. Armia potężna jak nigdy*, 2017, <https://www.defence24.pl/90-lecie-chińskich-sił-zbrojnych-armia-potężna-jak-nigdy-analiza>. [22.04.2024].

³ M. Pietrasiak, D. Mierzejewski, *Między wzrastaniem a harmonią – uwagi o chińskiej polityce zagranicznej*, [in:] *Chiny w stosunkach międzynarodowych*, red. D. Mierzejewski, Łódź 2012, p. 5-19; S. Guo, S. Hua, *New dimensions of Chinese Foreign Policy UK*, London 2007.

⁴ TikTok is an app available in dozens of languages around the world, created by China-based ByteDance, which was founded in 2017 as a result of the acquisition of another popular social networking site: musical.ly (popular in Europe and the United States). TikTok is known as Douyin in China.

⁵ M. Przychodniak, *Internet jako narzędzie polityki Chińskiej Republiki Ludowej*, Państwowy Instytut

a huge amount of data about them. From 2022 onwards, more and more countries are arriving whose authorities see this as a threat to national security. In order to prevent the national threat of internet surveillance, oppressive censorship and algorithmic learning by the Chinese Communist Party, the European Commission has banned the use of the Chinese TikTok app on business devices from 2023.

The present analysis concerns the TikTok application, characterized as one of the instruments wielded by China to exert influence on users in the USA and the rest of the world, thus posing a threat to national security, as corroborated by a report compiled by the American Federal Bureau of Investigation (FBI) in 2022⁶.

The aim of this article is to provide a preliminary analysis of the TikTok application in Poland vis-à-vis other countries on mobile devices, which has been distributed since 2016 and peaked at 3 billion downloads in 2022. Additionally, research findings have revealed that the TikTok application requires access to a significant amount of sensitive data and permissions to utilize device functions such as Wi-Fi, thus posing a threat to user security. In order to achieve the research objective, two research hypotheses were formulated: (H1) the TikTok application may expose users to risks, including the lack of protection and data breaches of personal information. TikTok, its infrastructure, and supporting systems are owned by the Chinese company "ByteDance." According to this company's privacy policy, user data collected may be shared in accordance with the interests of hostile agencies; (H2) the TikTok application may be utilized as a tool of influence in China's conducted international policy, including granting Chinese access to Polish data.

In this study, the decision was made to implement methodological triangulation as a research approach enabling the combination of quantitative and qualitative methodologies. The advantage of these research methods lies in the collection of information that will be verified for the correctness and authenticity of the gathered data. For this reason, the Desk research method was also employed, allowing for the analysis and processing of data and information sourced from existing analytical and expert reports.

The issue addressed in this study represents a significant contribution to the advancement of research on cybersecurity in the context of China's foreign policy, as an element of building influence. The research topic is particularly significant because an increasing number of countries are engaged in efforts to limit this application or are considering the implementation of various types of security measures.

The security of TikTok data

One of the most popular types of social media that offers communication to its users through concise video forms is the Chinese application TikTok. It should be noted that TikTok is an application originating from China, enabling users to create

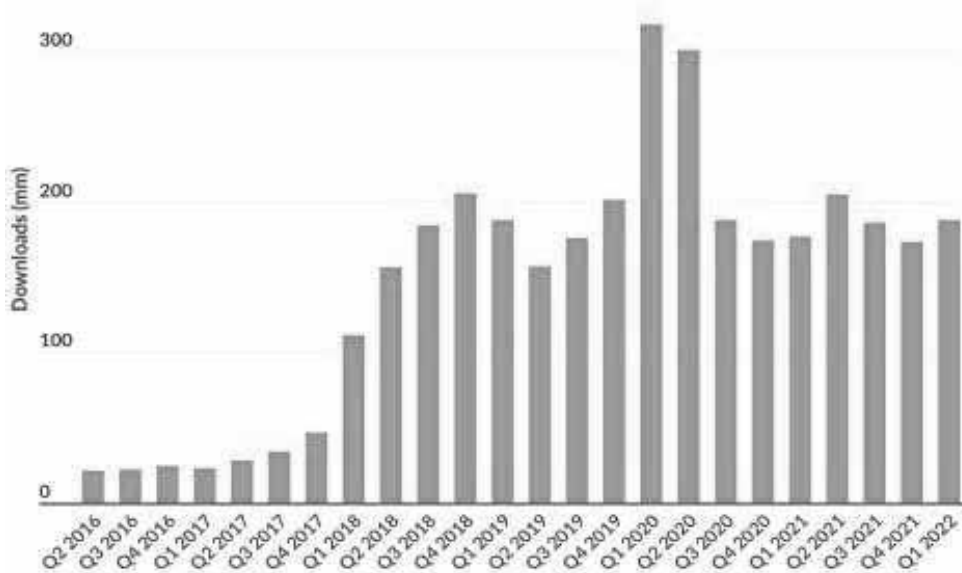
Spraw Międzynarodowych, https://www.pism.pl/publikacje/Internet_jako_narz_dzie_polityki_Chi_skiej_Republiki_Ludowej [22.04.2024].

⁶ FBI ostrzega: TikTok to narzędzie wpływu Chin na Amerykanów, <https://cyberdefence24.pl/cyberbezpieczenstwo/fbi-ostrega-tiktok-to-narzedzie-wplywu-chin-na-amerykanow> [22.04.2024].

and share short video materials ranging from 15 to 60 seconds in length. Thanks to its algorithms, TikTok adjusts content to users' preferences, effectively influencing their consistent engagement. Although TikTok is used by various social groups, regardless of age, it is significantly popular among younger internet users in the age range of 18 to 25 years. Analysing the specificity of this application, it should be noted that TikTok focuses on short videos that are creative and visual. They often relate to current information and correspond with other materials⁷. During the COVID-19 pandemic, it became the most frequently downloaded and used application. It is estimated that in 2021, TikTok generated revenue of \$4.6 billion, marking a 142% year-on-year increase;

- 1) TikTok had 1.2 billion active users monthly in the fourth quarter of 2021, and it is expected to reach 1.8 billion by the end of 2022;
- 2) In China, TikTok has over 600 million daily users;
- 3) The TikTok application has been downloaded over three billion times⁸.

Figure 1: Quarterly downloads of the TikTok app between 2016 and 2022 (in millions)



Source: Developed based on: M. Iqbal, *TikTok Revenue and Usage...*, p. 10.

As a result, the development of the analysed application, being a strategic asset, has transformed into both a weapon and a target for potential attacks. As experts note, the analysed application requires access to a large amount of sensitive data (such as the

⁷ S. Trzeciak, *Drzewo Kampanii Wyborczej 2.0. Czyli jak wygrać wybory*, Warszawa 2023, p. 335.

⁸ M. Iqbal, *TikTok Revenue and Usage Statistics*, 2022, p. 2, https://uploads2.craft.co/uploads/operating_source/document/982548/57cb7f410c237c8e.pdf [22.04.2024].

list of paired Bluetooth devices, device contacts, calendar, external memory, reading of accounts connected to the device, etc.). In total, the application requires access to 77 device parameters⁹.

During the analysis of the report prepared by the National Cyber Security Centre under the Ministry of National Défense of the Republic of Lithuania in the years 2016-2022, experts observed that the TikTok application established connections with 44 IP addresses¹⁰ located in 8 different countries. Among them, 12 were registered in Lithuania, 11 in Poland, 10 in the United States, 6 in India, 2 in Sweden, and 1 each in Luxembourg, the Netherlands, and Russia. Additionally, in the configuration files and database of the application, 287 unique IP addresses belonging to "TikTok" were identified. According to information from IP geolocation databases, 38% of these "TikTok"-related IP addresses were registered in the United States, 15% in Germany, 14% in Singapore, 7% in France, 6% in Lithuania, and 20% in other countries. Furthermore, it was observed that in accordance with TikTok's privacy policy, the system collects all user-provided personal data, including information about interests, gender, and age. For broader analysis, the platform also utilizes user-submitted video and audio materials (including live streams), photos, text information (comments, reviews, opinions, passwords), network information, time, and other device parameters. To determine the device's location, it uses GPS, SIM card information, and the device's IP address. If consent is given to access contact information stored in the phone's contact list or in the list of friends on the Facebook social networking platform, that information may also be collected¹¹.

Furthermore, among the analysed addresses, 185 unique IP addresses were found in the database, and 102 unique IP addresses were found in the configuration files. The configuration files contained 102 unique IP addresses, of which 80 were registered in the United States of America, 2 in Thailand, Brazil, the Netherlands, Germany, Singapore, 1 in Pakistan, South Africa, and other countries. During the analysis of the application, it was noted that between 2016 and 2022, this application connected to 44 IP addresses located in 8 countries. Among them, 12 were registered in Lithuania, 11 in Poland, 10 in the USA, 6 in India, 2 in Sweden, and 1 each in Luxembourg, the Netherlands, and Russia. It is worth noting that among them, 12 IP addresses were registered in the application's database (11 in Lithuania, 1 in Russia).

⁹ Nacionalinis Kibernetinio Saugumo Centras, *Mobiliosios aplikacijos "TikTok" kibernetinio saugumo analizė*, 2023, https://www.google.com/url?sa=t&source=web&rcrt=j&opi=89978449&url=https://www.nks.c.lt/doc/biuletiniai/2023_06_01_TikTok.pdf&ved=2ahUKEwi-utOazrKFAxVpQPEDHYAvCh8QFnoECBIQAQ&usq=AOvVaw2LfbZnvnPPwf-uXf5IeHse [22.04.2024].

¹⁰ An IP address (Internet Protocol address) is a number assigned by your internet service provider. An IP address can be compared to an online home address, as it is used to identify the user of a device among billions of others.

¹¹ Nacionalinis Kibernetinio Saugumo Centras, *Mobiliosios aplikacijos "TikTok"...*

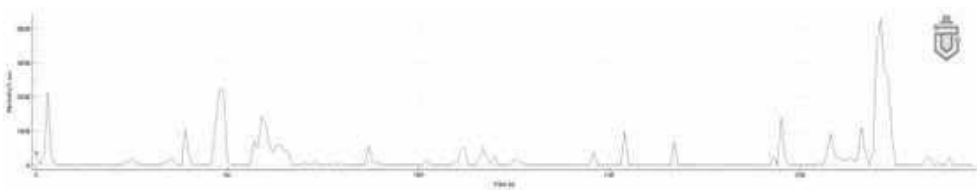
Figure 2. Countries reached by the TikTok application in the years 2016-2022



Source: Own research based on Nacionalinis Kibernetinio Saugumo Centras...

It is also noteworthy that during the study, it was found that the application downloads large amounts of executable code: during the initial launch, 600 MB of data was downloaded from servers, including program code that was not present in the installed application.

Figure 3. Data flow chart of the application from servers in the years 2016-2022



Source: Own research based on Nacionalinis Kibernetinio Saugumo Centras, *Mobiliosios aplikacijos "TikTok"...*

The analysed data transmitted by the "TikTok" application are encrypted using mTLS (Mutual Transport Layer Security). During the study, files containing mTLS certificates were identified¹². Collected user data may be disclosed for purposes related to legal proceedings, law enforcement requests, court proceedings, or government

¹² A list of products belonging to ByteDance, which can be found on their official website at <https://www.bytedance.com/en/products>. [12.12.2025].

inquiries. Furthermore, from a political standpoint, "TikTok" aligns with the trend in which various providers associated with Russia and China utilize infrastructure of data centres located in EU countries to provide their services. Due to the extensive network operation system, spread across a wide geographical area, it is difficult to reasonably ascertain that the final station transmitting sensitive user data is located in a country where GDPR regulations apply¹³.

It should be noted that these findings of the analysis translated into the internal policy of President Joe Biden's administration, which since 2023 has prohibited its employees from using it on official devices. More than half of the US states, Congress, and military structures have imposed similar regulations on their employees. Furthermore, the efforts of the Biden administration are focused on potentially banning the platform throughout the United States. Following the lead of the USA, TikTok has been banned on official phones in many Western countries and public sector institutions. This has already happened in Canada, New Zealand, Belgium, the United Kingdom, France, Taiwan, Denmark, as well as the European Commission, the European Parliament, and NATO. Meanwhile, TikTok's CEO Shou Zi Chew, speaking before the US House of Representatives in March 2023, assured that the company is independent of the political regime in Beijing. He also stated that the Chinese regime has never asked his company for data from the application¹⁴.

In 2024, the TikTok application issue gained momentum when in April the US House of Representatives voted on a bill potentially banning the use of TikTok in the United States. Furthermore, the bill proposes the possibility of banning TikTok's operations in the United States if the Chinese company ByteDance does not sell the platform to an entity unrelated to the authorities of the People's Republic of China. According to American political elites, the Chinese social media platform is subservient to the regime in Beijing and is used to spread propaganda, gather sensitive user data from the USA, manipulate algorithms, and potentially engage in device surveillance where the program is installed¹⁵. In response, the Chinese company invested in the "Texas project", simultaneously moving servers to the USA and ensuring that data does not leave the continent. Furthermore, a similar project is ongoing in the European Economic Area. Despite the lack of evidence that the application poses a threat to the national security of the United States, this has strategic significance for triggering a positive domino effect among other countries. This may prove significant in the election year in the USA and other countries¹⁶.

In the case of Poland, TikTok has no restrictions, and state institutions also use the platform. Mainly for communication, just like with Facebook, Instagram, or

¹³ *Nacionalinis Kibernetinio Saugumo Centras...*

¹⁴ *TikTok częściowo zakazany w Nowym Jorku. Czy w Polsce są jakieś ograniczenia?*, <https://forsal.pl/lifestyle/technologie/artykuly/9277230,tiktok-czesciowo-zakazany-w-nowym-jorku-czy-w-polsce-sa-jakies-ograni.html> [22.04.2024].

¹⁵ *Możliwy zakaz TikToka. Izba Kongresu USA przegłosowała ustawę*, https://wydarzenia.interia.pl/zagranica/news-mozliwy-zakaz-tiktoka-izba-kongresu-usa-przeglosowala-ustawe,nId,7463407#utm_source=paste&utm_medium=paste&utm_campaign=safari [22.04.2024].

¹⁶ *Amerykianie dyscyplinują Pekin za wspieranie Rosji*, „Dziennik. Gazeta Prawna”, 23.04.2024.

platform x (Twitter). Additionally, the analysed platform has been actively developing in the Polish market since 2021, as well as in key markets in Central Europe, including Romania, Hungary, and the Czech Republic, resulting in the opening of a TikTok office in Poland in 2021. The company's main goal is to shape awareness of the platform in the CEE region¹⁷.

Analysis of the TikTok Application in Poland

In January 2022, the total population of Poland reached 37.77 million. In the same month, there were 32.86 million internet users in Poland, with an internet penetration rate of 87.0 percent of the total population. Between 2021 and 2022, the number of social media users in Poland increased by 1.3 million (+5.0 percent), reaching a total of 27.2 million profiles across various platforms. At the beginning of 2022, Facebook had 17.65 million users in Poland, YouTube had 27.20 million, and Instagram had 10.70 million. Data published in ByteDance advertising resources indicate that TikTok, on the other hand, reached 7.70 million users aged 18 and above¹⁸. The undeniable popularity and influence of the TikTok application on Polish users align with the global trend. The increasing private sector investment in the application indicates its potential impact on user data security in Poland. It is projected that the advertising reach on TikTok in Poland will continue to grow steadily from 2024 to 2029, with an increase of 0.8 million users (+9.36 percent).

Analysing the Polish market, it is evident that the TikTok application demonstrates a dynamic growth trend in the country. The private sector, including small and medium-sized enterprises, shows significant interest in application, utilizing it as a platform to promote their businesses, concepts, products, and services¹⁹.

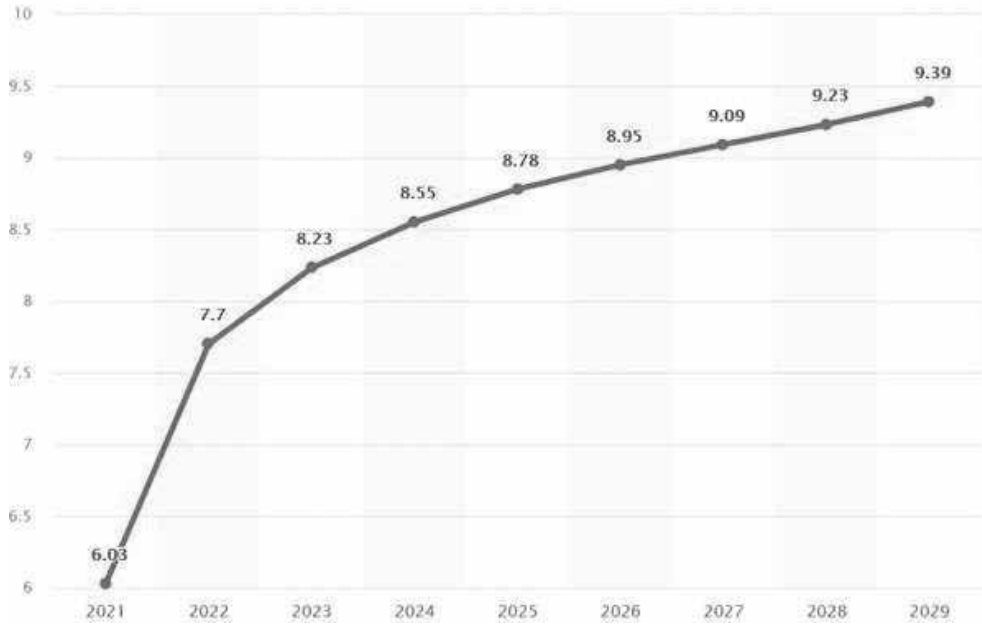
Regarding the security of the TikTok application in Poland, it was observed that, after conducting a static analysis of TikTok software files, a file named "local_prefs.json" was discovered, containing a list of server domains. Based on these domains, associated IP addresses were located. Utilizing the GeoIP database, cities in Poland associated with these IP addresses were identified. Additionally, upon analysing the "StrategyData.db" database related to TikTok software, a file named "node_optimizer" was found, containing information about servers and their associated IP addresses (see Table 1).

¹⁷ *TikTok otwiera biuro w Polsce, zatrudni kilkudziesięciu pracowników i przedstawi swoją ofertę dla biznesu*, Newsroom TikTok, 2021, <https://newsroom.tiktok.com/pl-pl/tiktok-opens-an-office-in-poland-will-hire-several-dozen-employees-and-will-present-its-offer-for-business> [22.04.2024].

¹⁸ S. Kemp, *Digital 2022: Global Overview Report*, Data Reportal 2022, <https://datareportal.com/reports/digital-2022-global-overview-report> [22.04.2024].

¹⁹ *Ilu Polaków korzysta z TikToka? Chińska firma ujawnia dane*, 2023, <https://www.benchmark.pl/aktualnosc/tiktok-zyskuje-popularnosc-w-polsce-juz-ponad-10-mln-uzytownikow.html> [22.04.2024].

Figure 4. Number of TikTok advertising users in Poland from 2021 to 2029 (in millions)



Source: Number of users of TikTok advertising in Poland 2021-2029, 2024.

Table 1: Analysis of the node_optimizer table in the StrategyData.db databas

Reference to the server	IP Address	City
https://tos-quic-gcppl.tiktokcdn.com	34.116.161.44	Warsaw
pull-flv-l1-va01.tiktokcdn.com	163.171.139.13	The specific city was not identified.
pull-flv-f1-va01.tiktokcdn.com	163.171.139.136	The specific city was not identified.
pull-flv-f1-gcp01.tiktokcdn.com	163.171pull-flv-f1-sg01.tiktokcdn.com.139.136	The specific city was not identified.
pull-flv-l1-sg01.tiktokcdn.com	163.171.139.136	The specific city was not identified.
pull-flv-l1-gcp01.tiktokcdn.com	163.171.139.136	The specific city was not identified.
pull-flv-l1-va01.tiktokcdn.com	163.171.139.136	The specific city was not identified.
pull-flv-f1-va01.tiktokcdn.com	163.171.139.136	The specific city was not identified.

pull-flv-f1-gcp01.tiktokcdn.com	163.171.139.136	The specific city was not identified.
pull-flv-l1-sg01.tiktokcdn.com	163.171.139.136	The specific city was not identified.
pull-flv-l1-gcp01.tiktokcdn.com	163.171.139.136	The specific city was not identified.
pull-cmaf-l10-gcp01.tiktokcdn.com	163.171.139.125 195.181.166.184	The specific city was not identified.
push-rtmp-l1-va01.tiktokcdn.com	101.33.10.13 203.205.224.23	The specific city was not identified.

Source: Own elaboration based on Nacionalinis Kibernetinio Saugumo Centras, *Mobiliosios aplikacijos "TikTok"...*

Additionally, during the simulation of the application's operation, connections were recorded with addresses associated with TikTok and ByteDance (see Table 2).

Table 2: List of persistent connections during simulated operation

Reference to the server	IP address	City
92.123.189.19	mcs-va.tiktokv.com.edgekey.net	Warsaw
92.123.189.40	mon-i18n.tiktokv.com.edgekey.net	Warsaw
92.123.189.58	starling-va.tiktokv.com.edgekey.net	Warsaw
92.123.189.96	feedback- va.tiktokv.com.edgekey.net	Warsaw
92.123.189.107	oec16-normal- useast1a.tiktokv.com.edgekey.net	Warsaw
104.94.100.160	mssdk16-normal- useast1a.tiktokv.com.edgekey.net	Warsaw
104.94.100.162	search16-normal-c- useast1a.tiktokv.com.edgekey.net	Warsaw
104.94.100.169	search16-normal-c- useast1a.tiktokv.com.edgekey.net	Warsaw
104.94.100.170	search16-normal-c- useast1a.tiktokv.com.edgekey.net	Warsaw
104.94.100.176	search16-normal-c- useast1a.tiktokv.com.edgekey.net	Warsaw
104.94.100.177	search16-normal-c- useast1a.tiktokv.com.edgekey.net	Warsaw

Source: Own analysis based on Nacionalinis Kibernetinio Saugumo Centras...

Analysing the above data, one can conclude that the TikTok application requires access to a significant amount of sensitive data. The most significant arguments to support this thesis include:

- a) "TikTok" requires access to a large amount of sensitive data. There is a probability that, alongside the necessary permissions for the application to function, additional permissions may exist, raising doubts.

- b) By downloading and executing program code without the user's knowledge, there is a risk that the functionality may be remotely altered. New features that previously did not exist could significantly modify the boundaries of potential impact scenarios. In the application's database and configuration files, several unique IP addresses were identified.
- c) During the investigation, the application connected to 12 addresses, of which 11 were found in the application's database (11 in Poland, see Table 2).
- d) According to TikTok's privacy policy, the system collects all personal user data, including information about interests, gender, and age.

The Chinese technology as an element of international policy strategy

Not only is the TikTok application increasingly embedded in social research in the context of escalating geopolitical tensions between China and other Western states. It is emphasized that TikTok has transformed from an entertainment digital platform into a discourse on state-focused security²⁰. At the same time, the growing importance of China in international relations has been recognized as one of the most significant changes in global relations at the turn of the century²¹. Chinese tools and techniques for conducting international relations are not only based on multi- and bilateral relations but extend much wider – to strategic infrastructure investments in specific countries. Chinese companies are, for example, a significant force in the African telecommunications market, which is a focus of Chinese foreign policy. For instance, Transsion Holdings holds an impressive 64% share in the African mobile phone sector and is also a leading player in the smartphone segment, controlling 36% of the market. Similarly, Huawei is a key player in building 4G telecommunication infrastructure in Africa, accounting for as much as 75% of the projects completed. However, controversies exist around the practices of these companies, especially concerning the export of surveillance technologies to certain African countries such as Angola, Ethiopia, and Zimbabwe²². The interest in Africa is evidenced by the construction of the African Union headquarters in Addis Ababa in 2012. Shortly after the completion of the building, which was supposed to be a gesture of assistance from the People's Republic of China, it was revealed through journalistic investigation that the servers in the building housing the headquarters of the African Union had been hacked by the Chinese, and the rooms were riddled with bugs²³. The hidden intent to acquire data and thus influence the global socio-political system by China also takes on surprising proportions in Europe: the quoted Estonian report indicates the possibility, through monopolizing Chinese expansion in selected industries, of

²⁰ W. Miao, D. Huang, Y. Huang, *More than Business: The de-Politicisation and Re-Politicisation of TikTok in the Media Discourses of China, America and India (2017–2020)*, "Media International Australia" 2023, nr 1, p. 97-114.

²¹ M. Lanteigne, *Chinese Foreign Policy: An Introduction*, Routledge, Taylor & Francis Group 2020, p. 15.

²² F. Kaczmarek, *Chiny jako aktor bezpieczeństwa w Afryce*, „Przegląd Politologiczny” 2022, no. 1, p. 29.

²³ A. Lelonek, *Siedziba Unii Afrykańskiej była zhakowana i podsłuchiwana przez ChRL? Pekin zaprzecza*, 2018, <https://cyberdefence24.pl/armia-i-sluzby/siedziba-unii-afrykanskiej-byla-zhakowana-i-podsluchiwana-przez-chrl-pekina-zaprzecza> [22.04.2024].

dependence on the market, and even Chinese components in photovoltaic farms can be used for their remote shutdown. According to the Estonian service, China aims to undermine the influence of Western countries in the technology sector, including that used in renewable energy sources (RES), in a non-obvious way affecting the energy sector in Europe. Meanwhile, the Americans found in purchased Chinese cranes in their ports communication devices that, in their opinion, were not used for normal work. A special investigation was initiated, during which, among other things, wireless modems were discovered that could be remotely controlled²⁴. Such actions, along with the Chinese enterprise's policy towards TikTok application users, once again seem to confirm the assumptions of the Estonian Foreign Intelligence Service: China is pursuing a long-term policy aimed at creating a gap between Europe and the United States. At the same time, the Chinese Global AI Governance Initiative is another example of building an anti-Western Chinese ecosystem²⁵. This policy is also pursued towards Poland: in the National Intelligence Law of the People's Republic of China, there are provisions enabling special services to collect and process intelligence data in cooperation with various institutions, organizations, and citizens. The use of 5G or LTE network technologies could provide access to data regarding user behaviours and preferences. For example, if Huawei had access to a 5G network in one of the major cities in Poland, Chinese services could use this data to create psychological profiles of Poles²⁶.

Conclusions

The examination of the presented research hypotheses proved to be justified - only within the year 2023, China significantly increased its influence in Europe²⁷. The TikTok application poses a threat of diverse nature: from health aspects such as orbital emphysema²⁸, through psychosocial aspects such as increased acceptance of plastic surgery²⁹, to the influence of disinformation - primarily through the phenomenon of memorization in political communication³⁰. The TikTok application may be part of a broader geopolitical strategy of China. Through the proven collection and processing of data of users beyond what is necessary for an entertainment service, both research

²⁴ B. Breczko, *Amerykianie podejrzewają, że Chiny szpiegują ich portowe dźwigi*, 2024, <https://wyborcza.biz/biznes/7,177150,30776171,amerykanie-podejrzewaja-ze-chiny-szpieguja-ich-portowe-dzwigi.html?disableRedirects=true> [22.04.2024].

²⁵ *International Security and Estonia 2024*, Estonian Foreign Intelligence Service 2024, <https://raport.valisluureamet.ee/2024/en/>, p.73 [22.04.2024].

²⁶ W. Jakóbiak, *Jakóbiak: Chiny szpiegują Zachód. Teraz Polska?*, Biznes Alert, 2018, <https://biznesalert.pl/nowy-jedwabny-szlak-telekomunikacja-huawei-bezpieczenstwo/> [22.04.2024].

²⁷ *International Security and Estonia...*, p. 72.

²⁸ E. N. Woertz, S. Srivatsan, R. Kersten, *Orbital Emphysema Caused by a Tik-Tok Challenge*, "Ophthalmology", 2023.

²⁹ E. Shiah, A. Weidman, L. Valentine, A. Alvarez, J. Foppiani, S. Lin, *Capitalizing on social media: An evaluation of the public's preferences for plastic surgery social media content*, "Journal of Plastic, Reconstructive & Aesthetic Surgery" 2023, vol. 83, p. 308-17.

³⁰ J. Zeng, C. Abidin, *'#OkBoomer, Time to Meet the Zoomers': Studying the Memefication of Intergenerational Politics on TikTok*, "Information, Communication & Society" 2021, vol. 24, no. 16, p. 2459-2481.

hypotheses have been confirmed:

- a) a) Hypothesis 1 (H1): The TikTok application exposes Polish users to the risk of protection and leakage of personal data, and according to the privacy policy of ByteDance, the accumulated user data may be shared in accordance with the interests of hostile services.
- b) Hypothesis 2 (H2): The TikTok application can be used as a tool of influence in China's international policy.

As shown, the lack of proper protection and leakage of personal data through the researched application has occurred in other countries, leading to the introduction of regulatory norms by, among others, the USA and the European Union, limiting the use of the application by users in those countries, especially in the public sector.

Economic and social development largely depends on efficiently functioning teleinformatics systems, providing various services, including digital services in the public sector³¹. As demonstrated in the article, cybersecurity between the public and private sectors is interdependent. Confirmation of the research hypothesis regarding the possibility of influencing political systems by the Chinese state services is evidenced by the fact that such espionage activities have occurred in the past (including deliberate eavesdropping on the headquarters of the African Union). The risk associated with using TikTok and the unawareness on the part of users regarding the quantity and quality of data collected by China through the application lies in the lack of compliance not only with European standards of personal data protection but also with the unawareness of the intended use of the collected data. This is all the more significant as the covert use of new technologies indicates a Chinese direction of an integrated political and technological ecosystem, based on its own tools to influence political systems worldwide. At the same time, such a policy of using new technologies seems to be an element of the strategy of international relations of undemocratic countries (but perhaps not only?).

Further research analysis would require addressing whether discrepancies between the security policy of the TikTok application and other espionage activities are still a tool of conducting foreign policy as soft power, or already a permanent and much more serious element of the political strategy of the People's Republic of China. Another area of research should be the analysis of different policies towards Chinese users of the TikTok application, where it may be used to engage youth in mental health³², compared to users from other parts of the world, where it serves a completely different function.

³¹ M. Karpiuk, *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, „*Studia Iuridica Lublinensia*” 2023, vol. 32, nr 2, p. 189.

³² Megan D. Chochol et al., *Harnessing Youth Engagement with Mental Health TikTok and Its Potential as a Public Health Tool*, „*Journal of the American Academy of Child & Adolescent Psychiatry*” 2023, vol. 62, no. 7, p. 710-712.

BIBLIOGRAFIA – REFERENCES**Studies:**

- Breczko B., *Amerykanie podejrzewają, że Chiny szpiegują ich portowe dźwigi*, 8.10.2024, <https://wyborcza.biz/biznes/7,177150,30776171,amerykanie-podejrzewaja-ze-chiny-szpieguja-ich-portowe-dzwigi.html?disableRedirects=true> [22.04.2024].
- Brunet A., Guichard J. P., *Chiny światowym hegemonem. Imperializm Państwa Środka*, Warszawa 2011.
- Brautigam D., *The Dragon's Gift: The Real Story of China in Africa*, New York 2009.
- Chochol M. D., *Harnessing Youth Engagement with Mental Health TikTok and Its Potential as a Public Health Tool*, „Journal of the American Academy of Child & Adolescent Psychiatry” 2023, vol. 62, no. 7, p. 710-712.
- Amerykanie dyscypliniują Pekin za wspieranie Rosji*, „Dziennik. Gazeta Prawna”, 23.04.2024.
- FBI ostrzega: TikTok to narzędzie wpływu Chin na Amerykanów*, 16.11.2022, <https://cyberdefence24.pl/cyberbezpieczenstwo/fbi-ostrzega-tiktok-to-narzedzie-wplywu-chin-na-amerykanow> [22.04.2024].
- Guo S., Hua, S., *New dimensions of Chinese Foreign Policy UK*. London 2007.
- Hładij A., *Międzykontynentalne pazury chińskiego smoka*, 1.02.2017, <https://www.space24.pl/miedzykontynentalne-pazury-chinskiego-smoka-analiza> [22.04.2024].
- Ilu Polaków korzysta z TikToka? Chińska firma ujawnia dane*, 23.10.2023, <https://www.benchmark.pl/aktualnosci/tiktok-zyskuje-popularnosc-w-polsce-juz-ponad-10-mln-uzytownikow.html> [22.04.2024].
- International Security and Estonia 2024*, 31.01.2024, <https://raport.valisluureamet.ee/2024/en/> [22.04.2024].
- Iqbal M., *TikTok Revenue and Usage Statistics, Business of apps*, 15.09.2022, https://uploads2.craft.co/uploads/operating_source/document/982548/57cb7f410c237c8e.pdf [22.04.2024].
- Jakóbiak W., *Jakóbiak: Chiny szpiegują Zachód. Teraz Polska?*, 31.10.2018, <https://biznesalert.pl/nowy-jedwabny-szlak-telekomunikacja-huawei-bezpieczenstwo> [22.04.2024].
- Jenkins H., *Kultura konwergencji. Zderzenie starych i nowych mediów*, przeł. M. Filiciak, M. Bernardowicz, Warszawa 2007.
- Kaczmarek F., *Chiny jako aktor bezpieczeństwa w Afryce*, „Przegląd Politologiczny” 2022, no. 1, p. 19-33. <https://doi.org/10.14746/pp.2022.27.1.2>.
- Karpiuk M., *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, „Studia Iuridica Lublinensia” 2023, vol. 32, no. 2, pp. 189-201. <https://doi.org/10.17951/sil.2023.32.2.189-201>.
- Kemp S., *Digital 2022: Poland*. 15 II 2022, <https://datareportal.com/reports/digital-2022-poland> [22.04.2024].
- Kowal R., *Chińska armia pokazała wideo z pociskami DF 16*, 7.02.2017, <https://tech.wp.pl/chinska-armia-pokazala-wideo-z-pociskami-df-16-6088523689538177a> [22.04.2024].
- Lanteigne M., *Chinese foreign policy: an introduction*, London-New York 2020.
- Lelonek A., *Siedziba Unii Afrykańskiej była zhakowana i podsłuchiwana przez ChRL? Pekin zaprzecza*, 1.02.2018, <https://cyberdefence24.pl/armia-i-sluzby/siedziba-unii-afrykanskiej-byla-zhakowana-i-podsluchiwana-przez-chrl-pekina-zaprzecza> [22.04.2024].
- Łoś R., *Potęga współczesnych Chin. Zarys problemu*, „Athenaeum. Polskie Studia Politologiczne” 2021, vol. 77, no. 1, p. 79-98. DOI:10.15804/athena.2023.77.05.
- Mozliwy zakaz TikToka. Izba Kongresu USA przegłosowała ustawę*, 20.04.2024, https://wydarzenia.interia.pl/zagranica/news-mozliwy-zakaz-tiktoka-izba-kongresu-usa-przeglosowala-ustawe,nId,7463407#utm_source=paste&utm_medium=paste&utm_campaign=safari [22.04.2024].

- Miao W., Huang D., Huang Y., *More than business: The de-politicisation and re-politicisation of TikTok in the media discourses of China, America and India (2017–2020)*, „Media International Australia” 2023, vol. 186, no. 1, p. 97-114. <https://doi.org/10.1177/1329878X211013919>.
- Mobiliosios aplikacijos „TikTok“ kibernetinio saugumo analizė*, 1.09.2023, https://www.nksc.lt/doc/biuleteniai/2023_06_01_TikTok.pdf [22.04.2024].
- Molo B., Cziomer E., Paterek A., *Współczesne stosunki międzynarodowe: wprowadzenie do stosunków międzynarodowych*, Kraków 2014.
- Number of users of TikTok advertising in Poland from 2017 to 2030*, 6.11.2024, <https://www.statista.com/forecasts/1259144/poland-tiktok-advertisement-reach> [22.04.2024].
- Pietrasiak M., Mierzejewski D., *Między wzrastaniem a harmonią – uwagi o chińskiej polityce zagranicznej*, [w:] *Chiny w stosunkach międzynarodowych*, red. M. Pietrasiak, D. Mierzejewski, Łódź 2012.
- Picquart P., *Imperium chińskie. Historia i terażniejszość chińskiej diaspory*, Warszawa 2006.
- Przychodniak M., *Internet jako narzędzie polityki Chińskiej Republiki Ludowej*, 04.08.2017, https://www.pism.pl/publikacje/Internet_jako_narz_dzie_polityki_Chi_skiej_Republiki_Ludo_wej [22.04.2024].
- Shiah E., Weidman A., Valentine L., Alvarez A., Foppiani J., Lin, S., *Capitalizing on social media: An evaluation of the public's preferences for plastic surgery social media content*, „Journal of Plastic, Reconstructive & Aesthetic Surgery” 2023, vol. 83, p. 308-317. <https://doi.org/10.1016/j.bjps.2023.05.010>.
- TikTok częściowo zakazany w Nowym Jorku. Czy w Polsce są jakieś ograniczenia?*, 18.08.2023, <https://forsal.pl/lifestyle/technologie/artykuly/9277230,tiktok-czesciowo-zakazany-w-nowym-jorku-czy-w-polsce-sa-jakies-ograni.html> [22.04.2024].
- TikTok otwiera biuro w Polsce, zatrudni kilkudziesięciu pracowników i przedstawi swoją ofertę dla biznesu*, 9.10.2021, <https://newsroom.tiktok.com/pl-pl/tiktok-opens-an-office-in-poland-will-hire-several-dozen-employees-and-will-present-its-offer-for-business> [22.04.2024].
- Trzeciak S., *Drzewo Kampanii Wyborczej 2.0. Czyli jak wygrać wybory*, Warszawa 2023.
- Woertz E. N., Srivatsan S., Kersten R., *Orbital Emphysema Caused by a Tik-Tok Challenge*, „Ophthalmology” 2023, p. 1476. <https://doi.org/10.1016/j.ophtha.2023.11.013>.
- Zeng J., Abidin C., *“#OkBoomer, time to meet the Zoomers”: studying the memefication of intergenerational politics on TikTok*, „Information, Communication & Society” 2021, vol. 2, no. 16, p. 2459-2481. <https://doi.org/10.1080/1369118X.2021.1961007>.



