

Krzysztof Stefan
Uniwersytet Jagielloński
ORCID: 0000-0003-2183-9078

Oleksandr Manachynskyi
Uniwersytet Jagielloński
ORCID: 0009-0005-2207-8399

Chińskie cyberspiegostwo na przykładzie case study TikTok'a i Huawei'a

Wstęp

W 2049 r. przypada setna rocznica powstania Chińskiej Republiki Ludowej. Władze ChRL – wschodzącego globalnego mocarstwa – wytyczyły ambitny cel: Chiny mają stać się najpotężniejszym państwem pod względem gospodarczym i militarnym, oraz uzyskać prymat na polu rozwiązań przemysłowych i technologicznych. Realizując te cele Chiny wykorzystują wszelkie dostępne do tego środki, w szczególności postęp technologiczny inwestując ogromne ilości pieniędzy w sektor badań i rozwoju, wspierając również w ramach tych działań chińskie firmy. Ekspansja na świat powstających na bazie chińskich ambicji firm, które często są niezwykle konkurencyjne, niesie ze sobą jednak szereg zagrożeń.

Temat zagrożeń powiązanych z chińskimi przedsiębiorstwami jest omawiany w wielu tekstach, szczególnie amerykańskich. Jest to także element tamtejszej debaty publicznej, pojawia się nie tylko w czasopiśmie naukowych, czy raportach rządowych, ale także w artykułach prasowych. W oparciu o analizę aktualnej literatury przedmiotu artykuł ten ma na celu

kompleksowo przedstawić dwa case study – Huawei i TikTok – oraz płynące z nich wnioski, aby zwiększyć świadomość społeczeństwa i społeczności akademickiej na temat potencjalnych zagrożeń.

TikTok

TikTok to chińska aplikacja społecznościowa, która umożliwia użytkownikom tworzenie, udostępnianie i oglądanie filmów, zazwyczaj trwających od 15 sekund do kilku minut, chociaż górny limit długości filmu to 60 minut. Aplikacja zyskała ogromną popularność na całym świecie, z ponad miliardem aktywnych użytkowników miesięcznie. TikTok jest znany z różnorodnych treści oraz z potężnego algorytmu rekomendacji, który dostosowuje treści do zainteresowań użytkowników, co przyczynia się do jego globalnego zasięgu i wpływu na trendy w mediach społecznościowych.

Ochrona danych

Jedną z głównych obaw związanych z aplikacją TikTok koncentruje się na jego spółce matczynej, ByteDance, i jej relacjach z chińskimi władzami. W Chinach ustawa o bezpieczeństwie narodowym z 2017 r. wymaga od firm „wspierania, asystowania i współpracy z wywiadem państwowym”. Doprowadziło to do obaw, że TikTok, pomimo twierdzeń o niezależności, może zostać zmuszony do przekazania danych użytkowników na żądanie chińskich władz. W przypadku uzyskania dostępu do tych danych przez chińskie władze, mogłyby one zostać wykorzystane do różnych celów, w tym inwigilacji, szpiegostwa i operacji wywierania wpływu. Ogromne bazy danych TikTok mogą zostać wykorzystane do wpływania na opinię publiczną lub do kierowania kampanii dezinformacyjnych na konkretne osoby¹.

Wpływ na zdrowie psychiczne i operacje psychologiczne

Badania wykazały, że długotrwałe korzystanie z aplikacji TikTok może prowadzić do zmniejszenia koncentracji uwagi. Korzystanie z TikToka przez ponad 90 minut dziennie jest szczególnie szkodliwe, zwłaszcza dla młodszych użytkowników. W odpowiedzi na te obawy TikTok podjął pewne środki w celu złagodzenia tych skutków. Platforma pozyskała popularnych

¹ P. Suciū, *The TikTok Ban Is Truly An Issue Of National Security*, „Forbes”, 15.03.2024, [on-line:] <https://www.forbes.com/sites/petersuciū/2024/03/15/the-tiktok-ban-is-truly-an-issue-of-national-security/> – 24.07.2024.

influencerów do promowania przerw od czasu spędzanego przed ekranem i emituje ostrzeżenia, aby przypominać użytkownikom o zrobieniu sobie przerwy. Pomimo tych wysiłków, podstawowy projekt aplikacji pozostaje niezmieniony, nadal stanowiąc zagrożenie dla koncentracji uwagi użytkowników².

Poza indywidualnymi efektami psychologicznymi, TikTok jest postrzegany jako narzędzie w szerszych ramach strategicznych, jako część chińskiej walki cywilizacyjnej z Zachodem, mającej na celu szerzenie dezinformacji i wspieranie podziałów wśród zachodnich społeczeństw³. ByteDance został również oskarżony o promowanie płytkich, pozbawionych jakiegokolwiek wartości treści wśród zachodnich dzieci, w przeciwieństwie do treści edukacyjnych serwowanych w chińskiej aplikacji Douyin⁴. Faktem jest, że naukowcy z Citizen Lab Uniwersytetu w Toronto nie znaleźli żadnych jawnie złośliwych zachowań w działaniach TikTok, to jednak obawy dotyczące jego potencjału co do manipulacji psychologicznej pozostają znaczące. Wpływ aplikacji na młodych, podatnych na wpływy użytkowników może prowadzić do długoterminowych skutków kulturowych i społecznych, wspierając strategiczne cele jej spółki matczynej, ByteDance⁵.

Cenzura i moderacja

Dochodzenia, przeprowadzone przez The Intercept, ujawniły, że TikTok tłumił posty zmarginalizowanych społeczności. Wewnętrzne dokumenty, które wyciekły z TikTok, wykazały, że moderatorzy zostali poinstruowani, aby tłumić treści od użytkowników, którzy wydawali się biedni lub niepełnosprawni, lub którzy opowiadali się za prawami osób LGBTQ+. Intencją tych działań było podobno zapobieganie nękanii, ale rezultatem była marginalizacja już niedostatecznie reprezentowanych grup, co jeszcze

² D. Price, *7 Reasons TikTok Is Bad for Everyone*, MUO, 16.02.2023, [on-line:] <https://www.makeuseof.com/is-tiktok-bad> – 24.07.2024.

³ S. Smalley, *TikTok data collection, influence operations potential draw U.S. NSA concern*, Reuters, 7.03.2023, [on-line:] <https://www.reuters.com/world/us/us-nsa-director-concerned-by-tiktok-data-collection-use-influence-operations-2023-03-07/> – 24.07.2024.

⁴ V. Jolly, *Comment la Chine protèges les enfants et rend les nôtres débiles avec le réseau social TikTok*, „Le Figaro”, 15.12.2022, [on-line:] <https://www.lefigaro.fr/secteur/high-tech/comment-la-chine-protege-ses-enfants-et-rend-les-notres-debiles-avec-le-reseau-social-tiktok-20221214> – 24.07.2024.

⁵ P. Lin, *TikTok vs Douyin: A Security and Privacy Analysis*, The Citizen Lab, 22.03.2021, [on-line:] <https://citizenlab.ca/2021/03/tiktok-vs-douyin-security-privacy-analysis> – 24.07.2024.

bardziej uciszyło ich głosy na platformie⁶. TikTok został również oskarżony o cenzurowanie treści związanych z tematami wrażliwymi politycznie. Badania i doniesienia medialne wskazują, że TikTok usuwał posty dotyczące masakry na placu Tiananmen, protestów w Hongkongu oraz krytyki chińskich władz⁷.

Działania prawne i regulacyjne

W 2020 r. Indie stały się pierwszym dużym krajem, który nałożył kompleksowy zakaz na TikTok. Władze indyjskie powołały się na obawy związane z bezpieczeństwem narodowym, twierdząc, że aplikacja ta była „szkodliwa dla suwerenności i integralności Indii, obrony Indii, bezpieczeństwa państwa i porządku publicznego”⁸.

W Stanach Zjednoczonych TikTok spotkał się z szeroko zakrojoną kontrolą. Administracja Donalda Trumpa próbowała zakazać aplikacji za pomocą zarządzeń wykonawczych, powołując się na zagrożenia dla bezpieczeństwa narodowego związane z możliwością uzyskania dostępu do danych użytkowników przez chińskie władze. Jednakże zaistniały przeszkody prawne i próby zakazania TikTok zostały ostatecznie wstrzymane przez sądy federalne. Za czasów administracji Joe Bidena sytuacja poszła jeszcze dalej. Od 24 kwietnia 2024 r., chińska firma ByteDance, ma 270 dni na sprzedaż TikTok. Niezastosowanie się do tego wymogu doprowadziłoby do poważnych konsekwencji: TikTok zostałby zakazany w Stanach Zjednoczonych⁹.

UE nie nałożyła całkowitego zakazu na TikTok, ale wyraziła poważne obawy dotyczące ochrony danych i prywatności. Instytucje UE zakazały swoim pracownikom posiadania TikTok na telefonach służbowych. W wewnętrznej wiadomości e-mail wysłanej do pracowników stwierdzono, że ruch ten miał na celu zmniejszenie narażenia na cyberataki, ponieważ aplikacja ta gromadzi wiele danych na urządzeniach mobilnych,

⁶ S. Biddle, P. Ribeiro, T. Dias, *Invisible Censorship*, The Intercept, 16.03.2020, [on-line:] <https://theintercept.com/2020/03/16/tiktok-app-moderators-users-discrimination> – 24.07.2024.

⁷ A. Hern, *Revealed: how TikTok censors videos that do not please Beijing*, „The Guardian”, 25.09.2019, [on-line:] <https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing> – 24.07.2024.

⁸ R. Zhong, K. Schultz, *With India's TikTok Ban, the World's Digital Walls Grow Higher*, „The New York Times”, 30.06.2020, [on-line:] <https://www.nytimes.com/2020/06/30/technology/india-china-tiktok.html> – 24.07.2024.

⁹ S. Nover, *The Grim Reality of Banning TikTok*, „Time”, 15.03.2024, [on-line:] <https://time.com/6952889/tiktok-ban-freedom-of-speech-essay> – 24.07.2024.

które mogłyby zostać wykorzystane do przeprowadzenia ataku na instytucje Unijne. Co więcej, Irlandzka Komisja Ochrony Danych, główny regulator prywatności TikTok w UE, ma zdecydować, czy firma bezprawnie przekazuje dane europejskich użytkowników do Chin¹⁰.

Perspektywy rozwoju ochrony danych TikTok na rynkach zachodnich

W odpowiedzi na obawy dotyczące prywatności i bezpieczeństwa danych, w szczególności ze strony amerykańskich i europejskich organów regulacyjnych, TikTok uruchomił Project Texas i Project Clover. Pierwsza inicjatywa ma na celu zlokalizowanie przechowywania danych dla użytkowników z USA przez firmę z siedzibą w Stanach. W ten sposób TikTok stara się złagodzić obawy o dostęp chińskich władz do danych użytkowników. Oprócz działań publicznych, TikTok znacznie zwiększył swoje wysiłki lobbingsowe w USA. Działania te mają na celu wywarcie wpływu na decydentów i odpieranie potencjalnych zakazów i restrykcyjnych przepisów¹¹.

Na rynku unijnym, TikTok uruchomił inicjatywę Project Clover, mającą na celu ochronę danych europejskich użytkowników. Plan TikTok obejmuje przechowywanie większej ilości danych na europejskich serwerach i umożliwienie europejskim firmom przeprowadzenia szeroko zakrojonego audytu środków cyberbezpieczeństwa i ochrony danych. Niemniej, główny europejski lobbysta TikTok, Theo Bertram, powiedział, że całkowite powstrzymanie wysyłania europejskich danych do Chin jest prawie niemożliwe¹².

Huawei

Huawei jako chiński czempion rozwoju technologii 5G

W czasach Internetu i nowych technologii niezbędne jest zapewnienie krytycznej infrastruktury cyfrowej, dzięki której zarówno podmioty państwowe, jak i prywatne będą mogły stabilnie funkcjonować. Infrastruktura

¹⁰ C. Goujard, *What the hell is wrong with TikTok?*, „Politico” 22.03.2023, [on-line:] <https://www.politico.eu/article/tiktok-china-west-europe-ban-app-espionage-surveillance> – 24.07.2024.

¹¹ M. Perault, *What Happened to TikTok's Project Texas?*, Lawfare, 20.03.2024, [on-line:] <https://www.lawfaremedia.org/article/what-happened-to-tiktok-s-project-texas> – 24.07.2024.

¹² C. Goujard, L. Kayali, *TikTok launches 'Project Clover' charm offensive to fend off European bans*, „Politico” 8.03.2023, [on-line:] <https://www.politico.eu/article/tiktok-pitches-data-security-plan-to-fend-off-european-bans> – 24.07.2024.

cyfrowa wymaga ciągłego wdrażania coraz to nowych rozwiązań celem zapewnienia jej adekwatności do potrzeb – jedną z najnowszych technologii, której wdrażanie jest aktualnie kluczowe jest 5G. Do niedawna jedynymi firmami, które miały możliwość skonstruowania kompletnej sieci 5G były Nokia, Ericsson i Huawei, co jednak zmienia się ze względu na nową powszechnie dostępną technologię Open Ran¹³. Równolegle podobna sytuacja dotyczy kwestii produkcji chipów do telefonów obsługujących technologię 5G – w tym przypadku na rok 2022 jedynymi firmami, mającymi technologię do produkcji takich chipów były MediaTek, Qualcomm, Samsung i Huawei¹⁴. To przykłady obrazujące znaczenie i przewagę technologiczną Huawei, który na początek 2023 r. był największym na świecie dostawcą sieci 5G oraz sprzedawcą sprzętu telekomunikacyjnego¹⁵. Te przykłady powinny jasno obrazować, dlaczego Huawei jest istotnym elementem chińskiego rozwoju technologicznego oraz dlaczego jego ewentualna sekurytyzacja czy wykorzystanie przez chiński wywiad są realnymi zagrożeniami.

Chińskie rozwiązania prawne

Podstawowym powodem obaw wobec ekspansji chińskich przedsiębiorstw są chińskie rozwiązania prawne, które obowiązują wywodzące się z Chin firmy, nawet jeśli te operują na terenie innych krajów. Konkretnie mowa o rozwiązaniu z chińskiego aktu prawnego *National Intelligence Law*, który, jak zauważa raport Federalnej Komisji Komunikacji USA w art. 7, obliguje wszystkie organizacje i obywateli do wsparcia, pomocy i współpracy z narodowymi działaniami wywiadowczymi¹⁶. Takie rozwiązania prawne oczywiście wprost wykazują, że chińskie firmy, jak właśnie Huawei, mogą być z łatwością wykorzystywane przez chiński wywiad. W erze globalizacji najsilniejsze gospodarczo państwa takie jak Chiny czy USA mają możliwość wykorzystywania swojej potęgi gospodarczej do stosowania swoich regulacji prawnych poza swoją jurysdykcją¹⁷, jednak chiński autorytarny system jest tutaj czynnikiem, który dalece wzmacnia

¹³ G.J. Moore, *Huawei, Cyber-Sovereignty and Liberal Norms: China's Challenge to the West/Democracies*, „Journal of Chinese Political Science” 2022, vol. 28, s. 152.

¹⁴ Tamże.

¹⁵ N. Berman, L. Maizland, A. Chatzky, *Is China's Huawei a Threat to U.S. National Security?*, Council on Foreign Relations, 8.02.2023, [on-line:] <https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security> – 24.07.2024.

¹⁶ US Federal Communications Commission, Designation Order DA 20-690, [on-line:] <https://docs.fcc.gov/public/attachments/DA-20-690A1.pdf> – 24.07.2024.

¹⁷ M. Cartwright, *Internationalising State Power through the Internet: Google, Huawei and Geopolitical Struggle*, „Internet Policy Review” 2020, vol. 9, no. 3, s. 4.

zdolność do przeprowadzania takich działań. Ponadto, odnośnie niepokojących rozwiązań prawnych, należy zauważyć, że dotyczy się to również firm operujących poza Chinami, ale będących własnością innych podmiotów z siedzibą w Chinach tak jak jest to w przypadku TikToka, którego właścicielem jest chiński ByteDance. Zostało to zauważone w liście z 2019 r. senatorów Charlesa E. Schumera i Toma Cottona do dyrektora amerykańskiego wywiadu¹⁸.

Przykłady zarzutów wobec Huawei

Oprócz problematycznych rozwiązań na poziomie systemu prawnego ChRL, wobec Huawei oraz innych chińskich firm pojawił się szereg konkretnych zarzutów, który dodatkowo potwierdza realność zagrożenia. Pierwszym przykładem mogą być nieprawidłowości wykazane w raporcie z 2012 r. stałej komisji ds. wywiadu, w którym stwierdzono, że Huawei nie był w stanie wykazać niezależności od rządu chińskiego. Założyciel Huawei Ren Zhengfei był wcześniej dyrektorem Akademii Inżynierii Informacyjnej chińskiej armii, a ponadto w toku śledztwa Huawei odmówił przekazania danych na temat prowadzonych przez firmę badań¹⁹. Kolejny z przykładów dotyczy potencjalnego zagrożenia związanego z zamontowaniem sprzętu Huawei w pobliżu amerykańskich silosów, w których znajdowały się międzykontynentalne pociski balistyczne z głowicami nuklearnymi – po znalezieniu tego sprzętu rząd J. Bidena podjął śledztwo dotyczące płynących z tego potencjalnych zagrożeń, takich jak poinformowanie Pekinu o wystrzeleniu rakiety w momencie jej odpalenia²⁰. W tym przypadku potencjalne zagrożenie zostało potwierdzone sytuacją z maja 2024 r., kiedy rząd USA zmusił powiązaną z Chinami firmę do sprzedania działki w pobliżu innego amerykańskiego silosu z rakietami balistycznymi²¹.

¹⁸ C.E. Schumer, T. Cotton, *TikTok letter to the Director of National Intelligence*, Senate Democrats, 23.10.2019, [on-line:] <https://www.democrats.senate.gov/imo/media/doc/10232019%20TikTok%20Letter%20-%20FINAL%20PDF.pdf> – 24.07.2024.

¹⁹ M. Rogers, D. Ruppertsberger, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, U.S. House of Representatives, 8.10.2012, [on-line:] [https://stacks.stanford.edu/file/druid:rm226yb7473/Huawei-ZTE%20Investigative%20Report%20\(FINAL\).pdf](https://stacks.stanford.edu/file/druid:rm226yb7473/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf) – 24.07.2024.

²⁰ A. Alper, *Exclusive: U.S. probes China's Huawei over equipment near missile silos*, Reuters, 21.07.2022, [on-line:] <https://www.reuters.com/world/us/exclusive-us-probes-chinas-huawei-over-equipment-near-missile-silos-2022-07-21> – 24.07.2024.

²¹ A. Alper, D. Ljunggren, *US to force China-linked firm to sell land near US missile silos*, Reuters, 13.05.2024, [on-line:] <https://www.reuters.com/world/us/us-force-china-linked-firm-sell-land-near-us-missile-silos-2024-05-13> – 24.07.2024.

Polityka USA wobec Huawei

Konkretne działania rządu Stanów Zjednoczonych wobec Huawei trwają od 2017, kiedy amerykański Kongres ograniczył możliwość stosowania sprzętu Huawei i ZTE przez Departament Obrony²². Kolejne restrykcje w 2018 r. dotyczyły już ograniczenia stosowania sprzętu tych firm przez wszystkie agencje rządu USA, a w latach 2019 i 2020 Departament Sprawiedliwości wytoczył pozwy wobec Huawei dotyczące oszustw finansowych, konspiracji celem kradzieży tajemnic czy złamania sankcji²³. Ponadto administracja prezydenta Bidena rozpoczęła również ostrą politykę przeciwko Huaweiowi naciskając na swoich europejskich sojuszników. To doprowadziło do wprowadzenia przez UE ostrzeżenia przeciw korzystaniu z produktów Huawei do obsługi sieci 5G, a później do wprowadzenia przez część państw UE oraz przez Wielką Brytanię legislacji bezpośrednio lub w perspektywie średniookresowej pozbywającej się sprzętu Huawei z ich krajowej infrastruktury telekomunikacyjnej²⁴.

Podsumowanie

Podczas gdy chińskie firmy jak ByteDance i Huawei oferują niezwykle atrakcyjne produkty i usługi, takie jak TikTok oraz technologia sieci 5G, potencjalni użytkownicy oraz nabywcy tych usług i produktów, ale także krajowi prawodawcy, muszą być świadomi związanych z nimi potencjalnych zagrożeń podejmując decyzję wobec oferty chińskich przedsiębiorstw. Dwa omówione w tekście przykłady przedstawiają ogólny zarys problemu w oparciu o fakty, opinie oraz prawodawstwo, kładąc grunt pod dalsze rozważania nad zagraniczną ekspansją chińskich firm i równoległymi do niej zagrożeniami związanymi z bezpieczeństwem danych oraz cyberszpiegostwem, na poziomie zarówno przemysłowym, jak i narodowym. Przykład TikToka wskazuje, że zasadne byłoby również dalsze badanie wpływu chińskich aplikacji na dzieci i młodzież, zwłaszcza w kontekście ich rozwoju oraz kształtowania poglądów i nawyków.

²² N. Berman, L. Maizland, A. Chatzky, dz. cyt.

²³ J.C. Gallagher, *U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests*, Congressional Research Service, 1.05.2022, [on-line:] <https://crsreports.congress.gov/product/pdf/R/R47012/2#:~:text=In%20December%202017%2C%20Congress%20prohibited,%2D232%2C%20%A7889> – 24.07.2024.

²⁴ L. Cerulus, S. Wheaton, *How Washington chased Huawei out of Europe*, „Politico”, 23.11.2022, [on-line:] <https://www.politico.eu/article/us-china-huawei-europe-market> – 24.07.2024.

Omówione przypadki TikToka i Huawei obrazują również istotne zjawiska zachodzące we współczesnym świecie. Są przykładem narastającej na arenie międzynarodowej rywalizacji o kontrolę nad przepływem danych i rozwojem technologicznym, a także zwracają uwagę na dylemat pomiędzy praktykami wolnego rynku a bezpieczeństwem narodowym, wskazując również na problem określenia granic suwerenności w sferze cyfrowej.

Wartym zasygnalizowania jest również wpływ narastających obaw wobec chińskich firm i produktów na relacje ChRL z państwami zachodu. W kontekście gospodarczym jest to istotny czynnik mogący wywoływać ostrożność w kontaktach handlowych i w efekcie prowadzić do wprowadzania regulacji ograniczających wolność przepływu towarów z Chin. Dodatkowo z perspektywy bezpieczeństwa wspomniane obawy mogą wzmacniać negatywną percepcję Chin jako potencjalnego zagrożenia dla bezpieczeństwa państw zachodu.

Bazując na tych przykładach konieczne jest także zwiększenie świadomości społecznej i akademickiej na temat potencjalnych zagrożeń wynikających z tego zjawiska. Istnienie i wszechobecność wspomnianych niebezpieczeństw jasno wskazuje, że konieczne są odpowiednie regulacje i polityka ochrony danych na poziomie państwowym, dla których prze-myślanym uzupełnieniem mogą być również kampanie edukacyjne. Roz-sądnym rozwiązaniem, które mogłoby przeciwdziałać tym zagrożeniom wydaje się polityka dążenia państw do niezależności technologicznej, poprzez chociażby wspieranie lokalnych firm technologicznych i rozwój alternatywnych standardów.

Bibliografia

- Alper A., *Exclusive: U.S. probes China's Huawei over equipment near missile silos*, Reuters, 21.07.2022, [on-line:] <https://www.reuters.com/world/us/exclusive-us-probes-chinas-huawei-over-equipment-near-missile-silos-2022-07-21/> – 24.07.2024.
- Alper A., Ljunggren D., *US to force China-linked firm to sell land near US missile silos*, Reuters, 13.05.2024, [on-line:] <https://www.reuters.com/world/us/us-force-china-linked-firm-sell-land-near-us-missile-silos-2024-05-13/> – 24.07.2024.
- Berman N., Maizland L., Chatzky A., *Is China's Huawei a Threat to U.S. National Security?*, Council on Foreign Relations, 8.02.2023, [on-line:] <https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security> – 24.07.2024.
- Biddle S., Ribeiro P., Dias T., *Invisible Censorship*, The Intercept, 16.03.2020, [on-line:] <https://theintercept.com/2020/03/16/tiktok-app-moderators-users-discrimination/> – 24.07.2024.

- Cartwright M., *Internationalising State Power through the Internet: Google, Huawei and Geopolitical Struggle*, „Internet Policy Review” 2020, vol. 9, no. 3, s. 1–18.
- Cerulus L., Wheaton S., *How Washington chased Huawei out of Europe*, „Politico” 2022, [on-line:] <https://www.politico.eu/article/us-china-huawei-europe-market/> – 24.07.2024.
- Gallagher J.C., *U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests*, Congressional Research Service, 1.05.2022, [on-line:] <https://crsreports.congress.gov/product/pdf/R/R47012/2#:~:text=In%20December%202017%2C%20Congress%20prohibited,%2D232%2C%20%2C%2A7889> – 24.07.2024.
- Goujard C., Kayali L., *TikTok launches ‘Project Clover’ charm offensive to fend off European bans*, „Politico”, 8.03.2023, [on-line:] <https://www.politico.eu/article/tiktok-pitches-data-security-plan-to-fend-off-european-bans> – 24.07.2024.
- Goujard C., *What the hell is wrong with TikTok?*, „Politico”, 22.03.2023, [on-line:] <https://www.politico.eu/article/tiktok-china-west-europe-ban-app-espionage-surveillance> – 24.07.2024.
- Hern A., *Revealed: how TikTok censors videos that do not please Beijing*, „The Guardian”, 25.09.2019, [on-line:] <https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing> – 24.07.2024.
- Jolly V., *Comment la Chine protègeses enfants et rend les nôtresdébiles avec le réseau social TikTok*, „Le Figaro”, 15.12.2022, [on-line:] <https://www.lefigaro.fr/secteur/high-tech/comment-la-chine-protège-ses-enfants-et-rend-les-notres-debiles-avec-le-reseau-social-tiktok-20221214> – 24.07.2024.
- Lin P., *TikTok vs Douyin: A Security and Privacy Analysis*, The Citizen Lab, 22.03.2021, [on-line:] <https://citizenlab.ca/2021/03/tiktok-vs-douyin-security-privacy-analysis> – 24.07.2024.
- Moore G.J., *Huawei, Cyber-Sovereignty and Liberal Norms: China’s Challenge to the West/Democracies*, „Journal of Chinese Political Science” 2022, vol. 28, s. 151–167.
- Nover S., *The Grim Reality of Banning TikTok*, „Time”, 15.03.2024, [on-line:] <https://time.com/6952889/tiktok-ban-freedom-of-speech-essay> – 24.07.2024.
- Perault M., *What Happened to TikTok’s Project Texas?*, Lawfare, 20.03.2024, [on-line:] <https://www.lawfaremedia.org/article/what-happened-to-tiktok-s-project-texas> – 24.07.2024.
- Price D., *7 Reasons TikTok Is Bad for Everyone*, MUO, 16.02.2023, [on-line:] <https://www.makeuseof.com/is-tiktok-bad> – 24.07.2024.
- Rogers M., Ruppertsberger D., *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, U.S. House of Representatives, 8.10.2012, [on-line:] [https://stacks.stanford.edu/file/dru-id:rm226yb7473/Huawei-ZTE%20Investigative%20Report%20\(FINAL\).pdf](https://stacks.stanford.edu/file/dru-id:rm226yb7473/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf) – 24.07.2024.
- Schumer C.E., Cotton T., *TikTok letter to the Director of National Intelligence*, Senate Democrats, 23.10.2019, [on-line:] <https://www.democrats.senate.gov/imo/media/doc/10232019%20TikTok%20Letter%20-%20FINAL%20PDF.pdf> – 24.07.2024.

- Smalley S., *TikTok data collection, influence operations potential draw U.S. NSA concern*, Reuters, 7.03.2023, [on-line:] <https://www.reuters.com/world/us/us-nsa-director-concerned-by-tiktok-data-collection-use-influence-operations-2023-03-07> – 24.07.2024.
- Suciu P., *The TikTok Ban Is Truly An Issue Of National Security*, „Forbes”, 15.03.2024, [on-line:] <https://www.forbes.com/sites/petersuciu/2024/03/15/the-tiktok-ban-is-truly-an-issue-of-national-security> – 24.07.2024.
- US Federal Communications Commission, Designation Order DA 20-690, [on-line:] <https://docs.fcc.gov/public/attachments/DA-20-690A1.pdf> – 24.07.2024.
- Zhong R., Schultz K., *With India's TikTok Ban, the World's Digital Walls Grow Higher*, „The New York Times”, 30.06.2020, [on-line:] <https://www.nytimes.com/2020/06/30/technology/india-china-tiktok.html> – 24.07.2024.

Streszczenie

Artykuł ma na celu kompleksowe przedstawienie zagrożeń związanych z chińskimi firmami technologicznymi, takimi jak TikTok i Huawei, w kontekście cyberszpiegostwa. Analiza ma na celu zwiększenie świadomości społeczeństwa i społeczności akademickiej na temat potencjalnych zagrożeń wynikających z działalności tych firm. W artykule zastosowano metodę analizy literatury przedmiotu oraz studium przypadku (case study) dwóch chińskich firm: TikTok i Huawei. Analiza obejmuje przegląd dostępnych raportów, artykułów naukowych oraz doniesień medialnych dotyczących działalności tych firm i związanych z nimi zagrożeń. Analiza wykazała, że TikTok, pomimo twierdzeń o niezależności, może być zmuszony do przekazywania danych użytkowników chińskim władzom, co stanowi poważne zagrożenie dla prywatności i bezpieczeństwa danych. Ponadto, długotrwałe korzystanie z TikToka może negatywnie wpływać na zdrowie psychiczne użytkowników, szczególnie młodszych. W przypadku Huawei, firma ta jest postrzegana jako istotny element chińskiego rozwoju technologicznego, co budzi obawy o możliwość wykorzystania jej infrastruktury do celów wywiadowczych przez chiński rząd. Wnioski z analizy wskazują na konieczność wprowadzenia odpowiednich regulacji i polityki ochrony danych na poziomie państwowym, a także zwiększenia świadomości społecznej na temat zagrożeń związanych z chińskimi firmami technologicznymi. Zaleca się również wspieranie lokalnych firm technologicznych i rozwój alternatywnych standardów, aby zmniejszyć zależność od chińskich produktów i usług.

Słowa kluczowe: cyberszpiegostwo, bezpieczeństwo danych, Huawei, TikTok

Chinese cyber espionage: TikTok and Huawei case study

Abstract

The objective of this article is to comprehensively present the risks associated with Chinese technology companies, such as TikTok and Huawei, in the context of cyberespionage. The analysis aims to raise awareness among the general public and the academic community regarding potential threats resulting from

the operations of these companies. The article employs a literature review method and case study of two Chinese companies: TikTok and Huawei. The analysis encompasses a review of available reports, academic articles, and media reports concerning the activities of these entities and the associated risks. The analysis reveals that TikTok, despite claims of independence, may be compelled to transfer user data to Chinese authorities, posing a serious threat to privacy and data security. Furthermore, prolonged usage of TikTok may negatively impact users' mental health, particularly among younger users. Regarding Huawei, the company is perceived as a crucial component of China's technological development, raising concerns about the potential use of its infrastructure for intelligence purposes by the Chinese government. The conclusion indicates the necessity of introducing appropriate regulations and data protection policies at the state level, as well as increasing public awareness of the threats linked to Chinese technology firms. It is also recommended to support local technology companies and develop alternative standards to reduce reliance on Chinese products and services.

Keywords: cyberespionage, data security, Huawei, TikTok