Digital Anarchy and Security Dilemmas: Unraveling the TikTok Controversy in the Landscape of Cyber Realism and Hegemony Struggles between the United States and China

Anarkis Digital dan Dilema Keamanan: Mengungkap Kontroversi TikTok dalam Lanskap Realisme Siber dan Perebutan Hegemoni antara Amerika Serikat dan Tiongkok

Aditya Permana[1*] Audrey Aurellie[2]
[12] Department of International Relations, BINUS University, Jakarta, Indonesia
[12] Jl. Kemanggisan Ilir III No.45, Kemanggisan, Kec. Palmerah, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta 11480
AdityaPermana84@binus.ac.id[1]*; Aurellie@gmail.com[2];
Corresponding author: AdityaPermana84@binus.ac.id[1]*

ARTICLE INFORMATION

Keywords
TikTok;
Cyber Realism;
Hegemony;
Digital;

ABSTRACT

This study delves into the intricate digital geopolitical dynamics surrounding the contentious relationship between TikTok and the United States (US) by employing the lens of cyber realism. The analysis focuses on the intricate interplay of digital anarchy, security dilemmas, and digital hegemony between the two entities. TikTok, originating from a Chinese company, faces scrutiny due to perceived threats to security and privacy. Within the framework of digital anarchy, characterized by the absence of a central governing authority in cyberspace, the TikTok case underscores the dynamic interplay of uncertainty and competition between US national interests and China's quest for digital dominance. The dilemma faced by the US lies in the imperative to secure national interests while preserving freedom and innovation in the digital era. Amidst the pursuit of digital hegemony, the US aims to sustain its pivotal role in the digital landscape, interpreting TikTok's expansion as a strategic move by China to extend influence and control over user data. Employing secondary data collection methods, including library research, this study reveals the US's responses to these challenges, involving attempts to restrict TikTok's operations within its borders, such as the ban on TikTok's operation and endeavors to gain control of its US operations. However, subsequent revelations indicate the inaccuracy of the US's allegations against TikTok.

Kata Kunci
TikTok;
Realisme Siber;
Hegemoni;
Digital;

ABSTRAK

Studi ini menyelidiki dinamika geopolitik digital yang rumit di sekitar hubungan yang kontroversial antara TikTok dan Amerika Serikat (AS) dengan menggunakan lensa realisme siber. Analisis ini berfokus pada interaksi rumit anarki digital, dilema keamanan, dan hegemoni digital antara kedua entitas tersebut. TikTok, yang berasal dari perusahaan Tiongkok, menghadapi pengawasan karena dianggap mengancam keamanan dan privasi. Dalam kerangka anarki digital, yang dicirikan oleh tidak adanya otoritas pemerintahan pusat di dunia maya, kasus TikTok menggarisbawahi interaksi dinamis ketidakpastian dan persaingan antara kepentingan nasional AS dan upaya Tiongkok untuk mendominasi dunia digital. Dilema yang dihadapi AS terletak pada keharusan untuk mengamankan kepentingan nasional sambil menjaga kebebasan dan inovasi di era digital. Di tengah pengejaran hegemoni digital, AS bertujuan untuk mempertahankan perannya yang penting dalam lanskap digital, menafsirkan ekspansi TikTok sebagai langkah strategis Tiongkok untuk memperluas pengaruh dan kendali atas data pengguna. Dengan menggunakan metode pengumpulan data sekunder, termasuk penelitian pustaka, studi ini mengungkap respons AS terhadap tantangan ini, yang melibatkan upaya untuk membatasi operasi TikTok di dalam wilayahnya, seperti larangan operasi TikTok dan upaya untuk menguasai operasinya di AS. Namun, pengungkapan selanjutnya menunjukkan ketidakakuratan tuduhan AS terhadap TikTok.

Article History
Send 11h October 2024
Review 9thNovember 2024
Accepted 18th December 2024

Introduction

Social media, functioning as a dynamic platform for user interaction, has garnered the attention of the United States Government, perceiving it as a potential tool for propaganda and a national security threat. Propaganda, strategically employed by groups or organizations, seeks to influence the perspectives and behaviors of its targets to achieve specific objectives. Noteworthy instances of propaganda on social media have been previously explored, as evidenced by Farkas et al.'s (2018) examination of Facebook serving as a conduit for propaganda related to radical Islam. Similarly, Shin et al. (2017) highlighted instances of political propaganda on Twitter, showcasing its potential to disseminate political rumors for strategic purposes.

However, the focus has now shifted to TikTok, which since 2020, has become a subject of intense political debate between the United States and China. The U.S. government, expressing concerns over potential espionage and data collection by the Chinese government through TikTok, took decisive action in August 2020. Following President Donald Trump's directives, TikTok usage was restricted within various government departments, and there were proposals to ban the application nationwide, citing threats to national security, foreign policy, and the U.S. economy (Supak. G, 2021). Although a ban was initially considered, it was later suspended after TikTok's announcement of a collaborative data storage initiative with Oracle in September 2020. President Trump emphasized the perceived threat to national security posed by TikTok's data collection system, characterizing the misuse of personal data as a potential weapon wielded by the Chinese government—a perspective viewed with concern by the United States (Supak. G, 2021).

TikTok, a dynamic platform resulting from the amalgamation of the Musical.ly app and Douyin under Beijing ByteDance, has witnessed an unprecedented surge in popularity since its inception in 2016. Boasting over 100 million users globally, TikTok's rapid ascent is comparable to tech giant Apple's user base in China and the West (Williams, 2021). Functioning as both a video viewing and content creation platform, TikTok experienced exponential growth, particularly during the global COVID-19 pandemic in 2020, as individuals sought entertainment and engagement, leading to a substantial increase in downloads (Koleson, 2020). Among its extensive user base, the United States stands out as a significant contributor, with a substantial number of residents actively using the TikTok application (Kusumawardhani, E., & Sari, D. S. 2021). Statistical data on TikTok users from 2018 to 2021 reveals that North America, with approximately 138 million users in 2021, ranks second globally, following the Asia Pacific region (Iqbal. M, 2021). Notably, TikTok's growth in the United States has been remarkable, with active users escalating from 26,739,143 in February 2019 to a staggering 100 million in August 2020 (Iqbal. M, 2021).

The actions taken by the United States Government in response to TikTok can be viewed as measures to address the perceived threat posed by China. With TikTok's user base continually expanding in the United States, the government expresses concern and perceives a threat to the nation. This apprehension is not unprecedented, as similar concerns were previously raised regarding another Chinese tech company, Huawei Technologies Co., Ltd. (Williams, 2021). Citing Williams, the anxiety exhibited by the U.S. Government can be categorized into two dimensions: concerns about new technology and apprehensions about China's governmental system.

The United States' response to the TikTok issue has generated considerable uncertainty and speculation, creating a ripple effect in international relations. Critics argue that the U.S. government's portrayal of TikTok as a national security threat lacks substantial evidence, potentially tarnishing the application's reputation on the global stage. The lawsuit filed by the U.S. against TikTok has been criticized for its perceived lack of robust evidence and a compelling argument against China. Against this backdrop, the primary objective of this study is to address the fundamental question: "Why does the US government perceive TikTok as a national security threat, and are the allegations substantiated?" Through a comprehensive analysis of the TikTok-US dispute, drawing on insights from diverse secondary data sources, this research endeavors to elucidate the veracity of the claims put forth by the U.S. government. Additionally, the study aspires to establish a foundational understanding for future investigations delving into the broader implications of misinformation through social media and its potential to undermine national security.

The evolution of cybercrime carries substantial implications for international security, a topic thoroughly examined by McGuire M, (2018). McGuire delves into the expanding scope of cyber threats, emphasizing the intricate challenges they present to global security. He underscores the growing complexity of cybercrime activities, encompassing hacking, data breaches, and cyber espionage. McGuire contends that the interconnected nature of digital networks intensifies the repercussions of cybercrime, posing threats to both state and non-state actors. His research underscores the imperative for international collaboration and robust cybersecurity measures to mitigate the risks associated with cyber threats.

In the domain of national security, (Murray, S., & Tama, J. 2017). offers insights into the intricacies of subject matter expertise within the framework of US national security policy. Murray elucidates the elaborate procedures inherent in decision-making processes, highlighting the paramount importance of knowledge in shaping national security strategy. His work provides valuable insights into the multifaceted nature of decision-making procedures and emphasizes the importance of knowledge in influencing the formulation of national security policies. While acknowledging the essential nature of expertise, Murray also highlights potential drawbacks such as bureaucratic rivalries and information imbalances that can impede effective decision-making.

In a broader perspective, (Jayakumar, S. (Ed.). 2016). explores the challenges and opportunities associated with national security in the 21st century. He underscores the transformations occurring in security threats and advocates for a comprehensive approach in addressing them. Jayakumar accentuates the significance of comprehending and adapting to new challenges, including terrorism, cyber threats, and environmental security. His work advocates for a proactive and flexible national security strategy that incorporates both traditional and non-traditional security issues.

One notable security threat emanates from the decentralized nature of digitalization, particularly in the realm of social media. Social media, emblematic of contemporary digital technology, is intricately linked to the potential for digital propaganda activities. Chaudhari, D. D., & Pawar, A. V. (2021) investigated this nexus, concluding that social media algorithms play a pivotal role in propaganda activities. Understanding these algorithms empowers propagandists to manipulate content for persuasive purposes. Employing mixed methods, Farkas et al. (2017) identified social media as a propaganda tool wielded by radical Islam, targeting racist and anti-Islam groups. The manipulation of social media algorithms facilitates the dissemination of radical ideologies and recruitment efforts by extremists. Farkas and Neumayer (2018) highlighted that propagandists can design content to appear non-propagandist, strengthening its persuasive impact on the target audience. Collectively, these findings suggest that social media, when used as a propaganda tool, holds potent potential. The ability to manipulate content discreetly and attract the attention of target audiences poses a security dilemma for nations, as outlined in the aforementioned articles.

Security dilemmas present intricate challenges to interstate cooperation and trust-building. Axelrod and Keohane's seminal work, "Achieving Cooperation under Anarchy: Strategies and Institutions" (1985), significantly contributes to our understanding of navigating security dilemmas. The authors delve into the potential for cooperation amid security concerns, focusing on the roles of interdependence and institutions. Axelrod and Keohane posit that, even in contexts of self-preservation and uncertainty, states can discover cooperative opportunities through mutual benefits and shared interests rooted in economic interdependence. Their analysis underscores how economic interdependence can incentivize states to temper their actions and seek collaborative solutions to security challenges. Moreover, Axelrod and Keohane highlight the pivotal role of institutions in facilitating cooperation under security dilemmas. They argue that international institutions play a crucial role in building trust, managing conflict, and establishing communication and cooperation mechanisms between countries. These institutions provide a platform for dialogue, information exchange, and coordinated actions, thereby reducing the likelihood of conflict escalation.

Comparatively, Axelrod and Keohane’s work offers unique insights into the possibilities of cooperation within security dilemmas when contrasted with Glaser’s complex interdependence framework and Tang’s conceptual analysis. While Glaser emphasizes interdependence’s importance, Axelrod and Keohane further explore how such interdependence can foster cooperation. Their emphasis on institutions aligns with Glaser’s and Tang’s perspectives on the significance of communication and institutional mechanisms.

The landscape of national security is increasingly shaped by the complexities of cyber threats, prompting scholars to explore various facets of this critical area. Notable contributions to this discourse are found in the works of Murray, S., & Tama, J. (2017) Jayakumar, S. (Ed.) (2016). Murray’s research, “U.S. Foreign Policymaking and National Security,” delves into the challenges of expertise in national security policymaking, with a specific focus on the United States. Murray’s exploration of bureaucratic dynamics underscores the pivotal role of expertise in shaping policy decisions. He contends that while expertise is crucial, it can lead to bureaucratic rivalries and information imbalances, potentially hindering effective decision-making processes. This analysis offers valuable insights into the intricate relationship between expertise and policymaking, raising pertinent questions about its role in national security.

In contrast, Jayakumar’s article, “State, Society, and National Security: Challenges and Opportunities in the 21st Century,” provides a broader examination of the challenges and opportunities faced by nations globally in the 21st century. Jayakumar adopts a more comprehensive approach, addressing the evolving nature of security threats. He emphasizes the importance of understanding and adapting to new challenges, including terrorism, cyber threats, and environmental security. Jayakumar advocates for a proactive and flexible national security strategy that encompasses both traditional and non-traditional security issues.

Research on TikTok's perceived threat to U.S. national security has unfolded across diverse perspectives, with Williams, R. D. (2021). spotlighting the escalating unease within the U.S. government regarding China's corporate expansion. ByteDance's acquisition catapulted TikTok's popularity in the U.S., yet the subsequent U.S. Government prohibition, outlined by Koleson, J. (2020). lacked concrete evidence surrounding alleged data access by the Chinese Government.

A critical examination of TikTok's concerns in comparison to other foreign entities like Facebook and Google, which enjoy expansive data access, underscores nuanced political and strategic dimensions. Remarkably, policies toward TikTok, as opposed to these counterparts, might mirror broader political and economic considerations, indicating potential competition dynamics. This underscores the necessity to probe deeper, considering broader perspectives to unravel the intricacies of policy implications for foreign technology companies and national security policy holistically (Horowitz et al, 2022).

In essence, the studies underscore the U.S. Government's apprehensions, framing TikTok as a national security threat. However, the research posits a vital caveat, emphasizing the imperative for meticulous analysis and broader considerations. Gray, J. E. (2021) echoes this sentiment, urging a balanced approach that navigates security concerns while fostering innovation and international cooperation. This holistic understanding becomes paramount in shaping effective policies that address the multifaceted challenges posed by emerging technologies on the national security frontier.

The TikTok phenomenon has prompted heightened concerns within the United States (US) government, transcending external threats to encompass potential internal challenges spanning national security, data privacy, and the influence of foreign technology entities. Miao, W., Huang, D., & Huang, Y. (2023) meticulous examination of the media discourse surrounding TikTok spanning China, America, and India from 2017 to 2020 unveils a nuanced evolution of perceptions influenced by geopolitical dynamics. In China, TikTok is lauded as a globally successful social media platform, with minimal emphasis on its political implications. In stark contrast, America and India grapple with concerns ranging from data privacy to national security and the perceived influence of the Chinese government.

Vidyarthi, A., & Hulvey, R. (2021). exploration of the US government's actions, specifically the endeavor to ban TikTok and other Chinese technology platforms, delves into the regulatory steps taken to restrict the operations of these entities within the US. The primary apprehensions revolve around data privacy, national security, and the perceived threat emanating from the ownership of TikTok and WeChat by Chinese companies, potentially affording the Chinese government access to user data. While both Miao, W., Huang, D., & Huang, Y. (2023) and Vidyarthi, A., & Hulvey, R. (2021). acknowledge the internal threat perceived by the US government in the TikTok context, they offer distinctive perspectives on various facets of this threat. Miao's analysis underscores the divergence in perceptions across China, America, and India, unveiling the influence of distinct political and cultural contexts. The depoliticization of TikTok in China sharply contrasts with its repoliticization in America and India, where concerns about national security and data privacy significantly mold public opinion.

The internal threats perceived by the US government in the TikTok conundrum span a spectrum, from data privacy to national security, extending even to broader geopolitical implications. The divergent media discourses across China, America, and India underscore the intricate nature of the issue, with distinct political contexts shaping varying views of TikTok. The US government's endeavors to curb TikTok and other Chinese technology platforms underscore a dedicated commitment to safeguarding national interests and mitigating potential risks arising from foreign-owned applications. As policymakers navigate this complex landscape, a nuanced understanding of these multifaceted challenges becomes imperative in formulating effective and balanced strategies.

The surge in TikTok's popularity has stirred apprehensions regarding the privacy and security of user data. Faison's (2021) scrutinizes the efficacy of the International Emergency Economic Powers Act (IEEPA) in overseeing personal data privacy on TikTok. Faison contends that the IEEPA, designed to address national emergencies and economic threats, falls short in regulating data privacy, primarily focusing on economic and trade measures. This limitation exposes a critical gap in protecting user data on social media platforms, necessitating alternative regulatory frameworks tailored to the distinctive challenges of the digital era.

As the United States perceived TikTok as a potential threat to national security and data privacy, measures were taken to curtail its operations within the country. These actions underscore the inherent tension between upholding national security and fostering an open and connected digital environment. Compounding the issue is the absence of a centralized authority exclusively responsible for regulating the digital ecosystem, prompting countries to adopt unilateral measures to safeguard their national interests (Buchanan. B, 2017).

In tandem with concerns about TikTok's impact on U.S. national security, there has been an exploration of cyber-realism theory. This theory delves into the intricate interplay between technology, online manipulation, and geopolitical dynamics in the digital era. From the cyber-realism perspective, conflicts manifest as power competitions on a global scale, where the utilization of digital technology serves as a tangible expression of state power. This lens offers a comprehensive understanding of how technology intertwines with geopolitical considerations, shaping the complex landscape of digital governance and national security.

In the realm of international relations, realism theory positions states as pivotal actors, centering on the pursuit of power and security interests. Realists assert that states, driven by self-interest, harbor suspicion due to the anarchic nature of the international system, lacking a central authority to regulate state interactions. In this paradigm, conflict and competition are deemed inevitable, with power emerging as a key determinant in shaping inter-country relations. This foundational perspective, as articulated by Morgenthau, H. J. (1973), underscores the relentless pursuit of relative power by states to safeguard their national interests.

Expanding upon the tenets of realism, neo-realism offers deeper insights into the dynamics of international relations. Neo-realism posits that states, acting rationally, strive to protect their security and national interests within an anarchic environment. What distinguishes neo-realism from classical realism is its focal point on the international system's structure as the paramount influence on state behavior. Waltz K (2010) defines the international system as inherently anarchic, where states act to ensure their security in the absence of a central governing authority. Waltz identifies the distribution of power within the international system as a critical factor shaping state conduct. Anarchy, according to Waltz, fosters uncertainty and mutual suspicion (termed the security dilemma), compelling states to seek relative power as a means of ensuring security. The security dilemma, a central concept in international relations studies, delineates a scenario where a country's efforts to enhance its security and defense may be perceived as a threat by others. Consequently, this perception triggers distrust and a competitive atmosphere regarding security matters. In the context of the security dilemma, actions taken by one country to bolster its national security inadvertently diminish the security of other nations, as these actions are construed as threats (Jervis, R. 1978).

The advent of cyber-realism theory marks a pivotal development in the study of international relations, particularly in the context of technological advancements and digitalization. This theoretical framework seamlessly blends classical realism's perspectives with the transformative influence of information and communication technology, casting the digital realm as a battleground for global power struggles. Within the realm of cyber-realism, the enduring factors of security and power retain their primacy in international relations. However, the theory acknowledges the novel role that information and communication technology plays in the competitive landscape of nations and their pursuit of national security. Cyber-realism posits that, in the digital era, countries are inclined to take actions to safeguard their national interests, viewing cyber-attacks as a newfound tool in international conflicts due to their potential to inflict severe impacts on critical infrastructure and acquire sensitive data (Jervis, R. 1978).

The nexus between neo-realism and cyber-realism lies in their shared consideration of technology's role in international relations. While neo-realism perceives technology as a variable influencing the distribution of power, cyber-realism directs its focus towards the transformative impact of digital technology as a force reshaping the international order. In an era marked by rapid digital advancement, cyber-realism emerges as a pertinent framework for comprehending the intricate dynamics of global politics and security. This theoretical approach accentuates the significance of digital technology in shaping interactions between states, emphasizing digital anarchy, security dilemmas, and the pursuit of digital hegemony. As the digital landscape becomes increasingly interconnected, cyber-realism underscores the importance of grasping the role of technology in influencing state interactions, cyber threats, and power dynamics. With the surge of destructive cyber-attacks and the escalating complexity of cyber espionage activities, cyber-realism positions technology as a fundamental factor fundamentally altering the landscape of international relations.

In the realm of cyber-realism, the concept of anarchy in the digital world signifies the absence of a centralized authority capable of effectively regulating and overseeing the activities within the digital ecosystem. According to this perspective, power and control in the digital environment are dispersed among diverse actors, encompassing both state and non-state entities, with no singular entity exercising complete authority over their conduct. Within this milieu of digital anarchy, power dynamics are fragmented, lacking a clear hierarchical structure or dominant authority. Consequently, power and influence in the digital domain are distributed unevenly, fostering complex and sometimes precarious dynamics where actors vie for advantages and safeguard their individual interests (Manjikian. M, 2018). Digital anarchy extends to the security domain, implying that no single entity bears sole responsibility for safeguarding digital infrastructure and sensitive data from cyber threats and attacks. Analogous to traditional security paradigms, cyber security threats give rise to security dilemmas, mirroring their traditional counterparts (Singer, P. W., & Friedman, A. 2014).

In the digital world, security dilemmas manifest when countries or actors in the digital ecosystem harbor suspicion and mistrust toward one another, fueled by doubts regarding their goals and intentions. Amidst a landscape rife with cyber-attacks, hacking, and cyber espionage activities, defensive actions taken by one country to fortify its security and protect national interests may be construed as a threat by other nations. These dynamic triggers defensive or even offensive responses, fostering an environment of tension and competition where nations strive for technological and security superiority (Manjikian. M, 2018).

The security dilemma in the digital realm is compounded by the challenges of distinguishing between attacks aimed at sabotaging infrastructure or pilfering sensitive data and routine network activities. Consequently, states are inclined to enhance their defense capabilities and adopt more assertive defensive measures, potentially setting off a cyber weapons spiral and heightening the risk of conflict escalation in the digital ecosystem (Buchanan. B, 2017). The security dilemma can also be attributed to a nation’s actions aimed at consolidating or preserving its hegemony in the digital sphere, fostering competition and potential conflict with its rivals.

In the context of the digital realm, hegemony denotes the dominance or significant influence wielded by specific countries or actors in controlling and regulating digital technology and the broader digital ecosystem. This supremacy encompasses prowess in technology development and utilization, command over digital resources, and the ability to shape norms and rules governing the digital environment. Digital hegemony emerges as a potent source of power and influence in international relations, as those in command of crucial digital technologies, infrastructure, or platforms can leverage them to gain economic, political, and security advantages. This control empowers nations or entities to influence the digital order, manage information flows, and manipulate the digital landscape to align with their interests.

In a digital world where technology reigns, countries or actors with digital hegemony exploit their advantages, giving rise to power imbalances that impact the dynamics of international relations. This can lead to inequities in accessing and utilizing digital technology, raising concerns about privacy, data security, and disparities in political influence. Consequently, it becomes imperative for the international community to conscientiously consider the implications of digital hegemony when formulating policies and fostering cooperation to preserve power equilibrium and ensure justice in the digital environment (Manjikian. M, 2018).

DeNardis (2014) delves into the notion of a global war for Internet governance, underscoring the geopolitical dynamics inherent in the power struggle to shape digital space. The author posits that control over Internet governance has become a pivotal aspect of establishing influence and power in the digital era. Similarly, Franda (2018) scrutinizes the role of global hegemony and the structural power of capital in the digital age, elucidating how economic control and capital accumulation mold digital space. Expanding on this viewpoint, Schiller (1999) investigates the concept of digital capitalism and its impact on the interconnection of the global market system. Emphasizing the nexus between digital technology and capitalist economic structures, the author contends that digital capitalism significantly transforms the global economy, fostering the expansion of transnational corporations and exacerbating economic inequality.

Hence, by delving into this discourse, we can delineate at least three key dimensions for a nuanced comprehension of the United States' apprehensions surrounding the popularity of TikTok: *firstly*, the notion of digital anarchy, which elucidates the lack of a centralized authority overseeing the digital landscape, exemplified by the U.S.'s independent decision to ban TikTok. The conceptual definition of digital anarchy encapsulates the absence of a centralized authority governing the digital ecosystem, leading to a dispersion of power among various state and non-state actors. This notion becomes palpable in the unilateral decision taken by the United States to prohibit the operations of TikTok. The action not only serves as a practical illustration but also underscores the deficiency of a singular entity exclusively responsible for safeguarding digital infrastructure and sensitive data from cyber threats, leaving nations to independently navigate and manage their digital security landscape.

Secondly, the manifestation of a security dilemma in the cyber realm, where actions taken for national security can be perceived as threats by other nations, exemplified by the concerns prompting the U.S. to curb TikTok's operations. In the realm of security dilemmas in the digital sphere, the conceptual definition emerges from situations where actions taken by a country to fortify its national security are perceived as threats by others, giving rise to a spiral of distrust and competitive security measures. The TikTok case and the subsequent prohibition by the United States exemplify digital security dilemmas. The decision reflects a dilemma rooted in the absence of a central authority exclusively regulating the digital ecosystem. The unilateral actions taken by nations to protect their national security interests in the digital realm underscore the challenges posed by the lack of such an overarching authority.

Thirdly, the assertion of digital hegemony, as witnessed in the U.S.'s strategic move to maintain control over its digital ecosystem, safeguard national interests, and sustain its dominant position vis-à-vis other global digital powers. Together, these dimensions provide a comprehensive framework for deciphering the multifaceted nature of the United States' reservations regarding TikTok's ascendancy. It signifies the substantial influence wielded by a specific country in controlling the digital ecosystem, leveraging technological prowess and norm-setting capabilities. The ban on TikTok by the United States can be interpreted as an assertion of its digital hegemony. In the broader competition between global digital powers, particularly the United States and China, this action is a strategic move to protect national interests and uphold the United States' dominant position in the digital landscape. These operational interpretations provide a tangible framework for understanding and applying the conceptual definitions, utilizing the TikTok and United States scenario as a pertinent illustration of the complexities inherent in digital anarchy, security dilemmas, and digital hegemony.

Method

In this study, we employed explanatory qualitative methods to explore the causal relationship between the United States Government's response to the perceived threat posed by the development of TikTok in the country. This method was chosen as it was deemed suitable for delving into related topics and serving as valid sources for the research. Explanatory qualitative research is designed to offer a thorough explanation and in-depth understanding of the social phenomenon under investigation. Secondary data, comprising government publications, international organizations' reports, news articles, and previous research, were utilized in this study to shed light on the TikTok case and gather relevant information.

We drew from journals, books, news sources, and official reports from pertinent parties whose information is recognized as credible concerning the United States' response to the perceived threat posed by the continued development of TikTok in connection with

China. The research variables, encompassing independent and dependent variables, were identified to conduct a more profound exploration to address the raised questions. The independent variable, in this case, pertains to China’s tactics in vying for the position of a hegemonic country. On the other hand, the dependent variable involves the United States Government’s apprehensions about the data collection system employed by the Chinese company ByteDance, based in China and the owner of the TikTok application. The primary aim of this research is to elucidate why the U.S. government views TikTok as a national security threat and to discern how it is responding to this perceived threat.

The collected data underwent comprehensive analysis to deepen the understanding of the studied phenomenon, identify causal relationships, and discern influential factors. The findings derived from the analysis were then synthesized with existing theories or frameworks. Through an in-depth interpretive process, the researchers aimed to furnish a comprehensive understanding of the phenomenon under scrutiny. The results of this research contribute to a more profound insight and understanding of the social phenomenon investigated, thereby advancing knowledge development in this field.

Result and Discussion

TikTok in Digital Anarchy

TikTok, owned by Beijing’s ByteDance company, came under scrutiny by the United States (US) government, leading to a ban on its use in 2020. The US government expressed concerns about potential connections between TikTok and the Chinese government, raising fears that the application could be exploited to gather US user data, posing a threat to national security (Weise. K, 2020). In July 2020, US intelligence officials initiated an investigation into whether TikTok could be leveraged to collect US user data, potentially facilitating espionage by Chinese authorities (Fung. B, 2023). Furthermore, apprehensions centered around the potential influence of TikTok on public opinion in the US, given its widespread popularity as a social media platform. These concerns revolved around the app’s capability to facilitate the collection of sensitive US user data, thereby posing a perceived threat to national security.

The concept of internet governance encompasses the processes, rules, and institutions responsible for managing and regulating the internet. The United Nations (UN), as an international organization, plays a pivotal role in addressing internet governance issues through various initiatives and institutions. Emphasizing inclusiveness, transparency, and multi-stakeholder participation, the UN Program on Digital Governance (UNPD) serves as one such institution facilitating collaboration on digital rights, privacy, cybersecurity, and information access. The UNPD, operating through diverse working groups, aims to develop policies supporting a secure, open, and inclusive internet. Despite these initiatives, the lack of a specific regulatory instrument for the digital ecosystem regarding the utilization of user privacy data collection has led the US to perceive TikTok as a potential espionage tool, threatening national security. Espionage, defined as the covert gathering of sensitive information for political, economic, or military purposes, is a significant concern in international relations. The US government's scrutiny of TikTok's data collection practices is embedded in a broader strategic rivalry between the US and China, highlighting a confluence of technological competition and national security considerations Koleson, J. (2020).

The concept of digital anarchy emerges as a national security dilemma, particularly in the context of widespread usage of social media applications, coupled with users' lack of awareness regarding the terms and conditions of these applications. This collective ignorance raises concerns about the potential endangerment of state security through the unrestricted use of personal data. Notably, on August 6, 2020, US President Donald Trump issued an Executive Order mandating ByteDance, TikTok's parent company, to divest TikTok's US operational assets to a non-Chinese-affiliated US company, citing concerns about potential access to TikTok user data by Chinese authorities (Figliola. P M, 2020). Legal battles ensued, but the conflict persisted, illustrating the significant role TikTok plays in bolstering national interests and security amid the geopolitical competition between China and the US.

The ban imposed by the US on TikTok highlights the ramifications of the absence of an effective central authority in regulating the digital ecosystem. This unilateral action by the US underscores the power that countries possess to protect their national interests in the face of cybersecurity threats within the framework of digital anarchy. However, it also raises pertinent questions about navigating cybersecurity challenges in this environment, emphasizing the necessity for international cooperation. Addressing complex cybersecurity issues requires collaborative efforts, including the exchange of information and intelligence among countries to enhance the detection of emerging threats and collective understanding of the tactics employed by threat actors (Dogrul et al., 2011).

Fast forward three years, a hearing was conducted by lawmakers from the US Energy and Commerce Commission with TikTok CEO Shou Zi Chew on March 23, 2023, at the United States Capitol in Washington, D.C. During this extensive hearing, Chew addressed questions raised by US lawmakers for approximately five hours. Concerns centered around the assumption that TikTok might be selling the personal data of its users in the US to the Chinese government, leading to fears that TikTok could be acting as a spy under Chinese government orders. Issues such as content censorship related to Hong Kong protests were also raised, reflecting worries about the potential spread of communist principles in the United States. Chew acknowledged past mistakes in managing user data and expressed TikTok's commitment to improving privacy and security policies. However, some members of Congress continued to criticize TikTok, insisting that the company prove that user data was not being provided to the Chinese government (Maheshwari et al., 2023; Williams. R D, 2021).

The Security Dilemma Posed by TikTok

The absence of a central authority in the digital ecosystem fuels a cycle of distrust between the involved parties in the TikTok and US case. The US government remains steadfast in viewing TikTok as a threat, contending that the app could potentially grant the Chinese government access to the data of TikTok users in the United States. However, TikTok's CEO, Chew, has contested these allegations. Chew characterized the accusations by the US Government as hypothetical scenarios that have yet to be substantiated (Fung. F, 2023). TikTok's data collection practices are integral to enhancing user experience as the application evolves. The Privacy Policy of TikTok (2023) outlines the data collected from its users, including:

1. Collecting user personal information such as name, email address, date of birth, and geographic location. This aims for user identification, authentication, and communication between users.
2. Data regarding user activity on the platform, including content uploaded, videos watched, interactions with other users and user preferences. This data allows TikTok to show and recommend relevant content to users, personalize the appearance of their feed, and improve the overall user experience.
3. Information about the user's device, such as device type, operating system, network information, and device settings. This information helps in resolving technical issues, improving application functionality, and identifying and preventing fraudulent activity.
4. TikTok can access and collect user location data if location permission is enabled on the user's device. This data is used to provide location-based features, such as local content,

filters, and challenges. It also helps TikTok to customize recommendations based on the user's geographic location, improving content relevance and user experience.

5. TikTok may use cookies and other tracking technologies to collect information about users and their behavior on the platform. This data is used for analytical purposes to gain insights into user behavior, trends, and demographics. This allows TikTok to improve algorithms, personalize content recommendations, optimize ad targeting, and improve overall platform performance.

As outlined in the TikTok privacy policy report, the data collected by TikTok is an essential aspect of the company's efforts to enhance and optimize the user experience within their application. Users are presented with TikTok's privacy policy and required to provide consent before registering their account, signifying that the data collection process is based on user permission. Despite this, the US government holds the perspective that TikTok's data collection system poses a potential cyber threat to national security (Weise. K, 2020).

The perceived threats by the US government related to TikTok's data collection system include:

1. Concerns and accusations have been raised regarding TikTok's data practices, including the allegation that the in-app browser engages in keylogging, tracking user typing (Pertiwi, WK. 2022). TikTok, however, asserts that this functionality serves debugging, troubleshooting, and performance monitoring purposes, as well as aids in detecting bots and spam (Mozur et al., 2022).
2. Another reported practice is TikTok's tracking of users' preferences on the internet even when the app is not in use, with the company stating that this data is utilized to enhance their advertising business. It's worth noting that similar tracking systems are employed by major US technology companies such as Meta and Google (Fung, 2023).
3. There are also claims suggesting that TikTok may be involved in spying on journalists by accessing user data and IP addresses to determine their locations. Nevertheless, these accusations lack strong evidence, prompting the US Government to initiate an investigation into the matter (Fung. F, 2023).

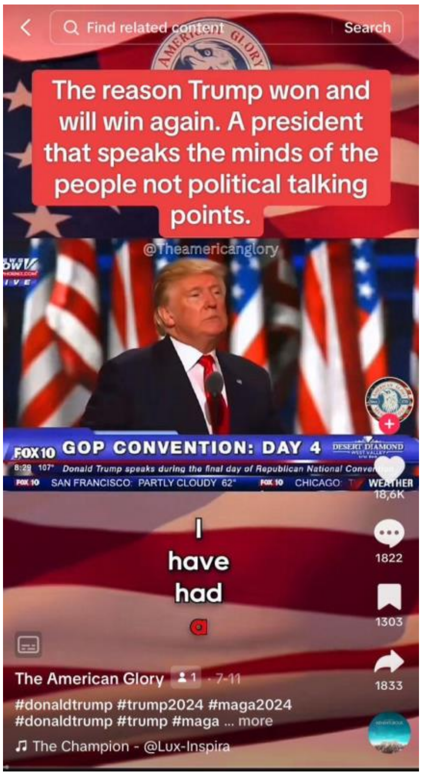
The accusations and security concerns stemming from the United States regarding TikTok highlight a security dilemma exacerbated by the digital anarchy within the current digital ecosystem. The absence of a governing authority above national governments in the digital realm intensifies the challenges of regulating and securing this space. Efforts from the United Nations (UN), such as the United Nations Program on Digital Governance (UNPD) and the Internet Governance Forum (IGF), aim to provide a platform for collaboration and discussion on digital governance, although their impact remains limited, especially in conflicts like that between TikTok and the US (Fattedad et al., 2022).

In the digital world's security dilemmas, countries often bolster their defense capabilities and take more aggressive defensive actions against perceived threats. The US government's decision to ban TikTok is framed as a protective measure for digital infrastructure and a response to potential risks associated with the app. The lack of trust in the goals and intentions of actors in the digital ecosystem contributes to tension, triggering defensive actions and potentially escalating a cyber weaponization spiral. The ban on TikTok by the United States represents an attempt to mitigate the security dilemma, safeguard national security, and protect users' personal data. However, this action involves complex considerations beyond cybersecurity, encompassing political and economic factors.

The strategic value of personal data collected by TikTok, including user information, geographic location, and preferences, raises concerns about commercial exploitation and the potential for influence or propaganda campaigns. In the context of national security, broad access to such data could facilitate surveillance or manipulation of US citizens. Social media platforms like TikTok wield substantial influence in shaping public opinion, making them potential instruments for information manipulation or the spread of propaganda that could impact political stability and public policy. Drawing parallels with the Cambridge Analytica case, where unauthorized access and misuse of Facebook user data occurred during significant political events, the potential misuse of TikTok's data could signal a similar threat to national security (Hinds et al., 2020). The unauthorized collection and use of personal data without consent underscores the vulnerabilities in data protection practices and the potential for compromising sensitive information. Therefore, addressing the security concerns associated with TikTok involves not only cybersecurity considerations but also broader implications for privacy, data security, and national security. Despite the US government's actions, including potential bans and advisories against TikTok, the platform continues to serve as a significant space for political engagement and campaigning. Political supporters leverage TikTok's extensive and diverse user base as a means to connect with various audiences. The platform's creative features and popularity among young users provide political actors with opportunities for outreach, fundraising, and mobilizing campaigns. Presidential candidates recognize the immense potential of social media platforms like TikTok in achieving their campaign objectives and shaping public opinion (Medina et al., 2020). An illustrative example of this ongoing political engagement on

TikTok is evident in the image below, captured by the author using the keyword "US President 2024 Election." This snapshot reflects the platform's role as a space for political expression, discussions, and campaigns, showcasing the active involvement of users in political discourse related to the upcoming presidential election.

Figure 1. Trump Campaign



The reason Trump won and will win again. A president that speaks the minds of the people not political talking points.

GOP CONVENTION: DAY 4

Donald Trump speaks during the final day of Republican National Convention

I have had a

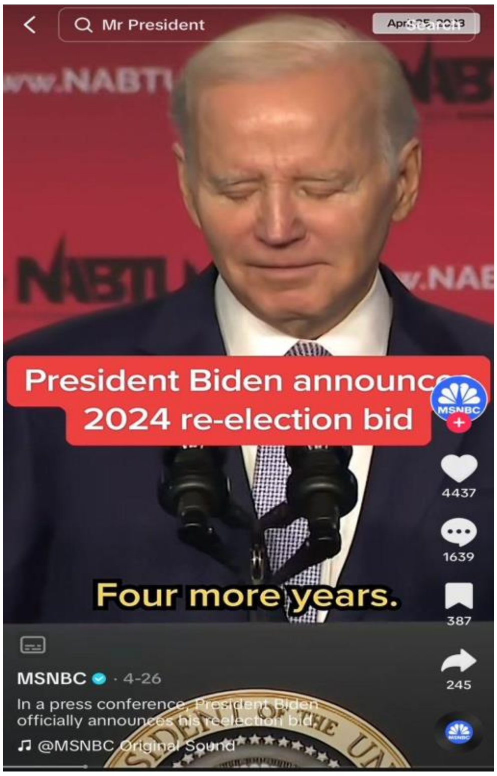
The American Glory · 7-11

#donaldtrump #trump2024 #maga2024 #donaldtrump #trump #maga ... more

♫ The Champion - @Lux-Inspira

Source: TikTok (2023)

Figure 2. Biden Campaign



President Biden announce 2024 re-election bid

Four more years.

MSNBC · 4-26

In a press conference, President Biden officially announces his reelection bid.

♫ @MSNBC Original Sound

Source: TikTok (2023)

To address concerns raised by the US government about TikTok's user data storage practices, TikTok has initiated collaboration with Oracle, a US-based data storage company. This joint effort, known as the Texas Project, aims to alleviate worries expressed by the US government and residents regarding potential risks associated with their personal data, including fears of data being sold to the Chinese government or misused. During this partnership, TikTok CEO Shou Zi Chew mentioned the company's efforts to relocate TikTok user data in the US from Singapore servers, where it was previously stored.

Following US President Donald Trump's announcement of a potential ban on the TikTok app in the United States due to national security concerns, reactions from TikTok users globally varied. While some users expressed concerns about data privacy and security, particularly in relation to the Chinese government, others defended TikTok, highlighting the platform's role in providing entertainment and joy during the pandemic. Some users also pointed out that other social media platforms, such as Facebook and Instagram, face similar privacy and data security issues. Questions were raised about why Congress seemed to be placing more emphasis on TikTok compared to other major tech companies. Many users and observers expressed worries about potential impacts on freedom of expression and access to information. However, the US government justified these measures as necessary to safeguard national security and counter foreign threats that could access personal data, potentially undermining US political and economic stability (Thorbecke & Fung, 2023). The US government's actions to address these concerns can be viewed as strategic steps in the competition for maintaining US digital hegemony.

In the realm of international relations, states often resort to deterrence theory to prevent or repel potential attacks or aggressive actions from adversaries. The US government's ban on the TikTok application within its borders can be interpreted as a deterrence strategy, aiming to uphold national security against perceived threats stemming from TikTok's data collection system. Likewise, TikTok's collaboration with Oracle in enhancing its user data collection practices can be seen as a deterrence strategy employed by TikTok to counter accusations made by the US regarding its data handling practices.

Issues of Digital Hegemony between The US and China

In the realm of digital hegemony, nations strategically utilize their control over technology and data to gain economic, political, and security advantages. The United States perceives TikTok as a potential threat to its national security and the data privacy of American users. By imposing a ban on TikTok's operations within its borders, the U.S. aims to limit the influence and control exerted by Chinese technology companies in the American digital environment. This action reflects the ongoing competition between two major global powers, the United States and China, for dominance and influence in the digital landscape. The United States leverages its authority over access and regulation of foreign technology firms as a means to safeguard its national interests and preserve its digital hegemony.

The nexus between data security and digital hegemony is rooted in the control and ownership of data. Powerful digital entities, including tech giants and multinational corporations, amass extensive user data through various online platforms and services. This data, often collected without explicit user consent, furnishes these entities with valuable insights into user behavior, preferences, and even political inclinations. This knowledge, derived from data, wields unprecedented influence over individuals, communities, and society, enabling these entities to shape online narratives, target specific audiences, and potentially manipulate public opinion (Andrejevic, 2019).

The digital hegemony struggle between TikTok and the United States mirrors the intense competition and dominance battles prevalent in the technology and social media industries. TikTok, as a Chinese tech company, faces scrutiny from the U.S. government regarding data security and alleged ties to the Chinese government. In contrast, the United States is home to some of the world’s largest tech companies, such as Facebook, Google, and Twitter, which wield significant influence in the digital domain and amass vast amounts of user data. The clash for digital dominance between TikTok and the United States encompasses the competition for users, data, and influence in the digital realm. Both parties strive to maintain their interests and supremacy in the global market. Political and security concerns also play a pivotal role in this conflict, with the U.S. government apprehensive about potential data exploitation by the Chinese government. The competition encapsulates broader debates about data privacy, technology regulation, and the government’s role in overseeing industry. The U.S. government has sought to regulate tech companies through legislation and policies, while China has adopted a stricter approach to controlling and filtering information domestically. The war for digital hegemony between TikTok and the United States continues to unfold, impacting global dynamics in the technology and social media sectors.

The concerns of the United States regarding potential national security threats from Chinese technology companies, exemplified by cases like Huawei, showcase the intricate dynamics of technological competition and geopolitical tensions. The accusations against Huawei, involving espionage and influence over global telecommunications infrastructure, triggered a multifaceted conflict, with the U.S. implementing restrictions and sanctions, and China responding with protective measures for its national technology firms. Similarly, in the case of TikTok, the U.S. expresses apprehension regarding the collection of user data by the app and the potential access of the Chinese government to sensitive information. The conflicts surrounding both Huawei and TikTok underscore the role of digital hegemony, where nations vie for power and influence in shaping the global digital landscape according to their national interests.

Viewed through the lens of cyber-realism theory, the clash between China and the U.S. over TikTok can be interpreted as a manifestation of the power struggle in the digital realm. According to this perspective, digital platforms, including TikTok, are regarded as forms of power that enable states to extend their influence globally. Consequently, the national security and foreign policy measures undertaken by both nations concerning TikTok carry significant implications for the stability of the digital world and the respective national security of each country (Rolf, S., & Schindler, S. 2023). This conflict, within the framework of cyber-realism theory, reflects a global-level competition for power, where the utilization of digital technology becomes a means of expressing and asserting state power.

Digital hegemony emerges as a unifying theme in the previous discussions, particularly in understanding the United States' actions concerning TikTok. The U.S.'s apprehensions about TikTok are rooted in concerns about potential threats to its digital hegemony, given the application's widespread use and the absence of effective instruments to regulate the utilization of user data upon registration. This absence of regulatory instruments creates a perceived vulnerability that the U.S. government seeks to address.

The accusations leveled against TikTok by the U.S. are viewed in this context as potentially baseless, as the U.S. contends that TikTok has access to substantial user data. It's noteworthy that other major U.S. interaction platforms, such as Facebook, possess control instruments for user data that are not open to the general public. The focus on TikTok may stem from its popularity among global youth, allowing TikTok to map search results for U.S. young people in the digital space. This mapping is seen as a way to understand the political inclinations of the youth. Consequently, the U.S. government, citing concerns about national security, alleges that China engages in espionage through TikTok. The U.S. response involves urging TikTok to merge with a U.S. company, a move that would ostensibly allow the U.S. government to exert control over the management of TikTok user data in the country. This strategic move reflects the broader dynamics of digital hegemony, where nations seek to safeguard their interests and control in the global digital landscape.

Conclusion

The initial ban on TikTok in the United States in 2020 underscored concerns that the app might enable the Chinese government to collect data on U.S. users, raising national security apprehensions. This situation highlights the absence of a centralized authority in governing digital ecosystems and prompts questions about navigating cybersecurity within the framework of digital anarchy. The conflict emphasizes the crucial need for international cooperation to address complex cybersecurity challenges through the exchange of information and intelligence. The ongoing TikTok conflict in the U.S. serves as a case study illustrating the intricate interplay of the security dilemma, the competition for digital hegemony, and the pivotal role of information and communication technology in shaping international relations. As a conclusion, digital hegemony emerges as a significant factor influencing U.S. actions against TikTok, reflecting concerns about the app's popularity among U.S. youth. Despite accusations and actions, further research is necessary to assess TikTok's privacy policy and explore the extent of Chinese government involvement in the app's development. This ongoing issue underscores the complexity of the evolving digital landscape and its implications for international relations and cybersecurity.

Acknowledgements

The authors would like to thank Binus University, Jakarta, Indonesia, particularly the Department of International Relations, for providing a supportive academic environment that made this research possible. We also extend our gratitude to the student co-author, Audrey Aurellie, whose dedication and contributions were instrumental in the completion of this study. Although this research received no external funding, the collaborative efforts and institutional support were invaluable to its success.

References

Andrejevic, M. (2019). Automated Media (1st ed.). Taylor and Francis. Retrieved from https://www.perlego.com/book/1514113/automated-media-pdf

Buchanan, B. (2016). The cybersecurity dilemma: Hacking, trust, and fear between nations. Oxford University Press.

Chaudhari, D. D., & Pawar, A. V. (2021). Propaganda analysis in social media: a bibliometric review. Information Discovery and Delivery, 49(1), 57-70.

Dogrul, M., Aslan, A., & Celik, E. (2011). Developing an international cooperation on cyber defense and deterrence against cyber terrorism. In 2011 3rd International Conference on Cyber Conflict (pp. 1-15). IEEE.

Farkas, J., Schou, J., & Neumayer, C. (2018). Cloaked Facebook pages: Exploring fake Islamist propaganda in social media. New Media & Society, 20(5), 1850-1867.

Farkas, J. (2018). Disguised propaganda on social media: Addressing democratic dangers and solutions. Brown J. World Aff., 25, 1.

Fattedad, S. C., DeVito, M., Góes, Y., Khorenyan, M., & Milgrim, L. (2022). Towards A Global Digital Governance Architecture. New York City: New York University.

Figliola, P. M. (2020). TikTok: Technolgy Overview and Issues. Retrieved March 28, 2023, from https://crsreports.congress.gov/product/pdf/R/R46543#:~:text=On%20August%206%20and%20August,TikTok%20in%20the%20United%20States.

Fung, B. (2023). TikTok collects a lot of data. but that's not the main reason officials say it's a security risk CNN business. CNN. https://edition.cnn.com/2023/03/24/tech/tiktok-ban-national-security-hearing/index.html

Gray, J. E. (2021). The geopolitics of" platforms": The TikTok challenge. Internet policy review, 10(2), 1-26

Hinds, Joanne; Williams, Emma J.; Joinson, Adam N. (2020). "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. International Journal of Human-Computer Studies, 102498–. doi:10.1016/j.ijhcs.2020.102498

Horowitz, M. C., Allen, G. C., Kania, E. B., & Scharre, P. (2022). Strategic competition in an era of artificial intelligence. Center for a New American Security.

Iqbal, M. (2021). TikTok revenue and usage statistics (2021). Business of apps, 1(1).

Jayakumar, S. (Ed.). (2016). State, Society and National Security: Challenges and Opportunities in the 21st Century.

Jervis, R. (1978). Cooperation under the security dilemma. World politics, 30(2), 167-214.

Kusumawardhani, E., & Sari, D. S. (2021). Gelombang pop culture tik-tok: studi kasus amerika serikat, jepang, india dan indonesia. Padjadjaran Journal of International Relations, 3(1), 19.

Koleson, J. (2020). TikTok is on the clock, will democracy stop?

Maheshwari, S., McCabe, D., & Kang, C. (2023, March 23). Lawmakers Blast TikTok's C.E.O. for App's Ties to China, Escalating Tensions. The New York Times. https://www.nytimes.com/2023/03/23/technology/tiktok-hearing-congress-china.html

Manjikian, J. D. (2018). Cyberrealism and International Relations. Oxford University Press.

McGuire, M. (2018). Beyond flatland: when smart cities make stupid citizens. City, Territory and Architecture, 5(1), 22.

Miao, W., Huang, D., & Huang, Y. (2023). 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, 186(1), 97-114.

Murray, S., & Tama, J. (2017). US Foreign Policymaking and National Security.

Mozur, P., Mac, R., & amp; Che, C. (2022). TikTok browser can track users' keystrokes, according to New Research. The New York Times. https://www.nytimes.com/2022/08/19/technology/tiktok-browser-tracking.html

Morgenthau, H. J. (1973). Politics among nations.

Pertiwi, W. K. (2022). Aktivitas browsing TikTok disebut Bisa Dipantau, Begini Cara Cek Apakah Pengguna terdampak Atau Tidak. KOMPAS.com. https://tekno.kompas.com/read/2022/08/22/17030037/aktivitas-browsing-tiktok-disebut-bisa-dipantau-begini-cara-cek-apakah-pengguna

Rolf, S., & Schindler, S. (2023). The US–China rivalry and the emergence of state platform capitalism. Environment and Planning A: Economy and Space, 55(5), 1255-1280

Shin, J., Jian, L., Driscoll, K., & Bar, F. (2017). Political rumoring on Twitter during the 2012 US presidential election: Rumor diffusion and correction. New media & society, 19(8), 1214-1235.

Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.

Supak, G. (2020). Political Posturing or a Move towards" Net Nationalism?": The Legality of a TikTok Ban and Why Foreign Tech Companies Should Be Paying Attention. NCJL & Tech., 22, 527.

Thorbecke, C., & Fung, B. (2023). The US government is once again threatening to ban TikTok. What you should know. Retrieved from CNN Business: https://www.cnn.com/2023/03/18/tech/tiktok-ban-explainer

Vidyarthi, A., & Hulvey, R. (2021). Building Digital Walls and Making Speech and Internet Freedom (or Chinese Technology) Pay for It: An Assessment of the US Government's Attempts to Ban TikTok, WeChat, and Other Chinese Technology. Indian JL & Tech., 17, 1.

Waltz, K. (2010). Theory of International Politics. Waveland.

Williams, R. D. (2021). Beyond Huawei and TikTok: Untangling US concerns over Chinese tech companies and digital security. Retrieved from Brookings: https://www.brookings.edu/research/beyond-huawei-and-tiktok-untangling-us-concerns-over-chinese-tech-companies-and-digital-security/

Weise, K. (2020). Why the U.S. Is Saying ‘No Way’ to TikTok’s Midnight Train to Washington. The New York Times. https://www.nytimes.com/2020/09/18/business/economy/tiktok-deal-explained.html