Threat Assessment

Digital Warfare: Assessing TikTok's Role as a Cyber Weapon in 21st Century

Kjersti Soberg

February 23, 2025

THREAT PROBLEM/THESIS STATEMENT AND INTRODUCTORY ORGANIZATION

The battlefield of the 21st century has transcended physical borders, evolving into a complex digital domain where the lines between traditional military conflict and covert cyber warfare have become increasingly blurred. The rise of cyber technologies and the pervasive influence of social media platforms have fundamentally altered the nature of warfare, demanding a broader understanding of weapons that extend beyond conventional armaments. Today, TikTok has been scrutinized by governments worldwide for its potential to be used as a tool for Chinese government surveillance, data collection, and influence operations. This paper will analyze the threats posed by TikTok and assess its role as a cyber weapon in the 21st-century. Additionally, it will address TikTok's overall threat to U.S. national security while exploring the evolving nature of this global threat.

THEORIES

One of the primary academic theories used to analyze TikTok as a national security threat is information warfare theory. This theory examines how state and non-state actors use information as a weapon to influence public perception, disrupt societal cohesion, and achieve strategic objectives.[1] Information warfare is particularly relevant when analyzing the potential risks of TikTok, as the platform can be used to spread disinformation, manipulate public opinion,

---

[1] Daniel Morabito, "National Security and the Third-Road Threat: Toward a Comprehensive Theory of Information Warfare," *Air & Space Power Journal* 35, no. 3, 2021, 19.

and collect vast amounts of user data for intelligence purposes. Recent research on information warfare has focused on the role of algorithmic manipulation in shaping political discourse and the implications of foreign influence campaigns. A study by Thomas Rid and Ben Buchanan explored how adversarial states leverage social media algorithms to amplify divisive content, creating societal polarization without direct confrontation.[2] Similarly, a 2024 report from the Center for Strategic and International Studies (CSIS) emphasizes concerns about China's ability to use TikTok for data-driven influence operations.[3]

Another critical academic theory used to analyze the potential national security threat of TikTok is the hybrid warfare theory. Hybrid warfare refers to a blend of conventional military tactics, cyber operations, disinformation campaigns, and other non-kinetic methods to weaken adversaries. This concept, widely studied in contemporary security studies, emphasizes how state and non-state actors use asymmetric strategies to undermine opponents without engaging in direct military conflict. Given government concerns over TikTok's potential links to the Chinese Communist Party (CCP), the platform fits within the hybrid warfare framework as a dual-use technology. The fear is not just about espionage but also about the ability to manipulate public discourse, shape narratives, and create social unrest—all hallmarks of modern hybrid warfare

---

[2] Florian J Egloff, "Public attribution of cyber intrusions, *Journal of Cybersecurity*, Volume 6, Issue 1, 2020, 1-2.

[3] James Andrew Lewis, "TikTok and National Security," Center for Strategic and International Studies, 2024.

strategies.[4] Both information warfare and hybrid warfare studies highlight the role modern technology and social media play in security and how TikTok has the capacity to be a used as a cyber weapon and shape geopolitical conflicts.

METHODS

Social Network Analysis (SNA)

When discussing research methods for analyzing TikTok as a potential cyber weapon within the frameworks of information warfare and hybrid warfare, it is crucial to select methods that can effectively capture the complexities of the digital realm. Social Network Analysis (SNA) can map how information, including disinformation, spreads on TikTok, identifying coordinated inauthentic activity and data harvesting.[5] It reveals connections between user accounts and the types of data they share. This can show how hybrid actors might collect sensitive information for targeted influence campaigns or other malicious purposes.

Legal and Policy Analysis

In addition to SNA, it is prudent to analyze ongoing policy and legal debates surrounding TikTok. This involves examining legislative acts, executive orders, and legal cases, focusing on national security concerns and First Amendment rights. Within this paper, policy discourse,

---

[4] William Pendergrass, "TikTok & The Art of War: A Qualitative Analysis of US Strategic Maneuvering Against Chinese Social Media Company ByteDance," *Proceedings of the ISCAP Conference*, Volume 2473, 2023, 1-3.

[5] David Camacho, Victoria Luzón, Erik Cambria, "New research methods & algorithms in social network analysis," *Future Generation Computer Systems*, Volume 114, 2021, 290-293.

including expert commentary and public opinion, will be assessed alongside comparative analysis of alternative regulatory frameworks. The effectiveness of U.S. policy will be evaluated, acknowledging the limitations due to the dynamic nature of the ongoing TikTok saga that is currently playing out. This approach aims to provide a nuanced understanding of the policy and legal challenges surrounding TikTok's regulation, contributing to the debate on balancing national security and individual rights.

THE NATURE OF TIKTOK AS A THREAT

TikTok's parent company, ByteDance, is a Chinese technology company based in Beijing. ByteDance's merger with musical.ly in 2018 catapulted TikTok into the prolific app that it is today. While many apps collect and store user data, the extent of TikTok's data collection practices, coupled with the potential for access by the CCP, raises significant privacy concerns. This includes worries about the type of data collected and how it is stored and used, as well as the possibility of it being shared with third parties. A hearing with the House Energy and Commerce Committee was held in March of 2023 where Chairwoman, Cathy McMorris Rodgers, addressed ByteDance's leaderships' affiliation and/or careers with the CCP. TikTok's CEO, Shou Chew, previously served as the Chief Financial Officer (CFO) of ByteDance and confirmed his ongoing communication with its executive team.[6] While Chew maintained that the platform does not share data with the Chinese government, U.S officials fear that China may

---

[6] "TikTok CEO Testifies at House Energy and Commerce Committee Hearing," CSPAN, 2023.

"harvest data about its U.S. users and provide it to the Chinese government or that TikTok's videos and algorithm could be programmed by the [CCP]."[7] Leaked audio confirmed some of those fears and Chairwoman Rogers subsequently concluded her examination by stating,

> To the American people watching today, hear this: *TikTok is a weapon*[8] by the [CCP] to spy on you, manipulate what you see and exploit for future generations. A ban is only a short-term way to address TikTok. A data privacy bill is the only way to stop TikTok from ever happening again in the U.S.[9]

Due to this, the U.S. has passed the Protecting Americans from Foreign Adversary Controlled Applications Act to protect citizens from potential national security risks posed by TikTok and the Chinese government. Army General Paul M. Nakasone testified in front of members of the House Armed Services Committee stating,

> If you consider one-third of the adult population receives their news from this app, one-sixth of our children are saying they're constantly on this app, if you consider that there's 150 million people every single day that are obviously touching this app, this provides a foreign nation a platform for information operations, a platform for surveillance, and a concern we have with regards to who controls that data.[10]

Additionally, assistant Secretary of Defense for space policy and principal cyber advisor to the secretary of defense, John F. Plumb, stated, "China has used its cyber capabilities to steal sensitive information, intellectual property and research from U.S. public and private-sector institutions, including the defense industrial base."[11] These concerns highlight the potential for

---

[7] NPR, Interview with Dave Davies and Drew Harwell, "Why are so many government officials concerned about TikTok?" *Fresh Air,* Podcast Audio, May 2, 2024.

[8] Emphasis added.

[9] "TikTok CEO Testifies at House Energy and Commerce Committee Hearing," 2023.

[10] David Vergun, "Leaders Say TikTok Is Potential Cybersecurity Risk to U.S," U.S. Department of Defense, 2023.

[11] Vergun 2023.

powerful platforms like TikTok to be used as a cyber weapon.

While there is no international universal definition for a cyber weapon, Thomas Rid defines it as "a tool that is used, or designed to be used, with the aim of threatening of causing physical, functional, or mental harm to structures, systems, or living things. This general definition is an essential building block for developing a more precise understanding of cyber weapons."[12] While TikTok may not directly cause physical damage in the traditional sense, it can manipulate its audience while subsequently collecting data. Moreover, its algorithms can spread misinformation, influence public opinion, and sow discord, potentially causing significant mental harm to individuals and societies. For these reasons, leaders within the U.S. Department of Defense believe that TikTok has the potential to be a serious cybersecurity risk.[13]

Global Response to TikTok

The fear of nefarious Chinese interference through TikTok has been felt globally. The U.S. is one of several countries to have already banned, or partially banned, the app due to cybersecurity concerns. While some countries have taken these actions due to the fear of misleading or influential content, the majority have banned the app solely on government-issued devices for fear of malicious malware that could be installed.[14] This reflects a growing global awareness of the potential security risks associated with the app, particularly regarding data

---

[12] Thomas Rid, *Cyberwar Will Not Take Place*, Oxford: Oxford University Press, 2013, 47.

[13] Vergun 2023.

[14] Kelvin Chan, "These countries have already banned TikTok," PBS, 2024.

privacy and the possibility of state-sponsored espionage and influence operations.

The Evolving TikTok Threat and Its Consequences

Much like other apps, TikTok's features and algorithms will continue to evolve as technology advances. This growing sophistication and constant evolution present the potential for the platform to be weaponized against not only its users but also their countries. This has potential long-term political, social, and economic consequences. While there is no concrete evidence of China directly using TikTok for espionage or influence operations, a recent article from the CSIS highlights concerns about China's broader data collection efforts on Americans. The report emphasizes that China may utilize collected data for counterintelligence purposes, potentially identifying individuals of interest, even if TikTok users themselves are not the primary targets.[15]

Academic Research and Theoretical Perspectives

Although the CSIS article states that there is no concrete evidence of China using TikTok nefariously, research shows us that this strategy has been used in the past and offers valuable insights into TikTok's potential risks. For example, historical cases of foreign interference in elections through social media platforms, such as the use of Facebook and Twitter to spread disinformation during the 2016 U.S. Presidential election, demonstrate the potential for social media to be weaponized for political purposes. Russia's 2016 election meddling highlights vulnerabilities in traditional intelligence gathering methods, particularly the ability to discern credible information from fabricated narratives on social media. At the Senate Select Committee

---

[15] Lewis 2024.

in 2017, the assistant director of the FBI Counterintelligence Division, Bill Priestap stated,

> Russia's 2016 presidential election influence effort was its boldest to date in the U.S. Moscow employed a multi-faceted approach intended to undermine confidence in our democratic process. Russia's activities included efforts to discredit Secretary Clinton and to publicly contrast her unfavorably with President Trump. This Russian effort included the weaponization of stolen cyber information, the use of Russia's English-language state media as a strategic messaging platform, and the mobilization of social media bots and trolls to spread disinformation and amplify Russian messaging.[16]

While these tactics were applied by Russia, similar strategies of information manipulation and influence operations have been observed throughout Chinese history.

Sun Tzu's *The Art of War* is one of the most influential works written on strategy. As it was written 2,500 years ago, it has been deeply threaded into China's strategic culture – thereby continuing to have a considerable influence over its actions to this day.[17] Three defining theories broached in *The Art of War* are (a) that excellence occurs without fighting or violence, (b) all warfare is based on deception, and (c) the significance of information/intelligence in achieving success.[18] Each of these tenets are present in the CCP's current strategic practices. China's attack stratagem reflects Sun Tzu's theory that "supreme excellence consists of breaking the enemy's resistance without fighting."[19]

This concept of achieving victory without direct confrontation aligns with the potential

---

[16] Bill Priestap, "Assessing Russian Activities and Intentions in Recent Elections," Statement Before the Senate Select Committee on Intelligence, 2017.

[17] Andrew, Scobell, "China and Strategic Culture," Strategic Studies Institute, US Army War College, 2002, 3.

[18] Thomas G. Mahnken and Joseph A. Maiolo, *Strategic Studies: A Reader*, London: Routledge Taylor and Francis Group, 2014, 77-80.

[19] Mahnken and Maiolo, 79.

use of TikTok as a cyber weapon. It also challenges the conventional definition of war and emphasizes that security must be reconsidered in the 21st century. By subtly collecting data, influencing public opinion, spreading disinformation, and exploiting social divisions, the CCP could potentially achieve its strategic objectives without resorting to overt military action. This "unrestricted warfare" approach, as outlined by Chinese military strategists, stresses the importance of exploiting all available means, including cyber and information warfare, to achieve national objectives.[20] TikTok, with its massive user base and sophisticated algorithms, presents a powerful tool for implementing this strategy, allowing for the subtle manipulation of information and the erosion of societal trust without the need for overt aggression.

POLICY

U.S. Policy: Background and Context

The threat posed by TikTok to U.S. national security remains a fluid and highly contested issue. Even as this paper is being written, the TikTok saga continues to unfold. The recent passage of legislation forcing ByteDance to divest its U.S. assets of TikTok marks a significant escalation, but it also raises new questions.[21] How will this forced sale be implemented? What safeguards will be in place to ensure data security and user privacy? Will alternative platforms emerge to fill the void left by TikTok, potentially presenting new challenges and security

---

[20] Paul J. Springer, *Cyber Warfare: A Documentary and Reference Guide*, New York: Bloomsbury Publishing USA, 2020, 217-218.

[21] David Shepardson and Mike Scarcella, "US appeals court upholds TikTok law forcing its sale," Reuters, 2024.

concerns? Moreover, will a new administration lead to shifts in policy direction and renewed debate over the appropriate response to the TikTok threat?

Since 2020, the national security concerns over TikTok have been contentiously debated, reflecting a deep divide in public opinion and raising fundamental questions about the balance between national security and individual liberties. On April 29, 2020, Secretary of State Mike Pompeo announced that, "as part of the 2019 National Defense Authorization Act, the State Department will require a Clean Path for all standalone 5G network traffic entering and exiting U.S. diplomatic facilities at home and abroad."[22] On August 5th, he announced the expansion of "The Clean Network," which was a multi-year initiative aimed to safeguard users from the long-term threats posed by authoritarian actors, such as China.[23] The following day, President Trump issued two Executive Orders, stating that the U.S. must,

> …find that additional steps must be taken to deal with the national emergency with respect to the information and communications technology and services supply chain declared in Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain). Specifically, the spread in the United States of mobile applications developed and owned by companies in the People's Republic of China (China) continues to threaten the national security, foreign policy, and economy of the United States. At this time, action must be taken to address the threat posed by one mobile application in particular, TikTok.[24]

To mitigate these risks, the order prohibited any transactions between U.S. persons or entities and ByteDance. While Trump's administration justified these actions citing national security

---

[22] Milton Mueller, "Trump and Pompeo: Stop the Internet, we want to get off," School of Public Policy, 2020.

[23] U.S. Department of State, "The Clean Network Safeguards America's Assets," 2020.

[24] U.S. Government, "Executive Order on Addressing the Threat Posed by TikTok," Executive Order, 2020.

concerns, critics argued that they were primarily driven by economic and geopolitical considerations. A month later, Trump's attempt to ban TikTok was blocked by several federal courts after judges cited concerns about the potential impact on free speech, the overreach of government power, and the stifling of innovation.[25]

The Evolving Landscape of U.S. Policy On TikTok'

Although Trump's efforts were thwarted, the discussion over the app's security threat continued into the next administration. In 2021, President Biden revoked Trump's Executive Order; however, he instructed the Commerce Department to conduct national security reviews of foreign-owned apps, particularly those linked to China.[26] In December 2022, the U.S. banned TikTok from all federal devices.[27] The RESTRICT Act – also known as "the TikTok bill" [28] – was introduced in March of 2023 and allowed the U.S. government broad authority to ban or restrict foreign-owned apps.[29] A major shift occurred in early March of 2024 when the U.S. House of Representatives overwhelmingly voted 352-65 on a bill that approved legislation giving ByteDance "six months to divest the U.S. assets of the…app, or face a ban."[30] As a result

---

[25] Madison Minges, "National Security and the TikTok Ban" American University, 2025.

[26] Bobby Allyn, "Biden Drops Trump's Ban on TikTok and WeChat — But Will Continue the Scrutiny," NPR, 2021.

[27] Noah Berman, "The U.S. Government Banned TikTok from Federal Devices. What's Next?" Council on Foreign Relations, 2023.

[28] Ani Jonnavithula, "The TikTok Bill Isn't Only About TikTok," Harvard Journal of Law and Technology, 2023.

[29] Peter J. Benson, "Restricting TikTok (Part II): Legislative Proposals and Considerations for Congress," Congressional Research Service, LSB10942, Version 4, 2024.

[30] David Shepardson, "US House passes bill to force ByteDance to divest TikTok or face ban," Reuters, 2024.

of this vote, President Biden signed legislation that required ByteDance to sell its platform to a U.S. owner within a year or it would be prohibited from operating within the U.S. Both TikTok and ByteDance filed a counter lawsuit, "claiming the security concerns were overblown and the law should be struck down because it violates the First Amendment."[31] TikTok and ByteDance's appeal was rejected by the U.S. Supreme Court and the platform went dark on January 18th. Upon accessing the platform, users received a notification that informing them that "a U.S. law banning TikTok will take effect on January 19th and force us [TikTok] to make our services temporarily unavailable."[32] The following day, the app became available again to users which, consequently, was President Trump's first day back in office. That day, he issued an order that delayed the TikTok's ban for 75 days.[33]

Assessing The Effectiveness of Current Policy

As the above has highlighted, U.S. policy surrounding TikTok has been ever-changing. Due to this, assessing its effectiveness has limitations. Thus far, there has not been a unified federal strategy, which leads to inconsistency in implementation, potential loopholes, and difficulties in enforcement. Even though both Trump and Biden's administrations have agreed that TikTok is a national security threat, their approaches to addressing the threat have varied. Moreover, many of their Executive Orders have faced legal challenges. This lack of a consistent and cohesive approach has undermined the effectiveness of U.S. policy towards the app, creating

---

[31] David Hamilton, "How TikTok grew from a fun app for teens into a potential national security threat," AP News, 2025.

[32] Alberto Vargas 2025.

[33] Minges 2025.

uncertainty for not only its users, but the government itself. Trump's Executive Order issued on January 20, 2025, stated that he would "consult with [his] advisors, including the heads of relevant departments and agencies on the national security concerns posed by TikTok, and to pursue a resolution that protects national security while saving a platform used by 170 million Americans."[34] A recent article reported that the Trump administration is "working on a plan to save TikTok that involves tapping software company Oracle and a group of outside investors to effectively take control of the app's global operations."[35] Moreover, it stated, "Under the deal now being negotiated by the White House…ByteDance would retain a minority stake in the company, but the app's algorithm, data collection and software updates will be overseen by Oracle, which already provides the foundation of TikTok's web infrastructure."[36]

FINDINGS

Ramifications & Recommendations

A lack of unified policy has hindered effective action against perceived national security threats posed by TikTok. While the current administration assesses what approach is best, other apps have emerged that may present similar national security concerns. A Chinese startup, DeepSeek, has developed powerful AI models that rival U.S. counterparts and are significantly

---

[34] U.S. Government, "Application of Protecting Americans from Foreign Adversary Controlled Applications Act to TikTok," Executive Order, 2025.

[35] Bobby Allyn, "Exclusive: White House in talks to have Oracle and U.S. investors take over TikTok," NPR, 2025.

[36] Ibid.

cheaper.[37] It quickly became the number one downloaded free app in the U.S., raising concerns about potential data collection and manipulation, as well as the potential for these advanced AI models to be used for malicious purposes.[38] This echoes the concerns expressed by cybersecurity experts and government officials regarding the potential for foreign-developed technologies to be used for espionage, sabotage, or to undermine democratic processes.

Experts have argued that U.S. policymakers "need to develop a more systematic and comprehensive framework for managing the data security and influence risks that come from cross-border data flows, Chinese software, and connected devices."[39] The U.S. would benefit from broader policy approaches that prioritize comprehensive data privacy and cybersecurity measures, rather than focusing solely on China-based companies. Nevertheless, addressing the potential threat posed by ByteDance requires a nuanced and multifaceted approach that balances national security concerns with the need to protect innovation and avoid unnecessary restrictions on trade and technological development. The U.S. also stands to gain significantly from collaborating with allies to establish shared regulatory frameworks. This collaborative approach would "reduce the risks that U.S. allies and partners will find themselves dependent on Chinese software and connected devices and that U.S. allies, concerned about their own vulnerabilities,

---

[37] Eduardo Baptista, "What is DeepSeek and why is it disrupting the AI sector?" Reuters, 2025.

[38] Kevin Williams, Chinese AI app DeepSeek was downloaded by millions. Deleting it might come next." CNBC, 2025.

[39] Peter Harrell, "Managing the Risks of China's Access to U.S. Data and Control of Software and Connected Technology," Carnegie Endowment for International Peace, 2025.

will impose restrictions of their own on both Chinese and U.S. firms."[40]

APPLICATION

Assessing TikTok's role as a cyber weapon in the 21st century is an incredibly timely topic. While I have researched this topic broadly throughout my studies, this is the first time I have researched TikTok specifically as a national security threat. This assignment has significantly deepened my understanding of how hybrid warfare has evolved in the digital age. It highlighted the increasingly blurred lines between social media, surveillance, and information warfare. TikTok exemplifies how modern conflicts can be waged not through direct military confrontation but through the control and manipulation of information. This is particularly important today because it highlights the vulnerabilities within national security frameworks that extend beyond traditional defense measures. The ability of foreign actors to influence public discourse, collect massive amounts of data, and subtly shape societal narratives without overt aggression presents a unique challenge. Understanding these dynamics is crucial for creating and maintaining a strong security policy. Policymakers must develop robust frameworks that balance national security with digital rights, ensuring that foreign influence operations do not undermine democratic institutions. As this is my final paper within the Intelligence and Security Studies program before I graduate with my master's degree, I was particularly motivated to produce a comprehensive and insightful analysis. I aim to contribute to the ongoing dialogue

---

[40] Ibid.

surrounding the growing complexities of national security in the 21st century.

CONLUSION

Determining TikTok's status as a cyber weapon presents a complex analytical challenge. As the U.S. is currently grappling with the evolving nature of digital threats, the case of TikTok serves as a critical lens through which to examine the intersection of national security, technological advancement, and individual liberties. The platform's potential for data exploitation, algorithmic manipulation, and influence operations, coupled with its ties to a foreign adversary, raises profound questions about the vulnerabilities inherent in our interconnected digital infrastructure. This analysis has highlighted the necessity for a nuanced approach that acknowledges the complexities of 21st-century warfare, where traditional kinetic conflicts are increasingly supplemented by covert cyber operations and information manipulation. The ongoing policy debates and legal challenges surrounding TikTok underscore the need for a robust and adaptable regulatory framework that can effectively address these emerging threats while safeguarding fundamental rights. Ultimately, the TikTok saga serves as a reminder that the security of a nation is no longer confined to physical borders, but extends into the vast and intricate digital domain, demanding a continuous reevaluation of our foundational understanding of national security, defense strategies, and a proactive approach to mitigating the risks posed by rapidly evolving technologies.

Bibliography

Allyn, Bobby. “Biden Drops Trump's Ban on TikTok and WeChat — But Will Continue the Scrutiny.” NPR, June 9, 2021. www.npr.org/2021/06/09/1004750274/biden-replaces-trump-bans-on-tiktok-wechat-with-order-to-scrutinize-apps.

Allyn, Bobby. “Exclusive: White House in talks to have Oracle and U.S. investors take over TikTok.” NPR, January 25, 2025. www.npr.org/2025/01/25/g-s1-44779/tiktok-ban-deal-trump-oracle.

Baptista, Eduardo. “What is DeepSeek and why is it disrupting the AI sector?” Reuters, January 28, 2025. www.reuters.com/technology/artificial-intelligence/what-is-deepseek-why-is-it-disrupting-ai-sector-2025-01-27/.

Benson, Peter J. “Restricting TikTok (Part II): Legislative Proposals and Considerations for Congress.” Congressional Research Service, LSB10942, Version 4, Updated March 14, 2024. https://crsreports.congress.gov/product/pdf/LSB/LSB10942.

Berman, Noah. “The U.S. Government Banned TikTok from Federal Devices. What’s Next?” Council on Foreign Relations, January 13, 2023. www.cfr.org/in-brief/us-government-banned-tiktok-federal-devices-whats-next.

Camacho, David, Victoria Luzón, Erik Cambria. “New research methods & algorithms in social network analysis.” *Future Generation Computer Systems*, Volume 114, pgs. 290-293, 2021. https://doi.org/10.1016/j.future.2020.08.006.

Chan, Kelvin. “These countries have already banned TikTok.” PBS, April 26, 2024. https://www.pbs.org/newshour/world/these-countries-have-already-banned-tiktok.

Egloff, Florian J. 2020. “Public attribution of cyber intrusions.” *Journal of Cybersecurity*, Volume 6, Issue 1, pgs. 1-12. https://doi.org/10.1093/cybsec/tyaa012.

“H.R.7521 - Protecting Americans from Foreign Adversary Controlled Applications Act.” Congress.gov, Accessed December 19, 2024. https://www.congress.gov/bill/118th-congress/house-bill/7521.

Hamilton, David. “How TikTok grew from a fun app for teens into a potential national security threat.” AP News, January 19, 2025. www.apnews.com/article/tiktok-ban-biden-timeline-india-119969bfc584e92d47baa189a3e1c4fc.

Harrell, Peter. “Managing the Risks of China’s Access to U.S. Data and Control of Software and Connected Technology.” Carnegie Endowment for International Peace, January 30, 2025. www.carnegieendowment.org/research/2025/01/managing-the-risks-of-chinas-access-to-us-data-and-control-of-software-and-connected-technology?lang=en.

Jaikaran, Chris. “Cybersecurity: Deterrence Policy.” Congressional Research Service, R47011, January 18, 2022. https://crsreports.congress.gov/product/pdf/R/R47011.

Jonnavithula, Ani. “The TikTok Bill Isn’t Only About TikTok.” Harvard Journal of Law and Technology, April 26, 2023. https://jolt.law.harvard.edu/digest/the-tiktok-bill-isnt-only-about-tiktok.

Libicki, Martin C. 2011. “The Strategic Uses of Ambiguity in Cyberspace.” Military and Strategic Affairs. Volume 3, Number 3. www.inss.org.il/wp-content/uploads/sites/2/systemfiles/(FILE)1333532281.pdf.

Lewis, James Andrew. “Deterrence and Cyber Strategy.” Center for Strategic and International Studies, November 15, 2023. www.csis.org/analysis/deterrence-and-cyber-strategy.

Lewis, James Andrew. “TikTok and National Security.” Center for Strategic and International Studies, March 3, 2024. www.csis.org/analysis/tiktok-and-national-security.

Kurlantzick, Joshua. “Is a TikTok Ban Coming?” Council on Foreign Relations, April 1, 2024. https://www.cfr.org/blog/tiktok-ban-coming.

Minges, Madison. “National Security and the TikTok Ban.” American University, January 23, 2025. www.american.edu/sis/news/20250123-national-security-and-the-tik-tok-ban.cfm.

Morabito, Daniel. "National Security and the Third-Road Threat: Toward a Comprehensive Theory of Information Warfare." *Air & Space Power Journal* 35, no. 3 (Fall, 2021): 19-39. http://ezproxy.bellevue.edu/login?url=https://www.proquest.com/scholarly-journals/national-security-third-road-threat-toward/docview/2575098829/se-2.

Mueller, Milton. “Trump and Pompeo: Stop the Internet, we want to get off.” School of Public Policy, August 7, 2020. www.internetgovernance.org/2020/08/07/trump-and-pompeo-stop-the-internet-we-want-to-get-off/.

NPR. Interview with Dave Davies and Drew Harwell. “Why are so many government officials concerned about TikTok?” *Fresh Air*. Podcast Audio. May 2, 2024. https://www.npr.org/2024/05/02/1248663706/why-are-so-many-government-officials-concerned-about-tiktok.

NPR. “Supreme Court Hears TikTok Case, Syrians Return Home, French Rape Trial Verdicts.” *Up First*. Podcast Audio. December 19, 2024.

Pendergrass, William. "TikTok & The Art of War: A Qualitative Analysis of US Strategic Maneuvering Against Chinese Social Media Company ByteDance." In *Proceedings of the ISCAP Conference ISSN*, vol. 2473, p. 4901. 2023.

Pendino, Stephanie, Robert K. Jahn, Sr., and Kirk Pedersen. “U.S. Cyber Deterrence: Bringing Offensive Capabilities into the Light.” Joint Forces Staff College, September 7, 2022. https://jfsc.ndu.edu/Media/Campaigning-Journals/Academic-Journals-View/article/3149856/us-cyber-deterrence-bringing-offensive-capabilities-into-the-light/.

Priestap, Bill. “Assessing Russian Activities and Intentions in Recent Elections.” Statement Before the Senate Select Committee on Intelligence, June 21, 2017. https://www.fbi.gov/news/testimony/assessing-russian-activities-and-intentions-in-recent-elections.

Rid, Thomas. 2013. *Cyber War Will Not Take Place*. Oxford: Oxford University Press. https://search-ebscohost-com.ezproxy.bellevue.edu/login.aspx?direct=true&db=e025xna&AN=678079&site=ehost-live.

Scobell, Andrew. “China and Strategic Culture.” Strategic Studies Institute, US Army War College, 2002. http://www.jstor.org/stable/resrep11270.

Shepardson, David. “US House passes bill to force ByteDance to divest TikTok or face ban.” Reuters, March 14, 2024. www.reuters.com/technology/us-house-vote-force-bytedance-divest-tiktok-or-face-ban-2024-03-13/.

Shepardson, David and Mike Scarcella. “US appeals court upholds TikTok law forcing its sale.” Reuters, December 6, 2024. www.reuters.com/legal/us-appeals-court-upholds-tiktok-law-forcing-its-sale-2024-12-06/.

Springer, Paul J. 2020. *Cyber Warfare: A Documentary and Reference Guide*. New York: Bloomsbury Publishing USA. ProQuest Ebook Central.

“TikTok CEO Testifies at House Energy and Commerce Committee Hearing.” CSPAN, March 3, 2023. www.c-span.org/video/?c5063344/tiktok-weapon.

U.S. Department of State. “The Clean Network Safeguards America’s Assets.” August 11, 2020. https://2017-2021.state.gov/the-clean-network-safeguards-americas-assets/.

U.S. Government. “Application Of Protecting Americans from Foreign Adversary Controlled Applications Act to TikTok.” Executive Order, January 20, 2025. www.whitehouse.gov/presidential-actions/2025/01/application-of-protecting-americans-from-foreign-adversary-controlled-applications-act-to-tiktok/.

U.S. Government. “Executive Order on Addressing the Threat Posed by TikTok.” Executive Order, August 6, 2020. https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/.

U.S. House Committee on Energy and Commerce. “The Protecting Americans from Foreign Adversary Controlled Applications Act.” Accessed December 19, 2024. https://energycommerce.house.gov/HR7521.

“US Supreme Court TikTok ban case: MSU experts can comment.” MSU Today, January 17, 2025. https://msutoday.msu.edu/news/2025/us-supreme-court-tiktok-ban-case-msu-experts-can-comment.

The Wall Street Journal. “The TikTok Ban Goes to the Supreme Court.” *The Journal*. Podcast

Audio. January 10, 2025. www.wsj.com/podcasts/the-journal/the-tiktok-ban-goes-to-the-supreme-court/34904083-8492-4442-b293-62f14783223e.

Vargas, Alberto. Personal Photograph. January 18, 2025.

Vergun, David. “Leaders Say TikTok Is Potential Cybersecurity Risk to U.S.” U.S. Department of Defense, April 6, 2023. www.defense.gov/News/News-Stories/Article/article/3354874/leaders-say-tiktok-is-potential-cybersecurity-risk-to-us/.

Williams, Kevin. “Chinese AI app DeepSeek was downloaded by millions. Deleting it might come next.” CNBC, February 2, 2025. www.cnbc.com/2025/02/02/why-deleting-chinas-deepseek-ai-may-be-next-for-millions-of-americans.html.