Fall 2023

Assessing the Threat of Social Media to National Security: Information Operations in the 21st Century

Brendan M. Cullen
University of South Carolina - Columbia

Director of Thesis: Katherine Barbieri
Second Reader: Josef Olmert

ABSTRACT

The ubiquity of social media has enabled an unprecedented amount of personal data to be accessible to various entities. Social media platforms leverage this data to optimize algorithmic recommendation systems, persuade users to engage, and promote monetization. The social media ecosystem's business model demands continuous engagement and the relentless collection of user data to grow and scale. Not only is social media massively popular around the world, but it has integrated heavily into users' daily lives. This integration is driven by social platforms' deliberate architectures and affordances. The intentionality of social media can be exploited by state and non-state actors for influence, espionage, and cybercrime. The extensive data collection and manipulation capabilities inherent to social media make it a highly effective vehicle for information operations and social engineering attacks. These tactics are vital assets in multi-domain operations and psychological warfare. This paper investigates how social media can be used maliciously, with a particular focus on TikTok. TikTok, one of the United States' most popular platforms, is connected to the People's Republic of China via its parent company, ByteDance Ltd. This thesis assesses the unique threat that TikTok poses to U.S. National Security by examining the PRC's strategic goals in cyberspace. Amidst rising tensions between the U.S. and PRC, this research seeks to explain the TikTok threat in deeper context.

TABLE OF CONTENTS

INTRODUCTION

The heightened integration of technology and humanity provides a wealth of centralized data available to tech companies, third party vendors, and government entities. While this data may improve the user experience (UX), the harvest of personal information can be exploited and applied to external objectives without consumer awareness. Collecting personal data is at the heart of social media's highly effective business model. Social media users often consent to the aggregation of device specifics, biometric identifiers, behavioral and usage habits, precise location tracking, and message surveillance. This surplus of data can be used to analyze behavioral trends, predict engagement, and strategically tailor content. For personalization to be effective on social media, platforms make inferences about consumers' personalities. With some limitations, psychometric profiling techniques enable platforms to interpret the motivation behind users' online activity and strategically target content. While users consent to the collection of personal data, the terms of most platforms' privacy agreements can be accepted with a single click. This informed consent model trusts users of all ages to understand not only what information is collected and why, but also the broader implications of their usage.

State and non-state actors can exploit the business models, privacy agreements, and intentional design of social media platforms. Agents with a vested interest in social engineering and manipulating groupthink on a wide scale find a highly capable vehicle for their efforts in social media platforms such as TikTok and Facebook. Furthermore, these platforms serve as a powerful medium for information operations, cyber espionage, and intelligence collection by adversaries of the United States.

TikTok, one of the most popular social platforms in the U.S., poses a unique threat to national security. The platform's extensive user data collection has led political leaders and cyber professionals to question the ethics and motive behind its privacy policy and integration with the American people. This concern over TikTok is highlighted by the platform's clear connection to the People's Republic of China via its parent company, ByteDance Ltd. This connection warrants an investigation into the platform and its threat to the United States. The Department of Defense has prioritized the pervasive threat the PRC poses to the U.S. in cyberspace amidst escalating tensions between the two nations. This paper argues that securing the social media ecosystem is important to the DOD's efforts to defend the homeland and deter PRC aggression. This thesis reveals how the PRC could utilize TikTok as a critical method of multi-domain operations against the U.S. and why using this platform as a targeted influence weapon and source of intelligence would be highly effective.

The first two chapters examine social media's capacity to be an attack surface for microtargeted information operations and manipulation. This research will then be applied to TikTok specifically. Beginning by analyzing the platform's history, design, and privacy, this paper will evaluate the scale at which TikTok could affect U.S. National Security if used by the PRC with malicious intent. An analysis of TikTok's connection to the Chinese Communist Party and the PRC's strategic goals for global dominance are integral to this research. This thesis will investigate the PRC's policies and how TikTok contributes to strategies such as the Belt and Road Initiative and the "Three Warfares" strategy. This paper will assess current efforts by the United States to mitigate the risk associated with TikTok. Lastly, it will conclude by asserting that the U.S. Government must reframe its understanding of the platform in order to minimize the TikTok threat and protect the United States' competitive advantage.

CHAPTER 1: ASSESSING THE SOCIAL MEDIA ECOSYSTEM

The prevalence of social media is a pivotal aspect of society in the 21st century. From the early iterations of social networking sites to the present day, social media has fostered an unprecedented global interconnectedness. In a sense, social media has empowered people to join and contribute to a massive public forum of ideas, content, and discussion. In 2022, more than 4.59 billion people were using social media across the world, and this number is projected to reach 5.85 billion by 2027 (Statista, 2022). With nearly 60% of the world's population on social media, social networking platforms possess a unique, asymmetric power over their users. Decisions made by the most popular platforms have the capacity to affect billions of people throughout the world. Regardless of the nature of these outcomes, this imbalance of power has demanded the attention of government officials, corporations, social scientists, and more. This chapter will explore the social media ecosystem, the intentionality behind platforms' overwhelming successes in engagement and revenue, and the potential implications of social media usage.

The Origins of Surveillance Capitalism

In order to understand the successes of the social media ecosystem in its current state, it is critical to articulate how user-dependent companies such as Google and Facebook built such profitable enterprises. Even prior to 2001, Google collected data on its users' behavior on the search engine. Yet at that time, the future tech giant did very little with this data and treated it as useless waste (Zuboff, 2019). Shoshana Zuboff, a professor emerita at Harvard Business School and author of the well-known book, *The Age of Surveillance Capitalism*, refers to this data that exceeds the needs of product improvements as human "behavioral surplus" (Zuboff, 2019, p.

13). Google discovered that this behavioral surplus could be used to improve the user experience and the effectiveness of searches. The issue, however, was that this application of user data acted to the detriment of the company's economic goals: user behavioral data accelerated the search process, users got what they needed more efficiently, and consequentially spent less time on the platform where they could engage with ads. Under pressure from investors in 2001, Google realized a new avenue for monetization must be established. The company's solution to this issue created a business model Zuboff refers to as "surveillance capitalism" (Zuboff, 2019, p. 12), and set the standard for how social networking sites of the future would monetize.

Surveillance capitalism refers to the business of claiming free, human behavioral data as raw material to be repurposed and marketed to third parties for profit. Google, before and at the outset of adopting this practice, merely found and applied this behavioral data. But as the supply of users increased and demand grew, human behavioral data came to be deliberately hunted and mined by means of persuasion and surveillance. Despite efforts to hide the impact of its new practice, Google clearly had discovered a gold mine. Zuboff notes that when Google went public in 2004, "the firm's revenue had increased by 3,590 percent, from $86 million in 2001 to $3.2 billion in 2004" (p. 14).

Surveillance capitalism feeds on the prediction and shaping of future behavior (Zuboff, 2019). Accurate predictions rely on thorough source data. The most thorough source data relies on a near-constant presence of digital technologies in a user's life. If success in the "surveillance economy" depends on the extraction of human behavioral data, the business model of participating companies demands the increase of supply interfaces in which users' data can be extracted (Zuboff, 2019, p. 16). Zuboff terms this demand for data accumulation the "economic imperative" of surveillance capitalism (p. 16). This principle has evolved exponentially since

Google's 2001 epiphany, and the attempt to penetrate human behavior can be seen today in powerful products such as Google's Home, Amazon's Alexa, and today's most popular social networking platforms (Zuboff, 2019). The late Mark Weiser, former CTO of Xerox's Palo Alto Research Center and the widely accepted father of ubiquitous computing, perfectly describes the goal of pervasive technology in *The Computer for the 21st Century*: "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it" (Weiser, 1991, p. 94).

Efforts to harvest data are only lucrative when there is active user engagement, when users buy into the ubiquity of the tool. In regard to social media, the question then becomes: how can platforms deliberately and effectively retain the attention of their users?

The 'Attention Economy': Data Collection and Persuasive Technology

When discussing innovations in the evolving cyber world, it is easy to lose sight of the human element embedded within technology. Technologies such as Artificial Intelligence (AI) are often prescribed a human-like agency, ignoring the many stages of human decision-making and action that facilitate their production. The way in which society interacts with the digital world is shaped by humanity—from the construction and installation of physical infrastructure and hardware, user-experience and design decisions made by engineers, to the policies formed by bureaucrats and voted on by citizens. Humanity and the material world are inseparable from the digital. The intentionality driving today's most popular social media platforms is indicative of this relationship.

As previously mentioned, the social media ecosystem was built upon the demands of surveillance capitalism. In order to meet and exceed the "economic imperative" described by

Shoshana Zuboff (p. 16), social media platforms need to gain and retain the attention of their users. This effort is supported not only by the affordances of social media platforms, but also the architecture and design of the platforms themselves. This section will investigate how social media platforms meet the demands of surveillance capitalism by collecting and applying personal data, deliberately implementing addiction-promoting design techniques, and leveraging the current model of informed consent on social media.

The harvest of user data is the crux of social media monetization. Social networking sites collect far more than just user-generated content (UGC) from a consumer's device, including unrelated digital activity, real-world behavior, and biometrics. This represents what Shoshana Zuboff terms an "extension" (p. 16) of surveillance from the virtual world into the physical world. She says, "Extension wants your bloodstream and your bed, your breakfast conversation, your commute, your run, your refrigerator, your parking space, your living room, your pancreas" (p.17). Zuboff's assertion that technologies such as social media operate as part of a broader industry centered on user-surveillance is echoed by other researchers. Data collected by social media companies serves as an "economic asset" that provides a detailed depiction of a user's personality, consumption habits, daily schedule, and interests (Fuller, 2018, p. 15). While this thesis will later discuss in-depth TikTok's privacy policy and data collection efforts, it is relevant to present here what might be collected by social platforms and how it is leveraged.

Social media companies collect personal data not only to be sold to third parties, but also to improve in-app processes such as algorithmic recommendation systems. An algorithm is a series of computational processes and decisions used to solve a known problem or complete a task (Congressional Research Service [CRS], 2023a). A recommendation algorithm, also referred to as a recommendation system, employs an algorithm to filter, curate, and provide

content to users that is likely to achieve an intended effect based on previous UGC, inferred preferences, and other relevant data (CRS, 2023a). These recommendation systems seek to maximize engagement with a platform by capitalizing on three methods of personal data collection: volunteered, observed, and inferred (World Economic Forum, 2011). Volunteered data refers to information that users might provide themselves upon registration or in-app purchase, such as their name, phone number, email address, credit card number, declared interests, and more. Observed data is gathered from the monitoring and storage of user activity both on the platform and via third-party cookies (i.e., usage habits, online interactions, UGC, search history, location services, etc.). Inferred data draws on the two former methods to connect the dots between datapoints and conduct probability assessments regarding users' future behavior (World Economic Forum, 2011).

In addition to these three methods of collection, information-sharing with third parties provides the relevant context needed to strategically curate content and advertisements. Accessible health records, financial transactions, locations services, institutional associations, communications metadata, personal relationships, internet search histories, sleep schedules, and more—the recommendation algorithms powering social networking sites access an overwhelming amount of personal data to compete with other industry leaders (World Economic Forum, 2011; Zuboff, 2019). Testing done by *The Wall Street Journal* indicated that Facebook has received particularly sensitive data from third parties without disclosure to users, even individuals with no connection to Facebook. The Journal's investigation found that Flo Health Inc.'s Flo Period & Ovulation Tracker, which hosts 25 million active users, informed Facebook when users were menstruating or had intentions to get pregnant. Though the platform claimed the data it sends Facebook is "depersonalized", the Journal discovered that sensitive information

was paired with a unique identifier that could match with a profile (Schechner & Secada, 2019). Combining data from multiple parties to produce a sellable, user profile is a common practice that often supersedes the privacy offered by data depersonalization or anonymization.

While recommendation algorithms fueled by aggregated personal data are crucial to success in the social media ecosystem, they are not the only ingredient to retaining users' attention. Social media platforms are strategically designed to keep consumers engaged for as long as possible, and to keep coming back. Designers of social platforms discovered that user attention could be *mined* by exploiting vulnerabilities in human psychology (Martin, 2022). Drawing on the neuroscience of addiction, dopamine became a key focus for keeping users hooked to their screen. More specifically, platforms draw on the tenets of "operant conditioning" developed by the late American psychologist B.F. Skinner. Operant conditioning refers to a process that influences the flow of dopamine based on the possibility (not guarantee) of a reward. Skinner calls these "variable rewards"—the possibility of a reward can manipulate subjects into repeatedly trying to achieve this outcome (Martin, 2022, p.10). Sean Parker, one of Facebook's founders, said that the platform attempts to, "give you a little dopamine hit every once in a while, because someone liked or commented on a photo or a post or whatever. And that's going to get you to contribute more content, and that's going to get you ... more likes and comments... It's a social-validation feedback loop ... exactly the kind of thing that a hacker like myself would come up with" (Solon, 2017).

The ability to like, dislike, repost, or comment on user-generated content is an important aspect of this feedback loop that Sean Parker references. These functions, which are regularly conflated with real-world value, enable social validation to be given with the click of a button and immediately received by the content creator (Martin, 2022). This system of social validation

creates its own variable reward system: the content a user provides may result in feedback or disappointment. This idea is also the basis for the 'pull-down to refresh' function, which was developed using the psychology that empowers the success of slot machines (Martin, 2022). The slot machines themselves, in addition to the surrounding sensory environment, attempt to create an intimate and enduring relationship between the player and the game (Martin, p. 11). The same is consistent with social media—recommendation algorithms immerse users in a data-driven, dopamine-induced loop of engaging content. Platforms attempt to limit opportunities for distraction by eliminating white space between content and embedding various ways to engage on the same screen. Just as gamblers do on a slot-machine: users swipe down on their screen, wait in anticipation of new content (with the possibility of it being favorable), and receive feedback (Martin, 2022). Infinite scrolling, the idea of eliminating natural stopping cues, compels social media users to stay engrossed in this loop (Bhargava & Velasquez, 2021). Break the cycle? Notifications nudge the user to dive back in. In today's competitive social media ecosystem, it is not sufficient to merely entice users to engage with content—platforms operationalize users' psychological tendencies against them and coerce engagement through the imposition of unconscious habits.

Using psychological research to promote monetization or achieve a certain business objective is neither uncommon nor a new practice. That said, the exploitation of human psychology on social media can be largely attributed to Stanford's Persuasive Technology Lab in the late 1990's and early 2000's. Many influential leaders at companies such as Facebook, Twitter, and Google studied under B.J. Fogg at this lab. Fogg preached the persuasive value that mobile technologies offer, and their capacity for intentional behavior modification. While Fogg may have envisioned ways to positively influence public health at the individual consumer-level,

engineers and designers quickly recognized the operational value of persuasive technology (Martin, p. 13-14). As Bhargava and Velasquez brilliantly point out, there is a unique distinction between the promotion of addiction on social media and traditional addiction. Take cigarettes, for example: a cigarette does not continuously and strategically improve its capacity to addict a particular user (Bhargava & Velasquez, p. 334). But as social media users engage with and generate content, platforms can test which persuasive techniques are most effective in real-time. Constant optimization of these techniques promotes further engagement, which creates more opportunities to collect data. Enhanced data collection fuels recommendation algorithms, which drives potential revenue. This cycle is the lifeblood of the attention economy.

Social media platforms are not designed to be passive applications. Rather, they operate as active participants in the life of the user with the capacity to influence behavior. This chapter illustrates the intentional, pervasive, demanding nature of the social media ecosystem. Platforms' collection of personal data and exploitation of psychological vulnerabilities treat users as a means to an end. In this chapter, financial growth was the intended "end". However, this ecosystem enables far more than just monetization. The architecture and affordances of social media provide state and non-state actors with a favorable environment to strategically target users and manipulate groupthink on a broad scale. The next chapter will explore how the social media ecosystem can be effectively leveraged for information operations and social engineering. It will also assess the threat potential of social media when applied maliciously.

CHAPTER 2: MICRO-TARGETING AND INFORMATION OPERATIONS ON SOCIAL MEDIA

The intentional design and surveillance-driven business model of social media yield a potent attack surface to be exploited by state and non-state actors. Social media is a powerful tool for targeted information operations and social engineering. Platforms' extensive data collection efforts and ability to retain user attention are valuable assets for malicious operations in the information environment. Just as platforms utilize user data to predict consumers' interests and tailor personalized content, third-party actors can leverage social platforms to 'micro-target' individuals and groups. Psychological profiling on social media enables the construction and manipulation of target audiences, which can result in real-world consequences.

This chapter will begin by presenting evidence that supports the effectiveness of micro-targeting and manipulation on social platforms. Then, it will move on to the threat potential of social media. Threat actors can utilize social platforms for psychological warfare, social engineering, intelligence collection, cyber operations, and more (Bialy, 2017). Therefore, the social media ecosystem is critical for multi-domain operations, cybercrime, and espionage. The operational value of social media today is deeply rooted in history. The tenets of propaganda, intelligence, and influence are certainly not new, but the massive potential scale and impact of social media operations present a unique threat to U.S. National Security and society.

Micro-targeting and Manipulation

Before assessing the threat social media poses to the physical world, it is critical to demonstrate its capacity to be a medium for behavioral and emotional manipulation. In 2012, a

Facebook data science team sought to answer whether ‘emotional contagion’ occurs in impersonal settings, specifically based on social media posts. Emotional contagion is a well-proven theory of emotional transfer from one person to another, leading the latter to express themselves similarly. The experiment, which lasted one week, tested whether reducing the amount of emotional content in the News Feed (the primary method of seeing friends’ posts on Facebook at the time) would lead to emotional contagion. The experiment had two main parallel studies: one group’s exposure to positive emotional content was reduced while another group’s exposure to negative emotional content was reduced. The team of researchers analyzed over 3 million posts and manipulated 689,003 English-speaking Facebook users for the experiment (Kramer, Guillory, and Hancock; 2014).

The results indicated that Facebook could use the News Feed to manipulate users’ emotions. When positive content was reduced on one’s feed, they would consequentially post more negative things. When negative content was reduced, the opposite occurred. The experiment suggested that Facebook can induce emotional contagion without direct interaction—simply witnessing or failing to witness emotionally charged content is sufficient for behavioral influence (Kramer, Guillory, and Hancock; 2014). Though Facebook claims that this experiment was allowed by its privacy policy, there are debates surrounding the validity and ethics of this study. While the ethical implications of digital manipulation are outside of the scope of this paper, this study demonstrates the influential power social platforms possess without even employing any sophisticated tactics. Now, imagine that the conclusions of this study were weaponized. Rather than almost 700,000 randomized users, what if a threat actor could identify and manipulate the emotions of *5 million* users with depressive or suicidal tendencies? What if an adversary of the United States could strategically target expatriates or the children of U.S.

government officials? Or propel groups of individuals to ideological extremes? These hypotheticals are not far-fetched. Psychological profiling and micro-targeting techniques enable such information operations to be conducted on social media without user awareness and with minimal cost and effort.

Evidence shows that digital persuasion and behavioral influence are more effective when powered by psychometric profiling. The OCEAN model, often referred to as "The Big Five", is the most common framework for psychometric profiling. This model categorizes the psychological motivations driving human action into five categories. "Openness" measures a person's inclination to seek new experiences, their curiosity, and imagination. "Conscientiousness" measures a person's aptitude for a spontaneous lifestyle as opposed to a more reliable and consistent one. "Extroversion" assesses a person's likelihood to interact socially for stimulation and express positivity. "Agreeableness" measures a person's tendency to prioritize maintaining relationships over asserting their opinion. Lastly, "Neuroticism" measures a person's tendency to experience mood swings and express unstable, negative emotions (Kosinski, 2014). Psychometric models can be used to infer a user's likelihood to make certain real-life decisions and even exploit weaknesses—for instance, targeting online casino advertisements at a user whose digital tendencies are consistent with pathological gambling traits (Matz et al., 2017). The OCEAN model was utilized in the infamous Cambridge Analytica scandal, which leveraged the data of nearly 87 million Facebook users to predict users' voting tendencies, micro-target advertisements, and strategically plan campaigns for the 2016 presidential election (Isaak and Hanna, 2018).

The reliability of psychometric profiling is dependent on the aggregation of individuals' digital footprints, the online form of "behavioral residue" (Matz et al., 2017; Kosinski, 2014). The behavioral surplus generated by surveillance capitalism and persuasive technology, as discussed in chapter one, is used to accurately predict personality. The results of three experiments that reached over 3.5 million individuals demonstrate a strong relationship between psychologically targeted advertising and intended behavior change. According to the researchers, "Persuasive appeals that were matched to people's extraversion or openness-to-experience level resulted in up to 40% more clicks and up to 50% more purchases than their mismatching or unpersonalized counter-parts" (Matz et al., 2017). This experiment supports the idea that psychological targeting could be applied to large-scale influence operations on social media. The researchers' findings are eerily consistent with the tenets of effective propaganda. The social media ecosystem reflects the characteristics of good propaganda and serves as a suitable vehicle for information operations.

Information Operations and Propaganda

Social media is a significant channel for global communication and facilitates collective sense-making. Nearly 60% of the world's population uses social media (Statista, 2022). Especially in populations where the majority of people use cell phones, social platforms host a rapid and massive spread of information without range limitations (Tunnicliffe & Tatham, 2017). Social media is interactive by nature—not only between users on an app, but also between the app and the individual his or herself. As discussed in the first chapter, surveillance capitalism demands constant and active participation by social media users through several methods. The same tactics that persuade users to behave in ways that boost monetization can be weaponized to support military objectives. Oftentimes, the only difference is who controls the operation and

who is the target (Dawson, 2021). Despite the many positive and harmless uses of social media, its ubiquitous nature invites threat actors and nation-states to exploit users for their benefit. This section will articulate how social media enhances the power of traditional psychological warfare campaigns.

Social media eases the difficulty of communicating with a foreign adversary's citizens directly. Even autocratic states that restrict the use of social media within their own borders can reap the benefits of its global interconnectivity. Social platforms are effective vehicles for mobilizing support, manipulating public opinion, disseminating narratives, and waging information operations (Bialy, 2017). The definition of Information Operations (IO), according to DOD Joint Publication 3-13, is the "integrated employment, during military operations, of Information Related Capabilities (IRC) in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own" (JP 3-13). IO play a crucial role in both war and peace time. Controlling the information environment can open doors for future attacks and support military operations in real-time. Social media is a valuable, yet contested space in which IO can masterfully complement "kinetic operations" (i.e., 'physical strikes') when executed thoughtfully. The timely use of IO in such "Multi-Domain Operations" (as coined by military scientists) can "amplify the effects of a kinetic strike, deny an adversary first-mover status in the information dimension, or be used to seed psychological effects in an adversarial target audience" (Cruickshank et al., 2023). The influential power and pervasiveness of social media in society elicit a highly potent attack surface for targeted IO and propaganda. In order to understand why, one must look to how past psychological operations relate to the current social media ecosystem.

Psychological operations (PSYOPS), also referred to as Military Information Support Operations (MISO), serve a critical role in many military operations, though their tangible effects are sometimes difficult to see (CRS, 2022). The use of propaganda as PSYOPS is well-documented in history. Propaganda, similar to IO and PSYOPS, refers to the propagation of ideas or narratives with the intention to influence an audience (CRS, 2022). In World War Two, propaganda was famously used by both the British and Nazis in several forms. Propaganda at this time was typically delivered via radio or physical literature (i.e., newspapers, pamphlets) which shows the historical importance of mass media in IO (Ellul, 1973). Though the vehicles for PSYOPS have evolved, the tenets remain the same.

Propaganda seeks to transform a target into an active or passive participant in a cause that supports the propagandist. It has often been used to undermine an adversarial power by degrading their capacity to fight, easing the responsibility of ground forces (Newcourt-Nowodworski, 2005). Propaganda comes in three primary forms: White, Grey, and Black. White propaganda comes from an undisguised source (ex: a leader delivers a persuasive speech to gain support for a cause). Grey propaganda comes from an anonymous source (ex: pamphlets dropped by aircraft with no signature). Black propaganda, the most subversive of all, hides behind false signatures (Newcourt-Nowodworski, 2005). An example of black propaganda, from *Black Propaganda in the Second World War* by Stanley Newcourt-Nowodworski, demonstrates the operational value of information during war. The following quote explains the approach behind a poster addressed to German forces in Norway, allegedly signed by the German commander of troops there:

> "It starts by condemning desertion in no uncertain terms, but then it offers the valuable information that Sweden will grant asylum to anybody wearing civilian clothing, who has stayed on Swedish territory for a minimum of 24 hours. It concludes by making it a duty of all members of the *Wehrmacht* to eradicate this 'growing evil'.
>
> … any document issued in the name of the OKW, denouncing vehemently desertion, but at the same time implying that it is neither difficult nor risky, would be more effective than a white leaflet describing a deserters' paradise… The solider would be much more impressed if he thought that he deduced the facts himself and that the conclusions were his own." (p. 158)

This example also shows that effective propaganda targets the individual, who is steered by information to serve a particular end. For this reason, effective IO through propaganda must give the impression of being personal (Ellul, 1973). Social media platforms are designed perfectly for this. Recommendation feeds such as TikTok's "For You" page, powered by the collection of personal data, appeal to individual interests and attempt to foster an intimate relationship with each user. Under the guise of a personalized environment, an individual could be the target of IO that aims at a larger group of likeminded users (of which he/she is unaware). Jacques Ellul, author of *Propaganda: The Formation of Men's Attitudes*, asserts that people are most susceptible to influence in this state—when they are "alone in the mass" (p. 9). What works to influence one target may not for another, yet the same end can be reached through strategically targeted IO at the individual-level.

Effective influence demands a steady presence in the lives of the target population (Ellul, 1973). In the age of WWII, such an operation would require careful coordination and abundant resources. Advances in technology have optimized the ease and effectiveness of IO and

significantly widened the scale of impact, while reducing the cost and manpower necessary to conduct operations. Additionally, many depend on social media for information and communication during crises (Stockton, 2021). Foreign actors can flood social networks with IO and propaganda during conflicts to confuse target populations and complement military operations. Surveys suggest that the average user spends around 2.5 hours on social media per day (Ali, 2023). This emphasizes not only the susceptibility of users to influence, but also the unceasing wealth of new intelligence and exploits that social media affords. Social media's ubiquitous nature enables threat actors to conduct thorough target audience analysis and respond to online activity in real-time. According to Ellul, "To undertake an active propaganda operation, it is necessary to make a scientific, sociological, and psychological analysis first" (p. 5). Psychometric profiling, enabled by the surveillance economy, supplies the necessary intel that Ellul references, on a scale he likely could not fathom at the time.

Influence operations can exist on the preparational or operational level. Social media serves as an effective medium for both. Preparational propaganda (or "pre-propaganda") aims to prime the target and modify his behavior and frame of mind so that it could be mobilized in future operations (Ellul, p. 30; Newcourt-Nowodworski, p. 13). Behavioral modification can be a slow, continuous process, but Ellul asserts that there is great value in training "conditioned reflexes" (p. 31). The same process exists on social media. Persuasive techniques establish unconscious habits in users which increase engagement and generate personal data. This process prepares the user to be targeted with ads that boost monetization, which is likely to be more effective than ads implemented at random. The same process is valuable for social engineering attacks, which will be discussed in the next section. Operational propaganda (or "active propaganda") calls the target into action or inaction (Ellul, p. 30; Newcourt-Nowodworski, p.

13). Recall, the most powerful propaganda empowers the target to *choose* the path that helps the propagandist's cause. Therefore, IO should primarily operate using the existing landscape of narratives and selectively intervene to advance the operation. IO should widen and deepen existing fault lines in an adversarial population, rather than continuously creating new ones (Newcourt-Nowodworski, 2005). In this manner, each subject becomes his own propagandist and PSYOPS on social media become a victim-controlled weapon.

Information operations on social media do not exist in vacuum. While social platforms offer a massive attack surface alone, the landscape does not end there. Social media users might unknowingly spread information that is part of IO to friends and family via text message. Though the scale of dissemination is drastically smaller, private messages from known individuals may have a great effect (Stockton, 2021). Meaningful contagion is critical to mass influence (Ellul, p. 91). Since recommendation algorithms promote content with high view counts or engagement, social media IO must garner some level of attention or virality to be seen. Threat actors amplify automatically generated and human-generated content via fake accounts and "botnets", which are networks of compromised devices and typically automated profiles (Bialy, 2017). Amplification tactics are often used for spreading misinformation (false information) and disinformation (deliberately false information). Research suggests that these efforts are most likely successful on social media. Studies have shown that fake news spreads much faster than true news, and fake news stories are 70% more likely to be retweeted (Stockton, 2021). Through the use of proxy chains and bots, attribution for IO on social media is difficult. Fake accounts are constantly sought out and deleted, yet the problem persists and grows. While the most effective IO persist through time, threat actors that leverage social media for propaganda and IO generally operate in a low-stakes, high-reward environment.

This section has argued the efficacy of information operations and influence on social media platforms. The question remains: why does this matter? Collective understanding and freedom from foreign influence are critical to the function of democracy. While global connectivity is positive in many cases, social media enables adversaries of the United States to transcend the traditional geographic boundaries that protect the minds and emotions of its citizens. The weaponization of social media transforms unaware social networks into hostile information battlegrounds—a fight to which the average user did not enlist (Bialy, 2017). Meta (owner of Facebook, Instagram, LinkedIn, and more) has tracked and disrupted over 200 covert influence operations networks since the company started publicly reporting in 2017. These uncovered operations took place in 68 countries and in at least 42 languages. The United States was the top target for influence operations (Nimmo & Agranovich, 2022). In Q2 of 2023, Meta removed thousands of pages and accounts that played a role in the "largest known cross-platform covert influence operation in the world" (Nimmo et al., 2023). This operation, launched by China, spanned more than 50 platforms and "included positive commentary about China and its province Xinjiang and criticisms of the United States, Western foreign policies, and critics of the Chinese government including journalists and researchers" (Nimmo et al., 2023). The anonymity offered by social media encourages threat actors to conduct operations on popular platforms (CRS, 2020). This operation represents just one covert influence network out of 200 discovered by Meta since 2017. In order to protect users and defend U.S. interests, other popular platforms must relentlessly detect and respond to covert influence operations. Platforms must also proactively defend themselves from IO through target-hardening and heightened understanding of adversarial IO campaigns.

The social media landscape will continue to evolve. Older generations who make up a small percentage of active social media users will phase out, likely increasing the potential scale of IO. Tactics, Techniques, and Procedures (TTPs) will become more powerful and effective with time in order to keep up with national and private sector defenses. Social media empowers threat actors in foreign countries to discretely stay up to date with linguistic developments, improving their ability to generate influence operations and deceive American citizens. Information operations and deception on social media can result in drastic tangible consequences. The next section will examine the use of social media for "social engineering" and intelligence collection.

Intelligence Collection and Social Engineering

The abundance of personal data on social media enables threat actors to collect valuable information on their targets. The last section focused on how social media is a potent attack surface for IO and propaganda. However, it is critical to understand how social media data leaves users and their assets vulnerable to various forms of attacks.

As discussed in Chapter One, the economic imperative of surveillance capitalism demands the harvest of user data not only on social media, but also through any available digital entities that capture personal or behavioral data (Zuboff, 2019). Chapter One provided examples that demonstrate the uses of third-party data for targeting ads and optimizing recommendation systems. The aggregation of data across platforms can also provide useful intelligence to threat actors and adversaries of the United States. Emails provided by consumers to register for one social platform can be tracked across other platforms and digital technologies that use the same address (Ünver, 2018). Furthermore, social media data can supplement intelligence collected via

Internet Communication Technology (ICT) monitoring, the Internet of Things (IOT), and other sources. The Internet of Things, simply put, is the network of consumer devices that exchange information and communicate with other devices in the network (Ünver, 2018). Popular examples of IOT devices include smart-home technologies such as Ring doorbells and Amazon's Alexa. Data collected by IOT devices could provide threat actors with valuable insight into an individual's personal life and behavior. Jessica Dawson, in "Microtargeting as Information Warfare", provides an excellent example of an IOT-enabled attack surface:

> "Consider when Sarah Huckabee Sanders, the White House press secretary, tweeted about her 2-year-old being able to buy toys via Alexa.[48] Sanders informed the entire world that she—a person with direct daily access to the President of the United States—had what was functionally a listening device in her home. While there is no evidence her smart speaker was hacked, it remains a potent vulnerability for everyone" (p. 70).

While smart-home technology is not the focus of this thesis, this example demonstrates the potential threats that emerge from the intersection of social media and the IOT. Social media, like the Internet of Things, provides information that can be used to deceive and manipulate individuals into complying with a malicious operation.

Human integration with digital technologies has created new attack surfaces in the cyber world. Government entities and many companies invest heavily in the protection of their digital assets, communications, and intellectual property. However, some aspects of cybersecurity efforts and information architecture are still managed by humans. Cyber threat actors often launch attacks that begin by targeting individuals that are responsible for access control or knowledge management. Socially engineered attacks can exploit this human element and allow

threat actors to infiltrate highly secure systems (Krombholz et al., 2014). Social engineering attacks manipulate individuals with valuable information or power into compromising a target (Krombholz et al., 2014). These attacks come in many forms, but oftentimes victims are deceived into providing sensitive information or access credentials that help attackers steal money and conduct espionage operations.

Social engineering relies on accurate intelligence to be effective. Social media can help threat actors understand their target and select the most optimal method of deception. For example, attackers could use LinkedIn to identify companies that seemingly do not prioritize security or to target employees with little experience (Krombholz et al., 2014). Social engineering attacks can disrupt a company's operations and result in massive losses. Casino giants MGM Resorts and Caesar's Entertainment were recently victims of social engineering attacks. The attack on MGM forced the company to temporarily shut down its operations, and MGM projected $100 million in losses to their third quarter results (Collier, 2023a). The attacks were launched by 'Scattered Spider' (also known as 'UNC3944'), a group notorious for using social engineering techniques to deceive password managers and tech support employees via SMS and phone calls (Collier, 2023b). These attacks are indicative of the complex threats facing major corporations, which also could endanger government agencies. Just as preparational propaganda can be operationalized as needed, seemingly irrelevant data collected from social platforms could later prove effective in a social engineering attack. For this reason, there is an incentive for foreign adversaries to relentlessly collect intelligence on social media. New opportunities for exploitation might arise during crises or changing U.S. administrations, and it critical to have accurate intelligence at-hand to attack strategically.

Evidence supports the danger and potential impact of social engineering attacks. According to a recent report by IBM, the global average total cost of a data breach is $4.45 million, and the United States had the highest total average breach costs at $9.48 million (IBM, 2023). According to the report, “Phishing and stolen or compromised credentials were responsible for 16% and 15% of breaches, respectively” (IBM, 2023). Spear-phishing campaigns, the micro-targeted version of phishing, attempt to acquire information or steal assets by masquerading as a trustworthy entity of the target (Krombholz et al., 2014). Social networking sites could be used to gather intelligence on a target’s relationship status, employment status, friends and family members, or frequented restaurants or shops. This information might help threat actors strategically craft an attack by gaining a target’s trust or appealing to their interests (Krombholz et al., 2014). The anonymity of social media enables attackers to construct networks of fake profiles, which can be used to collect intelligence on future targets or propagate links embedded with malware. These operations can even be implemented at scale using automation tools (Krombholz et al., 2014). Innovations in artificial intelligence, including deepfake technology, will likely improve the effectiveness and potency of spear-phishing campaigns and social engineering attacks (Stockton, 2021).

Conclusions

The architecture and affordances of social media empower state and non-state actors to conduct various operations on platforms, including information operations, social engineering, and intelligence collection. Traditional propaganda, intelligence, and influence tactics are not new, but social media offers an unprecedented scale and potential impact that present unique challenges to U.S. National Security and society. Micro-targeting techniques, powered by

psychometric profiling, highlight the manipulative power that social platforms possess. When these tactics are applied maliciously, social media can be effectively weaponized.

Social media companies like Meta prioritize their own interests, sometimes to the detriment of the U.S. competitive advantage and public safety. While social media platforms are powerful channels for global communication and collective sense-making, covert influence operations and groups of cyber threat actors can transform these online spaces into hostile battlegrounds. This chapter has argued that social media is a critical aspect of multi-domain operations and a dynamic medium for exerting power. This paper has provided evidence that articulates *why* social media poses a threat and *how* it might be operationalized. The rest of the paper will apply this research to a case study of TikTok, in order to assess the threat that the platform poses to U.S. National Security.

CHAPTER 3: INTRODUCING TIKTOK

TikTok is one of today's most popular social media platforms. With a global user base of nearly 1.6 billion, the relatively new platform has cemented itself as a leading mobile application amongst well-established media giants (Iqbal, 2023). Without any investigation, it is evident that TikTok has optimized how users engage with content. Other prominent social media platforms have tried to replicate TikTok's successful design—YouTube's "Shorts", Instagram's "Reels", Netflix's "Fast Laughs", and Snapchat's updates to how users view "Stories" are all examples of this mimicry. TikTok has proven itself to be a leading provider of short video-based content and was the most downloaded mobile app worldwide in 2022 (Apptopia, 2023). TikTok's popularity is highlighted by its prevalence in the United States. As of March of 2023, there were over 150 million active users in the United States, nearly 50% of the country's population (TikTok Newsroom, 2023). The platform's growth and success, however, has not gone untouched by controversy.

Many questions have been raised about TikTok's extensive collection of user data and its parent company, Chinese media giant ByteDance Ltd. The platform's integration with American citizens has led U.S. politicians and cyber professionals to question the motive behind the company's privacy policy and its effects on the nation. Similar concerns have been raised by several European countries, India, and Australia. This thesis seeks to evaluate the validity of recent concerns regarding TikTok's threat to U.S. National Security. The case study will begin by examining the platform's history, design, and privacy policy. This introduction highlights the ways in which TikTok is unique from other platforms in today's social media ecosystem and

why the differences are relevant to national security concerns. Lastly, this chapter will detail the platform's ties to the People's Republic of China.

TikTok's History and China's Douyin

TikTok is the international version of the app "Douyin", owned by the Chinese media conglomerate ByteDance Ltd. TikTok's predecessor, Musical.ly, which focused on basic lip-syncing/dancing videos, was created by a Chinese tech company and specifically targeted at the U.S. market in 2014. After the platform's success, it was bought out, re-designed, and re-marketed by ByteDance in 2017 as TikTok, as a means for ByteDance to enter the U.S. market (CRS, 2023b). This strategic move allowed ByteDance to combine the success Musical.ly had with young people in the West with the AI-driven capabilities of Douyin (Kaye et al., 2020). Douyin and TikTok appear very similar structurally and even showcase the same logo. On both platforms, users view content provided by a recommendation algorithm by swiping from video-to-video. At a glance, the two platforms are nearly identical, but there are some very interesting differences in the user-experience. Douyin includes a second 'Trending' tab on its toolbar entitled "positive energy", which is an "ideological buzzword in China that is emblematic of Chinese patriotism" (Kaye et al., p. 237). This umbrella term, also termed "playful patriotism", signifies content that is in accordance with the values of the Chinese Communist Party (Kaye et al., p. 238). Although this feature doesn't exist on TikTok, it is an example of how the PRC can exert influence on social media.

Through Douyin, the PRC can promote the State and filter out content that is not favorable. While TikTok has its own objectives for content moderation, the threshold for content that does not abide by Douyin's standards is much wider. Categories for reporting on Douyin

include pornography, political sensitivity, rumors/swindling, and insulting (Kaye et al., 2020). Efforts to control what Douyin users' see and interact with are consistent with China's internal governance of their information environment. Coined "The Great Firewall", China employs an internally locked-down internet service. The Golden Shield Project in 2000 created a data-driven surveillance network that monitors the online activity of Chinese citizens by filtering content and enforcing censorship (Lee, 2018). The next section will examine the PRC's use of cyber in greater depth. But, even in this locked-down environment, the PRC has taken action to curtail the usage of Douyin in China, especially for young users. For Douyin accounts using "youth mode", which is regulated through real-name authentication, children under the age of 14 are limited to just 40 minutes per day on the platform. There is a hard shutdown of the platform between the hours of 10 p.m. and 6 a.m. for these young users. Additionally, young Douyin users are recommended more videos that endorse science experiments, historical content, state museums, and patriotism (Wayt, 2021). ByteDance even injected a mandatory 5-second lag after some videos, in an effort to prevent addiction amongst Chinese youth (Humphries, 2021).

Some important conclusions can be drawn from these policies. ByteDance, which is innately and unquestionably tied to the CCP, designed TikTok to be targeted at the U.S. market. After doing so, significant regulations were implemented that influence how children use Douyin, China's internal, restricted version of TikTok. This timeline indicates that the PRC sees a serious problem with how the platform affects their nation's youth. They do not want their young citizens to engage in fad trends and strive to be culture "influencers". Rather, they want to reduce entertainment-media addiction, endorse nationalistic ideology, and promote STEM related careers. Despite this stark reality, the United States leaves its youth unguarded on

TikTok. Awareness of TikTok's history is critical to understanding the potential implications of its use in the United States.

TikTok's Design and Privacy Policy

TikTok's persuasive design and cutting-edge algorithmic recommendation system have revolutionized how social media platforms appeal to users. The platform's architecture establishes an intimate relationship with the user. Following the demands of surveillance capitalism, the 'For You Page' on TikTok provides users with strategically curated content and advertisements based on various sources of data. White space (negative space between features) is eliminated entirely on this feed by embedding actionable icons (like, comment, share, etc.) directly onto videos. Eliminating white space and embedding interactive features persuades users to remain immersed in the infinite feed of personalized content. TikTok's popularity, especially with younger generations, indicates the success of the platform's user-interface (UI) and user-experience (UX). According to a 2022 survey of American teenagers ages 13 to 17 by the Pew Research Center, 67% have ever used TikTok and 16% claim they use it constantly (Vogels et al., 2022). Another study, conducted by non-profit Common Sense Media and University of Michigan C.S. Mott Children's Hospital, determined that the median time spent on TikTok by children per day was 1 hour and 52 minutes (Radesky et al., 2023). The research sample consisted of 203 children aged 11-to 17-year-olds on Android phones. The study also noted that children were more likely to spend several hours (sometimes upwards of 7 hours) on the platform, while 3 hours was the longest amount of time spent on Instagram or Snapchat (Radesky et al., p.7). The following excerpt, synthesized from two quotes provided by 11th graders in the report, perfectly captures youth sentiments surrounding TikTok:

> Youth advisors explained to us that TikTok provides an experience that other social or video-sharing platforms don't. TikTok was described as "easy" because videos simply start to play— the user doesn't have to make any decisions, so there's no friction. Adolescents we talked to said that the TikTok algorithm "knows" them so well, they can expect that they will likely find something fun to watch. If the user isn't interested in the video that starts to play, the app quickly adapts to something more engaging or that fits their mood or desires (Radesky et al., p. 7)

As concluded in Chapter One of this thesis, social platforms are deliberately constructed to maximize engagement. The results of this study indicate that children are highly receptive to TikTok, largely due to the accuracy of recommendations. TikTok's eerie ability to predict desirable content stems from its extensive collection of user data.

Although the social media ecosystem is built on data collection, TikTok's privacy policy is cause for immediate concern. Given the platform's ties to China, it is extremely relevant to review the company's policy and connections to the PRC. Although the policy is too long to review in its entirety within this chapter, this section will review some of its key elements.

TikTok, of course, collects basic account information (name, age, language, email, phone number, profile image, etc.) and user-generated content (TikTok, 2023a). But according to technical analysis of TikTok's source code conducted by cyber security company Internet 2.0 in July of 2022, the "Permissions and device information collection are overly intrusive and not necessary for the application to function" (Perkins, 2022, p. 1). TikTok automatically collects device identifiers such as IP address, mobile carrier, device system, network type, screen resolution, operation system, app and file names and types, battery state, audio settings, and keystroke patterns or rhythms. The platform also claims it may associate users with information collected from devices they do not use TikTok on (TikTok, 2023a). Some of this information is

typically collected by social platforms. However, the collection of keystroke patterns could enable the platform to know specific actions users take outside of the platform, including what users type. Collection of keystroke patterns, which is typically a function of malware tools, might reveal users' login credentials, payment information, message content, and more (Mozur et al., 2022). Internet 2.0 claims that TikTok's data collection allows for device mapping, meaning that theoretically the platform could deduce the layout of your phone (Perkins, 2022).

From user-generated images and videos, TikTok can collect "face and body features and attributes", "the existence and location within an image of face and body features and attributes", and biometric identifiers such as faceprints and voiceprints (TikTok, 2023a). TikTok can scan and analyze messages on the app for content and even view the text, images, and videos found in the device's clipboard. Additionally, the platform can access users' phone and social network contacts. Through third-party associations and cookies, TikTok can gain access to users' activity on other sites and across devices. Conveniently, the platform is not responsible for the privacy practices of its providers and affiliates (TikTok, 2023a). A section of the policy titled "How We Use Your Information" details how user data is applied to platform improvement, troubleshooting, targeted ads, algorithm training, and more. This section closes by reserving the right to combine any information they collect or receive and use it for any purposes they disclose at the time of consent (TikTok, 2023a). TikTok has a separate privacy policy directed to children under the age of 13 that use "Kid's Mode". While this version of the app collects limited data, the platform still reserves the right to share information with their corporate group as needed (TikTok, 2023b).

The platform's privacy policy also explains that entities in TikTok's corporate group have "limited remote access" to the information the platform collects (TikTok, 2023a). To the

uninformed reader, this is likely a benign statement. TikTok's corporate group obviously would include its Beijing-based parent company, ByteDance Ltd. The diagram in *Figure 1* below, taken from ByteDance's website, shows how TikTok fits into ByteDance's corporate structure.

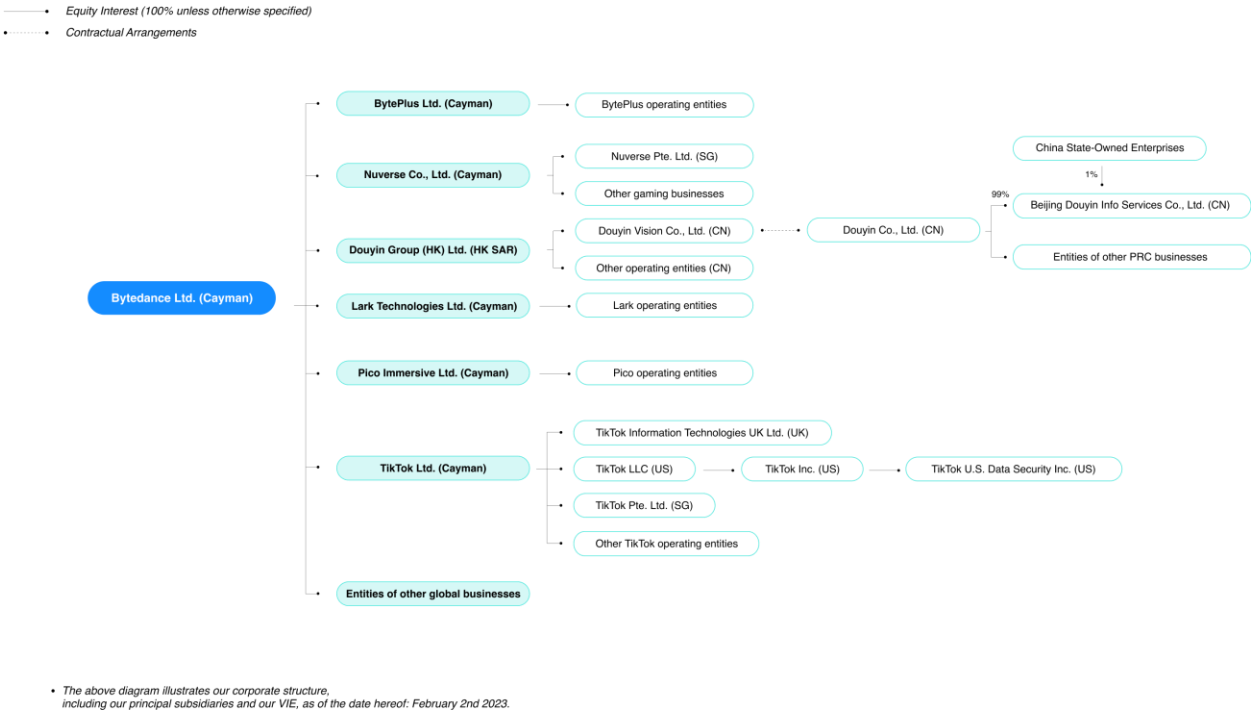

Figure 1: ByteDance Ltd.'s Corporate Structure

Based on this diagram, ambiguous "China State-Owned Enterprises" have a 1% stake in Beijing Douyin Info Services Co., Ltd., which is contractually connected to TikTok's parent-company ByteDance. TikTok's CEO, Shou Zi Chew, claims that this 1% acquisition was necessary to obtain a news license in China for several China-based applications such as Douyin (Chew, 2023). Douyin Co., Ltd. is also tied to "Entities of other PRC businesses". These connections indicate that some of ByteDance's subsidiaries are likely subject to PRC legislation. Despite ByteDance's corporate structure, TikTok asserts that all data is stored in the U.S. and Singapore and the company would not share data with the Chinese government if asked. However,

TikTok's efforts to portray independence from China disregard ByteDance's ability to access data. ByteDance and other PRC-based companies are subject to the PRC's cyber security and intelligence laws, which presents a threat to the United States.

Today, TikTok maintains offices in major U.S. cities such as Los Angeles and New York (CRS, 2023b). According to the Washington Post, some high-level executives have transferred from ByteDance to TikTok in 2023, some of which even relocated to the United States from ByteDance's Beijing headquarters (Wells, 2023). In response to pressure by the U.S., TikTok has tried to show its separation from the PRC by contracting with Oracle, an American software giant, in a partnership referred to as "Project Texas" (Chew, 2023). In a letter to nine U.S. Republican Senators, TikTok's CEO Shou Zi Chew claimed that the company has not and would not provide data to the CCP. In the same letter, however, he concedes that China-based employees could access user data in some cases. ByteDance engineers around the world work on TikTok's algorithm, and TikTok employees use software provided by ByteDance (Chew, 2023). Despite attempts to show allegiance to the U.S. interests and privacy, ByteDance's ties to the CCP should not be overlooked.

Conclusions

TikTok's connection to Beijing via ByteDance Ltd. has been a primary cause of concern for the United States Government. Amidst continued and escalating tension between the two countries, the U.S. seeks to protect its assets and its citizens from PRC influence. Given TikTok's widespread integration with U.S. citizens, particularly children, the United States should be wary to accept the platform's operations in the country. TikTok's extensive collection of user data and persuasive design make it a particularly effective vehicle for information

operations, propaganda, and cyber operations. Additionally, a Beijing-based media company like ByteDance is innately tied to the Chinese government due to the country's employment of digital authoritarianism. The PRC uses technology as a force multiplier to control its own citizens and exercise power abroad. For these reasons, TikTok should be addressed with caution and investigated for its threat potential. The next chapter will examine how PRC strategies and policies make clear the threat that TikTok poses to U.S. National Security.

CHAPTER 4: FRIEND OR FOE? WEAPONIZING TIKTOK AGAINST U.S. INTEREST

This chapter will assess the threat that TikTok poses to U.S. National Security given its clear connection to the People's Republic of China (PRC). Though TikTok has attempted to prove its distance from China, PRC policies shed light on the likelihood of continued, undisclosed ties to the Chinese government. This chapter will investigate how the PRC could exploit TikTok to gain a competitive advantage over the United States through information operations, propaganda, intelligence collection, and cyber-attacks. Building upon research from Chapter Two, it will assess how these tactics could contribute to current PRC strategies and multi-domain operations against the U.S. This assessment is critical as tensions between the U.S. and China evolve and conflicts reshape power structures in various regions throughout the world. The U.S. Department of Defense, in its recently released 2023 DOD Cyber Strategy, describes China as a "pacing" and "broad and pervasive" threat to the United States (DOD, 2023a). Given this designation, any platform with ties to China that hosts nearly 50% of the U.S. population should be addressed with extreme caution. This case study seeks to place the TikTok threat in its proper context by connecting the dots between vulnerabilities on social media and the PRC's efforts to undermine the United States.

TikTok's Strategic Value: Leveraging Cyber for Global Dominance

Modern communication technology and the informatized world afford new methods of exerting power and enable war to be conducted in unprecedented ways. As tensions continue to rise between the United States and China, the PRC's utilization of cyber for strategic influence and warfare has been a primary focus for the U.S. Intelligence Community, national security

experts, and policymakers. According to the 2023 DOD Cyber Strategy, China "seeks advantages in cyberspace in order to facilitate its emergence as a superpower with commensurate political, military, and economic influence" (DOD, 2023a). These advantages may be facilitated by controlling communications, strategically targeting information operations and psychological warfare campaigns, collecting intelligence, conducting cyber espionage, gaining access to critical systems, growing technological presence in different regions, or partnering with likeminded governments. The PRC utilizes all of these methods (and more) to reshape the world order, undermine the United States, and protect its own interests (DOD, 2023a).

While these techniques may not sound unique in comparison to other nations, the PRC places particular emphasis on cyber espionage. Collecting foreign intelligence in cyberspace presents several advantages that human intelligence often does not offer, including access to large, easily transferrable datasets and enhanced protection due to difficulty identifying a source (Wortzel, 2014). These cyber espionage efforts often include the stealing of intellectual property, trade secrets, and sensitive military information from the United States (Laskai & Segal, 2018). Espionage can support internal operations in China and promote the economy, but it can also enable the People's Liberation Army (PLA) to prepare for future conflict. By stealing valuable scientific and technological information from other countries, the PRC can save its own time and resources for the rapid development of rival military technologies (Wortzel, 2014). The same can be said for China's collection of foreign social data—understanding an enemy's values, activity, and fault lines can make easier the task of military forces. China's use of spies and intelligence collection has roots over a thousand years old, dating back to the writings of Sun Tzu. While the means for executing may be different, the idea remains the same: degrade the capacity of the adversary to fight back. As discussed in Chapter Two, social media can power targeted

information operations that prepare for and supplement other operations. TikTok's massive scale usage in the United States and extraordinary collection of data provides the PRC a double-edged sword with strategic and operational value.

China is said to aggregate immense amounts of data from various mediums for potential future use. This approach has been referred to as a "grains of sand" or "mosaic" strategy, originating from a popular quote in the world of security:

> "If the Russians want to get certain sand from a beach that's special, they'll have a submarine come in at night. […] They'll get a bucket full of sand, and they'll take it back to the submarine and leave. The Chinese will have 500 people having picnics on the beach, each picking up the sand in a small can (or, each picking up a grain of sand), and bringing it back" (Smith, 2023).

Seemingly irrelevant datapoints may prove valuable for social engineering campaigns and future operational propaganda. The PRC is able to covertly collect intelligence and conduct espionage operations through corporate proxies and by infiltrating the U.S. supply chain. TikTok enables the PRC to collect valuable social data, construct and influence target audiences, track expatriates, and open avenues for future operations under the façade of a harmless, creativity-promoting platform. Social media is only one aspect of the PRC's larger effort to erode the competitive advantage of the United States and establish global dominance. The PRC seeks to penetrate the U.S. information ecosystem and physical, technological infrastructure through a 2013 foreign economic strategy known as the Belt and Road Initiative (BRI).

The BRI, according to a report from the Congressional Research Service, "aims to develop China-centered and - controlled global infrastructure, transportation, trade, and production networks", which, "focuses on infrastructure, and related supply chain,

transportation, technology and financial integration that expands the use of China's credit information system and currency" (CRS, 2023c). The BRI seeks to establish Chinese firms overseas, employ PRC citizens abroad, and open new avenues for monetization, trade, and influence (CRS, 2023c). To the concern of the United States, the PRC's strategic investment and corporate governance are typically state-sponsored and concentrated in regions of shared critical interest to the U.S. Many intelligence analysts argue that the BRI serves alternate, military purposes, and that the PRC wants to establish, "standards that promote civilian and military interoperability and could make foreign infrastructure such as ports available for China's military use" (CRS, 2023c).

This concern largely arises from the digital influence aspect of the BRI, which includes the social media ecosystem. The "Digital Silk Road", a component of the BRI, seeks to enhance China's presence in overseas information and communications technology (ICT). Tech-giants such as Huawei and Alibaba, who answer to the central government, conduct operations in regions determined by the BRI and seek to implement foundational tech infrastructure (CRS, 2023c). The Belt and Road Initiative provides the PRC with access to critical infrastructure and (potentially sensitive) information environments in both the U.S. and developing regions of particular interest to the U.S. Through the Digital Silk Road, the PRC wants to infiltrate the supply chains of smart-cities, 5G communications, artificial intelligence (AI), fiber-optic cables, surveillance technology, satellite networks, transportation, vaccine development, and renewable resources (CRS 2023c; Gering, 2023). This paper argues that the BRI is reflected in the PRC's use of social media for cyber dominance.

The targets of the Digital Silk Road are aspects of what the PLA calls the "virtual battle space" (Wortzel, 2014, p. 8). Within each of these abovementioned sectors of infrastructure lies a

potent attack surface. The PRC maintains control of critical switches in target countries, including ones that do not support the BRI due to globalization and the ubiquity of technology. According to Wortzel, PRC strategists argue awareness is at the core of warfare in the information age. Therefore, the destruction of an enemy's ability to understand their surroundings through information could uproot their ability to attack (Wortzel, 2014, p. 7). The ability to deactivate methods of communications or paralyze the information ecosystem is a valuable weapon in modern warfare. Sabotaging an enemy's collective understanding is a key strategy of the PLA and will be examined in the next section of this chapter in the context of social media. In addition to these tactics, the PRC has the capacity to leave backdoors embedded within critical infrastructure and technology through the Digital Silk Road. These backdoors can be strategically placed for future attacks, once the potential scale and damage of the intended attack is optimal (Wortzel, 2014). Aside from cyber warfare operations, the PRC could utilize corporate proxies and espionage to collect intelligence on a region, particular leader, critical infrastructure sector, or emerging technology.

China's policies on cybersecurity and intelligence enable the harvest of data acquired by enterprises backed by the state. As Chapter 3 discussed, TikTok's relationship to its parent company ByteDance reveals a connection to the CCP that cannot be overlooked. Therefore, TikTok poses a threat to U.S. National Security due to policies that coerce PRC-based citizens and companies to comply with China's intelligence collection efforts. In 2019, the former U.S. National Counterintelligence and Security Center (NCSC) Director, William Evanina, issued a warning on how China extracts information from institutions that claim they are not owned by the government nor conduct business in China:

> "Article 7 of China's National Intelligence Law states, "Any organization or citizen shall support, assist, and cooperate with state intelligence work in accordance with the law, and maintain the secrecy of all knowledge of state intelligence work."
>
> Article 28 of China's Cybersecurity Law states, "Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law."
>
> Article 11 of China's National Security Law states, "All citizens of the People's Republic of China …. shall have the responsibility and obligation to maintain national security."
>
> What does this mean for you? If you're doing business in China or representing clients there, you will likely be a target" (Evanina, 2019).

By nature of these laws, companies acting at the discretion of the PRC are an arm of the Chinese government. These laws help the PRC exercise power abroad, prepare malign influence operations, and monitor expatriates, who are considered threats to the state. While TikTok claims they do not provide data to the CCP or PRC, Beijing-based ByteDance and its PRC-citizen employees could be required by law to provide information acquired by TikTok to the government. According to the company's website, ByteDance has over 110,000 employees based out of 200 cities globally, and its apps operate in 150 markets and 35 languages (ByteDance, 2023). ByteDance has offices in major U.S. cities such as New York, Washington, D.C., Chicago, Austin, and more. The Chinese media giant even showcases a picture of Manhattan, New York on its 'Jobs' site (ByteDance, 2023). In addition to the abovementioned federal laws, private companies that operate in China and employ CCP members have been pressured to establish internal CCP cells that promote party-aligned decision-making. It has been reported that employees at HSBC, for example, have formed internal CCP committees though

the company claims these cells have no influence on the overall business (Morris & Kinder, 2022). These policies and examples represent the global network of corporate entities with influential power that are the PRC's disposal.

The United States has already taken action to prevent investment in and cooperation with Chinese companies that threaten national security and undermine democracy. In November of 2020, the Trump administration issued Executive Order (E.O.) 13959 to respond to the threat that the PRC poses to the U.S. through its use of private companies to expand its military-industrial complex and intelligence apparatus (Exec. Order No. 13959, 2020). In 2021, the Biden administration expanded upon this E.O by prohibiting U.S. investment and cooperation with such Chinese companies. The Biden administration targeted 58 entities that supported China's defense, intelligence, and surveillance technology sectors, including the well-known companies Hangzhou Hikvision Digital Technology Co., Ltd. and Huawei Technologies Co., Ltd (The White House, 2021). This thesis contends that TikTok should also be considered as an extension of China's military-industrial complex and addressed with the same level of caution.

Prior to any assessment of TikTok's operational value, its connection to the CCP via its parent-company ByteDance presents a unique threat to the United States. As concluded in Chapter Two, social media can amplify the potency and scale of cyber operations and enable threat actors to collect an unprecedented amount of intelligence on a target audience. TikTok's addiction-promoting design and extensive collection of user data have helped establish itself as a leading social platform in America, especially for young users. Due to PRC policies that compel its constituents to provide information that assists national security and intelligence efforts, TikTok fundamentally is a tool for global surveillance and intelligence collection. This thesis argues that TikTok complements other PRC strategies such as the Belt and Road Initiative.

TikTok's integration with U.S. citizens provides the PRC a stream of social data that can be exploited to influence and undermine the U.S. This section has presented evidence that details *what* TikTok's connection is to the PRC's broader goals in cyberspace. Using recent examples and PLA strategy, the next section will assess *how* TikTok could be used in multi-domain operations against the U.S. if weaponized.

TikTok's Operational Value: Weaponizing Social Media

The PRC has recognized the value of leveraging social media in multi-domain operations. The PRC considers the information ecosystem a critical battleground to be won early in conflict and dominated in both war and peacetime. The informatized world has blurred the lines between military personnel and civilians and between war and peace (Cheng, 2013). This new gray area demands that countries take constant steps to dominate the information ecosystem in order to maintain power. To meet these demands, the PLA adopted a new warfare strategy in 2003 known as the "Three Warfares": legal warfare, public opinion warfare, and psychological warfare (Wortzel, 2014). Public opinion warfare creates, disseminates, and conceals information to gain domestic and foreign support for a cause or steer the enemy's public opinion. Legal warfare leverages international and domestic laws to generate narratives that support the PRC's interests, justify the PRC's actions, and undermine the enemy. The PRC uses psychological warfare, which is discussed at-length in Chapter Two, to deceive and coerce the enemy into behaving in a manner that supports the PRC's interests or corrupts the enemy's capacity to respond (Cheng, 2013; Wortzel 2014). The PLA seeks to combine these operations in cyberspace to create an environment that promotes the PRC's strategic and military objectives (Cheng, 2013).

The PLA appreciates social media's power, especially during crises, to promote narratives, gain support, and undermine an adversary's resolve to engage in conflict. While China's lockdown media ecosystem helps to defend against foreign influence, the openness of the U.S. market leaves users susceptible to Chinese-IO campaigns. Social media platforms enable the PRC to reach the U.S. audience discretely, cheaply, and effectively. The massive, Chinese-backed, cross-platform covert influence network discovered by Meta (as discussed in Chapter Two) is a perfect example of the "Three Warfares" concept in action. Other platforms are plagued by similar influence networks controlled by the PRC. In 2020, Twitter (now "X") disclosed a PRC-linked IO network that consisted of 23,750 highly engaged, "core" accounts, and approximately 150,000 "amplifier" accounts that engaged with the core accounts and artificially inflated engagement metrics. While this network was quickly detected and removed, it promoted content that was "predominantly in Chinese languages and spreading geopolitical narratives favorable to the Communist Party of China (CCP), while continuing to push deceptive narratives about the political dynamics in Hong Kong" (X Blog, 2020). The PRC has since taken steps to improve the effectiveness of its IO by incorporating technological advancements.

The PRC has developed a new psychological warfare strategy for the informatized world known as "Cognitive Domain Operations" (CDO). According to a DOD Report to Congress, "CDO blends previous Chinese concepts such as public opinion and psychological warfare with modern internet technologies and communication platforms, and is designed to achieve strategic national security goals by affecting a target's cognition and resulting in a change in the target's decision making and behavior" (DOD, 2023b). This strategy seeks to evolve current psychological warfare operations by leveraging AI, big data, neuroscience, and other emerging fields (DOD, 2023b). According to PLA articles, the goal of CDO is to achieve "mind

dominance" which will help to subdue an enemy without fighting (DOD, 2023b). Data harvested from TikTok can supplement the potency and scale of Chinese CDO and provide a susceptible target audience. Additionally, deepfake technology and other AI-powered tools could increase the effectiveness of targeted IO and public opinion warfare on TikTok. As these emerging technologies evolve, PRC methods of informatized warfare will grow into "intelligentized" warfare, presenting new challenges to U.S. National Security (Stockton, 2021).

The PLA seeks to advance cognitive operations on social media. According to a recent *People's Liberation Army Daily* article, "cognitive confrontation" on social media is a key element of successful multi-domain operations (Wenling & Jiali, 2023). The *People's Liberation Army Daily* is the official newspaper of the PLA. This source is valuable for understanding how the PRC could weaponize TikTok on a macro-scale, and begins with the following statement:

> "The 'invisible control' of social media in issue planning, the 'invisible embedding' of information production, and the 'seamless link' in information dissemination methods can effectively achieve an 'invisible' impact on the audience" (Wenling & Jiali, 2023).

The article details four main types of confrontation acts: "information disturbance", "discursive competition", public opinion, and "information blocking" (Wenling & Jiali, 2023). TikTok could be used as a vehicle for each of these cognitive warfare methods. According to the article, information disturbance manipulates the target audience's perception of real circumstances, resulting in a chain reaction of public confusion and distorted viewpoints (Wenling & Jiali, 2023). TikTok, due to its recommendation-algorithm, can rapidly disseminate misinformation and disinformation. It is important to note here that the weaponization of TikTok does not have to be directly controlled by the PLA or Chinese Government in order to promote its strategic interests. Recall, from Chapter Two—effective IO feeds off the existing landscape of narratives

and selectively intervenes when advantageous. In this manner, official control is only needed as an “invisible hand” and TikTok can operate as a user-controlled weapon (Wenling & Jiali, 2023).

The recent Israel-Hamas War provides a potential example of how TikTok could shape collective understanding, with and without deliberate interference. The hashtag “#Palestine” has received 27.8 billion views on TikTok and “#Israel” has received 23 billion (Lorenz, 2023). Shou Zi Chew, TikTok’s CEO, has publicly countered claims that TikTok’s algorithm amplifies antisemitism and has taken steps to remove such content (Maheshwari, 2023). According to a recent Pew Research study, 32% of U.S. adults aged 18 to 29 say they regularly get news on TikTok. Additionally, 43% of TikTok users say they regularly get news from the platform (Matsa, 2023). These statistics reveal a potential target audience for Cognitive Domain Operations, IO, and propaganda. Through TikTok, the PLA can not only generate and amplify narratives that align with the PRC’s interest, but also drive users to ideological extremes, sow confusion through disinformation, or even flood users’ feeds with irrelevant content.

Furthermore, many political leaders have TikTok accounts. If an adversary could gain access to a leader’s account (or use deepfake technology to impersonate one), threat actors could undermine domestic and foreign relations or exploit existing political fault lines during a regional crisis like the Israel-Hamas War (Stockton, 2021). Active participation by citizens is critical to the function of democracy. The ability to erode collective understanding can impact public opinion and consequentially, administrative decisions. Even though the tangible effect of IO is difficult to see, using TikTok as the vehicle could still provide the PRC with valuable social data to be operationalized during future conflicts.

The PRC wants to control and exert influence via social media during war and peacetime. This thesis argues that TikTok has operational value outside of traditional attempts to politically

polarize U.S. citizens and degrade collective understanding. Propelling users to *any* extreme could prove valuable for future IO or social engineering attacks. An experiment conducted by *The Wall Street Journal* demonstrated that TikTok's 'For You' page had a shocking tendency to recommend extreme content to users. Researchers from the Journal set up fake accounts that, undisclosed to TikTok, had predetermined interests such as forestry, politics, or depression. Each bot only expressed interest by rewatching or pausing on videos that aligned with its predetermined interest. The team discovered that after only 36 minutes of total watch time (224 videos), a bot with the assigned interests of "depression" and "sadness" was predominantly recommended videos about mental health struggles and depression (WSJ Staff, 2021). In fact, 93% (278 videos) of the videos recommended to the account were related to sadness or depression. The majority of the remaining 7% of videos were advertisements. Similar outcomes were reached by other bots—an account with an interest in sexual content was propelled to content promoting sexual power dynamics, while another account with an interest in politics was later served election conspiracies and QAnon videos. While TikTok executives said this experiment does not accurately represent the diverse interests of the average user, it still provides evidence that supports TikTok's capacity to propel users to extremes (WSJ Staff, 2021).

Considering half of the U.S. population uses TikTok, this manipulative power can be leveraged to undermine democracy and create fault lines in public opinion. The most recent example of extremist content on TikTok is the recent virality of Osama Bin Laden's 'Letter to America' (Moench & Shah, 2023). Just over a month after Hamas' invasion of Israel, videos with the hashtag "#lettertoamerica" have amassed 14 million views in just one day. The letter justifies the murders of 9/11 citing U.S. and other foreign-sponsored violence against Muslims and condemns U.S. support for Israel. In one video that had over 900,000 views, a user claimed

that “everything we learned about the Middle East, 9/11, and ‘terrorism’ was a lie” (Moench & Shah, 2023). This surge prompted TikTok to aggressively remove content that promoted the letter (Moench & Shah, 2023). The opacity of TikTok’s recommendation system enables such content to be rapidly spread covertly due to attribution issues. The PRC and non-state threat actors can strategically coerce individuals to similar extremes or exploit these susceptible users in future attacks.

TikTok’s ability to quickly understand users’ interests and target extreme content can be applied to social engineering and cyber operations. As discussed earlier in this chapter, TikTok provides the PRC with valuable intelligence that can support malicious operations. But like other social platforms, TikTok can be used as the actual vehicle for operations as well. The “Invisible Body” incident is a great example of TikTok being used as the medium for a cyber operation. In 2022, a trending challenge on TikTok was to record a video naked and then use TikTok’s “Invisible Body” filter to replace their body with a blurred background (Collins, 2022). Hackers exploited this trend by posting videos that promoted ‘software’ that could remove the filter and reveal the user. In reality, users were actually coerced into downloading software that could “harvest Discord account details, stored credit cards, passwords, cryptocurrency wallets and other computer files” (Collins, 2022). In theory, similar operations could target U.S. government officials and military personnel.

In an effort to secure its systems and prevent malign influence, the DOD banned TikTok from devices issued by the Federal Government. Additionally, more than two dozen states have banned TikTok from government issued devices, and many colleges (including the University of South Carolina) have banned TikTok from their campus networks (Maheshwari & Holpuch, 2023). While these efforts are a step in the right direction, they do not fully address the threat

that TikTok poses to U.S. National Security. Malicious operations that target military and government personnel can circumvent these policies in several ways. Firstly, and most obviously, these state and federal employees can still access TikTok from their personal phones. Let's say, for example, a high-ranking U.S. Government Official regularly uses TikTok on their personal phone and is victim to the abovementioned "Invisible Body" attack. Threat actors might be able to gain access to confidential information, sensitive documents, or valuable personal information. While the same operation could be conducted on any social platform, TikTok's connection to the PRC could lead to larger implications for national security.

Secondly, the aggregation of user data on TikTok enables accurate target profiles to be constructed, which could include the target's constituents, friends, colleagues, spouses, doctors, children, and more. Although a military intelligence officer, for example, may not use TikTok—maybe his spouse or children do. Valuable intelligence could be collected from a high-value target's associates and social connections. In a similar attack to the "Invisible Body", attackers might inject malware into this fictitious military officer's home-network via a family member's TikTok to conduct espionage or launch further cyber operations. PRC-based threat actors might target this officer's doctor or other constituents that possess valuable personal information which could be used as leverage in future attacks. TikTok's massive active user base in the U.S. enables the PLA to covertly conduct devastating operations like these at scale. While these examples do not detail the specific TTPs (tactics, techniques, and procedures) of actual attacks, they do help to depict the full scope of the TikTok threat.

The "pacing threat" that the PRC poses to the United States' competitive advantage is reflected in its military strategy (DOD, 2023b). The PRC's national strategy to "achieve the great rejuvenation of the Chinese nation" by 2049 is indicative of the country's ability to 'play the

long-game' (DOD, 2023b). This slow, pervasive strategy seeks to reshape the world order to be in favor of the PRC's interests and to establish China as the leading world power. This strategy is supported by the PRC's efforts to conduct espionage and collect any available intelligence that could prove useful in later operations. Even if American policymakers are not convinced of TikTok's current operational threat potential, it is critical that the U.S. take action to protect itself against future PRC operations.

This chapter has evaluated TikTok's capacity to be weaponized. While other platforms in the social media ecosystem have a similar capacity, TikTok's connection to the PRC poses a unique threat. The PRC notoriously uses seemingly innocuous companies to exert power and gain access to critical infrastructure and technologies. The United States, as discussed in this chapter, has taken action against companies that advance the PRC's military-industrial complex abroad. The United States' sanctions target Chinese defense and surveillance technology companies, yet they do not address TikTok. Considering the platform's popularity and pervasiveness in America, U.S. policymakers and national security experts must regard TikTok as an extension of the PRC's military-industrial complex.

This chapter's research demonstrates TikTok's potential to be used for espionage and social surveillance. Furthermore, the PLA has publicly detailed its goals of establishing an invisible dominance on social media (Wenling & Jiali, 2023). The PRC's efforts to aggressively collect intelligence are well-documented. As TikTok's active user base in the U.S. grows and users spend more time on the platform, the operational and strategic value of TikTok increases exponentially. Ignoring the TikTok threat, or failing to place it in its proper context, allows the PRC to collect intelligence and further develop an influence weapon within America's borders. Therefore, the United States should not hesitate to confront and neutralize the TikTok threat.

Conclusions

Although the threat that TikTok poses to national security has been the focus of many recent congressional hearings, its presence in the United States persists and grows. TikTok has distinguished itself from other popular platforms due to its extensive collection of user data, powerful recommendation algorithm, addictive design, sudden growth, and prevalence among children. While the broader social media ecosystem yields a potent attack surface, TikTok's clear connection to the People's Republic of China via its parent company, ByteDance Ltd., presents a unique threat. PRC policies coerce Chinese citizens, companies, and foreign businesses that operate in China to support its intelligence and national security efforts. Furthermore, social media is a critical aspect of the PRC's strategies for global cyber dominance. The People's Liberation Army has publicly detailed its use of social media in warfare, which further supports TikTok's capacity to be weaponized. The United States has failed to mitigate the actual and potential threat that TikTok poses to U.S. National Security. This thesis concludes that TikTok, and the broader social media ecosystem, should be viewed as highly effective mediums for collecting intelligence, targeting information operations, and strategically influencing public perception and behavior. The United States must take action to protect its citizens, assets, and competitive advantage in the social media ecosystem.

References

Ali, M. & AJLabs. (2023). How many years does a typical user spend on social media?. *Al Jazeera*. https://www.aljazeera.com/news/2023/6/30/how-many-years-does-a-typical-user-spend-on-socialmedia#:~:text=How%20much%20time%20on%20average,a%20little%20over%20a%20month.

Apptopia. (2023). Leading mobile apps worldwide in 2022, by downloads (in millions). *Statista*. https://www.statista.com/statistics/1285960/top-downloaded-mobile-apps-worldwide/.

Bhargava, V., & Velasquez, M. (2021). Ethics of the Attention Economy: The Problem of Social Media Addiction. *Business Ethics Quarterly, 31*(3), 321-359. doi:10.1017/beq.2020.32.

Biały, B. (2017). Social Media—From Social Exchange to Battlefield. *The Cyber Defense Review*, *2*(2), 69–90. http://www.jstor.org/stable/26267344.

ByteDance. (n.d.). Corporate Structure. https://www.bytedance.com/en/.

ByteDance. (n.d.). Locations. https://jobs.bytedance.com/en/footprint.

Cheng, D. (2003). Winning without fighting: the Chinese psychological warfare challenge. *The Heritage Foundation.* https://www.heritage.org/global-politics/report/winning-without-fighting-the-chinese-psychological-warfare-challenge.

Chew, S. (2022). Letter to Senators Blackburn, Wicker, Thune, Blunt, Cruz, Moran, Capito, Lummis, and Daines. https://www.blackburn.senate.gov/services/files/A5027CD8-73DE-4571-95B0-AA7064F707C1.

Collier, K. (2023a). Cyberattack cost MGM Resorts about $100 million, Las Vegas company says. *NBC News*. https://www.nbcnews.com/business/cyberattack-cost-mgm-resorts-about-100-million-las-vegas-company-says-rcna45712.

Collier, K. (2023b). Hackers tied to Las Vegas attacks known for sweet-talking their way into company systems. *NBC News*. https://www.nbcnews.com/tech/security/mgm-las-vegas-hackers-scattered-spider-rcna105238.

Collins, B. (2022). TikTok 'Invisible Body Challenge' hijacked to spread malware. *Forbes*. https://www.forbes.com/sites/barrycollins/2022/11/29/tiktok-invisible-body-challenge-hijacked-to-spread-malware/?sh=9953ab078ad1.

Congressional Research Service (2022). *Defense Primer: Information Operations.* https://crsreports.congress.gov/product/pdf/IF/IF10771.

Congressional Research Service. (2023a). *Social Media Algorithms: Content Recommendation, Moderation, and Congressional Considerations.* https://crsreports.congress.gov/product/pdf/IF/IF12462.

Congressional Research Service. (2023b). *TikTok: Technology Overview and Issues*. https://crsreports.congress.gov/product/pdf/R/R46543.

Congressional Research Service. (2023c). *China's "One Belt, One Road" Initiative: Economic Issues*. https://crsreports.congress.gov/product/pdf/IF/IF11735.

Cruickshank, I., Windmueller, K., & Benigni, M. (2023). "Reaching the tipping point: Lessons from combining kinetic and information operations". *Irregular Warfare Initiative*.

https://irregularwarfare.org/articles/reaching-the-tipping-point-lessons-from-combining-kinetic-and-information-operations/.

Dawson, J. (2021). Microtargeting as Information Warfare. *The Cyber Defense Review, 6*(1), 63–80. https://www.jstor.org/stable/26994113.

Ellul, J. (1973). *Propaganda: The formation of men's attitudes*. Vintage Books.

Evanina, W. (2019). "NCSC Director Warns of Nation-State Cyber Threats to Law Firms in June 4 Remarks at ILTA LegalSEC Summit 2019". *The Office of the Director of National Intelligence*. https://www.dni.gov/index.php/ncsc-newsroom/3346-ncsc-director-warns-of-nation-state-cyber-threats-to-law-firms-in-june-4-remarks-at-ilta-legalsec-summit-2019.

Exec. Order No. 13959. (2020). 85 FR 73185. https://www.federalregister.gov/d/2020-25459.

Fuller, M. (2019). Big data and the Facebook scandal: Issues and responses. *Theology*, *122*(1), 14-21. https://journals.sagepub.com/doi/full/10.1177/0040571X18805908.

Gering, T. (2023). "Full throttle in neutral: China's new security architecture for the Middle East". *Atlantic Council.* https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/full-throttle-in-neutral-chinas-new-security-architecture-for-the-middle-east/.

Humphries, M. (2021). China's TikTok adds mandatory 5-second pause between videos. *PcMag*. https://www.pcmag.com/news/chinas-tiktok-adds-mandatory-5-second-pause-between-videos#:~:text=As%20the%20South%20China%20Morning,too%20long%20continuously%20watching%20videos.

IBM Security. (2023). *Cost of a Data Breach Report 2023*. https://www.ibm.com/reports/data-breach.

Iqbal, M. (2023). TikTok revenue and usage statistics. *BusinessOfApps.* https://www.businessofapps.com/data/tik-tok-statistics/.

Kaye, D. B. V., Chen, X., & Zeng, J. (2021). The co-evolution of two Chinese mobile short video apps: Parallel platformization of Douyin and TikTok. *Mobile Media & Communication*, *9*(2), 229-253.

Kosinski, M., Bachrach, Y., Kohli, P. *et al.* (2014). Manifestations of user personality in website choice and behaviour on online social networks. *Mach Learn* 95**,** 357–380. https://doi.org/10.1007/s10994-013-5415-y.

Kramer, A. D., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences*, *111*(24), 8788-8790.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, 113-122.

Laskai, L., & Segal, A. (2018). A new old threat: Countering the return of Chinese industrial cyber espionage. *Council on Foreign Relations*. http://www.jstor.org/stable/resrep29903.

Lee, J. A. (2018). Great firewall. *The Chinese University of Hong Kong Faculty of Law*. Research Paper No. 2018-10.

Lorenz, T. (2023). Why TikTok videos on the Israel-Hamas war have drawn billions of views. *The Washington Post.* https://www.washingtonpost.com/technology/2023/10/10/tiktok-hamas-israel-war-videos/.

Maheshwari, S. (2023). TikTok's C.E.O. uses personal touch to address antisemitism concerns. *The New York Times*. https://www.nytimes.com/2023/12/01/business/shou-chew-tiktok-antisemitism.html.

Maheshwari, S. & Holpuch, A. (2023). Why countries are trying to ban TikTok. *The New York Times*. https://www.nytimes.com/article/tiktok-ban.html.

Martin, E. (2022). Persuasive Technology and Personhood on Social Media. *Science, Technology, & Human Values, 0(0).* https://doi.org/10.1177/01622439221137038.

Matsa, K. (2023). More Americans are getting news on TikTok, bucking the trend seen on most other social media sites. *Pew Research Center*. https://www.pewresearch.org/short-reads/2023/11/15/more-americans-are-getting-news-on-tiktok-bucking-the-trend-seen-on-most-other-social-media-sites/.

Matz, S. C., Kosinski, M., Nave, G., & Stillwell, D. J. (2017). Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the national academy of sciences*, *114*(48), 12714-12719.

Moench, M. & Shah, S. (2023). Why Osama bin Laden's 'Letter to America' went viral on TikTok. *Time*. https://time.com/6336280/osama-bin-laden-letter-to-america-tiktok/.

Morris, S. & Kinder, T. (2022). HSBC installs Communist party committee in Chinese investment bank. *Financial Times*. https://www.ft.com/content/eac99fd9-0c30-4141-821a-45348f61c113.

Mozur, P., Mac, R., & 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.

Newcourt-Nowodworski, S. (2005). *Black Propaganda in the Second World War*. The History Press.

Nimmo, B. & Agranovich, D. (2022). Recapping Our 2022 Coordinated Inauthentic Behavior Enforcements. *Meta*. https://about.fb.com/news/2022/12/metas-2022-coordinated-inauthentic-behavior-enforcements/.

Nimmo, B., et al. (2023). *Meta's Adversarial Threat Report, Second Quarter 2023*. Meta.

Perkins, T. (2022). *TikTok Analysis*. Internet 2.0. https://tinyurl.com/39x7m5zt.

Radesky, J., et al. (2023). *Constant Companion: A Week in the Life of a Young Person's Smartphone Use.* Common Sense & C.S. Mott Children's Hospital. https://www.commonsensemedia.org/sites/default/files/research/report/2023-cs-smartphone-research-report_final-for-web.pdf.

Schechner, S. & Secada, M. (2019). You give apps sensitive personal information. Then they tell Facebook. *The Wall Street Journal*. https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636.

Smith, H. (2023). Chinese spies are targeting access, not race. *Foreign Policy*. https://foreignpolicy.com/2023/09/22/china-spying-race-intelligence-targeting/.

Solon, O. (2017). Ex-Facebook President Sean Parker: Site made to exploit human 'vulnerability'. *The Guardian*. https://tinyurl.com/ptr6d7nz.

Statista. (2022). Number of social media users worldwide from 2017 to 2027 (in billions) [Graph]. *Statista*. Retrieved November 11, 2023, from https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.

Stockton, J. (2021). Defeating Coercive Information Operations in Future Crises. *The Johns Hopkins University Applied Physics Laboratory LLC*. https://www.jhuapl.edu/sites/default/files/2022-12/DefeatingCoerciveIOs.pdf.

The White House. (2021). *FACT SHEET: Executive Order Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China.* https://shorturl.at/vIMNR.

TikTok. (2023a). Privacy Policy. https://www.tiktok.com/legal/page/us/privacy-policy/en.

TikTok. (2023b). Children's Privacy Policy. https://www.tiktok.com/legal/page/global/childrens-privacy-policy/en.

TikTok Newsroom. (2023). Celebrating our thriving community of 150 million Americans. https://newsroom.tiktok.com/en-us/150-m-us-users.

Tunnicliffe, I., & Tatham, S. (2017). Social Media—The Vital Ground: Can We Hold It? *Strategic Studies Institute, US Army War College*. http://www.jstor.org/stable/resrep11695.

Ünver, H. A. (2018). Politics of Digital Surveillance, National Security and Privacy. *Centre for Economics and Foreign Policy Studies*. http://www.jstor.org/stable/resrep17009.

U.S. Department of Defense. (2023a). *2023 DOD Cyber Strategy Summary*.

U.S. Department of Defense. (2023b). *Military and Security Developments Involving the People's Republic of China*. https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-military-and-security-developments-involving-the-peoples-republic-of-china.pdf.

U.S. Department of Defense. (2012). *Information Operations.* Joint Publication 3-13. https://irp.fas.org/doddir/dod/jp3_13.pdf.

Vogels, E., Gelles-Watnick, R., & Massarat, N. (2022). Teens, Social Media and Technology 2022. *Pew Research Center*. https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/.

Wayt, T. (2021). Douyin, Chinese version of TikTok, adds time limit for kids under 14 and bans nighttime use. *New York Post*. https://nypost.com/2021/09/20/chinese-version-of-tiktok-adds-time-limit-for-kids-bans-nighttime-use/.

Weiser, M. (1991). The Computer for the 21st Century. *Scientific American*, *265*(3), 94–105. http://www.jstor.org/stable/24938718.

Wells, G. (2023). TikTok employees say executive moves to U.S. show China parent's influence. *The Wall Street Journal*. https://www.wsj.com/tech/tiktok-employees-say-executive-moves-to-u-s-show-china-parents-influence-ef5ff21f.

Wenling, D. & Jiali, L. (2023). Cognitive confrontation on the social media battlefield. *People's Liberation Army Daily*.

World Economic Forum. (2011). *Personal Data: The Emergence of a New Asset Class*. https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

Wortzel, L. M. (2014). The Chinese People's Liberation Army and Information Warfare. *Strategic Studies Institute, US Army War College*. http://www.jstor.org/stable/resrep11757.

WSJ Staff. (2021). Inside TikTok's algorithm: A WSJ video investigation. *The Wall Street Journal*. https://www.wsj.com/articles/tiktok-algorithm-video-investigation-11626877477.

X Blog. (2020). Disclosing networks of state-linked information operations we've removed. *X*. https://blog.twitter.com/en_us/topics/company/2020/information-operations-june-2020.

Zuboff, S. (2019). Surveillance Capitalism and the Challenge of Collective Action. *New Labor Forum*, *28*(1), 10–29. https://doi.org/10.1177/1095796018819461.