#1 on the U.S. Most Wanted List

Why the Push is on to Ban the World's Most Successful Startup from Academic, Government and Military Devices in the United States

AUTHOR TOM WATERS

A RESEARCH ARTICLE FROM

UNIVERSITY of
SOUTH FLORIDA
Global and National Security Institute

TikTok is # 1 on the U.S. Most Wanted List: Why the Push is on to Ban the World's Most Successful Startup from Academic, Government and Military Devices in the United States.

Abstract

TikTok is a social media application that has amassed over 100 million users in the United States. Yet the Biden White House, like the Trump Administration before it, seeks to ban TikTok, or at least force it's divestment from the parent company, Bytedance. For many the question is how can an app for sharing silly dance videos among teenagers be a national security threat? Unfortunately, the problem is considerably more complex than this simple question. TikTok's unprecedented success comes from its powerful artificial intelligence-based algorithm.

That activity produces a comprehensive psychological profile of each user and tailors the queue of forthcoming video selections based on that profile. TikTok's highly personalized content keeps users engaged longer than other social media platforms. The app's underlying algorithm understands the user's moods, political leanings, even their level of loneliness. The U.S. government is concerned that a China-based company with comprehensive dossiers on millions of Americans presents a significant national security threat, one that potentially justifies banning the app completely.

Key Words

TikTok, China, National Security, Social Media

About the Author

Tom Waters is the Assistant Director for Startups in the University of South Florida's Technology Transfer Office. He previously served on the CIA's Trade Security Team, advising U.S. companies who were targets of technology theft by foreign governments. Tom has been issued a dozen patents in biometrics, digital authentication, and encryption. He was featured on the cover of *Government Executive* magazine, and published in the *Cyber Defense Review* and the *Small Wars Journal*.

Introduction

In January 2020, the United States Army banned TikTok from its devices.[1] Several states have forbidden it on government provided IT systems. A handful of Attorneys General are trying to outlaw it from operating within their respective states. Amazon has forbidden employees from using it on any personal phone that accesses the company's email.[2] The reason for all this hand wringing can be summed up in one word: China. Or, more specifically, the Chinese Communist Party (CCP).

The Justice Department reports that 90% of all economic espionage conducted against the United States over the past decade has been committed by China.[3] The FBI's website states that confronting this threat is their primary counterintelligence priority.[4] TikTok is owned by a Beijing-based company called Bytedance. Launched in September of 2016, it has surpassed every other social media platform in revenue growth, achieving $12 billion annual revenue much faster than social media rivals like Facebook, Twitter, or YouTube.[5] Initially popular only with teenagers posting fifteen-second videos of dance moves and silly skits, TikTok invested heavily into more diverse content including financial services, video games, and music streaming.[6] Even the AARP has now published a user guide for its members on how to use TikTok.[7]

As social media and mobile apps have become become more integral to daily life, consumers have frequently been forced to choose between privacy and usability.

For example: though we don't want Google tracking us, we do want Google Maps to route us around a traffic accident that we don't know is four miles down the road. Google can only do that because it is tracking everybody with the app on their phone. We cannot have one without the other. We all realize this – it is the price we pay for using these platforms. But there are national security risks to these seemingly innocuous services. For example:

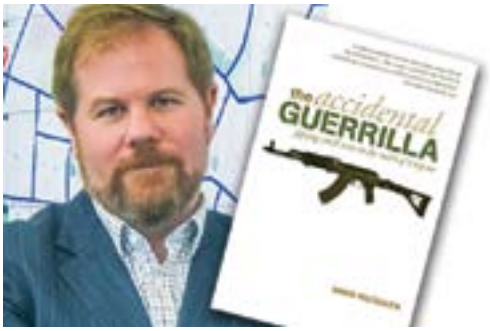
- Iran's IRGC used LinkedIn a few years ago to target senior DOD and defense aerospace executives by going through their families.[8] They were discovered because one of their faked profiles unwittingly used a photograph of New York Times bestselling author Alexander McCall Smith. From there the entire house of cards fell apart.

- A software developer in Tampa, Florida used data from Twitter to analyze the Arab Spring.[9] He was able to identify the ten people most responsible for the fall of Hosni Mubarak by analyzing how the protestors found each other in real time on the streets of Cairo. He did this using open source data freely available from Twitter, despite not speaking a word of Arabic himself.

- Five years ago, Russian agents poached user data from the smartphones of NATO soldiers in the Ukraine - including Americans.[10] Social media apps provided the names of soldier's families, and the phone's GPS chip provided their exact location. These agents walked up to servicemen in public and commented about family members by name, an effective bit of harassment.

Political / Military Concerns

In his book *The Accidental Guerilla*, (Australian Army) Lt Col David Kilcullen outlined the problem of wresting control of a population away from its own government. Conventional military campaigns pressure adversaries by defeating their armed forces through decisive military engagements, crushing their ability to make war. The population is intentionally detached from this fight, isolated within the territory as much as possible. Action is directed only at distinct military targets – command and control centers, fixed weapons platforms, and key government facilities specific to combat decision making. The population is the prize in such a conflict.



Contrast this with the unstructured application of Irregular Warfare. Here, the desire to influence and control is the same, but rather than targeting the military apparatus, it is instead marginalized, isolated away from the fight completely if possible. Gaining or dismantling support for the government remains the focus – but adversarial military services are sidelined. This is the application of nonlethal instruments which can be effective in halting or even preventing an armed conflict from occurring in the first place.

So what if this kind of approach was focused on a population rather than a location? Suppose the goal is not territory, but rather the hearts and minds of everyone in that territory? What if the population was the battlespace?

A population generally gets information from one of three sources: observation, authority, and belief. Kilcullen's model explains how the Taliban manipulated observation and belief in Afghanistan to marginalize government authority. When tribal leaders are executed or simply disappear, it was no doubt a strong observation point. If religious clerics are compromised into preaching fundamentalist rhetoric, followers have few competing voices to believe. The Taliban's takeover of the nation demonstrates that manipulating and influencing a population can be done relatively easily if one controls the information that population can see and hear. This is what alarms American and European authorities about TikTok.

Where is the U.S. population getting its information these days? It's not organized religion, for the first time less than 50% of the U.S. population participates in organized religion.[11] It's not from news sources; fewer than 40% of Americans tune in for the national broadcasts of ABC, CBS, or NBC.[12] Nor is it trust in government, hovering at a record low of under 20%.[13]

Eighty-six percent of adults say they get news from a smartphone, computer or tablet either "often" or "sometimes."[14] When asked what platform they prefer to get news from, just over half of Americans

(52%) say they prefer a digital platform – a news website, search engine, social media or podcast. Pew Research also showed an overall decline among all social media platforms as news sources – with the exception of TikTok, the only social media platform to see it's use as a regular news source rise.[15]

The Software Risk

Colonel Robert Killebrew (U.S. Army) now a senior fellow for the Center for New American Security, once wrote, *"The story you're trying to tell in future conflicts is the strategy by which it will be fought."*[16] If that's true, what is the story TikTok is trying to tell?

TikTok's value comes from its proprietary artificial intelligence algorithm. While most social media applications use metadata in their analysis of users, TikTok's system has three unique differentiators, each of which is a force multiplier on the others. These are:

- Computer Vision: The app analyzes not simply the faces within a video, it also recognizes objects, locations, and actions, crafting additional metadata not provided by the content's creator.[17] While facial recognition has been around for years, TikTok's assigns emotional qualifiers to the faces it reads.
- Linguistic Processing: The app quantifies the spoken language and text within a video. This is not simply the #hashtags a creator assigns as metadata. It's all of the language spoken within the video or via text included on screen, analyzing the contextual content across multiple dimensions.
- Behavioral Measures: While YouTube and Facebook require users to type inputs into their analytic engines, TikTok evaluates user's behavior. Users don't need to 'like' a video – it measures how long users watched, if they stopped before it finished, or if they replayed it, then bases its recommendations from that activity.

These three features automate what was a manual activity requiring multiple rounds of data collection (from the user) and focused analysis (by the app) on other social media platforms. The result is that within an hour or two, TikTok creates a comprehensive psychological profile that discerns a user's interests, hobbies, relationship status, political views, and more.[18]

This type of insight is something Facebook has pursued for years. Facebook anonymously entered a new artificial intelligence agent called Cicero into the online negotiation and strategy game Diplomacy, a favorite pursuit of both former President John F. Kennedy and Henry Kissinger.[19] Cicero successfully passed itself off as a human player, analyzing other player's goals, beliefs and intentions, and beating them handily.

According to Stanford Business School Professor Dr. Michal Kosinksi, these AI generated profiles are better than the ones created by human experts.[20] This is likely because the underlying data is more complete, unfiltered and nuanced, as opposed to filling out surveys and answering questions. TikTok refines their model in real time, using traditional A/B testing through additional video content, with the results immediately incorporated. Because this function is automated, it works extremely fast. The app will make calculated determinations of a user's most likely interests, then queue options up for them. Like the standardized tests we take in high school, it asks the same questions at different times and in different ways, learning a user's real interests and mitigating any chance of 'gaming' the system.

Their proprietary psychographic model is extremely accurate, able to measure the user's extraversion, likableness, neurosis, and agreeableness.[21] These are normally quantified by professional evaluation tools such as the Firo-B, the DISC Assessment, or the Minnesota Multiphasic Personality Inventory (MMPI). From this, TikTok knows a person's behavioral tics, their emotional state, and how they'll respond to specific stimuli. The algorithm could potentially calculate the best type of information to influence a user's behavior before specific events occur – which is the basis for the concern expressed by U.S. and European authorities.

TikTok users don't have to give the app explicit permission to do anything. TikTok automatically maps out their psyche to provide the 'best user experience possible'. But the flip side of that is the app could also manipulate users into justifying a range of disturbing actions, including suicide. Some of the loudest opposition to TikTok comes from its proclivity for recommending videos on suicide and eating disorders to vulnerable users.[22]

TikTok's artificial intelligence tool can read news from 5000 sources and summarize all of them into a custom written article of 400 words in two seconds.[23] A partner at the venture capital firm Andreessen Horowitz described TikTok as *"the first mainstream consumer app where artificial intelligence IS the product."*[24] While Facebook, Twitter, and YouTube require users to actively participate, TikTok makes decisions as users passively scroll on the app.

If belief is based primarily on what is read on line, then Kilcullen's model is alarmingly persuasive, and supports the concern that an app with the power and predictive capability of TikTok is a threat to U.S. national security. Pick any popular conspiracy: 'Flat-earthers', Area 51 aliens, chem trails from planes, the possibilities for manipulation are endless.

TikTok's misdirection potential was evident during the search for the killer of four college students at the University of Idaho.[25] While police and the FBI immediately honed in on a twenty-eight year old suspect via DNA evidence found at the scene, TikTok was awash in false accusations against the victim's roommates, a food truck driver, and even a local professor. Idaho later joined Alabama, Georgia, and Texas in banning TikTok from state university devices and WIFI.

What It All Means

Ten years ago, Target Corporation famously sent coupons for diapers and baby formula to a seventeen-year-old high school girl in Minneapolis.[26] Her very angry father contacted the local store to complain. What he didn't know was Target's market intelligence team had analyzed her credit card purchases against other young women with similar buying patterns. A few days later he called again to apologize. His daughter had admitted she was in her second trimester. Target knew she was pregnant before her own father did.

While this so-called surveillance capitalism created salacious headlines, as a nation we've fallen way behind in artificial intelligence research. Yes, it is a concern for a corporation to predict something as personal as a pregnancy, but it's another thing entirely for a hostile foreign power to hold sway on over one hundred million Americans. An investor noted at a recent conference that *"If data is the new oil, China is the new Saudi Arabia."*[27]

One national commentator shared the text of TikTok's privacy policy on his broadcast one night, noting it accesses information *"such as a user's mobile apps, file names, and even keystroke patterns."*[28] Those keystrokes could include passwords, not simply the user's ID. This means it could potentially pull data from Facebook, Twitter, Outlook and other device-hosted apps, explaining why Amazon doesn't want their employees to access company email from a smartphone that has TikTok installed. The app is capturing user ID's, passwords (including from remote hard drives),[29] face and voice prints; all allowed by the Terms of Service.[30]

While uncertainty over TikTok's American future plods along, other nations are taking action. In 2021, India banned TikTok, along with fifty eight other China-based apps, for unacceptable data security and privacy practices.[31] At the time of the ban over 200 million Indian citizens used the app.[32]

We have all seen 'deep fake' video images of Tom Cruise, Elon Musk, and Leonardo Dicaprio on the Internet. Bytedance and TikTok have created their own deepfake company.[33] The new feature, called Face Swap, allows users to insert their face onto videos of someone else, inviting even more scrutiny when TikTok doesn't need it.[34]

Over the past year, revelations about the company have included:

- Leaked audio from internal TikTok meetings suggests engineers in China have accessed U.S. users' data.[35]
- TikTok has admitted their staff can access European user's data.[36]
- TikTok officials in Australia confirmed their employees in China can access Australian user information.[37]
- Forbes showed ByteDance was planning to surveil two Americans using TikTok-collected data.[38]

There is no longer any question about whether or not China can access user data. The question becomes, what are they planning to do with it? Artificial intelligence-based video platforms like TikTok have the potential to not only radicalize, but also to educate and train. Not just basic bomb making, but also specialized tradecraft such as intelligence gathering and countersurveillance.

In 2008, a group took over the Taj Mahal and other luxury hotels in Mumbai, India killing hostages and setting buildings ablaze. One hundred and sixty nine people died, including six Americans. Lashkar-e-Taiba initially recruited two dozen operatives, culling them down to ten through a mix of psychological profiling, basic combat techniques, and specialized training by former Pakistani military personnel.[39] It required a lot of time and money to conduct that training, much of which could now be done with an app. (An American named David Headley is serving thirty five years in prison for providing the reconnaissance on those hotels - using his smartphone.)[40]

Artificial intelligence could identify potential operatives already in a country, even down to a specific neighborhood. There's no need to sneak anyone across borders if one can radicalize neighbors right down the street from their intended target. Shorter timelines, lower costs, and reduced risk of discovery would make them far more difficult to stop ahead of time.

Some will call this theoretical fear mongering, but examples are abundant. For instance, Americans are being recruited online to smuggle migrants across our Southern border. Why? Because the same model has already worked on TikTok in a 'sales push' to smuggle Albanians across the English Channel.

Future Outlook

This is not an Artificial Intelligence hate piece. Far from it. AI is doing incredible things:

- It is providing new approaches to low-cost, high-performance battery materials and increasing the manufacturing efficiency for electric vehicles.[41]
- Last summer, Google's DeepMind Technologies predicted the structure of nearly all known proteins, likely accelerating new drug discoveries.[42]
- Two doctoral candidates at the University of South Florida launched a new startup using artificial intelligence to aid in the early detection of Alzheimer's Disease.[43]

The threat does not come from computers or even from algorithms, it comes from people. Like any threat, the question is one of intent. TikTok is the world's most valuable startup because their technology is just that good. But the Chinese Communist Party is the United States' most critical global adversary, and Chinese law mandates businesses share data with the government.[44]

Since he came to power, Xi Jinping has accelerated his authoritarian rule, detaining a million Uighurs, employing torture in Xinjiang, and purging any government officials whose loyalty was not absolutely assured.[45] During this same period the CCP led some of the largest cyber hacks in U.S. history,

including the Office of Personnel Management (OPM), Marriott Corporation, Anthem Insurance, American Airlines, United Airlines, and the Department of the Navy.[46]

Beijing also clamped down on domestic Chinese companies, particularly those in the technology arena. In the U.S. we occasionally see activist in¬vestors take control of a company by acquiring one or two percent of its stock and gaining a Board seat. Beijing has copied this technique. Through so-called 'Golden Shares', state-controlled funds take similar control positions in ostensibly public companies. In 2021 Beijing pursued Full Truck Alliance Corporation (a trucking services platform) and Didi Global (Uber-style ride sharing) to gain access to user data.[47]

ByteDance created Beijing Douyin Information Service in May of 2022 to run the Chinese version of TikTok, and officials confirm the state owns a piece of it.[48] In early 2023 Newsweek reported the Chinese government was taking Golden Shares positions in tech giants Tencent and Alibaba.[49]

These are not investments for financial return – it is a means of enforcing control. Beijing's authoritarian leadership demands their private sector *"surrender with absolute loyalty."*[50] Questioning the state's monopoly on power is not permitted, a rule that extends overseas as well.

Last year, Forbes reported that three hundred Bytedance employees previously worked for the Chinese government, and some actually still do.[51] ByteDance has an internal Chinese Communist Party committee where employees discuss *"Xi Jinping thought"* and party doctrine.[52] According to leaked company documents, TikTok censors mentions of Tibet, Tiananmen Square, and the Falun Gong religious minority.[53]

Current and former Bytedance or TikTok employees have told Western media the company can manipulate content delivery outside the algorithm through a manual process called 'heating', (as in heating up specific content), confirming the worst of U.S. and European fears of influence and coercion.[54]

Some might take issue with comparing the Chinese Communist Party with recent conflicts in the Middle East. What most don't realize is that our wars in Iraq and Afghanistan drove some of the changes China made to its military strategy. In 1999, after Gulf War 1, the People's Liberation Army published a book by two Chinese Army Colonels. They posited that the whole concept of warfare had changed due to the U.S.'s technological advantage over Iraq. They foresaw the future as being one based on what they characterized as 'Unrestricted Warfare'. It is a fascinating book, but one thing in particular is worth quoting: *"...technological progress has given us the means to strike at the enemy's nerve center directly without harming other things, giving us numerous new options for achieving victory, and all these make people believe that the best way to achieve victory is to control, not to kill."*[55]

If the CCP came to that conclusion after the first Gulf War, we can certainly imagine how that strategy has evolved after 9/11, the second Gulf War, the Afghan withdrawal, the 2016 election debacle, and our continued political rancor. Quite frankly, we're making it very easy for them to steal us blind. For the past ten years it's been our industrial technology – now it's our individual privacy.

After President Trump pressured Bytedance to sell TikTok's U.S. operations or risk a national ban, the Chinese government amended its tech export rules. That list also now includes technologies for text analysis, content recommendation, speech modeling, and voice recognition.[56] These TikTok-centric technologies cannot be exported without a license from the government, according to Bytedance.[57]

TikTok's CEO On Capitol Hill

On March 23rd 2023, TikTok CEO Shou Zi Chew testified before the House Energy and Commerce Committee. Committee members found his answers evasive and unsatisfying.

After college in London Chew spent a couple of years at Goldman Saks, then went for an MBA at the Harvard Business School where he interned at a startup called Facebook. He then joined DST Global, founded by Russian investor Yuri Milner, where he was described as their *'point man for China.'*[58]

(Milner was an early and significant investor in Facebook.) Chew led DST's investment in Bytedance and secured some of the most lucrative investment deals in China's internet history, investing in JD.com, Alibaba, and the ride-hailing service Didi.[59]

From there he became the CFO of Xiaomi. He led their 2018 initial public offering, and was promoted to president of their international business. But in 2020, cybersecurity professionals found Xiaomi phones were sending extraordinary amounts of data to remote servers in Russia and Singapore, even though their domain names were registered in China.[60] The software had recorded all the websites visited, including searches via Google or DuckDuckGo, everything viewed on the news feed feature, even when the phone was set to private mode. In addition, it recorded what folders were opened and which screens were swiped, including the status bar and the settings page.

So what we have here is a CEO with a lot of experience capturing smartphone data and directing it through servers in third party countries before receiving it in China. Chew's supporters like to point out he's a citizen of Singapore, not a Chinese national.

One could argue Chew was named CEO because his Xiaomi experience demonstrated a mental toughness that Beijing liked – they consider him one of them, part of the CCP club. Consider all the

turnover in other big Chinese tech companies – Jack Ma at Alibaba, Colin Huang Zheng at PDD, even Bytedance's own CEO-founder Zhang Yiming.[61]

Forbes noted a couple of years back that Singapore straddles the divide between East and West.[62] In many ways Singapore is for this Cold War what Berlin was for the last one. Or to put it less diplomatically, it's a waypoint for data going to Beijing.

On average, TikTok users spend over an hour and a half a day on the app, more than any other social media platform.[63] Last year TikTok's website had more visits than Google's![64] It has turbo-charged the successful Tetris and Candy Crush models in an alarming new way that we are politically and administratively unprepared to counter.

In an article about video games five years ago, The Guardian cited an important difference between drug and digital dependencies. It noted *"substance addictions are nakedly destructive, while many behavioral addictions are quietly destructive acts, wrapped in cloaks of creation."*[65]

This is a perfect way to describe TikTok. The smart thing to do is delete the app from our phones and change every password these devices have ever contained.

[1]Cox, Matthew. 'Army Follows Pentagon Guidance, Bans Chinese-Owned TikTok App', MILITARY.COM. December 20, 2019. https://www.military.com/daily-news/2019/12/30/army-follows-pentagon-guidance-bans-chinese-owned-tiktok-app.html

[2]Brodkin, Jon. 'Amazon enforces TikTok ban on employee phones due to "security risks". ARSTECHNICA. July 10, 2020. https://arstechnica.com/tech-policy/2020/07/amazon-bans-tiktok-on-employee-phones-as-us-govt-scrutinizes-chinese-app/

[3]Viswanatha, Aruna and Volz, Dustin. 'China's Spying Poses Risk to U.S.', THE WALL STREET JOURNAL, April 28, 2019.

[4] https://www.fbi.gov/investigate/counterintelligence/the-china-threat

[5] https://www.chartr.co/stories/2022-06-29-2-tiktok-is-hitting-milestones-quickly

[6]Xie, Stella Yifan. 'Chinese Tech Companies Turn to Financial Services', THE WALL STREET JOURNAL. September 22, 2019.

[7]Baig, Edward. 'Surprise! TikTok App Defies Age Boundaries', AARP WEBSITE. July 26, 2021 https://www.aarp.org/home-family/personal-technology/info-2021/tiktok-app-defies-age-boundaries.html?itid=lk_inline_enhanced-template

[8]Nakashima, Ellen. 'Iranian Hackers are Targeting U.S. Officials Through Social Networks', THE WASHINGTON POST, May 14, 2014. https://www.washingtonpost.com/world/national-security/iranian-hackers-are-targeting-us-officials-through-social-networks-report-says/2014/05/28/7cb86672-e6ad-11e3-8f90-73e071f3d637_story.html

[9]Waters, Tom. 'Teaching Old Dogs New Tricks', BEP PRESS. November, 2022. https://www.amazon.com/Teaching-Old-Dogs-New-Tricks/dp/1637423403/ref=sr_1_1?

[10]Grove, Thomas and Barnes, Julian and Hinshaw, Drew. "Russia Targets NATO Solider Smartphones, Western Officials Say," The Wall Street Journal. 4 Oct 2017.

[11]Jones, Jeffrey M. "U.S. Church Membership Falls Below Majority for First Time", GALLUP, March 29, 2021. https://news.gallup.com/poll/341963/church-membership-falls-below-majority-first-time.aspx

[12]Sanders, Linley. 'Trust in Media 2022: Where Americans Get Their News and Who They Trust for Information'. YOUGOVAMERICA. Apri 5, 2022. https://today.yougov.com/topics/politics/articles-reports/2022/04/05/trust-media-2022-where-americans-get-news-poll

[13]Staff. 'Public Trust in Government: 1958-2022'. PEW RESEARCH CENTER. June 6, 2022. https://www.pewresearch.org/politics/2022/06/06/public-trust-in-government-1958-2022/

[14]Shearer, Elisa. 'More Than Eight in Ten Americans Get News From Digital Devices', PEW RESEARCH CENTER. January 12, 2021. https://www.pewresearch.org/fact-tank/2021/01/12/more-than-eight-in-ten-americans-get-news-from-digital-devices/

[15]Seymour, Emily. 'TikTok Grows As a News Source', INVESTIGATIVE REPORTING WORKSHOP, October 17, 2022. https://investigativereportingworkshop.org/2022/10/17/tiktok-grows-as-a-news-source/

[16]Waters, TJ. HYPERFORMANCE: USING COMPETITIVE INTELLIGENCE FOR BETTER STRATEGY AND EXECUTION. John Wiley & Sons Publishing, New York NY. 2010. Pg. 228.

[17]Trehan, Daksh. 'The inescapable AI algorithm: TikTok', TOWARD DATA SCIENCE. June 12, 2020. https://towardsdatascience.com/the-inescapable-ai-algorithm-tiktok-ad4c6fd981b8

[18]Patel, Ankur. 'How TikTok Uses AI to Engineer User Addiction', ANKURS NEWSLETTER. May 13, 2022 https://www.ankursnewsletter.com/p/how-tiktok-uses-ai-to-engineer-user

[19]Porterfield, Carlie. 'Meta's AI Gamer Beat Humans In Diplomacy, Using Strategy And Negotiation', FORBES. November 22, 2022. https://www.forbes.com/sites/carlieporterfield/2022/11/22/metas-ai-gamer-beat-humans-in-diplomacy-using-strategy-and-negotiation/?sh=6680adc7788b

[20] https://youtu.be/VUwBcTgzbtU

[21]Patel, Ankur. 'How TikTok Uses AI to Engineer User Addiction', ANKURS NEWSLETTER. May 13, 2022 https://www.ankursnewsletter.com/p/how-tiktok-uses-ai-to-engineer-user

[22]Klepper, David. 'Report: TikTok Boosts Posts About Eating Disorders, Suicide'. AP NEWS. December 14, 2022. https://apnews.com/article/technology-health-eating-disorders-center-government-and-politics-0c8ae73f44926fa3daf66bd7caf3ad43

[23]Trehan, Daksh. 'The Inescapable AL Algorithm: TikTok'. MEDIUM. June 12, 2020. https://towardsdatascience.com/the-inescapable-ai-algorithm-tiktok-ad4c6fd981b8

[24] https://www.ankursnewsletter.com/p/how-tiktok-uses-ai-to-engineer-user

[25]Ryu, Jenna. 'TikTok Tried to Solve the Idaho Murders,' THE USA TODAY. January 4, 2023. https://www.usatoday.com/story/life/health-wellness/2023/01/04/idaho-murders-tiktok-witch-hunt/10978940002/

[26]Hill, Kashmir. 'How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did', FORBES. February 16, 2012. https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=7abf8e8a6668

[27]Baker, Gerard. 'California's Tech Titans Fight Fires of Their Own', THE WALL STREET JOURNAL, November 16, 2018.

[28]Jain, Ujwal. 'What Did Joe Rogan Say About TikTok's Terms of Service?', SPORTSKEEDA. September 27, 2022. https://www.sportskeeda.com/mma/news-what-joe-rogan-say-tiktok-s-terms-service

[29]Touma, Rafqa. 'TikTok Has Been Accused of 'Aggressive' Data Harvesting. Is Your Information at Risk?' THE GUARDIAN. July 19, 2022. https://www.theguardian.com/technology/2022/jul/19/tiktok-has-been-accused-of-aggressive-data-harvesting-is-your-information-at-risk

[30] https://foreignpolicy.com/2023/01/12/tiktok-security-concerns-china-european-union-social-media/

[31]'India Permanently Bans TikTok and Fifty Eight Other Chinese Apps', NIKKEI ASIA. January 26, 2021. https://asia.nikkei.com/Business/Technology/India-permanently-bans-TikTok-and-58-other-Chinese-apps

[32] https://techjury.net/blog/tiktok-statistics/#gref

[33]Constine, Josh. 'ByteDance & TikTok Have Secretly Built a Deepfakes Maker', TECHCRUNCH. January 3, 2020 https://apple.news/AKaasqDprRByMSixX0RwFaw

[34]Hao, Karen. 'A Horrifying New AI App Swaps Women Into Porn Videos With a Click', MIT TECHNOLOGY REVIEW. September 13, 2021. https://www.technologyreview.com/2021/09/13/1035449/ai-deepfake-app-face-swaps-women-into-porn/

[35]Baker-White, Emily. 'Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China', BUZZ FEED NEWS. June 17, 2022. https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access

[36]Hetzner, Christiaan. 'TikTok Admits China Staff Can Access European User Data as FCC Commissioner Urges App Be Banned', YAHOO FINANCE. November 3, 2022. https://finance.yahoo.com/news/tiktok-admits-china-staff-access-135910756.html

[37]Mahdawi, Arwa. 'TikTok has been accused of 'aggressive' data harvesting. Is your information at risk?', THE GUARDIAN. July 19, 2022. https://www.theguardian.com/technology/2022/jul/19/tiktok-has-been-accused-of-aggressive-data-harvesting-is-your-information-at-risk

[38]Baker-White, Emily. 'TikTok Parent Bytedance Planned to Use TikTok to Monitor the Physical Location of Specific American Citizens', FORBES. October 20, 2022 https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/?sh=112d318c6c2d

[39] https://themoderatevoice.com/tv-review-hbos-terror-in-mumbai-six-stars-out-of-five/

[40] https://www.thehindu.com/news/national/US-shares-Headley's-phone-details-with-NIA/article60566353.ece

[41]Moine, Ahmed, et al. 'The role of artificial intelligence in the mass adoption of electric vehicles', JOULE. Volume 5, Issue 9, 15 September 2021, Pages 2296-2322. https://www.sciencedirect.com/journal/joule/vol/5/issue/9

[42]Angus, Loten. 'Chatty AI and Protein-Predicting Algorithm Defined the Year in Emerging Tech', THE WALL STREET JOURNAL. Dec. 30, 2022. https://www.wsj.com/articles/chatty-ai-and-protein-predicting-algorithm-defined-the-year-in-emerging-tech-11672419460

[43]Parker, Mark. 'USF Students Use AI to Detect Alzheimer's', ST PETE CATALYST. December 2, 2022. https://stpetecatalyst.com/usf-students-use-ai-to-detect-alzheimers/

[44]Tanner, Murray Scot. 'Beijing's New National Intelligence law: From Defense to Offense'. LAWFARE. July 20, 2017. https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense

[45]Dorfman, Jack. 'Beijing Ransacked Data as U.S. Sources Went Dark in China', FOREIGN POLICY, December 22, 2020. https://foreignpolicy.com/2020/12/22/china-us-data-intelligence-cybersecurity-xi-jinping/

[46]Dorfman, Jack. 'Beijing Ransacked Data as U.S. Sources Went Dark in China', FOREIGN POLICY, December 22, 2020. https://foreignpolicy.com/2020/12/22/china-us-data-intelligence-cybersecurity-xi-jinping/

[47]'Fretting about data security, Chinese government expands its use of 'golden shares', REUTERS, December 16, 2021. https://www.wionews.com/world/fretting-about-data-security-chinese-government-expands-its-use-of-golden-shares-437299

[48]Mayer, Chloe. 'Is TikTok Owned by the Chinese Communist Party?', NEWSWEEK. October 17,2022. https://www.newsweek.com/tiktok-owned-controlled-china-communist-party-ccp-influence-1752415

[49]Dillon, Hannah. 'China to Take "Golden Shares" in Alibaba and Tencent,' EXCHANGE WIRE. January 12, 2023 https://www.exchangewire.com/blog/2023/01/16/china-to-take-golden-shares-in-alibaba-and-tencent-age-checks-threaten-social-media-user-numbers/

[50]Yuan, Li. 'What China Expects From Businesses: Total Surrender', THE NEW YORK TIMES. July 19, 2021. https://www.nytimes.com/2021/07/19/technology/what-china-expects-from-businesses-total-surrender.html

[51]Baker-White, Emily. 'LinkedIn Profiles Indicate 300 Current TikTok And ByteDance Employees Used To Work For Chinese State Media—And Some Still Do', FORBES MAGAZINE. August 11, 2022. https://www.forbes.com/sites/emilybaker-white/2022/08/10/bytedance-tiktok-china-state-media-propaganda/?sh=3500dfbb322f

[52]Quinn, Jimmy. 'U.S. Intel Official Turned TikTok Lawyer Claims 'Anti-China Xenophobia', NATIONAL REVIEW. August 12, 2022. https://www.nationalreview.com/corner/u-s-intel-official-turned-tiktok-lawyer-claims-anti-china-xenophobia/

[53]Quinn, Jimmy. 'Why Top Tech Journalists Are Wrong about TikTok', NATIONAL REVIEW. July 14, 2022. https://www.nationalreview.com/corner/why-top-tech-journalists-are-wrong-about-tiktok/

[54]Leffer, Lauren. 'Behind the Scenes, TikTok Employees Are Pulling the Strings of Virality', GIZMODO, January 19, 2023. https://gizmodo.com/tiktok-viral-bytdance-heating-influencer-1850012660

[55]Liang, Qiao and Xiangsui, Wang. UNRESTRICTED WARFARE. People's Liberation Army Literature and Arts Publishing House, Beijing, China. February 1999. Page 27.

[56]Xiao, Eva and Lin, Liza. TikTok Talks Could Face Hurdle as China Tightens Tech Export Rules', THE WALL STREET JOURNAL, Aug 30, 2020. https://www.wsj.com/articles/china-tightens-ai-export-restrictions-11598703527

[57]Lin, Liza and Xiao, Eva. 'China Has to Approve TikTok-Oracle Deal Too, Bytedance Says', THE WALL STREET JOURNAL. Sept 17, 2020. https://www.wsj.com/articles/china-has-to-approve-tiktok-oracle-deal-too-bytedance-says-11600354975

[58]Mac, Ryan and Che, Chang. 'TikTok's C.E.O. Navigates the Limits of His Power', THE NEW YORK TIMES. January 27, 2023. https://www.nytimes.com/2022/09/16/technology/tiktok-ceo-shou-zi-chew.html

[59]Mac, Ryan and Che, Chang. 'TikTok's C.E.O. Navigates the Limits of His Power', THE NEW YORK TIMES. January 27, 2023. https://www.nytimes.com/2022/09/16/technology/tiktok-ceo-shou-zi-chew.html

[60]Brewster, Thomas. 'Warning Over Chinese Mobile Giant Xiaomi Recording Millions Of People's 'Private' Web And Phone Use'. FORBES. April 30, 2020. https://www.forbes.com/sites/thomasbrewster/2020/04/30/exclusive-warning-over-chinese-mobile-giant-xiaomi-recording-millions-of-peoples-private-web-and-phone-use/?sh=46d522181b2a

[61]He, Laura. 'The young CEO who helped make TikTok a global hit is latest Chinese tech entrepreneur to quit', CNN BUSINESS. May 20, 2021. https://edition.cnn.com/2021/05/20/tech/zhang-bytedance-ceo-resignation-intl-hnk/index.html

[62]Thorbecke, Catherine. 'Who is Shou Zi Chew? Mounting Scrutiny on TikTok Could Put New Spotlight On Its CEO', CNN BUSIENESS. January 20, 2023.
https://www.cnn.com/2023/01/20/tech/tiktok-ceo-shou-zi-chew/index.html

[63] https://sensortower.com/blog/tiktok-power-user-curve

[64]Harwell, Drew. 'How TikTok Ate the Internet. THE WASHINGTON POST. October 14, 2022. https://www.washingtonpost.com/technology/interactive/2022/tiktok-popularity/?itid=hp-top-table-main

[65]Alter, Adam. 'How Technology Gets Us Hooked', THE GUARDIAN. February 28, 2017. https://www.theguardian.com/technology/2017/feb/28/how-technology-gets-us-hooked

UNIVERSITY of
SOUTH FLORIDA

Global and National Security Institute

4202 E. Fowler Avenue, CGS 401
Tampa, Florida 33620
813.974.9800 | www.usf.edu/gnsi