Institute for National Defense and Security Research
Volume 12 | Issue 3 | December 2023 | ISSN 2

DEFENSE SECURITY BRIEF

01 WHY IS TIKTOK A SECURITY THREAT? A TECHNOLOGICAL AUTHORITARIANISM PERSPECTIVE
Shu-Ting Liu

10 INTERNATIONAL MONEY LAUNDERING PREVENTION AND LOOPHOLES DURING THE RUSSO-UKRAINIAN WAR
Joyce Chia-Yi Lin

17 TAIWAN'S FIRST INDIGENOUS DEFENSE SUBMARINE "HAIKUN"
Hsiao-Huang Shu

THE INSTITUTE FOR NATIONAL DEFENSE AND SECURITY RESEARCH (INDSR)

The Institute for National Defense and Security Research (INDSR) is dedicated to fueling knowledge-based policy analyses and strategic assessments on Taiwan's security. Our mission is to safeguard Taiwan's democracy and prosperity by strengthening mutual understanding and advancing common interests in the defense and security community both domestically and internationally. INDSR was formally inaugurated on May 1, 2018, and is headquartered in Taipei, Taiwan. We are an independent, nonpartisan, nonprofit organization.

To bring together great minds in policymaking, industry and research, we convene international forums, network civil societies, engage in Track Two dialogue and conduct wargame simulations. INDSR's dynamic research agenda and activities are used to develop pragmatic policy recommendations for the Taiwan government.

DEFENSE SECURITY BRIEF

Defense Security Brief (DSB) is an English-language publication aimed at strengthening research exchanges with security-related experts both domestically and abroad. Established in 2011, DSB was originally founded and compiled by the Office of Defense Studies, Ministry of National Defense. INDSR continued the publication in 2018.

OFFICE

Institute for National Defense and Security Research
No.172, Bo-Ai Road, Zhongzheng Dist., Taipei City, Taiwan (R.O.C.)
Tel: 886-2-2331-2360 Ext.705 | Fax: 886-2-2331-2361
Printed in Taiwan
ISSN 2225360-2

WHY IS TIKTOK A SECURITY THREAT? A TECHNOLOGICAL AUTHORITARIANISM PERSPECTIVE

Shu-Ting Liu

INTRODUCTION: IS TIKTOK A SECURITY THREAT OR NOT?

TikTok (or "Douyin" in China) has become one of the most influential social media in the world in recent years to. Several governments, commentators and studies have warned against the security issues presented by TikTok, but except for the fact that the platform sends users' data back to China and this constitutes an information security problem, there remains no direct evidence showing that it influences the mind, cognition and therefore interests of the audience. This has led some commentators to argue that the threat posed by TikTok should be re-examined.[1]

This paper engages with this issue, suggesting that reframing the debate surrounding TikTok may expand the scope of research. Currently, most discussion focuses on the effects of TikTok, and an implicit assumption is that if no negative effects are observed, then TikTok poses no security threats. Consequently, when TikTok is "securitized" in Taiwan, the discussion often is construed as political attacks of domestic party-politics or even a struggle between different political parties' Cross-Strait relations agendas without recognizing the danger of the authoritarian regime behind this technology, rendering society further divided.[2] INDSR's "2022 Survey of

1. "Second U.S.Judge Blocks Commerce Restrictions on TikTok," *Reuters*, December 8, 2020, https://reurl.cc/QWoA9M.

2. "Movie/Defeat Blames TikTok, Zhao Shaokang Criticizes 'Digital Control Department'," *Broadcasting Corporation of China*, December 14, 2022, https://reurl.cc/58NWOG; "Taiwan's Public Affairs Departments Completely Ban Douyin, Luo Zhiqiang: The DPP is Afraid that Douyin Will Make Its Own Cyber Army Useless," *Global Times*, December 14, 2022, https://reurl.cc/7jqQV1.

China's Threats to Taiwan and the United Front Work" (2022 年中國對台威脅與統戰網路調查) also shows that Taiwanese people hold divergent views of TikTok. When asked if the government should regulate TikTok because of information security concerns, 43.1% of the respondents disagreed, while 56.9% agreed. When asked if TikTok should be regulated because of the concern about China's united front work, 45.6% of those surveyed disagreed, while 54.2% agreed.[3]

Given the rapid development of technology, the ways in which new media such as TikTok affect the audience may not be readily observed. It is therefore suggested that the TikTok issue is re-assessed, based not on its effects but on its use as a political instrument of the Chinese Communist Party (CCP). This paper adopts the perspective of "technological authoritarianism" to establish a relationship between the CCP, TikTok, and Chinese society. Through control of the Internet, media, and technology by the state, the CCP has been able to consolidate its control and advance its influence with seemingly non-political but more nuanced instruments. New media such as TikTok infiltrate Chinese people's daily life as it has become part of their socializing, entertainment, and consumption. It has been further weaponized by the CCP to project influence overseas. It is this complex relationship between the state and media that TikTok is a threat to Taiwan's national security.

TECHNOLOGICAL AUTHORITARIANISM AND ITS DEVELOPMENT IN CHINA

The concept of "technological authoritarianism" refers to the use of technology by an authoritarian regime to strengthen its control over society and even export this model to the outside world. China is the most prominent example of this. A study contends that by using technology to control the people's words, deeds and even their hearts in an all-round way, China has crafted a system of "perfect dictatorship" not seen in other authoritarian regimes, and its essence may be termed "controlocracy."[4] The CCP's use of technology can be divided into three levels: mastery, application, and innovation. First, in terms of the mastery of technology, the CCP uses laws, institutional designs and the co-optation of technology companies

3. This online questionnaire survey was designed by scholars invited by the Institute for National Defense and Security Research (INDSR) and commissioned by IPSOS to conduct a survey on adults in Taiwan who are over 20 years old. The investigation period is from August 30 to September 8, 2022, and a total of 1,400 valid samples were recovered.

4. Stein Ringen, *The Perfect Dictatorship: China in the 21st Century* (Hong Kong: Hong Kong University Press, 2016).

to integrate resources and technology, making them a perfect tool for its rule. Second, in terms of the application of technology, the CCP incorporates information technology in its "despotic power," making it possible for the state to implement its will through various policing mechanisms and without the consent of society.[5] Finally, with regard to innovation, technology is a means to strengthen the CCP's "infrastructural power." The development of technology improves China's (digital) infrastructure, which in turn makes the state able to intervene in people's social and economic lives. The people accept the role and control of the state not because of fear or subjugation, but because of the convenience and pleasure of consumption, entertainment and other social services that are heavily monitored and regulated by the state. This soft social control model, which is also termed "popular techno-authoritarianism" (受歡迎的科技威權主義), is a combination of soft and hard power.[6]

Consequently, the CCP's authoritarian governance of society in an age of rapid development of science and technology consists of three aspects. The first is surveillance. The mastery and application of technology helps realize physical and networked surveillance. For example, both the "Skynet" (天網) and "Sharp eyes" (雪亮) projects deploy such technologies as face recognition, big data, and artificial intelligence to transform street cameras into a real-time monitoring system, in which people's whereabouts and their social activities are constantly monitored. In recent years, the CCP has further tightened its control of cyberspace as well as censorship of speech, exploiting information technology to detect, identify and block unfavorable public opinions on the Internet. The second is collection. In the name of the people's economic wellbeing, health, and safety, the CCP combines despotic and infrastructural powers to comprehensively collect the people's personal information for social control purposes. It can collect the people's digital footprints from the platforms operated by huge technology companies, reconstruct their online behavior, habits, and preferences, and make use of them. The third is manipulation. With the information of the people at hand, the CCP can manipulate their thoughts and behavior through incentive mechanisms. The "social credit system" (社會信用系統) is a good example. An individual's personal information such as his or her credit card records, traffic records, and opinions on the internet are gathered,

5. Hsin-Hsien Wang, "The Social Governance and State Society Relations in Xi Jinping's China," *問題と研究*, 47, no. 3 (September 2018): 35-74.

6. Guo Jiaming, "Discuss the Possibility of Being Monitored from the Implementation of Digital ID Card," *Science Monthly*, August 15, 2020, https://reurl.cc/10WDLD.

classified, and rated. Consequently, individuals with a good rating can enjoy benefits in transportation, employment, children's schooling, social subsidies, and even entertainment and shopping, while those with a poor rating are subject to certain restrictive measures. Through this system of reward and punishment, or carrot-and-stick, the CCP manages people's behavior without resorting to physical violence.

THE ADVANCEMENT OF THE CCP'S TECHNOLOGICAL AUTHORITARIAN MEASURES: DOUYIN AS AN EXAMPLE

Different from past authoritarian regimes that stressed only the oppressive aspects of power such as domination, surveillance, and policing, the CCP's "tech dictatorship" manifests the characteristics of soft governance that make its social control more delicate. Scholars find that the CCP's power over the media is threefold. First, through coercive power the state forces the media to "do what it (the media) doesn't want to do." Second, through institutional design, the state constrains the media, leaving the latter "unable to do what it wants to do." The third and the highest expression of power is the construction of culture, values, and norms, which makes the media not able to "think of doing or not doing certain things."[7] This conception of power derives from the work of French thinker Michel Foucault, whose "the technologies of power" describes how modern subjects have come to internalize social discipline and engage in self-identification, monitoring, and restraint.[8]

From this perspective, a variety of measures deployed by the CCP can be understood as instances of "the technologies of power" and "technologies of the self." These include laws, official media, new media, internet public opinion analysis industry, Nmslese (小粉紅), and the notion of the security of national culture, among others.[9] With these means and practices, the CCP's power is decentralized, externalized, and becomes relatively intangible, but the effect is that its power and influence penetrates to every corner of society. As a result, there is a tendency for people to follow the rules voluntarily.

Douyin is an example of this advanced technological authoritarian in contemporary China. First and as mentioned above, the CCP integrates resources

---

7. Fen Lin, "Power and Information Paradox: A State Perspective on Studying Chinese Media," *Communication & Society*, no. 45 (2018): 19-46

8. Michel Foucault, *Surveiller et punir: Naissance de la prison, trans. Shaozhong Wang* (Taipei: China Times Publishing, 2020).

9. Guobin Yang, "Killing Emotions Softly: The Civilizing Process of Online Emotional Mobilization," *Communication & Society*, no. 40(April 2017): 75–104.

and technology through institutional innovation. This is shown in the CCP's policy of content review on platforms including Douyin, as well as its demands for Douyin to launch an recommendation mechanism algorithm that meets political requirements. Furthermore, the CCP purposefully supported "ByteDance" (字節跳動), the parent company of Douyin, when it established a party branch within the company,[10] and listed its CEO as a key target of the united front work,[11] all of which sought to control and make use of the technology company.

Second, Douyin serves as a means for "incorporating management into service" (寓管理於服務). As a company that seeks to maximize economic interests, Douyin has developed convenient, easy-to-use, eye-catching services and functions, as well as a variety of preferential measures, so that people are willing to give out their personal information and digital footprints in exchange for Douyin's selection of popular and automatically broadcasted audio-visual services, music, and special effects. Given the close connection between the technology company and the state, the people's personal information can be easily assessed by it. The latter is, therefore, able to perform a kind of social control where the people's daily lives and entertainment are the target.

Finally, there is affective guidance. Technological authoritarianism in China not only seeks the people's voluntary submission to the state, but also aims to guide public opinion and effect. For example, the CCP promotes a movement of "developing a more civilized and well-regulated cyberspace" (「新時代網路文明建設」運動). As a result, patriotic youth groups on the internet, also known as the Nmslese, propagate nationalism as an emotional call on platforms including Douyin. They not only internalize the spirit of "conforming to the norms" and self-censor their comments on social media, but also engage in collective surveillance, asking others to like and share content that conforms to the norms. Creating hot topics through tags and memes on Douyin is therefore a more delicate operation of Chinese technological authoritarianism.[12]

---

10. "The List of Party Branches is Exposed, Where Will Douyin Go?" *The Epoch Times*, August 5, 2020, https://reurl.cc/mlp4OG.

11. "The United Front Work Department of the Central Committee Trains New Media Practitioners in Rotation for the First time, Including Chen Tong, Zhang Yiming and Deng Fei," *The Paper*, May 5, 2015, https://reurl.cc/odzd75.

12. Chang Jiang, "Popular Propaganda: Patriotic Mobilization in China in the Digital Era," *Twenty-First Century*, no. 182 (December 2020): 38-50.

THE EXPORT OF TECHNOLOGICAL AUTHORITARIANISM: THE WEAPONIZATION OF TIKTOK

To successfully move onto the international stage, the CCP has presented and promoted TikTok as a product that suits the free market. However, TikTok's parent company is still registered in China and must obey the CCP's orders by the laws of the People's Republic of China. In this sense democracies are not competing with China in the area of international communication on a level playing field.

In recent years, several countries have realized that the CCP is exporting technological authoritarianism overseas,[13] using technology companies in particular to expand its influence. There are two main approaches. First, Chinese technology companies directly cooperate with other authoritarian regimes. Supported by the Chinese state, these technology companies have signed investment or cooperation agreements with other governments, providing the latter with technologies of face recognition and cyber monitoring and helping them establish monitoring equipment and databases. The second approach is for Chinese technology companies to expand overseas markets. They brand their companies and promote their products in a capitalist fashion, striving to win the favor of international consumers. Most of their products, such as search engines and audio-visual platforms, are "depoliticized" and related to ordinary livelihood and entertainment. By so doing, consumers are more likely to ignore potential security implications and become dependent on these products. Over time, a direct and close connection between these Chinese companies and democratic societies is established.

It is the latter that is worrying. Several democratic governments are vigilant against the monitoring systems and communications equipment exported by Chinese technology companies and have tightened regulation. However, there remains a lack of consensus among democratic countries on how to deal with the circulation of those seemingly apolitical products and services by Chinese technology companies in the name of free market. Take the issue of TikTok in the United States as an example. Due to security concerns, several U.S. government agencies such as the Department of Defense, the Department of Homeland Security, and the State Department have banned their employees from using TikTok on government devices, with more and more departments likely to follow. Yet, as TikTok has become the most popular app among people under the age of 35 in the

13. Adrian Shahbaz, "The Rise of Digital Authoritarianism," *Freedom House*, November 4, 2018, https://reurl.cc/KQVzGg.

United States, an announcement by then President Donald Trump to ban TikTok caused a backlash.[14] Internet celebrities who have 100 million followers issued a petition against the proposal,[15] and there were even reports suggesting that Trump might lose a large number of young votes and affect his re-election.[16]

The lack of consensus on TikTok brings division and confrontation to democratic societies. In Taiwan, this is further utilized as an instrument of united front work. On July 30, 2022, Xi Jinping attended the central conference on the united front work, underscoring that "certain profound changes" (某些重大變化) have taken place. In this new era, united front work requires "new ideas, thoughts and strategies"(新理念新思想新戰略). It is necessary for "the united front work in Hong Kong, Macao, Taiwan and overseas to play a role in winning people's hearts" (發揮港澳台和海外統戰工作爭取人心的作用), and "enhance cyberspace united front work"(做好網絡統戰工作，走好網絡群眾路線).[17] As Douyin is an instrument of united front work in China, there is no reason not to infer that its overseas version, TikTok, also serves the same purpose.

There are three possible ways in which TikTok performs its united front work function. The first is cooptation. TikTok has driven an international trend and has become a popular social media for young people in Taiwan. On September 15, 2021, spokesperson for the Taiwan Affairs Office Zhu Fenglian (朱鳳蓮), claimed that Taiwanese teenagers are accustomed to using TikTok. It is a new phenomenon, and it is believed that "using simplified characters, listening to mainland songs, watching mainland movies and TV dramas, and using popular words in Mainland China"has become a fashion for Taiwanese teenagers.[18] Consequently, the CCP can exert its influence on Taiwanese youth through TikTok. Moreover, as TikTok collects users' personal information including basic information, digital footprints, habits and preferences, and even emotional responses, it is able to identify issues

14. "Trump Issues Orders Banning TikTok and WeChat from Operating in 45 Days If They Are Not Sold by Chinese Parent Companies," *CNN*, August 7, 2020, https://reurl.cc/vDyEnL.
15. "Dear President Trump: An Open Letter from The TikTok Creator Community," *Medium*, August 3, 2020, https://reurl.cc/ROoApr.
16. "Banning TikTok Could Have Devastating Electoral Consequences For Trump," *Forbes*, July 9, 2020, https://reurl.cc/rxz01x.
17. William Zheng, "Xi Jinping Urges Chinese Communist Party to Step up Efforts to 'Win Hearts and Minds' in Hong Kong and Taiwan," *SCMP*, July 31, 2022, https://reurl.cc/mZQaEA.
18. "Press Conference of Taiwan Affairs Office of the State Council (2021-09-15)," *Taiwan Affairs Office of the State Council*, September 15, 2021, https://reurl.cc/EZn4va.

that interest young people in Taiwan, the types of audio-visual material that attract them, and the content that satisfies them, thereby further bringing them closer to China.

The second is to divide Taiwanese society. The media features of TikTok, such as hashtags, emotional contagion by the audio-visual services, a recommendation mechanism algorithm, and the emergence of highly popular internet celebrities,[19] may be instrumentalized. They can be used to disseminate hate speech and disinformation that discredit the governments of Taiwan and the United States,[20] and/or promote views favoring the CCP.

The third is to target the CCP's main enemy, namely the DPP government and those so-called Taiwan independence separatists. Through manipulating public opinion in Taiwan, the CCP is able to "turn the people against the government" (以民逼官), discrediting Taiwan's government and even interfering in its decision-making process, thereby hindering the normal operation of Taiwan's democracy.

These are possible scenarios for TikTok is weaponizationby the CCP to undermine Taiwan's national security. While it may not have caused harm to Taiwan, the complex relationship between the platform and the CCP makes such a threat very likely if not imminent.

CONCLUSION: IS TIKTOK A SECURITY THREAT?

Adopting a perspective of technological authoritarianism, this paper contends that since the CCP uses Douyin as a tool in its internal rule, there is no reason that it will not use TikTok, the international version of Douyin, to extend its influence overseas. The bigger TikTok's share in the global market, the more serious is its threat to democracies. In an era where the international community has become wary of China and its threats in terms of military expansion, "wolf warrior diplomacy," economic coercion, disinformation, and cyber threats, the CCP is more likely than ever to exert its influences in areas that are usually taken as apolitical. Chinese social media like TikTok hence become powerful instruments for the CCP's united front work.

Currently it remains difficult to prove that TikTok has seriously undermined Taiwan's national security. The absence of effects, however, does not necessarily

19. "TikTok Rises in Taiwan," *huaxia.com*, September 4, 2020, https://reurl.cc/OEoorX.

20. "Xie Jinhe Facebook: Douyin's Cognitive Operations," *Facebook*, November 28, 2022, https://reurl.cc/deook8.

mean that TikTok poses no threat to Taiwan. The paper suggests that in addition to—or instead of—looking for effects such as the spread of disinformation and the risk of information security, we should note the complex relationship between the CCP and TikTok (and other new media platforms). A perspective of technological authoritarianism suggests that as technological companies are coopted and controlled by the CCP, the development and promotion of media platforms such as TikTok necessarily carries a political dimension. In other words, it is always possible that TikTok functions as a channel through which the CCP exerts its influence on Taiwan. Consequently, it is imperative for various governmental bodies to coordinate with one another, enhance communication with society, and bolster the public's media literacy to continue discussion on and raise awareness of the threat of TikTok.

※

Ms. Shu-Ting Liu is a Policy Analyst at Division of Defense Strategy and Resources, INDSR. Her research interests include Digital content industry, Communication technology, Chinese society and media.

※

INTERNATIONAL MONEY LAUNDERING PREVENTION AND LOOPHOLES DURING THE RUSSO-UKRAINIAN WAR

Joyce Chia-Yi Lin

INTRODUCTION

From an anti-money laundering perspective, Russia's invasion of Ukraine in 2022 poses significant risks related to money laundering and terrorist financing. Conflict areas are particularly vulnerable to these risks, as criminal and terrorist organizations exploit chaos and instability to carry out illicit activities. In the case of Ukraine, the conflict has resulted in large amounts of money being moved across borders, often with little regulation and high money laundering risks. This situation is further exacerbated by the use of cryptocurrencies, which provide anonymity and can be easily used to transfer funds across borders.

On February 24, 2023, the international anti-money laundering organization the Financial Action Task Force (FATF) suspended Russia's membership.[1] Russia, which joined the FATF in 2003, is suspended, however, it is still obliged to implement FATF's anti-money laundering rules.[2]

Anti-money laundering regulations and requirements have changed significantly as a result of Russia's invasion of Ukraine. Governments around the world are aware of the need to strengthen anti-money laundering regimes to prevent criminal and terrorist organizations from exploiting conflicts for financial gain. Other measures have also been taken to prevent money laundering and terrorist financing in affected

1. "FATF Statement on the Russian Federation", *Financial Action Task Force*, February 24, 2023, https://www.fatf-gafi.org/en/publications/Fatfgeneral/fatf-statement-russian-federation.html.
2. Mengqi Sun, "Global Financial Watchdog Suspends Russia's Membership", *Wall Street Journal Chinese Edition*, February 24, 2023, https://www.wsj.com/articles/global-financial-watchdog-suspends-russias-membership-ec59980a.

areas, including taking real action to deal with complex transactions, remittance and drawdowns in banking systems in a detailed way.

There has been a major shift in the global anti-money laundering landscape, as governments and financial institutions have recognized an urgent need to consolidate their anti-money laundering regimes to mitigate the risks posed by illegal actions. In response, regulators have introduced a number of changes and requirements to strengthen anti-money laundering compliance in affected regions. For example, governments and financial institutions have strengthened due diligence requirements and increased monitoring of financial transactions to prevent illicit financial activities in conflict areas. These measures aim to increase the transparency and traceability of financial transactions to mitigate risks associated with money laundering.

This article intends to explore the loopholes in international money laundering prevention measures in recent years and the overall situation vis a vis circumvention of sanctions since the Russo-Ukrainian war began.

RUSSIA CIRCUMVENTS SANCTIONS THROUGH OFFSHORE FINANCIAL SPECIAL ADMINISTRATIVE ZONES AND TAX HAVENS

As early as 2018, Russia established two offshore financial special administrative zones,[3] in the easternmost and westernmost parts of Russia, to attract foreign investment and domestic enterprises with low taxes. Before the Russo-Ukrainian war, Russian overseas enterprises that were attracted by tax incentives and transferred their registration places to the afore-mentioned two administrative regions had successfully evaded the economic sanctions which had been imposed on Russia, which indirectly shielded the assets of Russian billionaires from being frozen. In mid-2018, four months after the U.S. Treasury Department imposed sanctions on seven Russian tycoons suspected of having ties to Valdimir Putin, the Russian government created additional escape clauses for these tycoons in exchange for extremely favorable terms of interests.[4] Therefore, since 2018, more

3. One is a small Russian island located on the border with China and North Korea; the other is a small island in the Kaliningrad region between Lithuania and Poland.

4. For Russian businessmen, the benefits provided by this law for transferring the place of registration back to Russia are almost impossible to refuse: as long as an investment of 50 million rubles is made, stock transactions, dividends and capital gains are tax-free; if the original overseas company is transferred to this Transactions can still be made using foreign bank accounts for six months after SAR, making it easier to move funds across borders.

than 70 companies have transferred their registration places from overseas to the afore-mentioned Russian special zones, because these overseas areas[5] are not Russian territories and they cooperate with US sanctions.[6] If these companies want to evade sanctions, they newly register in the Russian special zones, which is the most effective way.

Currently, the world's well-known tax havens include the Cayman Islands, British Virgin Islands, Bahamas, Bermuda, and Monaco, etc. Most of them use low taxes and loose regulations to attract multinational enterprises to register and then, through layers of subsidiaries, use highly liquid "non-entity asset transactions" such as stocks, bonds, and hedge funds, and use tax haven confidentiality clauses to block relevant institutions from accessing "non-physical assets" when financial regulatory standards in various countries are loose or inconsistent.[7] The inability to trace the "Ultimate Beneficial Owner" has provided cover for wealthy people to launder money or evade taxes.

EASTERN EUROPEAN COUNTRIES HAVE BECAME A MONEY LAUNDERING CHANNEL FOR RUSSIA

The Organized Crime and Corruption Reporting Project (OCCRP)[8] exposed the methods used by Eastern European countries to assist Russia in money laundering in 2014. It was the first comprehensive study that analyzed how billions of dollars flowed out of Russia after money was laundered from 112 bank accounts in Eastern European countries, and then flowed into banks around the world. Finally, most of the funds flowed to the overseas accounts of Russian businessmen.

In addition, to remit funds out of Russia, many Russian companies use 21 shell companies established in the United Kingdom, Cyprus and New Zealand to post

---

5. Including the European Union and its member states, such as Cyprus, it was the most popular offshore financial center for Russian billionaires in the past.
6. "Inside The Russian Tax Havens Set Up By Putin To Help Sanctioned Billionaires," *Forbes*, February 2, 2022, https://www.forbes.com/sites/giacomomotognini/2022/02/02/inside-the-russian-tax -havens-set-up-by-putin-to-help-sanctioned-billionaires/?sh=40c4db4bb6ec.
7. "Quan qiu pin fu cha ju zhi yi yu-xi qian tian tang zhi mei li tang yi" [全球貧富差距之一隅－洗錢天堂之美麗糖衣 One Corner of the Global Wealth Gap - the Beautiful Sugar Coating of Money Laundering Paradise], *Qing liu Bimonthly*, July 2016, https://tainan.swcb.gov.tw/Content/Files/Article/4a7efba5

274d4f68a7028bf8ad70e9d4.pdf.

8. Founded in 2006, OCCRP is a global organization of investigative journalists specializing in organized crime and state corruption.

between accounts, use transactions between different shell companies to create false debts, and then transfer funds to a court in Moldova, a small country in Eastern Europe, and apply for a payment order. A Russian company that intended to launder money in the form of a court order then transferred the money to a bank designated by the court in the disguised form of payment of debts. The Russian company also had an account with the designated bank and finally transferred US$8 billion from the bank's related accounts to various countries for use; this method was also used by the Latvian bank Trasta Komercbanka, which has successfully replicated it, and US$13 billion has been laundered through various shell companies.[9] This money laundering model has been around for many years, and most Eastern European countries are still high-risk countries for money laundering. In addition, after the rise of blockchain and cryptocurrency, a large number of ransomware and cryptocurrency-based money laundering activities have also appeared in Eastern Europe. Eastern Europe is the fifth largest market for cryptocurrency activities in the world. Since the Russo-Ukraine war, high-risk or illegal encryption currency activities have increased rapidly in Eastern Europe, with up to 18.2% of all cryptocurrencies received in Eastern Europe coming from the addresses associated with high-risk or illegal activity, much higher than other regions.[10]

CONCLUSION

It is very difficult to track down cross-border money laundering or tax evasion. The EU passed an anti-money laundering law as early as 1990. In 2015, the EU launched the fourth version of the Anti-Money Laundering and Terrorist Financing Directive (AMLD IV), which allows the public to inquire about beneficiary information to increase the transparency of the ownership of listed companies. After the International Consortium of Investigative Journalists (ICIJ) disclosed the Panama Papers in 2016, it made real money laundering records of politicians and wealthy businessmen public, showing that it is very difficult to trace the ultimate beneficiaries in practice. Therefore, in 2018, the European Union revised and released the fifth version of the Money Laundering Prevention Law (AMLD V,) allowing the public to

9. "The Russian Laundromat Exposed," *OCCRP*, March 20, 2017, https://reurl.cc/EGX0q1.

10. (Chainalysis : Affected by the Russia-Ukraine war, high-risk and illegal chain activities increased sharply in Eastern Europe) , " Mobile Zone ", October 13 , 2022 , https://www.blocktempo.com/chainalysis-high-risk-and-illicit-crypto-activity-surges-in-eastern-europe-amid-russia-ukraine-war/.

inquire about the ultimate beneficiary information of listed companies, increasing corporate transparency.[11]

After the outbreak of the Russo-Ukrainian war, money laundering prevention, exposing the sources of false information and combating terrorism have become even more important. The sanctions launched by Europe and the United States to freeze the overseas assets of Russian tycoons and politicians only scratch the surface and fail to address the core issues - offshore finance and inter-bank money laundering. This is the weakness of European and American sanctions against Russia. If they want to cut off Russia's money, European and American countries should work together and start from two directions. One is to crack down on overseas finance to legally cover various illegal transaction methods, and the other is to punish relevant financial institutions that assist Russia in money laundering.

Taiwan enacted the Money Laundering Prevention Law in 1996 and joined the Asia-Pacific Money Laundering Prevention Group (APG) in 1997. However, in the following years, the relevant legal system did not keep pace with the times. In 2011, it was listed by the APG on the enhanced tracking list. Fortunately, in 2022, Taiwan was selected as the North Asia representative of APG, which shows that the world is beginning to recognize Taiwan's performance in money laundering prevention in traditional financial institutions; however, it lags behind in cryptocurrency money laundering. Taiwan defines cryptocurrency as "a digital representation of value with the use of cryptography and distributed ledger technology or other similar technology that can be digitally stored, exchanged, or transferred, and can be used for payment or investment purposes,"[12] which seems to have narrowed the definition of virtual assets and created regulatory loopholes. It is also inconsistent with the definition

---

11. "European Corporate Governance Retrograde? An EU Ruling Opens A Back Door for Putin: The Dilemma between Money Laundering and Privacy Protection for Gangster Politicians," *Today*, December 5, 2022, Https://reurl.cc/lvZxdq.

12. Article 2, 'The terms as used in these Regulations are defined as follows:

    1. "A enterprise handling virtual currency platform or transaction" (hereinafter referred to as the enterprise) refers to a business that engages in the following activities on behalf of others.

        (1) Exchange between virtual currencies and fiat currencies, such as New Taiwan Dollar (hereinafter referred to as NTD), foreign currencies, and currencies issued by Mainland China, Hong Kong, or Macao.

        (2) Exchange between one and more forms of virtual currencies.

        (3) Transfer of virtual currencies.

        (4) Safekeeping or administration of virtual currencies or instruments enabling control over virtual currencies.

        (5) Participation in and provision of financial services related to an issuer's offer or sale of virtual currencies.

of the technology neutrality principle proposed by FATF. In practice, cryptocurrency fraud groups are mostly located in Russia, China, Thailand, the United States and other countries, and use cryptocurrency exchange and money laundering to transfer money. After transferring several times, it is difficult to trace the link between the final withdrawal and the initial fraud.[13] In terms of law enforcement, the government should break away from the traditional banking and financial concept of identifying the "ultimate beneficiary" and the legal concept of uninformed "bona fide third parties" and change it to " chasing people with cash flow " in order to keep up with the new criminal method of money laundering in a generation of cryptocurrencies.

---

2. "A virtual currency" refers to a digital representation of value with the use of cryptography and distributed ledger technology or other similar technology that can be digitally stored, exchanged, or transferred, and can be used for payment or investment purposes. However, virtual currencies do not include digital representations of NTD, foreign currencies, currencies issued by Mainland China, Hong Kong, or Macao, securities, and other financial assets issued in accordance with laws.
3. "The establishment of business relationship" refers to the acceptance of customer applications for registration or establishment of similar business transaction relationships.
4. "An occasional transaction" refers to a transaction involving activities specified in Subparagraph 1 with an individual that has not established a business relationship with the enterprise.
5. "The beneficial owner" shall mean the natural person(s) who ultimately owns or controls the customer or the natural person on whose behalf a transaction is being conducted, including those persons who exercise ultimate effective control over a legal person or arrangement.
6. "Risk-based approach" (RBA) shall mean the enterprise shall identify, assess and understand the money laundering and terrorist financing (hereinafter referred to as ML/TF) risks to which they are exposed and take appropriate anti-money laundering and countering terrorist financing (hereinafter referred to as AML/CFT) measures commensurate with those risks in order to effectively mitigate them. Based on the RBA, the enterprise shall take enhanced measures for higher risk situations, and take relatively simplified measures for lower risk situations to allocate resources efficiently and use the most appropriate and effective approach to mitigate the identified ML/TF risks.

   The term "the enterprise" used in Subparagraph 1 of the preceding paragraph refers to those registered domestically.

   Where the financial institutions and designated nonfinancial businesses or professions specified in Article 5 of the Money Laundering Control Act engage in activities specified in the items in Subparagraph 1, Paragraph 1 herein, they shall execute businesses in accordance with the related AML/CFT regulations established by these central competent authorities governing target businesses and these Regulations shall not apply..', Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises Handling Virtual Currency Platform or Transaction.

13. "Fraud Syndicates Launder Money Through Cryptocurrency Exchange and It Is Difficult to Recover in Law. Legislators Call for 'Strict Management and Chasing People with Money'," *Key Commentary*, February 8, 2023, https:// www .thenewslens.com/article/160245.

※

Ms Joyce Chia-Yi Lin is a policy analyst in the Division of National Security Research, Institute for National Defense and Security Research (INDSR) in Taipei, Taiwan. Her areas of expertise encompass industry and supply chain security, international economy and trade security, as well as anti-money laundry.

※

TAIWAN'S FIRST INDIGENOUS DEFENSE SUBMARINE "HAIKUN"

Hsiao-Huang Shu

INTRODUCTION

Taiwan's first domestically built submarine was named "Haikun" (海鯤) during a completion and naming ceremony at the state-run CSBC Corporation Taiwan (台灣國際造船公司) on September 28, 2023. President Tsai personally hosted the ceremony. The name "Haikun," meaning Narwhal, is derived from the Chinese classic Zhuangzi (莊子).[1] Narwhal embodies the qualities of vastness and elusiveness. The choice of the name Haikun for the submarine signifies the expectation that it will operate adeptly in a stealthy manner, navigate the deep-sea environment, and be hard to detect. This article aims to analyze the implications of Haikun and broaderly indigenous defense submarine (IDS) project for Taiwan.

IMPLICATIONS OF THE INDIGENOUS DEFENSE SUBMARINE

First of all, submarines have emerged as the primary assets in modern naval warfare, particularly for smaller states like Taiwan. They play a pivotal role in safeguarding maritime interests by thwarting potential enemy invasion. Given Taiwan's strategic island location, maintaining maritime transportation routes for the import of energy and food is crucial for wartime resilience.

In the event of a blockade by the People's Liberation Army (PLA) Navy, Taiwan can leverage its submarines to counteract the blockade. This involves ensuring the safety of waterways, protecting the Navy's surface ships, and preventing PLA Navy

1. "guo zao hai kun qian jian ming ming you lai hai jun: xiang zheng ju da yin ni bu yi cha jue" [國造海鯤潛艦命名 由來 海軍：象徵巨大、隱匿不易察覺 The Origin of the Name of the Taiwan-made Haikun Submarine Navy: Symbolizing Hugeness, Concealment and Difficult to Be Detected], *CNA*, September 28, 2023, https://www.cna.com.tw/news/aipl/202309280095.aspx.

submarines from posing a threat to our surface vessels. Effectively countering the operations of PLA Navy surface ships will also be within the capabilities of Taiwan's Navy, showcasing the versatility and value of submarines in maritime defense strategies

China's persistent gray zone harassment, including the near-daily deployment of warships in Taiwan's vicinity, poses a significant threat to Taiwan's maritime security. To counter this threat, the Taiwanese Navy has dispatched ships to monitor and deter Chinese incursions. However, China may increasingly employ submarines for these activities. A robust Taiwanese submarine fleet could effectively patrol surrounding waters, detect underwater threats, and exert pressure on the PLA Navy's surface ship deployments.[2]

Generally speaking, the tasks Taiwan's submarines are expected to take on in the future include:

1. Deployed in underwater ambush areas in key sea lanes or combat areas to attack the PLA Navy's surface combat forces.
2. Protecting the operational safety of the Navy's surface ships and avoiding threats from PLA Navy submarines.
3. Deployed to ambush the PLA Navy's surface combat ships: waiting for opportunities to attack important targets (such as aircraft carriers, large landing ships, and supply ships) on the PLA Navy's ship routes or in combat deployment areas; launching joint antisubmarine operations with Taiwan's Air Force and Navy.
4. Performing underwater patrol missions, cooperating with air and surface anti-submarine ships, detecting the activities of PLA Navy submarines, and strengthening joint anti-submarine warfare capabilities.
5. Carrying out intelligence surveillance and reconnaissance missions in critical areas.
6. Carrying out special operations or mine-laying missions.

The PLA Navy's submarine force's capability is growing rapidly. In addition to traditional diesel-electric submarines, the number of nuclear-powered attack submarines and strategic missile submarines is also gradually increasing, posing a major threat to the United States, Australia, India and other neighboring countries. Due to this challenge, Taiwan must strengthen its underwater combat capabilities. It needs to improve the monitoring capabilities with regard to the PLA Navy's underwater activities, and cooperate with neighboring countries to strengthen comprehensive monitoring of PLA Navy submarines in the Western Pacific.

---

2. Interview with a Navy officer.

FIGURE: Launching Ceremony of Haikun (Source: The Author)

DESIGN AND CONSTRUCTION OF HAIKUN

The type and design of the submarine Haikun were mainly completed by Taiwan domestically. The Navy found the best configuration through ship model testing. Haikun is similar to the diesel-electric submarine design of the world's advanced countries, such as the German Type 212 and the Japanese Soryu class.

It is a fact that Taiwan has no experience in building submarines in the past. To develop from scratch, many difficult problems, including the cost, construction cycle and risks, had to be tackled. In order to reduce technical risks and shorten the research and development cycle, the construction team followed the existing submarine type with assistance from international allies who provided design and construction guidance and various support. These factors helped make the building of the submarine successful.

The submarine Haikun adopts a composite hull design. The middle section is a single hull, a pressure hull. The front and rear sections are double hulls. The pressure hull is the inner layer, and the outer hull does not bear water pressure.

At the same time, because the outer hull is relatively small and thin, the most appropriate hull shape could be identified based on ship model testing to facilitate stealth and underwater navigation.

The pressure hull is one of many key technologies for submarine building. The pressure hull must be able to maintain a true round cross-section configuration to ensure resistance to underwater pressure. At the same time, welding process requirements are extremely demanding. In addition to pre-heating, the welding position also needs to be checked by X-ray to ensure there are no micro-cracks. Without the ability to fabricate and weld the pressure hull, it would be impossible to build an advanced submarine.

Currently, Taiwan's China Steel Corporation (CSC) is able to produce HSLA80 steel plates. They were produced experimentally in 2019 and the welding technology verified. Non-breakage tests were conducted in 900-meter-deep sea off Taiwan's east coast and underwater blast tests carried out, and these tests were passed.[3]

The HSLA80 steel plate can reach a tension of 550MPa, which is higher than the 350MPa tension of the Swordfish-class FE510 steel plate. The Haikun class's diving depth may reach about 300-400 meters, and its performance will be better than the Swordfish-class submarine.

Haikun's special design includes propeller and tail rudder. Many parts of the hull of this submarine were "wrapped" at the ceremony, including the bow of the ship covered with a curtain decorated with the national emblem of blue sky and white sun, the sonar array on the side, and the propeller on the stern of the ship. This was for reasons of secrecy.

The X-type tail rudder design features four rudder surfaces that can be controlled independently. All four rudder surfaces can play a combined role in horizontal or pitching movements, making underwater maneuverability better. If one rudder surface is damaged, the other rudder surfaces can also be accepted. Control is complicated and requires a computer. There are also two horizontal stabilizer surfaces, which may increase the submarine's operational performance.[4]

Haikun is equipped with 7 sonars. The high-frequency sonar above the bow is used for precise positioning, determining underwater navigation obstacles, and ensuring navigation safety. The active/passive sonar under the bow is used to emit

3. Fu S. Mei, "Updates on Taiwan's Indigenous Submarine Program," *Global Taiwan Brief*, January 16, 2019, https://globaltaiwan.org/2019/01/updates-on-taiwans-indigenous-submarine-program/.

4. "Scholars Analyze Taiwan's 'Narwhal' Sub's X-shaped Tail, Sonar System," *Focus Taiwan*, October 1, 2023, https://focustaiwan.tw/sci-tech/202310010006.

sound waves and detect echoes. It can also passively listen to other sound sources and detect underwater objects. Another three sets of low-frequency passive sonar are installed on the side to locate targets at longer distances. They can also be used for underwater listening to increase detection capabilities.[5]

The difficulty in Taiwan's production of submarines lies in "red zone" equipment, which refers to equipment or technologies that Taiwan cannot develop and for which it must seek assistance from outside. This includes combat systems, sonar, power systems such as diesel main engines, generators and motors, and weapon systems, such as torpedoes or submarine-launched missile systems. In addition, although the "yellow zone" equipment is difficult to obtain, Taiwanese companies should have the ability to make such products in the future; the "green zone" refers to equipment that can be produced in Taiwan.

Most of the combat systems come from specialized manufacturers from various countries. Due to fear of interference by China, Taiwan keeps the source of its equipment highly confidential. It is because of the assistance of friendly countries that the nation's submarine manufacturing was successful.

The main weapons of submarines include torpedoes, missiles, mines, etc. Haikun is expected to be equipped with US-made MK48 heavy-duty torpedoes and should also be equipped with submarine-launched Harpoon missiles.

Other sensing systems include an advanced integrated periscope system that integrates visible light, near infrared (SWIR), medium wave thermal imaging (MWIR), and low-light, as well as electronic warfare system antennas, direction finding antennas and GPS Receiving antennas that can reduce the number of antennas and help strengthen shielding.[6]

Taiwan's Navy pays attention to the quietness of this submarine. In addition to using large 7-piece scimitar blades, it can reduce the speed of the blades to reduce the source of noise.[7] The main engine and other machinery are equipped with

---

5. "Academics Offer Insights into Sub," *Taipei Times*, October 2, 2023, https://www.taipeitimes.com/News/taiwan/archives/2023/10/02/2003807087.

6. "OPTRONIC IMAGING, NAVAL UNDERSEA IMAGING AND COMMUNICATIONS," *L3Harris*, https://www.l3harris.com/all-capabilities/optronic-imaging-naval-undersea-imaging-and-communications; also see H. I. Sutton, "America Providing Advanced Systems For Taiwan's New Submarine," *Naval News*, October 11, 2023, https://www.navalnews.com/naval-news/2023/10/america-providing-advanced-systems-for-taiwan-new-submarine/.

7. "qian jian yuan xing jian 9 yue ru qi feng ke xia shui zhe ge bu wei "bao qi lai" bu gei kan" [潛艦原型艦 9 月如期封殼下水 這個部位「包起來」不給看 The Submarine Prototype Will Be Sealed and Launched in September as Scheduled. This Part is "Wrapped" and Will Not be Shown], *Liberty Times Net*, August 22, 2023, https://def.ltn.com.tw/article/breakingnews/4403943.

shock-absorbing seats to reduce vibration and noise. The streamlines of the hull and the surface treatment of the hull also pay attention to reducing noise. Currently, the hull does not have silencer tiles installed. If the construction technology matures in the future, it is not ruled out that they can be added.

CONCLUSION

The submarine Haikun is the Taiwan's first domestically built submarine, though it's a still prototype. Taiwan's Navy expects to conduct static tests in 2024, and then conduct sea trials to verify various systems and correct deficiencies. Ideally, if the construction of 8 submarines is successfully completed, the Taiwanese navy will significantly enhance its combat capabilities, and will be able to effectively resist PLA Navy's maritime threats.

※

Hsiao-Huang Shu is an Assistant Research Fellow, Institute for National Defense and Security Research, Taiwan. His research interests cover PLA, military operation concept, and weapon and strategy.

※

SUBMISSION

Defense Security Brief (DSB) is a bimonthly, open access, and peer-reviewed journal published by the Institute for National Defense and Security Research (INDSR) Taipei, Taiwan. Established in 2011, DSB was originally founded by the Ministry of National Defense and continued by the INDSR from 2018. We aim at strengthening research collaboration and fostering exchanges between researchers and experts both domestically and internationally.

DSB publishes original papers, reviews, comments and case studies. Contributions that engage with contemporary international affairs, defense, security, strategy, Indo-Pacific issues and policy reviews are particularly welcome.

All manuscripts must be in English and should be submitted via email to DSB@indsr.org.tw. Please note that the editorial review process can take up to three months. For further information and previous volumes, please visit the official website of DSB:
https://indsr.org.tw/en/download/2/DEFENSE-SECURITY-BRIEF

GENERAL GUIDELINES

Authors are advised to follow these guidelines:

- All manuscripts should be between 1,500 - 2,500 including footnotes.
- Citation tyle: *The Chicago Manual of Style*, 16th edition.
- Co-authorship is allowed.
- A short author's biography no more than 100 words need to be provided but not be included in the manuscript.
- An honorarium is provided upon successful publication up to NT$ 4,075 (NT$1,630/1,000 words or US$50-58/1,000 words per paper).
- For any further information, please email the Associate Editor, Dr. Tsung-Han Wu, at *t.h.wu@indsr.org.tw.*

Institute for National Defense and Security Research