# INDSR Newsletter



Institute for National Defense and Security Research

No.8 March 2022

# About Us

The Institute for National Defense and Security Research（財團法人國防安全研究院） is dedicated to fueling knowledge-based policy analyses and strategic assessments on Taiwan's security.

INDSR was formally inaugurated on May 1, 2018, and is headquartered in Taipei, Taiwan. We are an independent, nonpartisan, nonprofit organization.

INDSR aims to shape innovative ideas and lead constructive debates on issues pertaining to international security and national defense, Chinese politics and military affairs, non-traditional security, hybrid and cognitive warfare, and cybersecurity, among other security areas.

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.

INDSR was listed among the "best new think tanks" in 2020 in the latest Global Go To Think Tank Index Report, for the second year in a row. INDSR's English-language podcast collaboration with Ghost Island Media called "The Taiwan Take" was nominated in the podcast category for the Excellent Journalism Award ( 第 19 屆卓越新聞獎 ) in 2020.

**Institute for National**
**Defense and Security Research**
No. 172, Bo'ai Rd.,
Zhongzheng Dist., Taipei City-100057
Taiwan (R.O.C.)
https://indsr.org.tw/en

# Contents

# Political and Economic Logic of Beijing's 'Sanctions' against Lithuania

**Che-chuan Lee**
**Associate Research Fellow**

Division of National Security Research

## 1. News Highlights

On February 9, 2022, the Chinese General Administration of Customs (GAC) announced it would suspend accepting import declarations for Lithuanian beef with the immediately commenced shipment. The following day, the Lithuanian State Food and Veterinary Service stated that the Chinese GAC had informed Lithuania that it would stop importing Lithuanian beef into China due to a "lack of proper documentation". The move indicated that Beijing's "sanctions" against Lithuania were not yet over; however, Lithuania has not exported any food products, including beef, to China since early December 2021.[1]

In 2021, Lithuania's relations China rapidly deterioratied.[2] In May 2021, Lithuania announced its withdrawal from the "17+1" China and Central Eastern Europe (CEE or CEEC) cooperation, and in July agreed for Taiwan to establish its representative office in the Lithuanian capital. Lithuania and China both withdrew their ambassadors to each other, and diplomatic relations were downgraded to the chargé d'affaires level. In addition, Beijing imposed a number of economic

1. "China Suspends Import of Lithuanian Beef without Official Explanation," *Central News Agency*, February 10, 2022, https://reurl.cc/3jbLlM; "Lithuania Has Stopped Food Exports to China in December Last Year," *Central News Agency*, February 10, 2022, https://reurl.cc/VjmXOy.
2. Changes in Lithuania's relations with China in recent years can be traced back to 2019. In January of the year, the Lithuanian Ministry of National Security listed China as a national security threat for the first time in its national threat assessment report. In July 2019, President Gitanas Nausėda said that China's investment in the construction of Lithuania's Port of Klaipėda could harm Lithuania's national security. In November, Defense Minister Raimundas Karoblis stated that if China took control of the port of Klaipėda, it would pose a strategic risk to the passing US and NATO forces.

coercive acts on Lithuania, and the dispute has not yet ended (see table below). This article will briefly analyze Beijing's means of "sanctioning" Lithuania and discuss its intentions as well as possible effects.

## 2. Security Implications

The first wave of disputes between China and Lithuania in 2021 were related to the "17+1" CEE cooperation. On February 9, Lithuania sent only ministerial-level officials to present in the China-Eastern Europe Leaders' Video Summit hosted by Xi Jinping. The Lithuanian Parliament agreed to withdraw from the "17+1" mechanism in March and officially announced its withdrawal in May. On May 20, the Lithuanian Parliament passed a resolution condemning China's "genocide" of the Uighurs in Xinjiang and also called for the UN to investigate the "re-education camps" and urged China to repeal Hong Kong's National Security Law. Since May, Lithuanian cultural and artistic activities in China have been cancelled or suspended as the first wave of pressure from China.[3] After Lithuania agreed for Taiwan to establish a representative office in July, its relations with China deteriorated even further; Beijing's coercion quickly expanded from a downgrading of diplomatic relations into the economic field.

### 2.1 Diplomatic coercion strategy: strong pressure without severing formal ties

On July 20, 2021, Lithuania agreed to the establishment of the "Taiwanese Representative Office in Lithuania" in Vilnius, the capital, making it the first representative office in Europe bearing the name of "Taiwanese". After unsuccessful negotiations with Lithuania, Beijing announced on August 10 that it was recalling its ambassador to Lithuania; on September 3, Lithuania recalled its ambassador at the request of the Chinese government, and the embassy was overseen by the chargé d'affaires ad interim. On November 18, the Taiwanese

3. Revealed by Tomas Ivanauskas, Cultural Counselor of the Lithuanian Embassy in China, to the Lithuanian National Radio and Television (LRT). See Stephanie Chiang, "Lithuanian Art, Cultural Events Suspended in China Amid Tension," *Taiwan News*, September 3, 2021. https://reurl.cc/dXq9Lk.

Representative Office in Lithuania was officially established, and the Chinese side downgraded the relationship between Lithuania and China to the level of chargé d'affaires on November 21. On November 25, the consular service of the Chinese Embassy in Lithuania was suspended; the following day, the Chinese Embassy in Lithuania changed its name to the Office of the Chargé d'Affaires and requested Lithuania to change the name of its embassy accordingly.

On December 15, all Lithuanian diplomats and their families in China left Beijing and China affairs were handled remotely. It is worth noting that although Beijing quickly recalled its ambassador and lowered the level of relations between the two countries, it did not break off diplomatic relations with Lithuania after the withdrawal. In this regard, the spokesperson for the Chinese Foreign Ministry and Lu Shaye, the Chinese Ambassador to France, both said they hoped Lithuania would "admit its mistake and take action to correct the wrongful act of recognizing the 'one China, one Taiwan' status, and return to the right track of the 'one China' principle." In other words, Beijing will not cut diplomatic ties with Lithuania to prevent Taiwan and Lithuania establishing diplomatic ties, which would further challenge the "one China principle".

### 2-2. China coerces MNCs to pose pressure, thereby dividing EU

The recall of the ambassador was quickly followed by economic coercion from Beijing. First, China Railway Group's China Railway Container Terminal (CRCT) cancelled several Chinese railway shipments from late August to early September, and on December 1, Lithuania was removed from China's customs system, preventing the country's goods from entering China. After Lithuania's appeal to the EU, it was restored on December 7. But Lithuanian goods were again faced with lengthy customs clearance and procedure delays, resulting in many losses for Lithuanian companies. Although the unofficial boycott caused Lithuanian goods to suffer a 91% year-on-year decline of exports to China in December 2021, Lithuania's economy was not seriously affected since its dependence on the Chinese market is

quite low — exports to China account for only 1% of total exports, and imports from China account for only 5%.[4]

Since the end of October 2021, it has been reported that China has demanded a number of multinational companies, such as German tire maker Continental AG, to stop selling their products or sourcing supplies in the Chinese market if they continue to use Lithuanian parts and products,[5] while companies from Germany, France, Sweden, and other countries are unable to gain clearance from Chinese customs because their goods contain parts and machinery from Lithuania. The German-Baltic Chamber of Commerce informed the Lithuanian Foreign Minister and the Minister of Economy that the import of machinery and parts from China and the export of Lithuanian products to China had been suspended, urging Lithuania to mend its relations with China or they would withdraw from Lithuania. Between December 2021 and January 2022, Lithuanian Prime Minister Ingrida Simonyte and President Gitanas Nauseda were also told in meetings with top business executives that the situation would continue to deteriorate if the dispute with China was not resolved. This was the first time that China, leveraging its enormous market and economic power, asked European companies to sever their ties with Lithuania. The pressure from Beijing caused European companies, which are in the same EU alliance with Lithuania, to oppress Lithuania for their own interest; this has not only put even larger pressure on Lithuania but also divided the unity of the EU.

### 2-3. China denies all economic coercion to circumvent WTO sanctions

Unlike diplomatic reprisals or downgrades that require an official note, Beijing's approach to economic

4. Lithuanian statistics show that in 2020 the country exported 358 million USD goods to and imported 1.34 billion USD goods from China. According to the Chinese customs statistics, in 2020 China exported 1.808 billion USD to Lithuania and imported 488 million USD. China's surplus with Lithuania had amounted to 1.32 billion USD.
5. On December 9, 2021, Lithuanian Deputy Foreign Minister Mantas Adomenas told Reuters that China had sent a message to multinational companies that they would no longer be allowed to sell to the Chinese market or receive Chinese supplies if they use Lithuanian parts and supplies. Some companies have already cancelled their contracts with Lithuanian suppliers. See John O'Donnell and Andrius Sytas, "Exclusive: Lithuania Braces for China-led Corporate Boycott," *Reuters*, December 9, 2021, https://reurl.cc/12OE7G.

coercion has always been subtle and elusive. On December 24, 2021, Chinese Foreign Ministry spokesperson Zhao Lijian stated that it was not true that China had removed Lithuania from its customs declaration system, suspended Lithuania's import licenses, nor pressured multinational companies not to use Lithuanian parts, claiming that China always abides by World Trade Organization (WTO) rules. On December 27, the Global Times also quoted Chinese customs and industry sources as saying that Beijing had not blocked Lithuanian goods at all, but that Chinese companies had cut off their dealings with Lithuanian companies due to the rising domestic calls for punishment.

China has tried to force some specific countries to change their positions through economic coercion, but in practice it used tactics to avoid implementing them through open or official measures in order to circumvent WTO constraints and sanctions. Without strong supporting evidence, the WTO will find it difficult to impose sanctions on China. China's malicious behavior will remind countries that they must be prepared to take unpredictable risks when dealing with China's authoritarian system.

## 3. Trend Observation

Although Lithuania's Foreign Minister still insists on supporting Taiwan and says there is no plan to change the official name of the Taiwanese Representative Office, the President of Lithuania raised the issue of renaming the office twice in January this year, indicating the enormous pressure Lithuania is facing.[6] Despite the EU declaring its support for Lithuania, most European countries have not explicitly expressed their attitude. Miriam Lexmann, a member of the European Parliament

6. There are still views within Lithuania that the name change of the Taiwan Representative Office will help improve relations between Lithuania and China. But an editorial in the Global Times on January 26, 2022 pointed out that a name change will not solve the problem, and that at least the following four things must be done to stop the damage to relations between the two countries: 1. the name and activities as well as the nature and manner of such activities of the Taiwan Representative Office must return to the framework promised by Lithuania at the time the two countries established diplomatic relations; 2. Lithuania publicly apologizes to China for the previous mistakes and declare that the relationship between Taiwan and Lithuania is civil only; 3. reaffirm the "One-China principle" and ensure in a credible manner that this political bottom line will never be challenged; 4. take actions to eliminate the adverse effects in the EU and the international community. See "Editorial: Lithuania is Releasing a Probing Balloon of Political Speculation," *Global Times*, January 26, 2022, https://reurl.cc/02Wl6b.

from Slovakia, initiated a public letter in Parliament urging the EU to take concrete action against China, but this letter was signed by only 40 out of 700, or 5.7%, European parliamentarians.[7] This means that the EU's pursuit of a "coherent foreign policy" is extremely difficult and even gives China an opportunity to divide Europe.

### 3-1. EU sanctions or "anti-coercion measures" legislation may not help

On January 27, 2022, the EU filed a complaint against China at the WTO, emphasizing that the "discriminatory trade practices" adopted by China have affected the entire EU supply chain and violated a number of international agreements such as the General Agreement on Tariffs and Trade (GATT). The US, Australia, the UK, Canada, Japan, and Taiwan have all announced that they will participate in the case. However, the WTO dispute resolution mechanism calls for bilateral consultations and dispute resolution panels, with the former taking as long as 30 days and the latter possibly up to 9 months, making the procedure quite time-consuming. Even if the EU wins the preliminary ruling, China can still file an appeal, and the whole case may last several years.

In December 2021, the European Commission proposed the Anti-Coercion Instrument (ACI) bill to counter coercion by non-EU countries against its members, as the EU needs an effective tool to contend with economic coercion.[8] However, since the bill requires the approval of the European Parliament and the Council of the European Union, in addition to the consent of the majority of the 27 EU members, the legislation would take a long time from review to completion. The French Presidency of the EU in the first half of 2022 has indicated that would like to act against economic coercion in advance of the establishment of ACI, but the details are not known at this time.

7. Mindaugas Laukagalis, Justina Ilkevičiūtė, "'What Have You Done?' Why the EU is Slow to Shield Lithuania from Chinese Pressure," *LRT*, January 24, 2022, https://reurl.cc/AK3Lr3.
8. On December 8th, 2021, the European Commission introduced the "Anti-Coercion Instruments" bill. The bill includes 12 countermeasures, including tariff and quota increases, market access suspension, intellectual property rights blocking, and expulsion from EU financial markets to promptly respond to or deter economic coercion by third-party countries, such as China and Russia, against any EU member state. See "EU Strengthens Protection Against Economic Coercion," Press Release, *European Commission*, December 8, 2021, https:// reurl.cc/akMzeG.

### 3-2. Self-help and "naming and shaming" may be effective

Faced with the strong threat from China, the Lithuanian parliament and government have not only assisted enterprises in distress through diplomatic channels but also discussed the establishment of a fund to protect local companies from Chinese retaliation. They also discussed with affected companies the financial assistance from the government while attempting to develop new trading markets.[9]

For instance, the US has reached a US$600 million export credit cooperation agreement with Lithuania and has repeatedly declared its strong support for the country. Taiwan has also strongly supported Lithuania by sending economic and trade missions, purchasing Lithuanian black rum and a container of milk rejected by China, and setting up a US$200 million Middle/East Europe Investment Fund as well as a US$1 billion financing fund. The US, Australia, the UK, Canada, Japan, and Taiwan also joined the European Union's lawsuit against China with "naming and shaming" the latter for its despicable economic coercion. Only strong countermeasures from united like-minded countries can deter Beijing from repeating the same tricks in the future.

9. John O'Donnell and Andrius Sytas, "Exclusive: Lithuania Braces for China-led Corporate Boycott," *Reuters*, December 9, 2021, https://reurl.cc/12OE7G.

**Table: Chronology of deterioration between Lithuania and China since 2021**

| Date | Key Events | Description |
|---|---|---|
| February 9, 2021 | Xi Jinping hosted the China-Central and Eastern Europe Leaders' Video Summit (17+1 Cooperation Summit). | Lithuania was represented only by ministerial-level officials. |
| March | Lithuanian Parliament agrees to withdraw from "17+1 Cooperation". | |
| March | Lithuanian Parliament agrees to the opening of Taiwanese Representative Office in Lithuania. | |
| May 20 | Lithuanian Parliament passes a resolution condemning China's "genocide" of Uighurs, calling on the UN to investigate Xinjiang re-education camps, and urging China to repeal Hong Kong's National Security Law. | Tomas Ivanauskas, cultural counsellor at the Lithuanian Embassy in China, noted that cultural and artistic events in China have been cancelled or suspended since May. |
| May 22 | Lithuania's Foreign Minister officially announces the country's withdrawal from the "17+1 Cooperation". | Chinese Foreign Ministry said on May 24 that "the China-Central Eastern European Countries Cooperation... has been fruitful in the past 9 years and will not be affected by individual incidents." |
| July 20 | Lithuania agrees to the establishment of the Taiwanese Representative Office in Lithuania, the first in Europe under the name of "Taiwanese". | The Chinese Foreign Ministry said "China is firmly opposed to any form of official exchanges between diplomatic allies and Taiwan, and to the establishment of so-called 'representative offices' between diplomatic allies and Taiwan." |
| August 10 | Chinese Ministry of Foreign Affairs recalls its ambassador to Lithuania and requests the latter to recall its ambassador to China. | The Ministry of Foreign Affairs of Lithuania expressed regret and reiterated its determination to develop mutually beneficial relations with Taiwan under the principle of one China. |

| | | |
|---|---|---|
| August 17 | Media reveals that China National Railway Group's China Railway Container Terminal (CRCT) will interrupt direct rail shipments to Lithuania in August and September. | Lithuanian State Railways confirmed that several Chinese shipments were cancelled from the end of August to the beginning of September. |
| September 3 | Lithuania recalls its ambassador at the request of China. The embassy is operating normally with the chargé d'affaires ad interim acting as the agent for foreign affairs. | |
| September 23 | Lithuanian Ministry of Defense's National Cyber Security Center reports that China's Xiaomi flagship phone has a speech censorship feature and Huawei's P40 5G phone has a security vulnerability, advising users to discard the phones and consumers to avoid buying them. | |
| Since late October | China has asked several multinational companies, including Continental of Germany, to sever their ties with Lithuania. If they continue to use Lithuanian parts and products, China will stop them from selling products or sourcing supplies in China. | Companies from Germany, France, and Sweden have reported that their cargoes were intercepted at Chinese ports and could not be cleared because they contained parts and machinery made in Lithuania. |
| November 18 | "Taiwanese Representative Office in Lithuania" officially opens in Vilnius, the capital city. | On November 19, the Chinese Foreign Ministry expressed its strong protest and resolute opposition, saying that Lithuania "has taken the blame and will have its own consequences." |
| November 21 | China downgrades diplomatic relations with Lithuania to the level of chargé d'affaires. | |
| November 25 | Chinese Embassy in Lithuania suspends its consular operations. The following day, the Chinese Embassy changes its name to the Chargé d'affaires and requests Lithuania to change the name of its diplomatic missions accordingly. | |

| | | |
|---|---|---|
| December 1 | Chinese customs removes Lithuania from the system, effectively banning Lithuanian goods from being exported to China. | The media revealed this the next day, and the Chinese customs system is quietly restored four days later. |
| December 15 | All 19 Lithuanian diplomats and their families in China leave Beijing, including Chargé d'affaires Audra Čiapienė. Diplomatic affairs with China are being conducted remotely. | |
| In December | Chinese customs allegedly refuse clearing Lithuanian goods and reject Lithuania's import applications. | Taiwan Tobacco and Liquor Company bought 20,000 bottles of Lithuanian Rum staying at sea and Good Land Food & Tech. Company bought a container of milk. |
| February 9, 2022 | China's General Administration of Customs notifies Lithuania that it will stop accepting import declarations for Lithuanian beef shipments starting February 9, citing a "lack of proper documents". | |

Source: Compiled by author based on public information.

(Originally published in the 48th "National Defense and Security Biweekly", February 25, 2022, by the Institute for National Defense and Security Research.)

(The contents and advice in the assessments are the personal opinions of the authors, and do not represent the position of the Institute for National Defense and Security Research.)

# What Russia's Hybrid Warfare in Ukraine Reveals for Taiwan

**Shiau-shyang Liou**
**Associate Research Fellow**

Division of National Security Research

## 1. News Highlights

On February 21, 2022, Russian President Vladimir Putin declared Ukraine an inseparable part of Russia and signed an order recognizing the Donetsk People's Republic and the Luhansk People's Republic. Putin also called on the Ukraine authorities to cease hostile acts against the two "countries", or else they would have to assume all responsibility for any subsequent bloody conflict.[1] The Russian army then moved into the eastern region of Ukraine under the guise of "peacekeeping," which the US deemed to be equivalent of an invasion. Russia then announced the establishment of diplomatic relations with the Donetsk People's Republic and the Luhansk People's Republic. For now, there is still no light at the end of the tunnel regarding the escalation of the conflict.

The crisis in Ukraine, which has been heating up again since October 2021, can be traced back to the Russo-Ukrainian War in 2014. The Russian Federation annexed Crimea without a fight and caused the declaration of independence of the Donetsk People's Republic and the Lugansk People's Republic in the eastern region of Ukraine, resulting in the division of the country. However, the war did not end there as Russia still continued to wage hybrid warfare against Ukraine. Since

1. "Обращение Президента Российской Федерации," Президент России, 21 февраля 2022, http://kremlin.ru/events/president/news/67828; Ilya Tsukanov, "Russia Recognises Donbass Republics' Independence," *Sputnik International*, February 21, 2022, https://sputniknews.com/20220221/russia-recognises-donbass-republics-independence-1093241178.html.

the Chinese PLA is deeply influenced by Russian military thought,[2] and there is a possible chain effect to China-Taiwan relations in the similarities from the Russia-Ukraine situation, it is necessary to look into Russia's hybrid warfare in Ukraine in preparation of a similar situation in cross-Strait relations.

## 2. Security Implications

Russia's hybrid warfare against Ukraine has been a long-running operation. It was in the making long before the 2014 Crimean Crisis and the Donbas War, and it has continued to wage hybrid warfare since then. The following is a list of important points that can be compared to the situation of cross-Strait relations.

### 2-1. Grey zone tactics

Russia's hybrid warfare against Ukraine is most widely known for its operation of unidentified covert armed personnel in green uniforms, dubbed "little green men", to carry out "strategic deception" to annex Crimea through deceptive drills, delivery of "humanitarian supplies", and other cover-up operations. Russia has also used this grey zone tactic in eastern Ukraine while consistently denying outside accusations; Russia even used civilian security companies to cover up its military intervention. On February 21, 2022, Russia sent troops into the pro-Russian region of eastern Ukraine under the guise of "peace-keeping" to camouflage its military operations.

At this stage, China's military aircraft incursions into Taiwan airspace are most similar to such actions by Russia. The moves not only can exert pressure on Taiwan but also spy on Taiwan's air defense capability; these make up China's "battlefield management" in that while conducting "strategic deception" it can, if required, be immediately transformed into a military invasion. On February 5, 2022, there was another incident in which a Y-12 civilian transport plane approached Taiwan's ADIZ in Dongyin Island, indicating that China's means of grey zone

2.For more than a decade, Russian and Chinese military exercises have been conducted in the Russian language using common codes from the Russian command system, a tacit understanding has developed between the two sides; and a large number of PLA officers also studied in Russia to adopt the latter's traditions, strategies, and tactics of the Russian forces.

tactics are not limited to military aircraft.

### 2-2. Information warfare

Today, many people consider hybrid warfare a description of the unconventional and conventional warfare waged by Russia against Ukraine; in fact, the term was first used in the US and was seen by Russia as a way to promote a "color revolution" in the former Soviet Union countries to contain Russia. However, the widespread outbreak of color revolutions has exposed that, although Russia is relatively powerful in terms of politics, economics, and military in the former Soviet Union territory, its political system is far less attractive or appealing to others. Portrayed as an aggressor by the West during the Caucasus War with Georgia in 2008, Russia reorganized its state propaganda machine and established Russian state-owned news agency Sputnik International during the Ukraine crisis in 2014 to launch a strong anti-Kyiv, anti-Western information warfare. Sputnik International not only spreads disinformation to vilify the Ukrainian authorities, accuses the West of manipulating the relationship between Russia and Ukraine, but also stresses that Russia is being persecuted by NATO's eastward expansion to win the approval and support of the Ukrainian people and the rest of the world — this tone has continued to this day. Moreover, Russia is good at creating and disseminating indistinguishable information to confuse the world. For example, during the Crimean crisis in 2014, Russia said that it was invited by exiled former Ukrainian President Viktor Yanukovych to send troops to protect Ukraine; in May 2021, Russian troops participating in an exercise near the border with Ukraine left their heavy equipment behind and returned to their base to create the illusion of being unaggressive; and Putin openly stated that he did not want war when some of the troops participating in the exercise returned to their barracks. However, it's just another deception and the same aggression happens again.

China's information warfare against Taiwan also bears similarities. After Xi Jinping took office, he continued to promote the "grand external propaganda" to enhance the positive international image of the CCP and China; and he continues the "one-China" principle and opposition to Taiwan independence while promoting reunification. In terms of tactics, in addition to the continuous defamation of

current Taiwanese authorities, the CCP also focuses on attracting groups such as small or medium-sized enterprises, people of central and southern Taiwan, working classes, and younger generations; and it also uses Taiwanese media as its propaganda agents to disguise its psychological infiltration. In addition to the common "united front" propaganda, China also attempts to disturb the morale of Taiwanese people through disinformation. For example, in November 2020, a disinformation stating that a Taiwanese F-16 fighter jet had landed at China's Xiamen Airport appeared on the Internet immediately after the plane went missing during a training mission.

### 2-3. Division through "united front"

After the annexation of Crimea and the division of Ukraine, Russia has continued its "united front" strategy to further divide Ukraine. One of the tricks is issuing Russian passports to Ukrainian citizens. The threshold for foreigners to become Russian citizens is quite high, as they must not only master the Russian language but also give up their original nationality; however Russia has lowered the bar for Ukrainian people. The move is considered to strengthen the separatist forces in Ukraine so that Russia can intervene with force in the future. On February 21, 2022, Russian troops were sent to the eastern states of Ukraine to "protect the local Russians." Since Russia has always committed to the protection of Russians abroad, including Russian citizens, ethnic Russians, Russian speakers, and Orthodox Christians, the pro-Russian tendency in eastern Ukraine has become the basis for Russia's "united front" to divide Ukraine.

China has its own version of the strategy for Taiwan but is fine-tuned to meet the actual situation: the "31 Taiwanese Beneficiary Articles" issued in February 2018 provide citizen privileges to Taiwanese in China, while the "26 Actions" in November 2019 being a further enhanced version. Moreover, China has recently planned a new wave of offensive to divide the Taiwanese society by mobilizing well-known Taiwanese people who have moved their careers to China to declare their naturalization in China and give up their Taiwanese status and health insurance.

### 2-4. Fostering proxies

The fostering of proxies is one of

Russia's major hybrid warfare tactics, with the famous example of Vladimir Yanukovych, the ex-President of Ukraine, who left his country behind during the Crimea crisis in 2014. Russia's purpose of supporting proxies is to expand its influence over Ukraine and, if necessary, to become its own fifth column working from inside. On January 20, 2022, the US Department of State announced sanctions against four current and former Ukrainian officials, accusing them of spreading disinformation at the behest of Russia to destabilize the country.

Similarly, China also takes advantage of the openness of Taiwan's democratic society to foster pro-China forces. In response, Taiwan amended the "National Security Law" in June 2019 to plug up loopholes in other laws, stipulating that the people of Taiwan are not allowed to develop organizations for China; and enacted the "Anti-Infiltration Law" in January 2020 to prevent the infiltration and interference of foreign adversaries. However, given the invisible and hard-to-prove nature of hybrid warfare and the fact that Taiwan is a democratic society governed by the rule of law, it is a tough challenge to block all foreign infiltrations.

**2-5. Cyber warfare**

Before and after the 2014 Ukraine crisis, Russian cyberattacks on Ukrainian public sector continued unabated, which is believed to be associated with Russian hackers and intelligence services; and the popularity of Russian media and social software in the pro-Russian eastern and southern regions of Ukraine has also inevitably contributed to the Russian hybrid warfare offensive. Media coverage can conduct cognitive warfare on the audience, while the widespread use of Russian social software by the Ukrainian people contributes to the enrichment of the Russian database, which in turn facilitates big data analysis of user perceptions and preferences and assists in cognitive warfare against Ukraine. To address this, the Ukrainian authorities banned the transmission of Russian media and public access to such social network sites in May 2017 to defend against Russian cyber warfare.

Similar things happen between Taiwan and China. Due to exchanges and the need to live and work in China, Taiwanese people use a considerable amount of Chinese computer, communication, and consumer

electronics and websites, making Taiwan, like Ukraine, a testing ground for the opponent's cyber warfare. In January 2019, Taiwan announced the principle of banning Chinese computer, communication, and consumer electronics, WeChat service, and Chinese websites such as Baidu in the public sector. At the end of 2021, the public sector is banned from all Chinese computer, communication, and consumer electronics.

The Chinese has been launching countless cyberattacks against Taiwan. They are not only targeting the public sector but also academics or private citizens they are associated with, to steal secrets. The PLA has set up the Strategic Support Force after the military reform, but the real situation is largely unknown due to its secrecy; but the discovered Base 311 in Fuzhou, Fujian Province, is believed to aim at cyber attacking Taiwan. Although Taiwan has also established the Information, Communications and Electronic Force, with a democratic nature, in contrast to China's closed and censoring environment, the restriction and imbalance in the cyberspace environment are Taiwan's disadvantage in defense and countermeasure in cyber warfare.

## 3. Trend Observation

From the comparison and analysis above, we can see that Russia's hybrid warfare in Ukraine has inspired China to a certain level, and it is possible that China will refine the Russian hybrid warfare model and apply it to Taiwan. The following discussion offer several possible inferences for Taiwan to have an in-depth view and prepare for possible scenarios.

### 3-1. China's grey zone tactics toward Taiwan will be more diversified and expanded

Hybrid warfare is an operation of undeclared war, and the grey zone tactic is one of its core techniques that makes the victim country lower its guard or even be caught off guard. In China's current grey zone tactics, the most threatening one is sending military aircraft to approach or circumnavigate Taiwan since the moves can be converted into invasion operations at any time. The recent approach of the Y-12 transport aircraft to Taiwan's Dongyin Island proves that China has begun to experiment with a variety of grey zone tactics against Taiwan using non-military aircraft or vessels in attempts to make Taiwan less wary, just as the people of Kyiv were accustomed to the

pressure from Russian forces. Since the PLA's amphibious landing capability is still immature, it's yet to have either the confidence to defeat the US in naval or air combats in the Taiwan Strait, or to conquer the Taiwan island; however, the outlying islands are shrouded in the shadow of China's grey zone tactics, and the risk of being attacked is likely to rise due to China's internal instability and desire to shift focus from any domestic troubles.

### 3-2. Hybrid warfare will be trend of future conflicts

Russia's hybrid warfare against Ukraine is not only to prevent the latter from joining NATO but also to expect it to rejoin Russia someday; this is the reason why Russia oppresses Ukraine but patronizes it at the same time. China and Russia are very similar in terms of such objectives. Observed from the long history of the Russia-Ukraine conflict, hybrid warfare is actually Russia's response to the similar warfare ("color revolution") launched by the West against it, and then evolved into Russia's own counterpart of the strategy. Facing the Russian version of hybrid warfare tactics, Western countries are also trying to create proper countermeasures. Take the recent crisis in Ukraine as an example, the US revelation of Russia's possible attack timing on Ukraine may not only be a means to disturb Russia but also a way to counteract it, which means using "disinformation" to counter the grey zone tactics. At a time when China is constantly using grey zone tactics against Taiwan as hybrid warfare could become prevalent in future conflicts, Taiwan can also think about how to resist China in the same way.

### 3-3. China's "naturalization campaign" may divide Taiwan's unity, but not effective for military intervention

Currently, Taiwan does not allow its citizens to obtain Chinese ID cards or Chinese passports, and violators will be subject to revocation of their Taiwan household registration, ID cards, and passports. Therefore, even if China were to issue Chinese ID cards or passports directly to Taiwanese citizens, that would not become a viable excuse for China to interfere in the internal affairs or even initiate military intervention toward other countries like what Russia did; but China will continue to divide Taiwan's social solidarity by offering economic incentives

in the form of citizen privileges. According to Taiwan's National Immigration Agency, the number of Chinese residents in Taiwan is about 21,000 as of December 2021,[3] and there are about 345,000 spouses from China as of June 2019.[4] The two types of immigrants take only a very small percentage of the total Taiwanese population, and they are hardly comparable to the number of ethnic Russians in Ukraine. Since Chinese residents and spouses must give up their original nationality before naturalization in Taiwan, it's clear that China cannot follow the Russian model of issuing passports while allowing dual citizenship for Ukrainians and use it as an excuse to "protect Russians abroad".

### 3-4. China keeps seeking proxies and expanding cyber warfare, Taiwan needs to find countermeasures

China's establishment of proxies in other countries is seen by the National Endowment for Democracy and some countries as a demonstration of "sharp power" similar to Russia's hybrid warfare tactics. Alerted to the threat posed by China in this area, Taiwan has amended the National Security Law and enacted the Anti-Infiltration Law; but since the legal proceedings would take considerable time, the laws might not be immediately effective in the prevention of such threats. Although Taiwan intended to amend the laws again in 2021, it was immediately criticized by Taiwan's pro-China media. This is a major difficulty Taiwan must overcome as a democratic country when resisting infiltration by foreign authoritarian forces, and it also provides a chance for China to keep seeking and cultivating its proxies in Taiwan. In this regard, in addition to enacting relevant laws and regulations to prevent this, Taiwan also needs to cultivate the awareness and correct understanding of all the people in order to effectively curb

3. In 2021, 7,422 people came to Taiwan from mainland China and 13,810 from Hong Kong and Macao for residence and emigration. For details, see "Statistics of the number of People from Mainland China, Hong Kong and Macao, and Nationals Without Household Registration Entering Taiwan for Residence and Emigration," *National Immigration Agency, Ministry of the Interior, Republic of China (Taiwan)*, December 3, 2021. https://www.immigration.gov.tw/media/74903/ 大陸地區人民 - 港澳居民 - 無戶籍國民來臺居留 - 定居人數統計表11012.xls.
4. "National Information Report (No. 152)," *National Statistics, R.O.C (Taiwan)*, August 14, 2019. https://www.stat.gov.tw/public/Data/9814162455MKFO31MR.pdf.

China's tactics of cultivating proxies.

Russia's hybrid warfare strategy shows that cyberattacks are not only a precursor to conventional military operations but also an adjunct to major attacks. There is no doubt that Taiwan will face the same threat in the future. Taiwan is already adopting information security measures similar to that which is practiced in Ukraine, aiming at preventing Chinese cyberwarfare targeted at the public sector, however, this only applies to the public sector so far. To further apply to the general public, it will require not only a perfect timing, but also raised awareness in information security.

(Originally published in the 48th "National Defense and Security Biweekly", February 25, 2022, by the Institute for National Defense and Security Research.)

(The contents and advice in the assessments are the personal opinions of the authors, and do not represent the position of the Institute for National Defense and Security Research.)

# Analysis of the Implications of the CCP's New Regulations to Strengthen Network and Data Management

**Chia-ling Hung**
**Assistant Research Fellow**

**Min-chen Tseng**
**Research Assistant**

Division of Cyber Security and Decision-Making Simulation

## 1. News Highlights

The Cyberspace Administration of China (CAC), together with 12 other departments, jointly revised and released the "Regulations on Network Security Review" ("Security Regulations") with 23 articles,[1] which take effect February 15, 2022. The Security Regulations include situations where the processing of data by network platform operators affects or may affect national security in the scope of review. The CAC, together with the Ministry of Industry and Information Technology (MIIT), the Ministry of Public Security, and the State Administration of Market Supervision, also jointly issued the "Regulations on the Recommendation of Algorithms for Internet Information Services" ("Algorithm Regulations") with 35 articles, which take effect March 1, 2022. It focuses on requiring technology enterprises to comply with business ethics and principles of fairness when implementing "algorithms," such as not using algorithms to create fake user accounts or create other false impressions,

1. The 12 departments include National Development and Reform Commission, Ministry of Industry and Information Technology, Ministry of Public Security, Ministry of State Security, Ministry of Finance, Ministry of Commerce, People's Bank of China, State Administration of Market Supervision, State Administration of Radio and Television, China Securities Regulatory Commission, State Secrets Bureau, and State Cryptography Administration. "State Internet Information Office and Other 13 Departments Revised and Issued 'Regulations on Network Security Review'," *Cyberspace Administration of China*, January 4, 2022, https://www.12377.cn/wxxx/2022/295c592b_web.html.

and all information must be filed with the CCP authorities within 10 working days.[2]

## 2. Security Implications

### 2-1. Strict review of listing overseas of online platforms

The CAC originally published the "Measures for Security Review of Internet Products and Services (for trial implementation)" in May 2017 and published the "Security Regulations (draft for comments)" in 2019, and formally promulgated the regulations in April 2020,[3] focusing on the "Critical Information Infrastructure" (CII) with a relatively simple scope. Only 15 months later, the Security Regulations were amended again to meet the implementation of the "Data Security Law" on September 1, 2021. The new version of the Security Regulations added "Internet platform operators" and "critical information infrastructure operators" as two key targets for scrutiny, and listed three "shall" and one "must" (as shown in the attached table) to emphasize that "overseas listing of platforms with user data of millions is subject to 'cybersecurity examination'". The "examination" focuses on the risk of critical core data or massive personal information being influenced, controlled, or maliciously manipulated by foreign governments before and after the enterprise goes public abroad, which could "affect or may affect national security". Since the new Security Regulations do not specify which industries and the scope of scrutiny, they would apply to almost all large Internet and technology-related enterprises in China; and it will take longer than before to determine whether national security is affected in terms of regulations and business perspective, causing a lot of anxiety for online platform enterprises that wish to go public abroad.

### 2-2. Controlling online opinions through strict scrutiny of algorithm business model

As the world economy becomes

2. Regulations on the Recommendation of Algorithms for Internet Information Services," *People.com*, January 4, 2022, http://politics.people.com.cn/BIG5/n1/2022/0104/c1001-32323657.html.
3. Regulations on Network Security Review Require Online Platforms with Over a Million Users Must File for Security Review Before IPO Abroad," *China Times*, January 4, 2022. https://www.chinatimes.com/realtimenews/20220104001732-260409?chdtv.

"Internet platform-centric", the CCP is aware of the common problems of Internet platforms using algorithms to censor information, make excessive recommendations, manipulate search results and rankings, and forged "likes" as well as "shares" that seriously affect online opinions. In order to keep the chaos under control, the CCP promulgated the Algorithm Regulations that monitor a wide range of technology companies that provide algorithm recommendation services, such as food delivery, taxi hailing, and e-commerce, and prohibit these platforms from evading supervisory and management responsibilities by claiming "technology neutrality".[4] In addition, online platforms are required to inform users of the status of their recommendation services in a conspicuous manner, and to file the platforms with "public opinion attributes" or "social mobilization capabilities" in the hope to solve the long-term data transparency and misuse problems through this "general disclosure" and "selective filing" approach.[5] Although the CCP claims that the purpose of the new regulations is to promote fairness and transparency in online recommendation services and stipulates that service providers should "adhere to mainstream values" and "actively communicate with positive energy" to the information consumers, but in fact, it's giving warning messages to online media companies: they should avoid spreading opinions unfavorable to the state or manipulating information to influence people's judgment, which will be seen as disrupting public order by indirectly challenging "ideological security" and even attempts to challenge the ruling power of the CCP.

4. In Chapter 2, Article 6: "Regulations on Network Security Review" proposes that providers of big data computing recommendation services should "adhere to the mainstream value actively communicate with positive energy"; Article 7: "clarify the main responsibility of algorithm recommendation service providers" to build a platform accountability system; Article 9: "establish a functional feature database for identifying illegal and undesirable information".

5. Chapter 4, "Supervision and Management," requires that providers of big data computing recommendation services with "public opinion attributes" or "social mobilization capabilities" should provide information to the CCP authorities within 10 working days from the date of service provision, and cooperate with the authorities to carry out "security assessment" as well as "supervision and inspection work" in Article 24.

## 3. Trend Observation

### 3-1. Chinese companies caught in confrontation between China and US

In the first half of 2021, 35 Chinese companies went public on the US stock market with a record-high US$12.3 billion raised in financing.[6] However, the CCP authorities have been conducting cybersecurity audits to Didi Chuxing Technology, Full Truck Alliance Group (a truck-matching information platform), and BOSS Recruiting (a recruitment website and mobile phone app) on the grounds of "national security" since July 2021. In the second half of the year, under pressure from the CCP, Little Red Book (an online shopping and social networking platform), Hello Inc (a bike-sharing service provider), Qiniu Cloud (a cloud computing company), and Keep (a fitness app) withdrew their US IPO (or fundraising/stock offering) plans; and Himalaya (an online audio sharing platform) as well as Huolala (a logistics business) simply cancelled their IPO plans in the US. The Security Regulations further underline the CCP regulators' restrictive attitude towards overseas IPOs. Since the CCP has data collection methods and regulations that are different from or even contradict those of other countries, overseas companies are also forced to make choices under the CCP's strict data security regulation framework. For example, LinkedIn, a talent social networking site, and Yahoo, a search engine company, withdrew from the Chinese market or changed their business direction in October 2021 due to "changes in the business environment".[7]

While the CCP tightens its control over data, the US is also becoming more stringent on incoming Chinese companies. The US Securities and Exchange Commission (SEC) officially announced the implementation of the Holding Foreign Companies Accountable Act (HFCAA) on December 2, 2021, which requires foreign companies listed in the US to file documents with the SEC to prove

6. "Chinese stocks in the US set off a second listing in Hong Kong," *Economic Daily News*, July 8, 2021. https://money.udn.com/money/story/11038/5585910.
7. "LinkedIn to Shut Down Service in China, Citing 'Challenging' Environment," *New York Times* Chinese, October 15, 2021

that they are not owned or controlled by foreign governments.[8] The more a Chinese company listed abroad is subject to the jurisdiction and investigation of foreign regulators, the more likely it will be also subject to cybersecurity scrutiny by Chinese regulators for "national security" reasons, which will further affect its trustworthiness overseas, creating a vicious cycle. The new regulations are expected to make it extremely difficult for Chinese companies, especially those in the Internet industry, to list on the New York Stock Exchange (NYSE) or Nasdaq in the future.[9] Ordained by Chinese President Xi Jinping, the official opening of the Beijing Stock Exchange on November 15, 2021, is intended to urge Chinese companies to leave the US and list locally instead to facilitate the financial disconnection between the US and China and create a "Chinese Nasdaq". The new regulations do not prohibit listing in Hong Kong since the city is not considered a foreign territory under the "one country, two systems" concept, a large number of Chinese technology giants may give priority to listing in Hong Kong to be exempted from cyber security scrutiny. Under such a policy, it is expected that more Chinese companies will choose to stay domestic or list in Hong Kong; but Hong Kong is not what it used to be, it remains to be seen whether Chinese technology enterprises can really stay under the cybersecurity radar of the CCP.

### 3-2. Effectiveness of first algorithm regulations remain to be seen

With the widespread use of artificial intelligence (AI), Internet companies turn information of millions of users into product recommendations through sophisticated algorithms to generate enormous profits today. In recent years, governments including the US and India have attempted to enact regulatory measures to prevent AI abuse but were caught in a legislative stalemate; and most countries hesitate to impose

8. "International Economy: SEC Finalizes Accountability Law for Foreign Companies, Didi Announces Delisting from the US," *China Times*, December 3, 2021
9. "Beijing Stock Exchange Opens with 81 Companies in First Transactions," *Radio France Internationale*, November 15, 2021. https://www.rfi.fr/tw/ 中國 /20211115- 北京證交所開張 -81 家企業首批交易。

punitive regulations as they might hinder economic growth and technological innovation. Europe was once a pioneer in data-related legislation that regulates large US technology companies, but now the EU countries are still exploring the regulation for AI technology due to different economic constraints and regulatory concepts. Since the end of 2020, the CCP has launched a series of crackdowns on online enterprises, such as financial services, taxi services, and data management, and started to conceive control plans for algorithms in September 2021. It's the world's first systematic legal document for such regulations and has attracted attention from the international community.

The CCP had previously adopted a successful European approach to data regulation; but with the release of China's first governance regulation focusing on algorithms, it is clear that its legislature has explored new possibilities that Europe and the US will be closely observing the effectiveness of the CCP's subsequent regulation. In particular, Chapter 3 of the Algorithm Regulations on user rights protection followed the common consumer consensus to provide the "right to know" about the status of recommendation services, and the "right to choose" to turn off recommendation services without providing personal information. If the implementation of Algorithm Regulations is a success, the US and European countries may consider adopting this approach to some extent. For the development of AI technologies such as algorithms , however, an open, innovative Internet environment and a free, tolerant atmosphere are crucial. Although data is a key resource for computing power to evolve, technology platforms in China are still receiving more restrictions on data processing as the Chinese authorities constrain the environment of innovation and cut incentives for technology development for local consumer technology companies. To China's goal of becoming the world's technological powerhouse, this is contradictory.

**Table: The key amendments of the Security Regulations**

| | |
|---|---|
| Article 2<br>Article 5<br>Article 6<br>Two key targets for scrutiny | 1. Critical information infrastructure operators:<br>(i) The purchaser of network products and services should anticipate the national security risks that may arise after they are put into use.<br>(ii) Products and services that affect or may affect national security should be reported to the Office of Network Security Review for examination.<br>(iii) For procurements applied for cybersecurity audits, critical information infrastructure operators should require product and service providers to cooperate with cybersecurity audits through procurement documents, agreements, and other papers. |
| | 2. Internet platform operators:<br>Overseas listing of platforms with user data of over one million must declare cybersecurity examination. (Article 7) |
| Article 8<br>4 types of review filing Materials | 1. Declaration forms<br>2. Analytic reports on products that affect or may affect national security<br>3. Procurement documents, agreements, contracts to be signed or listing application documents to be submitted for IPO<br>4. Other materials needed for cybersecurity audits |
| Article 10<br>7 types of reviews focused assessment of national security risk factors | 1. Risks of illegal control, interference or damage to the critical information infrastructure from the use of products and services.<br>2. Risks of disruptions in the supply of products and services could jeopardize the business continuity of critical information infrastructures.<br>3. Security, openness, transparency, diversity of sources, reliability of supply channel, and risk of supply disruption due to political, diplomatic, and trade factors.<br>4. Compliance of product and service providers with Chinese laws, administrative regulations, departmental rules and regulations.<br>5. Risk of theft, leakage, destruction, illegal use, or illegal exit of core data, important data, or large amounts of personal information.<br>6. Risk of product sales causing critical information infrastructure, core data, important data or a large amount of personal information to be influenced, controlled or abused by foreign governments, as well as the risk of network information security.<br>7. Other factors that may jeopardize the security of critical information infrastructure, network security and data security. |

Source: "Regulations on Network Security Review," Cyberspace Administration of China, January 4th, 2022. http://www.cac.gov.cn/2022-01/04/c_1642894602182845.htm.

(Originally published in the 48th "National Defense and Security Biweekly", February 25, 2022, by the Institute for National Defense and Security Research.)

(The contents and advice in the assessments are the personal opinions of the authors, and do not represent the position of the Institute for National Defense and Security Research.)

# Deterrence by Detection: US Warnings for Russia-Ukraine Conflict

**Jyun-yi Lee**
**Associate Research Fellow**

Division of National Security Research
Keywords: Russia, Ukraine, Deterence_by_Detection

On February 11, 2022, international media reported that US Central Intelligence Agency (CIA) and Pentagon alerted NATO members that Russia could invade Ukraine as soon as February 16. The US allegedly had obtained detailed information about the routes of individual Russian military units in Ukraine and their role in the conflict, and it was considering disrupting Russia's operations through publicizing the latter's plans. Meanwhile, US National Security Advisor Jake Sullivan said at a press conference on February 11 that the risk of conflict was so imminent that US citizens should evacuate as soon as possible but stressed that this did not mean that Russian President Vladimir Putin had decided to go to war. In subsequent interviews, neither Sullivan nor Defense Department spokesman John Kirby would confirm reports that Russian forces would take action on February 16.[1]

The information available did not yet support the credibility of the US claim that a conflict between Russia and Ukraine was imminent, but it could have

1. News about the Russian actions against Ukraine on as soon as February 16 can be found in: Maik Baumgärtner, Matthias Gebauer, Martin Knobbe and Fidelius Schmid, "CIA Rechnet Mit Russischem Angriff Kommende Woche," *Der Spiegel*, February 11, 2022, https://tinyurl.com/bdhrhd36; Alexander Ward and Quint Forgey, "Putin Could Attack Ukraine on Feb. 16, Biden Told Allies," *Politico*, February 11, 2022, https://tinyurl.com/2p9abtvp. For Jake Sullivan's address in The Whitehouse press conference, see "Press Briefing by Press Secretary Jen Psaki and National Security Advisor Jake Sullivan, February 11, 2022," *The White House*, February 11, 2022, https://tinyurl.com/2p97kaum. The news report regarding Jake Sullivan and John Kirby, see: David Lawder and David Lawder, "U.S. Officials Won't Confirm Reports on Possible Russia Invasion of Ukraine on Wednesday," *Reuters*, February 13, 2022, https://tinyurl.com/2s9b5k6c.

been a demonstration of US "deterrence by detection". The concept was developed by a US think tank, with Marine Corps Commandant David Berger as one of the main proponents. Berger advocates that the US military should apply the concept to the current tensions between Russia and Ukraine. Media commentary has also pointed out that the US government has revealed possible Russian actions several times since December 2021; while the government agencies did not explicitly use the concept, it is actually applied in their practice.[2]

## US military emphasizes "situational awareness" to shape information environment

One of the lessons learned from US counterterrorism operations since 2001 and the Russian annexation of Crimea in 2014 is the importance of controlling and shaping the information environment. With the advent of information and communications technology and the rise of new media of all kinds, both state- and non-state actors have been able to develop narratives in their favor to gain support from certain populations or/and to undermine their rivals. In the 2014 Ukraine crisis, Russian used disinformation to shift outsiders' focus from its military actions and launched a media war to denigrate the legitimacy of the Ukrainian government, emphasize the danger to the ethnic Russian population in Ukraine, and forge public opinion that both Russian and Ukrainian people support Crimea joining Russia. Partly because of this, the US has increasingly emphasized the importance of gaining an information advantage, so that its decision-making can be aided by the enhancement of "situational awareness." "Deterrence by detection" can be seen as an extension to this development.

Originally developed by a US think tank in response to the "grey zone conflicts" initiated by China and Russia, the core of the "deterrence by detection" concept is to fully acquire and then reveal the opponent's every move, so the

2. Justin Katz, "US Should Pursue 'Deterrence By Detection,' Says Marine Corps Commandant," *Breaking Defense*, September 1, 2021, https://tinyurl.com/34r4ph4p; Justin Katz, "Berger Calls for 'Deterrence by Detection' in Light of Russia-Ukraine Tensions," *Breaking Defense*, February 8, 2022, https://tinyurl.com/4au3n7wb.

opponent thinks twice before acting rashly. In other words, it is a "name and shame" strategy. The think tank advocating this concept of warfare emphasizes the deployment of the intelligence, surveillance, and reconnaissance (ISR) network, especially the extensive use of drones.[3] It is yet to know whether the US military has used a large number of drones in the Ukraine crisis, but some of the US government's actions to "call out" the Russian operations can be seen as the implementation of "deterrence by detection."

## US deterred Russia by revealing intelligence

Since January 2022, the US has warned several times that Russia intends to legitimize its actions against Ukraine through "false flag" operations that made up false facts (such as videos) that Ukraine was the first to attack Russian forces or pro-Russian rebels in Ukraine.[4] If such scenarios were to happen after the US made such accusations, the outside world would question their authenticity regardless of whether they were orchestrated by Russia. The legitimacy of the Russian efforts to escalate would then be seriously undermined. On February 7, the media reported that US officials had leaked allegedly intercepted internal Russian conversations, in which Russian intelligence and military officials expressed doubts about the effectiveness of a large-scale invasion of Ukraine and complained that their plans had been publicly revealed by the West.[5] The US move, along with the aforementioned

3. Thomas G. Mahnken, Travis Sharp and Grace B. Kim, "Deterrence by Detection: A Key Role for Unmanned Aircraft Systems in Great Power Competition," Center for Strategic and Budgetary Assessment (CSBA), 2020, https://tinyurl.com/38sft4wd; Tzuli Wu, "Deterrence by Detection: the Embodiment of US's "Integrated Deterrence" Concept," *National Defense and Security Biweekly,* Issue 45, January 7, 2022, https://tinyurl.com/33dkv4ee

4. "Russia-Ukraine: US Warns of 'False-flag' Operation," *BBC News*, January 14, 2022, https://tinyurl.com/2p99fy52; Natasha Bertrand and Jennifer Hansler, "US Alleges Russia Planning False Flag Operation Against Ukraine Using 'Graphic' Video," *CNN*, February 4, 2022, https://tinyurl.com/2p8e4rzz; Shane Harris, Ashley Parker and Ellen Nakashima, "New Intelligence Suggests Russia Plans a 'False Flag' Operation to Trigger an Invasion of Ukraine," *The Washington Post*, February 11, 2022, https://tinyurl.com/2ytp22y3; Connor O'Brien, "U.S. 'Watching Very Carefully' for Phony Russian Reason to Kick off Ukraine Invasion," *Politico*, February 13, 2022, https://tinyurl.com/mr33d6r7.

5. Natasha Bertrand, Jim Sciutto and Katie Bo Lillis, "US Intel Indicates Russian Officers Have Had Doubts About Full Scale Ukraine Invasion," *CNN*, February 7, 2022, https://tinyurl.com/ywymzxhh.

warning that Russia would launch an attack as soon as February 16, was intended to highlight the fact that Russian actions are under US surveillance, which could have weakened Russian morale and discouraged Russia from acting recklessly. On the other hand, these measures would have the effect of encouraging Ukraine, other NATO members, and the US military. In this regard, the "deterrence by detection" concept is designed to create an information environment that appears to have all the hostile actions under control, so that the adversary might decide to give up since its actions have lost the upper hand and may end up being futile.

**"Deterrence by detection" is vital part of deterrence but not all**

Nonetheless, there are some limitations to the "deterrence by detection" concept. In terms of the current US response to the situation, it has deficiencies in two ways:[6] first, simply knowing and disclosing the adversary's movements may not be sufficient for it to stand down. If the adversary considers the planned actions still have a good chance of success, or the loss affordable, it may not stop just because of the revelation of the plans. Some commentators have argued that so far the US efforts to deter Russia are not sufficient, as it has refused to send troops to defend Ukraine, only issued warnings of economic sanctions alongside other NATO allies, and sent more troops to some of NATO's eastern members. If Putin is indeed prepared to launch an armed conflict against Ukraine, the initiative still lies on Putin's side after all.[7]

Second, since the "deterrence by detection" concept involves the collection and disclosure of intelligence, it's not immune to the opponent's countermeasures. For instance, when intelligence of possible action is revealed by the deterrent, the deterred party

6. Emily Harding, "Bad Idea: Deterrence by Detection," *Defense 360*, Center for Strategic and International Studies (CSIS), December 3, 2021, https://tinyurl.com/2p8f68ut. In addition to the limitations discussed, if "deterrence by detection" involves the deployment of a large number of sensors and platforms (e.g., drones), it will be costly to build and maintain; in order to grasp the opponent's actions, the deterrent party will inevitably need to deploy drones to the opponent's border, to which the opponent may accuse to be provoking or used for escalating the situation.
7. Zachary Wolf, "What Created the New, More Aggressive Putin," *CNN*, February 12, 2022, https://tinyurl.com/2p9e43kv.

can deny and instead accuse the other side of "making up false alarm or even deliberately creating a conflict." If the deterrent party discloses (some) evidence to demonstrate credibility, the opponent may use it to detect the source of leakage or take a denial position and shift the focus; if the deterrent party does not provide evidence, the opponent, other countries, and the media may question its credibility, creating a "believe it or not" situation. In response to several US accusations, Russia denied and accused the US of "being hysterical." The fact that US officials refused to provide evidence at press conferences not only was highlighted by the media but also became the subject of Russian propaganda that the US governments was untrustworthy to its public.[8] As the crisis in Ukraine continues to develop, the credibility of US intelligence is to be tested in the future. Yet the current situation is a good indicator for the deficiencies of the "deterrence by detection" in handling intelligence.

Good surveillance and intelligence capability can be utilized to identify and monitor the aggressive behavior of an adversary, and is necessary for accurate decision-making. In this regard the "deterrence by detection" concept is important. However, since intelligence acquisition and revelation alone may not be sufficient to achieve the objective of deterrence, "deterrence by detection" should be part of the overall strategy rather than an alternative. For the US and NATO to successfully deter Russian aggression against Ukraine, it is ultimately up to the administrations to demonstrate their ability and will to deter their opponents.

(Originally published in the "National Defense and Security Real - time Assessment", February 17, 2022, by the Institute for National Defense and Security Research.)

(The contents and advice in the assessments are the personal opinions of the authors, and do not represent the position of the Institute for National Defense and Security Research.)

8. Jack Guy, Anna Chernova and Nathan Hodge, "Kremlin Accuses US of Stoking 'Hysteria' Over Ukraine, As UN Security Council Meets," *CNN*, February 1, 2022, https://tinyurl.com/5ajryavh; "US Whips up Hysteria Around 'Invasion' While Pumping Kiev with Weapons – Kremlin," *TASS*, February 13, 2022, https://tinyurl.com/bdx3uwsd; Tom O' Connor, "Russia Envoy: US Has No Evidence of Ukraine Invasion During, After Olympics," *Newsweek*, February 11, 2022, https://tinyurl.com/mr32743c.


Institute for National Defense and Security Research