FRIEDRICH NAUMANN FOUNDATION For Freedom.
Europe

CHINA STRATEGIC RISKS INSTITUTE

Study Paper
June 2026

Andrew Yeh, Athena Tong

Shielding Democracy

Strengthening Germany's and Europe's Democratic Resilience through Partnerships with Like-Minded Allies

Imprint

Publisher

Friedrich Naumann
Foundation for Freedom
Europe
Rue d'Idalie 11–13
1050 Brussels
Belgium

www.freiheit.org/european–union

LinkedIn: fnfeurope
Instagram: fnfeurope
Facebook: fnf.europe
X: fnfeurope

Authors

Andrew Yeh
Executive Director
China Strategic Risks Institute

Athena Tong
Research Associate
China Strategic Risks Institute

Editors

Katharina Osthoff
Senior Policy Advisor International and Institutional Affairs

Hanna Glarmin
Programme Officer

Date

June 2026

Contact

Phone: +32 2 282 09 30
Fax: +32 2 282 09 31
E–mail: brussels@freiheit.org

Notes on using this publication

This publication is an information offer of the Friedrich Naumann Foundation for Freedom.

It is available free of charge and not intended for sale. It may not be used by parties or election workers for the purpose of election advertising during election campaigns (federal, state or local government elections, or European Parliament elections).

Table of Contents

The China Strategic Risks Institute (CSRI) is a global policy think tank providing in–depth analysis of the risks and opportunities posed by the rise of the People's Republic of China. We aim for our research to be accessible to the general public, with recommendations for policymakers, international businesses and NGOs.

www.csri.global

Friedrich Naumann Foundation for Freedom Europe (FNF Europe) is a regional office of the Friedrich Naumann Foundation for Freedom (FNF). FNF is a German political foundation dedicated to promoting liberal values and policies. Headquartered in Potsdam, Germany, it maintains offices throughout Germany as well as in numerous countries around the world.

Acknowledgements

The authors would like to extend their gratitude to all the researchers and experts who contributed to this report. In particular, the authors would like to thank Tau Yang for his contributions to research, analysis and graphic design, Chihhao Yu for providing expert review and feedback, and the many other interviewees who shared their valuable insights.

This report is produced in cooperation with financial support from FNF Europe.

Andrew Yeh

Andrew Yeh is the Executive Director of the China Strategic Risks Institute (CSRI), a global think–tank headquartered in London, England. He previously served as a Visiting Research Fellow at Taiwan's Institute for National Defence and Security Research (INDSR) and as a Visiting Scholar at the Research Institute for Democracy, Science and Emerging Technology (DSET). His research has focussed on a range of issues at the intersection of geopolitics, technology and security, including China's grey–zone warfare, Cross–Strait relations, Europe–Taiwan relations, green technology supply chains and economic security.

Athena Tong

Athena Tong is a Research Associate and Program Lead at the China Strategic Risks Institute, a Visiting Researcher at the University of Tokyo, a Non–resident Vasey Fellow at the Pacific Forum, and one of the Asia Pacific Foundation of Canada's 2026 Indo–Pacific Young Leaders. She specializes in PRC political warfare, telecommunications infrastructure resilience, and economic security in East Asia. Her analysis and commentary have been quoted and published by platforms such as Nikkei Asia, Reuters, Le Monde, ARD, CNBC, RTI, the Jamestown Foundation, The Wire China, The Diplomat, Oxford Analytica, and the Council on Geostrategy.

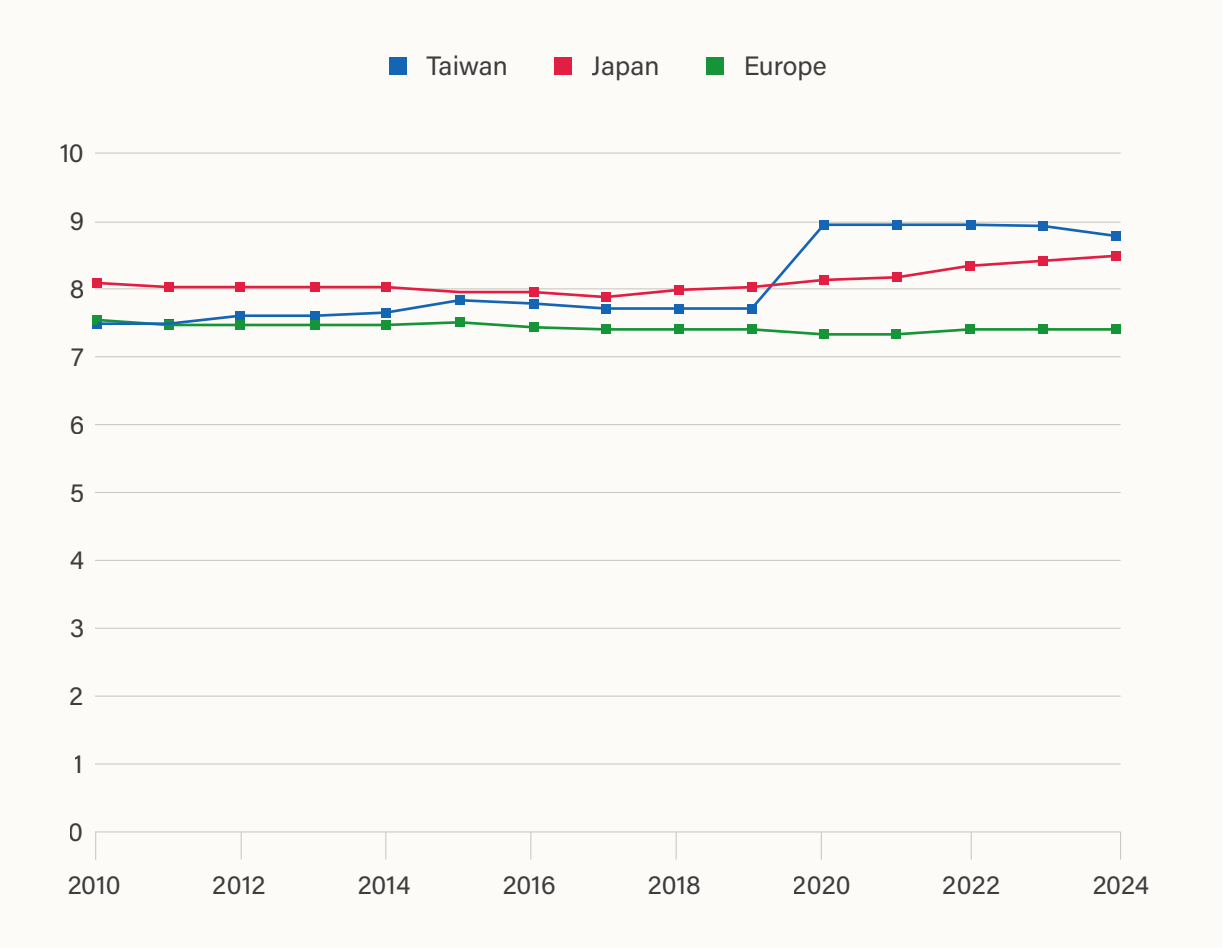
Executive Summary

As a democratic society, Germany is built on a free and open information environment. Yet adversaries are proving increasingly adept at exploiting this openness to influence, disrupt and undermine democratic states. This is the tension that sits at the heart of one of the most pressing challenges facing German and European policymakers today. As European leaders concede that the continent has entered 'the most momentous and dangerous of times',[1] the information domain is rapidly emerging as a key site of contestation.[2] At a time of increasing digitalisation, information fragmentation and political polarisation, concerns are growing over the ability of hostile actors to conduct Foreign Information Manipulation and Interference (FIMI) operations as part of broader sub–threshold or 'grey–zone' attacks. In Germany, these concerns have become increasingly prominent. In this year's Munich Security Report 'disinformation campaigns from enemies' was identified as one of the most immediate security risks perceived by German respondents.[3] While Russia and China remain the primary threat actors in the European information environment, similar techniques could be employed by a range of hostile state and non–state actors.[4] Germany's experience is therefore part of a broader challenge confronting democracies around the world. As a central actor within the EU, Germany has a particular interest in identifying effective responses that strengthen resilience while preserving the openness that underpins democratic debate.

This paper seeks to analyse what lessons Germany and the European Union (EU) can learn from two Asian democracies – Taiwan and Japan – that have faced persistent FIMI threats for well over a decade. China views Taiwan as a breakaway province and has consistently sought to use FIMI as part of broader efforts to undermine its de facto independence and coerce it into unification. China's FIMI operations against Japan are less ambitious in their strategic objectives but still far–reaching in results,

with significant political and economic ramifications. Despite coming under increasing pressure, both Taiwan and Japan have successfully maintained their open information environments and consistently rank amongst the freest democracies globally. While Taiwan offers lessons from a frontline democracy facing sustained and direct pressure from China, Japan provides a complementary example of how a large, technologically advanced democracy can institutionalise resilience against FIMI while maintaining strong protections for freedom of expression. As EU leaders set out to mobilise the European Democracy Shield – the EU's umbrella initiative to protect democratic life from foreign interference – the experiences of Taiwan and Japan offer valuable insights for European policymakers.

Figure 1 Europe trails Taiwan and Japan in the EIU Democracy Index



Sources: Economist Intelligence Unit; Our World in Data[5]

The first part of this paper examines how FIMI fits within Russia and China's broader strategies of competition and coercion, and the implications for Germany and the EU. Despite their history of mutual mistrust, Moscow and Beijing share a number of objectives in the European information environment. These centre around undermining NATO and Europe's security alliances but also include a broader objective of weakening European societal cohesion through polarising and diluting public debates. This is particularly relevant as both Russian and, to a lesser extent, Chinese information operations have amplified narratives aligned with positions frequently adopted by far–right actors in Europe, including Germany's Alternative für Deutschland (AfD).[6] Therefore, this section maps out the FIMI toolkit that Russia and China have at their disposal – ranging from sponsoring content in well–established European news outlets to large networks of thousands of directed or fake accounts to influence and distort debates on social media. This first part of the paper concludes with a consideration of whether Russia and China are coordinating on FIMI operations in Europe, which while difficult to prove directly, is consistent with a series of parallel activities linked to both actors.

The second part of this paper examines the response of Taiwan and Japan to FIMI threats. Successive Taiwanese governments have taken a range of approaches to upholding information integrity in Taiwan. These approaches have varied from proactive attempts to build trusted channels of communication between the government and its citizens, to more prohibitive actions to protect against more overt forms of FIMI. Notably, Taiwan's 'Whole–of–Society Resilience' defence concept is an ambitious programme that intends to bring together a wide range of government, private sector and civil society stakeholders to address a range of threats – of which FIMI is one part. However, such action is not limited to the government alone. Taiwan has developed a rich ecosystem of civil society groups working on fact–checking, media literacy and monitoring the information environment. These groups are often highly localised and engage across different sectors of society.

Taiwan's tech–enabled civil society solutions are vastly different from the approaches taken by most European countries – which are often led by governments and reliant on the goodwill of large tech corporations.

Japan, by contrast, has taken a more incremental approach characterised by institutionalising work across different government departments and enhancing strategic communications, rather than passing dedicated legislation. For example, Tokyo has embedded FIMI countermeasures into its national security and digital-governance strategies rather than passing dedicated 'anti-disinformation' laws. The Japanese model emphasises coordination between ministries, joint rule–setting with major online platforms (with the government setting the objectives and the platforms implementing and reporting on them), and international partnerships through the G7 and others. It relies heavily on strategic communications, fact–checking cooperation and diplomacy to expose and counter hostile narratives, while maintaining a strong legal commitment to free expression.

Finally, this paper considers the lessons learned for Germany and the EU. Policymakers should take the best of both Taiwan and Japan's experiences. From Taiwan, policymakers should learn the importance of developing a civil society ecosystem to assist with fact–checking, media literacy education and FIMI investigations. Similarly, Germany should emulate Taiwan's public exercises, drills and planning for responding to hostile FIMI operations. Crucially, modelled on Taiwan's 'whole–of–society' approach, such activities should include businesses, civil society organisations and community groups.

From Japan, three lessons stand out. First, the integration of FIMI into broader foreign and security policy, with strategic communications seen as a core security function. Second, Japan's use of government issued guidance, protocols and multi-stakeholder coordination, shows how governments can make responses to hostile information operations more effective. Third, its experience demonstrates the value of international coordination: anchoring domestic responses within G7, EU–Japan and US–Japan frameworks enables faster detection, attribution and collective messaging against foreign information manipulation.

1. Part One: Russia and China's Strategies Targeting Information Spaces (FIMI)

FIMI within Russia and China's grey-zone warfare

Both Russia and China use Foreign Information Manipulation and Interference (FIMI) as part of efforts to weaken adversaries, neutralise opposition and build political support for strategically beneficial goals. Because of the ways in which such activities go beyond the traditional realm of propaganda, diplomacy and foreign influence common in peacetime, but do not in themselves constitute acts of war, they can also be understood within broader grey–zone or sub–threshold strategies increasingly deployed by both Russia and China.

The importance of the information domain within warfare is well established in China's military doctrine. PLA military strategy is divided into the 'Three Warfares':[7] public–opinion warfare, psychological warfare and legal warfare, with all three seen as critical to advancing the CCP's interests during both peacetime and wartime. As will be analysed in the case provided below, China's FIMI operations in Europe can be understood as crossing all three domains, predominantly to influence public opinion, but in some cases also targeting implicit and explicit threats against European populations and supporting China's positions on contentious issues of international law.

Similarly, Russian military thinking embeds FIMI operations within a broader concept of 'information confrontation' (informatsionnoe protivoborstvo), described as a permanent strategic struggle in the information sphere that spans both times of peace and war.[8]

In this framework, the 'information space' encompasses technical networks, data, media, and psychological influence, of which FIMI can be part of broader efforts to penetrate, and neutralise an adversary's critically important information infrastructure.[9]

As a union of free and open information environments, the EU is a fertile ground for both Russian and Chinese FIMI operations. This section begins by examining the goals of Russia and China's FIMI operations in Europe, which have considerable overlap in the field of undermining NATO and the broader Western alliance. It then considers the tools available to Russia and China, which are increasingly difficult to detect among sophisticated attempts to manipulate information environments on social media and non–traditional media. Finally, this section concludes by considering whether China and Russia could be coordinating FIMI operations in Europe, suggesting that at least some degree of tacit alignment may be plausible.

Goals of Russia and China's FIMI in Germany and Europe

While Russia and China's FIMI operations in Europe differ in their objectives and methods, there are several areas of overlap in terms of political objectives.

Despite a shared history of rivalry, conflict and mistrust, today China and Russia share a broad interest in undermining what leaders in both countries perceive to be a world order dominated by the broadly framed 'West.'[10] Both countries see the US as their prime adversary, and undermining NATO – the most capable Western military alliance – as a common goal. China shares Russia's concerns about NATO's eastward expansion, particularly as it pertains to the Indo–Pacific, as well as the growing use of economic statecraft by the US and its allies against their adversaries.

These overlapping interests are reflected in the information domain, with a number of common themes emerging in Russia and China's information operations:

- → **Undermining support for NATO:** Both Russian and Chinese information operations have attempted to weaken support for NATO among European populations. This has included, but is not limited to, platforming local politicians holding anti–NATO positions, amplifying content blaming NATO for the start of the Ukraine war, highlighting debates about the US commitment to NATO or highlighting other internal divisions, and casting doubt over NATO capabilities and its ability to defend Europe.[11] [12]
- → **Discrediting dissenting voices:** Both Russia and China are highly sensitive to criticism from European actors, including both policymakers and the broader public. This means that those airing critical views of Russia and China may find themselves subject to FIMI operations discrediting their person or their viewpoints, as well as threats and surveillance. Particular efforts are made to neutralise dissent within diaspora communities in exile, which are seen by Russia and China as especially dangerous.[13]
- → **Polarising and diluting public debates:** With the exception of some countries in Central and Eastern Europe where pro–Russian viewpoints are popular with large segments of the population, neither Russia nor China expect to build large–scale popular support for their policies among most European populations. However, both countries still have an interest in weakening social cohesion in European countries, which in turn reduces the ability of European states to govern and exercise power effectively. At the FIMI level, this includes efforts to exacerbate polarisation and fragmentation, such as by amplifying content or issues associated with far–right or far–left political positions, or through generally reducing the quality of public debates through circulating conspiracy theories or disinformation.[14] This is particularly evident in Germany, where several AfD politicians have frequently

appeared on Russian state media and promoted narratives aligned with pro–Kremlin positions.[15] Germany's economic weight, central role within the EU and pluralistic media landscape make it a particularly attractive target for hostile information operations seeking to shape wider European debates and policy outcomes.

Alongside these areas of commonality, there are also a number of areas in which Russia and China's FIMI objectives are distinct from each other. Notably, Russia has a far greater interest and capability in seeking to influence elections and secure regime, government or policy change across Europe. These efforts are primarily focused in European countries where there are large Russian–speaking populations, with reports identifying 44% of all Russian FIMI operations in Europe being conducted in Russian.[16] Examples of Russia's FIMI operations in support of pro–Russian actors in Europe include Moldova, where in 2025, a BBC investigation unearthed the existence of an extensive network with Russian connections, coordinated through Telegram and controlling at least 90 TikTok accounts to post unfounded allegations against the current Moldovan government and boost support for the country's pro Russia opposition.[17] In Georgia and Romania, similar methods are also deployed by Russian linked operators, including spreading hate speech and fake news, to sow mistrust in the countries' electoral process and bolster support for pro–Russian political parties and candidates.[18] In contrast, while China does seek to influence its diaspora across Europe, these are generally not focused on influencing elections – in which Chinese diaspora groups are generally a minority group. Instead, Chinese aims to promote narratives beneficial to its broader strategic goals, such as those listed above.

Russia and China's FIMI methods / toolkit

Both Russia and China have a range of tools available to conduct information operations in Europe. These include what might be considered traditional tools for propaganda efforts, including traditional media outlets with clear ties to the Russian and Chinese state, many of which target European populations through publishing in local languages, both in print and online. Notably, Russia Today and Sputnik services have developed substantial numbers of mirror sites to circumvent EU content bans and target different–language audiences in Europe, including German, Spanish, English, and French.[19] Chinese state media often takes a slightly different approach, arranging free–of–charge or sponsored content agreements with local media outlets with already established audiences. For example, China Daily has had paid media placement arrangements with German media outlets such as Handelsblatt, Süddeutsche Zeitung and DPA.[20] These examples illustrate that Germany's information environment is not insulated from foreign influence efforts and should be understood as part of a broader European contest over information integrity. Messages and statements put out by China and Russia's and Embassies in Europe can also play a propaganda role, targeted at local audiences. In some cases, statements from Chinese officials have gone beyond propaganda and have also played a role in spreading disinformation – such as Zhao Lijian, China's MoFA spokesperson during the COVID–19 pandemic, who disseminated conspiracy theories about the virus originating from a US military biolab.[21]

The importance of non–traditional media within public debates in Europe has been accompanied by increasingly novel and sophisticated information operations from Russia and China. While state–controlled media outlets such as Xinhua and Russia Today and other forms of Russian and Chinese traditional media can be easily identified as state–linked operations, this is often not the case for news platforms which only exist online or on social media, which may not require the same levels of registration and regulation. This includes a number of YouTube channels, which appear to be run by bots posting AI–generated content,

praising China's economic rise while criticising Western governments.[22] Other suspected bot accounts depict civilian life under Russia's aggression and occupation of eastern Ukraine in a positive light.[23] While the majority of Chinese state controlled outlets are now labelled as 'state–linked media' on YouTube, and Russian state affiliated channels have faced a global YouTube ban since the invasion of Ukraine,[24] it is often challenging for platforms to quickly and accurately identify what accounts may or may not be state–linked. This raises the possibility of users being exposed unknowingly to Chinese or Russian state sponsored content and highlights the reliance of European polities on the resources, capabilities and willingness of social media companies to conduct such investigations. Notably, since April 2023 X has removed the 'state–affiliated media' and 'government–funded media' labels that had been applied to various news organizations.[25]

The use of directed social media accounts is perhaps the most challenging form of FIMI operation deployed by Russia and China. Such actions are often described as 'spamouflage', whereby paid workers and/or bots create fake accounts which can amplify strategically important narratives and disinformation, driving up engagement and pushing issues to the top of social media algorithms.[26]

Doublethink Lab's analysis of the GoLaxy documents[27] illustrates why civil society investigations matter. The leaked materials suggest that PRC–linked actors are seeking to automate the full FIMI cycle: monitoring political narratives, profiling targets, generating tailored content, and distributing it through humanised bot accounts. For Taiwan, the documents point to granular targeting of political parties, civil society groups, religious organisations, companies and key online accounts.

AI–enabled FIMI is not only a problem of false content, but also of data infrastructure, target mapping, automated amplification, and rejections of accounts and narratives seen to be hostile to Russia and China's aims. Such activity is often difficult to detect, as fake accounts may on the surface look like authentic accounts, but easy to duplicate and re–generate. Even if accounts are suspected as being fake, attributing

this to Russian or Chinese state directed action is also extremely difficult. Uncovering and managing fake accounts is reliant on the willingness and capabilities of social media platforms. While in 2020, 2023 and 2024, Twitter/X and Meta removed large numbers of suspected Chinese linked accounts, no such large–scale removals have been reported since.

Table 1 Examples for Russia and China's FIMI Methods

Mechanism	China	Russia
State officials	Senior Chinese officials have spread disinformation about COVID–19 originating from a US bio–lab.[28]	Russian Foreign Minister Sergey Lavrov and other spokespeople claimed the mass killings in Bucha in 2022 were staged or faked.
State media	China Daily sponsors 'China Watch' supplements in English, French, Spanish, and German with European partner media outlets.	Russia Today and its mirror sites continue to disseminate content in Europe, both online and by broadcast, despite content restrictions in the EU.[29]
'Spamouflage' – fake and directed social media accounts	In 2020, Twitter removed 170,000 directed accounts targeting Hong Kong, Covid–19 and Taiwan narratives, while in 2023 Meta removed 9,000 Facebook and Instagram accounts promoting pro–China messaging and attacking Western critics.[30 31]	In 2023 Meta removed Russian–linked networks that praised Russian activity in West Africa while attacking France, while suspected Russia–linked inauthentic 'doppelganger' accounts have impersonated trusted international media to spread disinformation about the war in Ukraine.[32 33]
Social media influencers (not proven state linked)	Social media influencers, including Uyghur ethnic individuals appearing in YouTube/TikTok videos to whitewash human rights abuses in Xinjiang.[34]	Social media influencers, pro–Russian key opinion leaders, such as Dmitry Puchkov, the social media personality who had three million subscribers on YouTube before being removed for supporting Russia's invasion of Ukraine.[35]

Case study matrix: Russia and China's FIMI operations in Europe

Table 2 Russia and China's FIMI operations in Europe

	Russia	China
Undermining NATO	Frequent highlighting of internal disagreements, such as over military spending or immigration policies, and exacerbating doubts over US commitments.[36]	Chinese officials and state–linked media organisations have frequently pushed media articles blaming NATO for provoking Russia into invading Ukraine, as well as claiming that the US wanted to provoke the war in order to extinguish European 'strategic autonomy.' [37 38]
Neutralising dissent	Exiled Russian intellectuals are frequently doxxed and framed by the state as puppets of the British and American governments for receiving scholarship and thinktank fundings.[39]	Suspected Chinese state–linked accounts on social media disseminated AI deep–fake videos purported to show a conversation between UK–based Hong Kong activists, while sexually explicit deep–fakes have targeted female activists.[40 41]
Polarising/ diluting debates	AfD politician Petr Bystron has been accused of receiving payments linked to the pro–Russian platform Voice of Europe, allegations he denies. Former AfD MEP Maximilian Krah (now a Member of the Bundestag) is also alleged to have received money from this platform. Krah's former accredited parliamentary assistant (APA) has been arrested on allegations of spying for China.[42 43 44]	State–linked media such as CGTN have platformed anti–NATO politicians such as George Galloway MP (UK),[45] while AfD politician Alice Weidel has been amplified and reinterpreted in Chinese social media platforms like Xiaohongshu and Weibo (including through false claims about her statements on China).[46] These platforms have a wide user base among the Chinese diasporas in Europe.

Are Russia and China coordinating on FIMI campaigns?

While there is no direct evidence of Russia and China establishing formal coordination in conducting FIMI operations, it is clear that their respective operations can occasionally work in unison to reinforce each other, with Moscow or Beijing linked operations often quick to amplify or promote narratives and information put out by the other.[47]

Notable examples include:

- → **Justifying Russian aggression against Ukraine:** In the early stages of Russia's invasion of Ukraine, Chinese officials and state media outlets were quick to push Russian narratives and terminology. For example, Chinese state media repeated Russia's language of the exercises being part of a 'special military operation,' rather than an invasion, and frequently referenced Russia's 'legitimate security concerns,' while blaming Ukraine and NATO for provoking Russia.[48]
- → **Discrediting evidence of Russian war-crimes:** Russian state-linked media and social media was quick to discredit widespread reports of war-crimes and other abuses by Russian soldiers in Bucha, Ukraine, 2022. A number of suspected Chinese-state linked online commentators reinforced these narratives by publishing content doubling the validity of reports, as well as articles in Chinese state-linked media re-iterating Russian perspectives. Chinese state media also amplified the Russian government's claims about the US funding and developing biological weapons in Ukraine.[49]
- → **Amplifying COVID-origin conspiracies:** Amidst growing scrutiny on the Chinese government's response to the outbreak of the COVID-19 pandemic, some Chinese officials pushed back by circulating theories that the virus emerged as a result of a US bioweapons programme. This was quickly picked up

by Kremlin linked networks of media organisations and social media accounts, which played a large role in spreading the conspiracy theory.[50]

Against a background of a rapidly deepening strategic partnership between Moscow and Beijing, the prospect of formal coordination in information operations becomes more plausible. As evidenced by a spike in high level diplomatic engagements between Russia and China, an increasing number of joint military exercises across the globe, and trade in dual–use technologies between the two countries, Moscow and Beijing are increasingly aligned on both strategic communications and military operations. While coordination may be extremely difficult to prove, short of open admission from either parties, it would not be inconsistent with the overlapping objectives and reinforcing behaviours of Chinese and Russian FIMI operations as outlined here.

2. Part Two: Japan and Taiwan Responses to FIMI

Case study: Taiwan

Taiwan's threat environment

Taiwan has been the most significant target of China's FIMI operations globally, as part of Beijing's broader strategy of using grey-zone warfare to coerce Taiwan into acquiescence to so-called 're-unification' with China. From this overarching strategy flow a number of sub-objectives for China's FIMI operations in Taiwan. These include, but are not limited to: discrediting politicians with positions perceived as hostile to China; exacerbating doubts about the US commitment to Taiwan; portraying resistance to 're-unification' as futile; and portraying Taiwan as a failed state. As with China's FIMI operations in Europe, there is also evidence of attempts to dilute and polarise debates by amplifying divisive or false content.[51]

Taiwan's free information environment, the linguistic commonalities with China, and the popularity of Chinese-owned social media apps such as Douyin/TikTok (and until recently, Xiaohongshu) make it highly vulnerable to Chinese FIMI operations. China deploys all of its tools analysed in the previous section – including non-traditional media and spamouflage – to great effect within the Taiwanese context.

While Europe is a vastly different context, Taiwan's role as a testing ground for China's FIMI operations means that tactics which prove successful in Taiwan may be later emulated in Europe. As such, learning from Taiwan's experience in countering China's FIMI operations can provide many valuable lessons to Europe.

Taiwan's government response

Successive Taiwanese governments have taken a range of approaches to upholding information integrity in Taiwan, with the first government–led task force launched as early as 2018.[52] Government approaches have varied from proactive attempts to build trusted channels of communication between the government and its citizens, to more prohibitive actions to protect against more overt forms of FIMI. Perhaps most importantly of all, Taiwan's 'Whole–of–Society Resilience' defence concept is an ambitious programme that intends to bring together a wide range of government, private sector and civil society stakeholders to address a range of threats – of which FIMI is one part. While its implementation remains in its early stages, it offers a valuable conceptual framework that European governments can emulate.

→ **Whole–of–Society defence resilience committee:** Launched by Taiwan's President Lai Ching–te in June 2024, the Whole–of–Society Defence Resilience Committee aims to bring together a range of stakeholders to analyse and improve Taiwan's preparedness for a range of crisis contingencies.[53] Alongside representatives from the National Security Council, representatives from departments which do not traditionally focus on security issues are also represented, including Ministers of Economic Affairs, Transportation and Communications and Agriculture. However, what makes the Committee unique is the involvement of individuals from outside government, including businesses, academics, civil society groups and religious associations. Information protection is included as one of the key focus areas for the Committee, and has formed the basis of a number of table–top exercises and field–exercises.[54] These exercises have simulated how different societal actors would respond to a major 'cognitive warfare' campaign, as well as the role that hostile information operations could play in a range of other attacks on Taiwan. While the work of the Committee remains in its early stages, these exercises have already allowed a diverse set of actors to understand the role that information operations

could play in a range of crisis scenarios, as well as considering how government and civil society groups can improve their response to such challenges. For Germany, this raises the question of whether existing federal, Länder and civil protection exercises sufficiently incorporate information manipulation scenarios alongside cyberattacks, critical infrastructure disruption and other hybrid threats. Given Germany's federal structure, strengthening coordination between these authorities will be essential if similar whole–of–society approaches are to be implemented effectively.

→ **Legal enforcement against FIMI actors:** In March 2025 the Taiwanese government revoked the residency permit of a Chinese social media influence living in Taiwan. The influencer was a Chinese national but had lived in Taiwan for several years under a family–based residence permit. Her videos frequently espoused pro–China and pro–unification narratives, including encouraging China to take 'non–peaceful' measures to forcibly achieve 're–unification'. The decision to revoke her residency permit was controversial – with many criticising the unclear ramifications on freedom of speech for other foreign national residents in Taiwan. The government's Mainland Affairs Council maintains that freedom of speech remains upheld, including expressing pro–China and pro–unification views, but that encouraging military threats against Taiwan would not be protected under such freedoms.[55] The case illustrates the difficult balance democratic governments face between countering hostile influence and protecting freedom of expression. While Taiwan's authorities viewed the case as crossing a clear legal threshold, the controversy highlights the importance of ensuring that counter–FIMI measures remain proportionate and consistent with democratic freedoms. Other legal measures include penalties for the dissemination of damaging rumours or falsehoods in specific domains such as disaster prevention and communicable disease control.[56]

→ **Innovative government–citizen engagements.** Taiwan's government has been developing strategies to improve its strategic communications when faced with disinformation or misinformation online. Some of these have used novel means to engage broad swathes of citizens, such as the 'humour over rumour' approach taken during the COVID–19 pandemic. This approach saw government ministries put out memes, cartoons and other engaging and easily–shareable content to dispel myths around COVID–19, ease public panic and put out government advice – with a target of providing a response to misinformation is provided within 20 minutes, in 200 words or fewer, alongside two fun images.[57]

→ **'Pre–bunking' false information:** Another concept within Taiwan's strategic communications pioneered by Taiwan's first Minister of Digital Affairs, Audrey Tang, included prioritising rapid responses to misinformation or disinformation being circulated online. This was based on the logic that it is far easier for governments to 'pre–bunk' – to reach people before they have encountered misinformation – than to 'de–bunk' existing beliefs after such misinformation has become widespread. During the 2024 Presidential and Legislative elections, when Taiwan faced an onslaught of Chinese FIMI operations, Taiwan's Ministry of Digital Affairs actively monitored online debates, and forwarded developing rumours to relevant government departments – who then had a target of drafting a counter–narrative within 60 minutes.[58]

→ **Embedding information preparedness within crisis planning:** The Taiwanese government has taken a proactive approach to integrating counter–FIMI work into broader citizen preparedness for war and other crisis contingencies. The government issued 2025 Civil Defence Handbook includes a dedicated section on helping citizens prepare for hostile information operations in the event of a military attack from China. These include a clear

assertion for citizens to disregard any claim that the government has surrendered or been defeated as false, as well as to check and verify information received before believing it or forwarding it.[59]

Figure 2 Cartoon posted by Taiwan's then Premier Su Tseng-chang on Facebook in February 2020[60]

Designed to dispel popular rumours circulating online of Taiwan being at risk of running out of toilet paper due to materials being diverted to face-mask production during the COVID-19 pandemic. The infographic shows that both the materials and sources of materials for Taiwan's face masks are different to that of its toilet paper.

Figure 3 Screenshot from Taiwan's 2025 Civil Defense Handbook, page 19.

The text encourages citizens to refrain from sharing unverified information, and warns against believing claims that the Taiwanese government has surrendered.[61]

Taiwan's civil society response

Although governments have an important role to play in countering FIMI operations, responses cannot be left to the state alone. Firstly, because the state is not always seen as a trusted or neutral actor by all citizen groups. This is particularly a challenge in Taiwan, where partisanship has increased in recent years – a trend both exploited and exacerbated by China's FIMI operations.[62] Secondly, relying on the state to identify and counter disinformation risks establishing the notion of the state as the arbiter of truth. These are powers which could easily be exploited to undermine freedom of expression and media freedoms in the long run, should more authoritarian rulers take power.

In response to this challenge, a growing ecosystem of civil society groups has developed in Taiwan with a focus on information integrity and media

literacy. While Germany already benefits from a strong landscape of media literacy initiatives, public broadcasters, fact–checking organisations and political foundations, Taiwan demonstrates the value of deeper coordination between these actors and public institutions.

- → **Community based fact–checking:** The nonprofit Cofacts has developed an open–source, citizen–driven, collaborative fact–checking platform that aims to combat disinformation and fake news. The platform allows users to forward news articles or social media content to a panel of fact checkers. Fact checkers are made up of both volunteers and fact–checking professionals, such as the Taiwan Fact Check Center, MyGoPen and journalists.[63] Fact checkers can give their opinion or not on whether such information might constitute misinformation – with the rationale for their judgment also given. Both the forwarded content and the response from fact checkers is publicly accessible on a searchable online database. Integration with Line – a popular messaging app – allows for citizens to forward information quickly and easily.
- → **Civil society led FIMI investigations:** Civil society led research initiatives have been at the forefront of efforts to uncover evidence of China's FIMI operations in Taiwan. Examples such as the Taiwan Information Environment Research Center (IORG) collate evidence on FIMI incidents to raise public awareness and inform policymakers. For example, one study exposed 147 Chinese propaganda accounts targeting Taiwan on Duoyin/TikTok, and others have collated evidence of Chinese FIMI operations in Taiwan's elections.[64]
- → **Media literacy skills:** Media literacy skills are included as a core competency under Taiwan's national curriculum. Under this curriculum, students are encouraged to develop critical thinking skills, analyse media organizations and evaluate media representations. While some centralised guidance on teaching media literacy is issued to teachers, a number of civil

society groups, such as the Taiwan Pangphuann Association of Education,[65] help teachers develop learning materials for middle and high school students.

→ **Highly-localised networks:** Taiwan has a plethora of civil society groups that work at the community level to encourage debate and educate citizens on information integrity and media literacy. For example, grassroots group Fake News Cleaner has hosted more than 500 events with students, children and elderly citizens to identify misinformation and discuss media consumption habits.[66]

Case study: Japan

Japan's experience shows a layered response to foreign information manipulation and interference (FIMI), built around strategic communications led by the Ministry of Foreign Affairs (MOFA), Ministry of Internal Affairs and Communications (MIC)-driven platform and literacy policy, and the National centre of Incident readiness and Strategy for Cybersecurity (NISC)'s cyber and critical-infrastructure coordination. For Europe, this offers a potential model for how governments can organise and implement counter–FIMI work.

Japan's threat environment

Japan is a natural FIMI target because of its alliance with the US, economic and technological rivalry with China, and unresolved territorial disputes make it central to wider strategic competition in the Indo-Pacific. At the same time, its high internet penetration and advanced digital economy give hostile actors many channels through which to operate.

As detailed in the case studies below, recent campaigns have focused on several sensitive fault lines: controversies around the release of treated radioactive water from the Fukushima Daiichi nuclear plant; longstanding tensions over the heavy concentration of US military facilities on Okinawa;

Japan's stance on China's territorial claims over Taiwan and the Senkaku Islands; and more recently, attempts to discredit Prime Minister Takaichi.[67] FactLink's investigation into Chinese FIMI targeting Prime Minister Sanae Takaichi after her 'Taiwan contingency' remarks shows how Taiwan–related narratives can be repurposed to pressure Japan's domestic politics. The campaign combined official diplomatic pressure, Chinese state media narratives, social media amplification, misogynistic attacks, WWII historical grievance narratives, Ryukyu/Okinawa–related claims, and false corruption allegations, including a forged–document style rumour alleging that Takaichi had received jewellery from former Taiwanese representative Frank Hsieh. The case suggests that Beijing's information operations against Japan are not simply about shaping perceptions of bilateral disputes, but about deterring Japanese political leaders from articulating clearer positions on Taiwan.

In parallel, Russian actors have experimented with using large-scale automated accounts and generative–AI tools to produce and spread tailored propaganda such as AI–generated images, videos and text that echo Kremlin narratives into social media ahead of elections in an attempt to normalise divisive themes and undermine trust in the government.[68]

Election-related interference remains more limited than in Taiwan, but concern is growing. During the 2025 Upper House race, experts highlighted Russian bots and AI-generated content pushing divisive themes, such as the pro–independence movement for Okinawa and mistrust towards the U.S., alongside broader anti-government narratives.[69][70] These findings led commentators to call for stronger monitoring, transparency and platform cooperation rather than a new criminal law which could risk chilling legitimate speech.

Japanese businesses have also suffered as a result of hostile FIMI campaigns. Chinese disinformation around the release of treated water from the Fukushima Daiichi nuclear plant – framing it as 'nuclear–contaminated water' despite IAEA assessments that the discharge met international safety standards[71] – fuelled public anger in China. This in

turn led to the harassment of Japanese businesses in China and provided domestic political cover for Beijing's blanket ban on Japanese seafood imports and informal pressure on Chinese tourists to avoid Japan.[72]

Government response: MOFA, MIC, NISC

Japan still lacks a dedicated foreign influence or FIMI statute, and instead leans on existing sectoral frameworks, so coordination mechanisms and strategic communications play a central role in its response. This approach has been built around 'soft law' – meaning non-binding instruments such as guidelines, voluntary codes of conduct and multi-stakeholder compacts that shape platform and media behaviour without creating new criminal offences or hard regulatory obligations. This experience is particularly relevant for Germany, where policymakers continue to grapple with how to strengthen resilience against foreign information manipulation without undermining freedom of expression or introducing overly restrictive regulation.

Japan's MOFA has become the lead on FIMI in the realms of diplomacy and internationally facing public communications, rather than domestic content regulation. Diplomatic Bluebooks, Japanese MOFA's annual foreign policy white papers, now frame foreign information manipulation as a threat to Japan's security and democracy, describe internal cooperation across information, policy and public-diplomacy divisions, and highlight the need to defend a 'free information space' while actively rebutting hostile narratives.[73] Japan's MOFA also runs a public 'responses to information manipulation' page, issues rapid statements on incidents around Fukushima, Okinawa, Senkaku and Taiwan, and uses data-rich factsheets and IAEA references to undercut Chinese claims.[74]

MIC is the main coordinator for Japan's domestic online information space and for how large digital platforms (search engines, social networks, video-sharing sites) are governed and engaged by the state. It led the 'Existing Practices against Disinformation' (EPaD) project, which systemically collects, organises and publishes examples of how platforms, media and NGOs are already handling fact-checking, political-ad

transparency, crisis communication and media literacy, with the aim of encouraging replication, benchmarking and voluntary improvement across stakeholders. For instance, EPaD highlights measures such as clearer labelling and archiving of political ads, and the creation of rapid response channels between platforms, newsrooms and fact–checkers during disasters or elections, as practices other companies and organisations are encouraged to emulate. The project is periodically updated via public consultation to allow for newer practices (such as responses to generative AI risks) to be incorporated and debated.[75]

MIC also oversees platform and content-governance policy through expert 'study groups'[76] — formal advisory panels that bring together outside specialists and industry representatives to analyse issues, take submissions, and formulate recommendations that often feed into guidelines or legislation. One concrete outcome is the 2024 Act on Information Distribution Platforms Response, which creates a governance and reporting architecture within the platforms and how they report to the government, which in turn can be leveraged when FIMI overlaps with illegal content.[77]

Finally, MIC runs literacy and 'Digital Positive Action' projects, which are public-private programmes involving platforms, telecoms, tech companies, educators and NGOs aimed at promoting safe, constructive and informed use of digital services, particularly among youth.[78] 'Resilient social-media use' here means equipping users to recognise suspicious content, avoid contributing to harmful amplification, and make more informed choices about privacy and security settings, so that disinformation and abuse have less impact even in the absence of heavy-handed censorship.

Within the Cabinet Secretariat, NISC/National Cybersecurity Office provides the backbone for cyber and hybrid-threat coordination. It drafts the Cybersecurity Strategy and critical-infrastructure protection policy, acts as the governmental computer emergency response team (CERT), and coordinates incident response and information-sharing across ministries, ensuring that cyber incidents, hybrid campaigns

and infrastructure-focused information operations (including those touching undersea cables and telecoms) are treated within one risk-management framework.[79]

Strategic communications and high-profile test cases

Japan's evolving response is clearest in a handful of high-profile test cases that combine security, local politics and foreign information operations:

- → **Fukushima treated water.** After the Fukushima Daiichi nuclear accident, Japan decided to release ALPS-treated water that met international safety standards, backed by IAEA reviews. Chinese state and aligned actors amplified narratives about 'nuclear-contaminated water'.[80] Tokyo countered these claims with government issued data dashboards, IAEA-based factsheets and public rebuttals (see images below). The Japanese experience suggests that governments can play a more proactive role in strategic communications and public rebuttal efforts while remaining consistent with democratic norms and free expression. This contrasts with Germany's traditionally more cautious approach to state involvement in counter–disinformation efforts and highlights the potential value of more proactive government communication during information crises.
- → **Amplifying political divisions over Okinawa.** China has sought to amplify real events and concerns to increase political divisions in Japan. Notably, Okinawa hosts a large share of US forces in Japan, and there are longstanding local grievances about the base burden and linked accidents. Chinese–linked messaging selectively amplifies real protests and incidents, portraying Okinawa as fundamentally alienated from mainland Japan and the US–Japan alliance, and in some cases suggesting that the prefecture might 'break away'. While there is genuine local discontent, there is also evidence that Chinese–linked narratives may seek to deepen internal divisions and amplify existing social and political tensions.[81]

→ **Coercive military activity around Japan.** As tensions over Taiwan have grown, Chinese military flights and naval movements around Taiwan and Japan's Ryukyu islands have been accompanied by narratives depicting Japan as a US 'vassal' preparing to interfere in 'China's internal affairs.'[82]

For Fukushima, Tokyo framed disinformation as a coordinated campaign and responded with a combined science-and-diplomacy package: constant IAEA referencing, live data dashboards, multilingual explainers, and explicit labelling of some Chinese claims as disinformation.

Figure 4 Official communications by the MOFA of Japan on Fukushima treated water.

Ministry of Foreign Affairs of Japan
外務省

Skip to main content | FAQ | Site Map | Links | Japanese | Other Languages

ENHANCED BY Google | Search | Font Size S M L

About Us | News | Foreign Policy | Countries & Regions | Consular Services

Top > News > Press Releases > Visit of IAEA Officials and International Experts for a Review on the Discharge of ALPS Treated Water from TEPCO's Fukushima Daiichi Nuclear Power Station into the Sea (Results)

Press Releases

Visit of IAEA Officials and International Experts for a Review on the Discharge of ALPS Treated Water from TEPCO's Fukushima Daiichi Nuclear Power Station into the Sea (Results)

Post | Share 0 | e-mail | Print

May 15, 2026
Japanese

From May 11 to 15, the IAEA Task Force, consisting of the IAEA officials and international experts, visited Japan for a review of the discharge of ALPS treated water from TEPCO's Fukushima Daiichi Nuclear Power Station (FDNPS) into the sea (the sixth review mission since the start of the discharge of ALPS treated water).

1. This IAEA review is based on the Terms of Reference (TOR) for reviews of safety aspects of handling ALPS treated water, signed in July 2021 with the IAEA.
2. The review focused on the monitoring activities related to the discharge of ALPS treated water into the sea, and the Government of Japan, Fukushima Prefecture and TEPCO shared and explained Japan's efforts on sea area monitoring and monitoring on the premises of TEPCO's FDNPS, associated with ALPS treated water. In addition, the IAEA Task Force held meetings with the Government of Japan, Fukushima Prefecture and TEPCO to discuss Japan's efforts consistent with international safety standards after the start of the discharge and confirmed that the discharge of ALPS treated water into the sea has been carried out safely.
3. On May 13, the IAEA Task Force visited the FDNPS site to review the condition of the facilities for the discharge of ALPS treated water and to receive a briefing from TEPCO staff on the latest situation at the site.
4. The independent review by the IAEA, an international organization with authority in the field of nuclear energy, is extremely important in ensuring reliability and transparency regarding the safety and handling of ALPS treated water and fostering better understanding both domestically and internationally. The Government of Japan will continue to work firmly to gain further understanding of the discharge of ALPS treated water into the sea both domestically and internationally, in close cooperation with the IAEA, which firmly maintains neutrality.

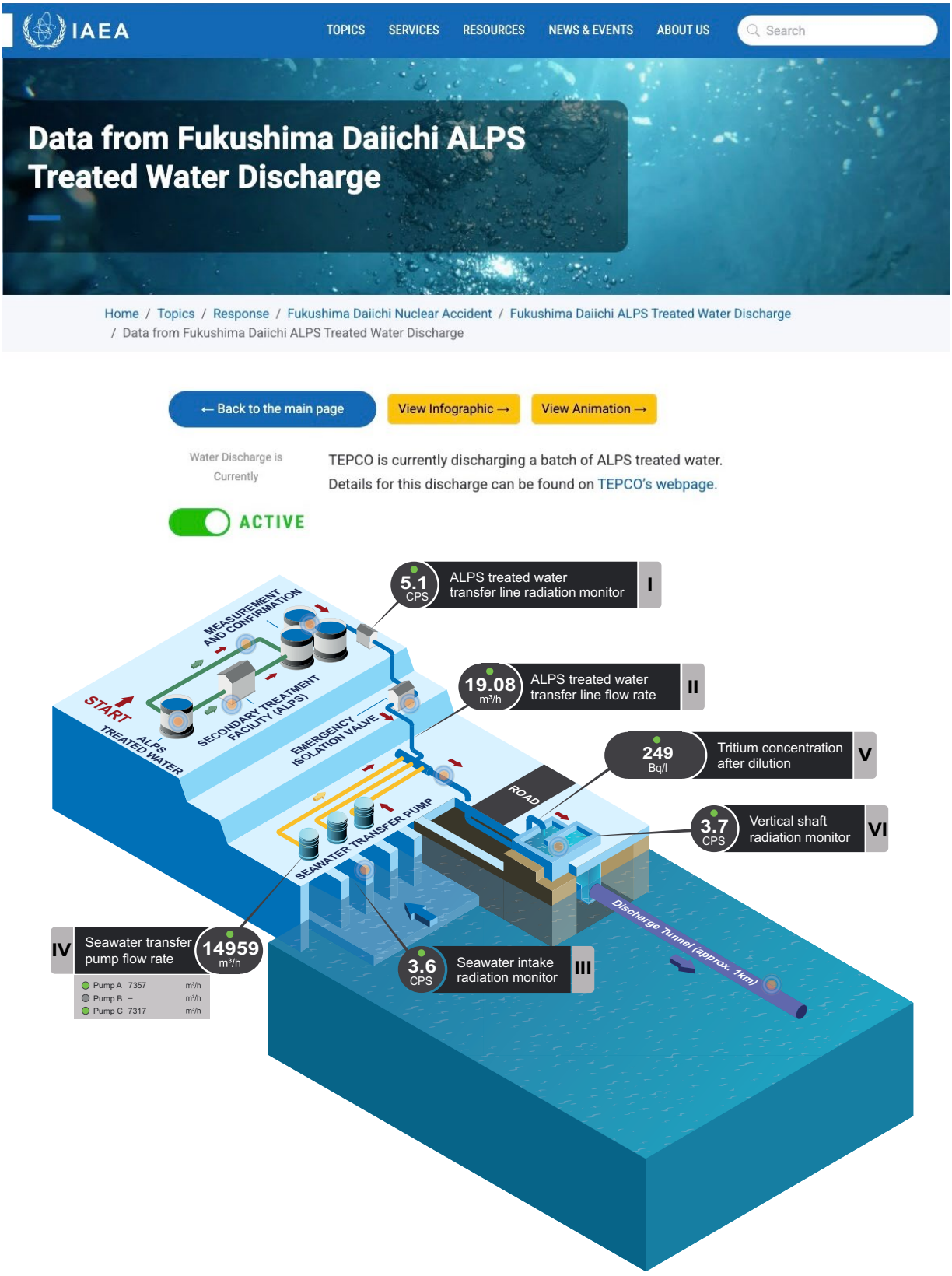
(Reference1) ALPS Treated Water
ALPS treated water is water which is processed by devices such as ALPS (Advanced Liquid Processing System) to ensure that the concentration of the radioactive materials other than tritium surely meet the regulatory standards for safety. In addition, ALPS treated water is sufficiently diluted before discharge into the sea so that radioactive materials, including tritium, are far below the regulatory standards for safety.

(Reference2) Composition of IAEA Task Force
The IAEA Task Force includes 11 international experts, serving in an independent position, from Argentina, Australia, Canada, China, France, Republic of Korea, the Marshall Islands, Russia, the United Kingdom, the United States, and Viet Nam.

(Reference3)

https://www.mofa.go.jp/press/release/pressite_000001_02343.html

Figure 5 Live data from IAEA website on Fukushima Daiichi ALPS Treated Water Discharge.



https://www.iaea.org/topics/response/fukushima-daiichi-nuclear-accident/fukushima-daiichi-alps-treated-water-discharge/tepco-data

In Okinawa, officials and researchers have highlighted how genuine grievances over the heavy concentration of United States military facilities in the prefecture from noise and accidents to land use and crime are instrumentalised by PRC narratives portraying the prefecture as alienated from both mainland Japan and the US–Japan alliance, and have adjusted messaging to acknowledge local concerns while exposing manipulation. Around Senkaku and Taiwan, this concerns recent close-encounter incidents reported by domestic media, such as episodes in which Chinese coast guard or naval vessels and aircraft operate in ways Japan deems coercive or unsafe near Japanese–administered territory or in airspace close to Japan and Taiwan.[83] Japan's MOFA has challenged and rebutted Chinese narratives that cast Japan and PM Takaichi as remilitarising or provoking crisis, embedding rebuttals in security and legal language and situating them in a broader pattern of hybrid tactics aimed at eroding Japan's democratic cohesion and alliance credibility.[84] China has been attempting throughout 2025 to strengthen the link between Japan and its history from WWII, and thus trying to antagonise the country within the region.

The Takaichi case also demonstrates the value of cross–border civil society monitoring. FactLink's findings[85] show that narratives first familiar to Taiwanese researchers, including fabricated diplomatic scandals, accusations of provocation over Taiwan, and attempts to manufacture 'local' outrage, were adapted for Japanese political debates. This reinforces the need for Japan and Taiwan to share monitoring methods, platform evidence and narrative typologies, especially during moments of heightened cross–strait tension.

Regarding China's narratives about its military activities around Taiwan and the East China Sea, Japan has adapted its strategic communications to respond to these propaganda efforts. Ministries now increasingly pair statements on specific PLA activities with explicit rejection of these narratives, tying physical coercion and information manipulation together in their public communication. MOFA has increasingly issued rapid, on-the-record statements condemning Chinese actions, explicitly rejecting Beijing's legal and historical claims, and warning that Chinese state

media and online narratives misrepresent the situation at sea. Below is an example where the Chinese Coast Guard was found to have infringed upon Japanese territorial waters around the Senkaku Islands at around 12pm on 3 May 2025. On the same day, MOFA issued a social media post on Facebook mentioning the incident and detailed the Japanese formal diplomatic protest to the incident.

Figure 6 The MOFA of Japan issued a statement condemning the intrusion by four China Coast Guard vessels near Senkaku Islands on 3 May 2025.

https://x.com/MofaJapan_en/status/1918664739305210196?s=20

Civil society and media

Civil society responses, such as initiatives by the Japan Fact–Check Centre, FactCheck Initiative Japan, InFact, and Litmus, provide fact-checking and media literacy content across multiple platforms – websites, social media, and collaborations with mainstream outlets – on domestic and foreign disinformation, including Fukushima rumours, Russia–Ukraine narratives, and election–related falsehoods. Using JFC as an example, it publishes article–style fact–checks, short graphic explainers, and educational materials that are shared via X, the principal social media platform used in Japan, as well as YouTube and partner media.[86] These are increasingly used in schools and by teachers' associations, but reach and funding remain modest compared with the scale of the problem, and there is no systematic mechanism for their assessment to directly trigger regulatory or legal action.[87]

Although fact-checkers and NGOs produce high-quality analysis, they typically lack stable funding, staff and formal channels into ministries, so their outputs may inform officials informally or via ad-hoc consultations but are not structurally embedded in decision-making processes or legislative drafting. For example, JFC's work on Fukushima rumours and COVID-era misinformation has been cited in public discussions and referenced by MIC-linked literacy initiatives, yet there is no institutionalised requirement for ministries or platforms to act on specific findings beyond voluntary commitments.[88]

Think tanks and academic researchers systematically map information operations, particularly those targeting Japan, and publish their findings in policy briefs, reports and conference presentations that are then shared with ministries through briefings, advisory councils and closed-door workshops.[89] Examples include policy briefs on China's Okinawa narratives detailing how Beijing selectively amplifies base-related incidents and independence-leaning voices, and comparative studies of authoritarian disinformation in Japan that identify specific content clusters

and cross-platform behaviours.[90] These materials have been used in MOFA and MIC study sessions, and have informed shifts in strategic messaging and the design of multi-stakeholder initiatives like EPaD.

There is also growing, albeit modest, cooperation with Taiwan at the level of research and civil society: Japanese FIMI experts and NGOs have engaged in exchanges and joint events with Taiwanese counterparts on fact-checking methods, election-time monitoring and counter-narratives, using Taiwan's experience as a benchmark while adapting it to Japan's more cautious legal and political environment.[91]

Mainstream media remain cautious gatekeepers, as big newspapers and broadcasters still have strong editorial filters and tend not to amplify fringe or unverified stories, which slows the spread of some falsehoods but can also delay active debunking. However, they are slowly expanding disinformation desks and explainer formats, launching dedicated fact-checking or 'verification' columns and producing visual explainers on contested topics. For example, NHK and major dailies have run recurring features that verify viral claims about Fukushima treated water and AI-generated election content, using Q&A articles, infographics and short videos to walk readers through why certain posts are misleading or false.[92] [93] Editorials increasingly call for stronger platform accountability and safeguards against AI-generated falsehoods in elections and disasters, even as regulation remains largely voluntary and reliant on MIC-mediated co-regulation rather than EU-style enforcement.

International and alliance-based tools

A key feature of Japan's approach is the extent to which counter-FIMI has been internationalised. Japan participates in the G7 Rapid Response Mechanism, where like-minded states exchange analysis and coordinate responses to foreign information manipulation, and has used these platforms to highlight China's narratives around Ukraine, the Middle East, and Indo–Pacific security as part of a shared threat picture.[94]

Tokyo has also concluded a specific Memorandum of Cooperation (MoC) with the United States on countering foreign information manipulation,

signed in December 2023, which commits both sides to closer information-sharing, joint analysis, and capacity-building.[95] MOFA has followed this up with online and hybrid workshops on disinformation and election–related information threats that bring together officials, researchers and civil society actors from ASEAN and wider Indo-Pacific partners, using Japan's experience with Fukushima narratives and Okinawa 'malinformation' as case studies and positioning Japan as both a learner and a provider of expertise.[96]

These efforts sit alongside Japan's broader push in G7 and OECD settings to link FIMI with generative AI risks and trusted data flows. The G7 Hiroshima Process on AI[97], launched under Japan's 2023 G7 presidency, produced principles and a code of conduct for advanced AI systems that explicitly highlight risks of disinformation, deepfakes and content authenticity, while the 'Data Free Flow with Trust' agenda[98] seeks to enable cross–border data flows under robust privacy, security and transparency safeguards, including expectations on platform governance and algorithmic accountability. As a result, counter-FIMI is no longer treated as a niche communications project but as part of digital governance and economic security policy, an approach that aligns naturally with many EU debates.

3. Part Three: Lessons for German and European Policymakers

What lessons German and European Policymakers can learn from Taiwan

Germany occupies a unique position within Europe's response to FIMI. As the EU's largest member state (by population) and a major target of hostile information operations, Germany's approach to democratic resilience is likely to influence broader European efforts in the years ahead. Taiwan has been the target of China's well–resourced and multi–pronged FIMI operation for well over a decade. As is increasingly the case with Russia's threats against Europe, FIMI is integrated into a broader set of grey–zone activities that only just remain below the threshold of open conflict. Despite this pressure, Taiwan has remained a thriving democracy and one of the freest countries in Asia. German and European policymakers should learn from Taiwan's hard–earned experience, adopting an approach that is innovative, pro–active and goes beyond the realm of government:

→ **Integrating FIMI into crisis preparedness:** Policymakers should follow Taiwan's example by integrating FIMI preparedness into broader efforts to increase societal resilience to hybrid threats. Public education initiatives, such as the crisis manuals published by the Taiwanese government, can help prepare citizens for hostile propaganda, disinformation, rumours and mass panic in the event of grey–zone or conflict activities. As demonstrated by Taiwan's Whole–of–Society Defence Resilience Committee, civil society

groups, businesses and community groups should be brought into table–top exercises, live drills and planning processes for hostile FIMI operations.

→ **Supporting a vibrant civil society ecosystem:** Germany and other European countries should seek to emulate Taiwan's rich network of civil societies working on fact–checking, media literacy and information space monitoring. While this ecosystem should operate independently of the government, seed–funding, fellowships and grants disbursed by arms–length institutions can help support these organisations financially. Governments should seek to establish meaningful and regular communication channels with civil society groups to learn from their insights, be alerted to developing issues and consider their policy recommendations.

→ **Delivering pro–active and innovative government–citizen communications:** Rather than reacting to false information or hostile FIMI operations after such ideas have become widespread, Germany and other European governments should seek to emulate Taiwan's pro–active stance: 'pre–bunking' developing rumours and setting time–limited targets to respond to issues. Taiwan's 'humour over rumour' efforts also show the benefits of developing creative approaches to reaching citizens on social media and not being limited to government statements and traditional media, though many of these ideas need to be standardised into government processes in order to become sustainable.

→ **Integrating media and digital literacy into education:** Including media literacy skills as a core component of school curriculums can help develop citizens who are able to exercise critical thinking skills, check and verify information, and be less susceptible to FIMI operations. This can be built into broader efforts to establish 'digital citizen' literacy, which also help citizens understand issues around use of AI, data security and privacy. This is particularly important for younger generations among whom engagement with traditional media is declining. As with Taiwan, such efforts

can be supported by government delegating universities or other third–party institutions to develop training and teaching materials to support schools delivering such content.

What lessons German and European Policymakers can learn from Japan

For Europe, Japan's experience offers several practical lessons that complement existing EU instruments like the Digital Services Act (DSA), Code of Practice, and the European Digital Media Observatory (EDMO).

- → **Integrating strategic communications into foreign and security policy:** Japan embeds FIMI in its National Security Strategy and Diplomatic Bluebooks, translating that into MOFA-led fact-based campaigns on key disputes. EU Member States should also integrate FIMI as a core part of their foreign and security policy, in recognition of its growing importance. At the EU level, capacity building to support counter–FIMI work can be integrated into neighbourhood and enlargement tools, which are already used to support independent media, civil society, rule of law and resilience to hybrid threats. Funding media literacy and fact–checking in candidate and neighbourhood countries or integrating FIMI awareness into security and hybrid threat assistance can be ways to do this.
- → **Developing external facing information hubs:** Japan has built a hub inside MOFA, dedicating structures to monitor hostile narratives, coordinate analysis and rebuttals, maintain a 'responses to information manipulation' page, and lead international outreach and capacity-building. This model illustrates how foreign ministries can host counter-FIMI capabilities tied to evidence-based communication and cooperation with independent fact-checkers.

→ **Alliance-driven resilience and capacity-building:** Japan's intensive use of G7 RRM, the US-Japan Memorandum of Cooperation, and Indo-Pacific workshops shows how a middle power can leverage alliances to amplify responses and learn from partners. The EU can deepen EU–Japan and G7 cooperation to compare responses to existing case studies, conduct joint horizon-scanning, and share methodologies for attribution and incident logging. The results can feed into both the EU Rapid Alert System and national capabilities. While much of this exists in embryonic form via the G7 Rapid Response Mechanism, systematic two-way linkage with the Rapid Alert System and member-state systems still needs strengthening. For Germany and the EU, cooperation with Japan and Taiwan should therefore include joint incident logging, shared taxonomies for Chinese FIMI narratives, researcher exchanges, and structured channels between civil society investigators, platforms and foreign ministries.

→ **The vulnerability of critical infrastructure to FIMI operations:** The Okinawa and Fukushima episodes highlight how hostile actors can exploit controversies to both increase local grievances and threaten the political viability of key aspects of critical-infrastructure. For Europe, where gas pipelines, LNG terminals and nuclear plants have repeatedly been targeted by Russian disinformation and hybrid campaigns, these vulnerabilities also exist. The Japanese government's efforts to publish clear, accessible information on issues around safety, environmental impact, and regulatory oversight of controversial projects, as well as actively engaging with municipalities, local media and community groups that are directly affected by such projects, helped address genuine concerns and reduced the space for external actors to instrumentalise them.

At the same time, Tokyo still lacks robust pre-bunking, comprehensive election-specific protections, and binding platform rules. Japan is only in a relatively preparatory stage compared with the EU's more developed

regulatory tools on platforms and political advertising. Japan therefore works best not as a regulatory template but as a partner and reference case for how to integrate FIMI into foreign and security policy, how to build effective strategic communications, and how to handle narratives around sensitive issues like treated water, Okinawa, Senkaku and Taiwan in ways compatible with democratic norms.

Comparison with the European Democracy Shield and other initiatives

The EU's European Democracy Shield (EDS), unveiled in November 2025, presents an ambitious programme to coordinate and bolster attempts to protect the EU's democratic life from foreign interference.[99] It is welcome to see the EDS emulate many of the strengths highlighted in Japan and Taiwan's response to FIMI. However, much work is needed to ensure these ambitions are realised, both in Germany and across the EU as a whole.

- → **Engagement with civil society:** Given the important role played by civil society in Taiwan, it is welcome to see the EU Democracy Shield put efforts to engage non–governmental actors at the forefront of the EDS. The establishment of a Stakeholder Platform bringing together EU civil society organisations, think tanks, researchers and academia, fact–checkers and media providers is a good step in the right direction. However, to be effective, this work must also be emulated at the Member State level. As demonstrated in Taiwan, localised networks are important to gain social trust and address FIMI issues within the unique linguistic and political context of each country. While the EDS and EDMO present important frameworks for civil society groups to collaborate and learn from each other at the EU level, this cannot be a replacement for civil society action at the nation level.
- → **Media literacy:** The EDS rightly highlights media and information literacy as pillars of long-term resilience. Information literacy is

also to the importance of youth, education and critical thinking skills, which echoes Taiwan's integration of critical thinking and information-handling skills into school curricula and public education. To translate this into practice, Member States should be encouraged to embed media and digital literacy as core learning outcomes in primary and secondary education, supported by teacher training and age-appropriate materials developed with universities and independent experts, as seen in Taiwan's partnerships with academic institutions.

→ **Strategic communications and foreign policy:** The EDS does recognise FIMI as a major foreign policy challenge, not just for Member States, but also for the broader EU neighbourhood. For this reason, the European External Action Service (EEAS) will continue to play an important role in counter–FIMI initiatives, by hosting the already established Rapid Alert System between Member States and through conducting counter–FIMI work through its network of delegations and missions. A more proactive approach is also promised in EU candidate and prospective candidate states, which have been targets of Russian FIMI operations. However, there is not yet much detail on how the EDS will work more systematically with the EU's external partners, aside from established mechanisms in the G7 and NATO. Notably, neither Japan nor Taiwan were specifically mentioned as potential partners in the EDS Communication.

→ **Crisis response:** The EDS does reference a number of proposed and existing mechanisms to deal with major FIMI operations, including preparing an incident and crisis response protocol under the Digital Services Act (with a particular focus on FIMI risks on large platform providers and AI generated content) and extending the mandate of EDMO to conduct more monitoring of FIMI threats. Elections are specified as moments of particular focus for counter–FIMI resources. However, such an approach would

benefit from dedicated crisis planning, war–gaming and drills to test out these mechanisms – as emulated by Taiwan's Whole–of–Society Defence Resilience Committee.

While there are important parallels between these approaches and existing European initiatives, not all aspects of Taiwan's and Japan's responses can be directly replicated in Europe. Differences in constitutional traditions, media systems, threat perceptions and public attitudes towards state intervention mean that any lessons must be adapted to local circumstances.

4. Policy Recommendations

For Germany and Other EU Member States

→ **Integrate FIMI into public preparedness initiatives:** Germany should integrate FIMI preparedness into broader efforts to increase societal resilience to hybrid threats. In particular, federal and state–level governments should work together to stage public preparedness drills and exercises and publish crisis manuals for citizens, raising awareness of the role that hostile information operations could play in a crisis. Civil society groups, businesses and community groups should be brought into table–top exercises, live drills and planning processes hosted by government actors.

→ **Strengthen media literacy and civic education:** Policymakers should define media literacy skills as a 'basic competency' within school curriculums, helping citizens to exercise critical thinking skills, check and verify information, and be less susceptible to FIMI operations. This can be built into broader efforts to establish 'digital citizen' literacy, which also help citizens understand issues around use of AI, data security and privacy. Promises to support digital and media literacy under the DigitalPakt Schule programme are welcome.[100] Such efforts can be supported by government delegating universities or other third–party institutions to develop training and teaching materials to support schools delivering such content.

→ **Support a vibrant civil society ecosystem:** Governments should seek to emulate Taiwan's rich network of civil societies working on fact–checking, media literacy and information space monitoring. While this ecosystem should operate independently of the government, seed–funding, fellowships and grants

disbursed by arms-length institutions can help support these organisations financially. Funding for civil society innovations against disinformation through the *Live Democracy! (Demokratie leben!)* programme are welcome and should be continued and expanded.[101]

→ **Establish civil society engagement platforms:** Governments must establish platforms to enable direct engagement with civil society groups, researchers, experts and tech platforms on issues around FIMI. Meaningful and regular communication channels with such groups can help policymakers learn from their insights, be alerted to developing issues and consider their policy recommendations.

→ **Deliver pro-active and innovative government-citizen communications:** At a minimum, governments should host a 'response to misinformation' page, as seen in Japan. More innovative tools – such as the 'humour over rumour' and social-media friendly graphics developed in Taiwan – should also be considered and systematised into government operations. Responding quickly to 'pre-bunk' rumours before they take root more widely should be a goal of government communications.

For the EU

→ **Deepen counter-FIMI alliances:** Strategic communications and counter-FIMI work must be a top priority for the EU's collective foreign policy. The EU should look to expand alliances beyond its traditional G7 and NATO partners, and also include Japan, Taiwan and other like-minded countries facing similar challenges. Such exchanges can share best practice, share information on emerging threats, and consider coordinated responses.

→ **Develop EU-wide crisis drills:** The EU should test out established and developing mechanisms for FIMI incident response by

running crisis simulations. As demonstrated by Taiwan's Whole–of–Society Defence Resilience Committee, war–games, drills and exercises should engage a broad range of government, private sector and civil society actors.

→ **Increase funding for civil society initiatives:** The proposed AgoraEU programme should include a dedicated budget for civil society groups working to protect democratic processes by upholding the integrity of the information environment. The fund should seek to support activities including research into FIMI operations, independent fact–checking, raising public awareness, and media and digital literacy campaigns – all of which civil society is best placed to do.

→ **Deepen counter–FIMI work in the EU neighbourhood:** The EU should continue efforts to strengthen counter–FIMI work among its immediate neighbours, including EU candidate and prospective candidate states, who have often been the prime target of Russian FIMI work. Capacity building efforts, particularly at the civil society level, can be complementary to existing efforts to support the independent media, rule of law and resilience to hybrid threats in these countries.

Bibliography

1 AFP Hong Kong. 'Chinese Social Media Posts Falsely Claim German Right-Wing Leader Praises China | Fact Check.' 13 June 2025. https://factcheck.afp.com/doc.afp.com.49VD6CW.

2 Al Jazeera. 'Twitter Drops 'State-Affiliated', 'Government-Funded' Labels.' April 2023. https://www.aljazeera.com/economy/2023/4/21/twitter-drops-state-affiliated-government-funded-labels.

3 Alaphilippe, Alexandre, Gary Machado, Raquel Miguel, and Francesco Poldi. 'Doppelganger – Media Clones Serving Russian Propaganda.' EU DisinfoLab, 27 September 2022. https://www.disinfo.eu/doppelganger/.

4 Alliance For Securing Democracy. 'Chinese State Media Bolster CCP Narratives to Potentially Unaware Audiences in Germany.' no date. https://securingdemocracy.gmfus.org/incident/chinese-state-media-bolster-ccp-narratives-to-potentially-unaware-audiences-in-germany/.

5 All-out Defense Mobilization Agency, M.N.D. '2025 Urban Resilience (All-Out Defense Mobilization) Exercise of Taipei City Has Been Completed Successfully on July 17 (Thursday).' 24 July 2025. https://adma.mnd.gov.tw/uniten/100008/7923.

6 BBC Monitoring. 'Analysis: China, Russia Media Narratives on Ukraine War Converge.' 23 August 2022. https://monitoring.bbc.co.uk/product/c203oxco.

7 BBC News. 'Wuhan Lab Leak Theory: How Fort Detrick Became a Centre for Chinese Conspiracies.' US & Canada. 22 August 2021. https://www.bbc.co.uk/news/world-us-canada-58273322.

8 Bundesministeriums für Bildung, Familie, Senioren, Frauen und Jugend. 'DigitalPakt Schule.' BMBFSFJ, no date. https://www.bmbfsfj.bund.de/bmbfsfj/themen/bildung/schule/digitalpakt-schule-275098.

9 Tobias Bunde and Sophie Eisentraut (eds.), 'Munich Security Report 2026: Under Destruction, Munich: Munich Security Conference,' February 2026, https://doi.org/10.47342/JWIE5806

10 Cai, Derek. 'Fukushima: China's Anger at Japan Is Fuelled by Disinformation.' Asia. BBC News, 2 September 2023. https://www.bbc.co.uk/news/world-asia-66667291.

11 China Global Television Network. 'Workers Party of Britain Leader George Galloway: The West Knows Its Own Democracy Isn't Working.' 23 March 2023. https://news.cgtn.com/news/2023-03-23/George-Galloway-The-West-knows-its-own-democracy-isn-t-working-1ipDlpgG4M0/index.html.

12 CSIS. 'Combating Disinformation: A View from Japan.' 10 July 2024. https://www.youtube.com/watch?v=erCM1OxKzi0.

13 D'Ambrogio, Enrico. 'Japan's Preparedness Strategies: Lessons for the EU.' European Parliamentary Research Service, 2025. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/777941/EPRS_BRI%282025%29777941_EN.pdf.

14 Davidson, Helen. 'China Revives Conspiracy Theory of US Army Link to Covid.' World News. The Guardian, 20 January 2021. https://www.theguardian.com/world/2021/jan/20/china-revives-conspiracy-theory-of-us-army-link-to-covid.

15 Davidson, Helen. 'China Using Influencers to Whitewash Human Rights Abuses, Report Finds.' World News. The Guardian, 20 October 2022. https://www.theguardian.com/world/2022/oct/20/china-using-influencers-to-whitewash-human-rights-abuses-report-finds.

16 Deutsche Welle 'Faktencheck: Wie Russland versucht, die Wahl zu beeinflussen". Dw.Com, February 2025. https://www.dw.com/de/faktencheck-russland-bundestagswahl-desinformation-und-fakes-v3/a-71601152

17 Deutsche Welle. 'Germany: AfD's Krah Faces Probe on Russia, China 'Payments". Dw.Com, April 2024. https://www.dw.com/en/germany-afds-krah-faces-probe-on-russia-china-payments/a-68912872.

18 Digital Agency, Government of Japan. 'Data Free Flow with Trust (DFFT).' 16 October 2024. https://www.digital.go.jp/en/policies/dfft.

19 Doroshenko, Larissa. 'Catch Me If EU Can: How RT and Sputnik Evade EU Content Bans.' Interference Matters. Alliance For Securing Democracy, 23 June 2025. https://securingdemocracy.gmfus.org/catch-me-if-eu-can-how-rt-and-sputnik-evade-eu-content-bans/.

20 Dreyer, June Teufel. 'The Gloves Come Off.' Comparative Connections, 15 May 2021. https://cc.pacforum.org/2021/05/the-gloves-come-off/.

21 Economist Intelligence Unit. 'Democracy Index 2024.' n.d. Accessed 9 January 2026. https://www.eiu.com/n/campaigns/democracy-index-2024/.

22 European Commission. 'Communication on the European Democracy Shield.' 12 November 2025. https://commission.europa.eu/document/2539eb53-9485-4199-bfdc-97166893ff45_en.

23 European Union External Action. '1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a Framework for Networked Defence.' 2023. https://euvsdisinfo.eu/uploads/2023/02/EEAS-ThreatReport-February2023-02.pdf.

24 European Union External Action. '4th EEAS Report on Foreign Information Manipulation and Interference Threats: Dismantling the FIMI House of Cards.' 2026. https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf.

25 FactLink. '日本首相高市早苗「台灣有事說」事件：拆解中國資訊戰與謠言攻勢.' 22 February 2026. https://www.factlink.tw/p/takaichi-sanae-china-information.

26 Fakultät für Bildungswissenschaften. 'Demokratie Leben! / Live Democracy!' no date. https://www.uni-due.de/edu-research/demokratieleben_en.php.

27 Gang, Wang, and Liam Scott. 'Trolling of Female Asian Journalists on Rise as Beijing Seeks to Discredit Media.' Voice of America, 2 January 2023. https://www.voanews.com/a/trolling-of-female-asian-journalists-on-rise-as-beijing-seeks-to-discredit-media/6898789.html.

28 Gershaneck, Kerry. 'Political Warfare: Strategies for Combating China's Plan to 'Win without Fighting.' Quantico, VA: Marine Corps University Press, 2020.

29 Giles, Keir. "Information Troops' – A Russian Cyber Command?' NATO Cooperative Cyber Defence Centre of Excellence, 2011. https://www.ccdcoe.org/uploads/2018/10/InformationTroopsARussianCyberCommand-Giles.pdf.

30 Gleichgewicht, Daniel. 'How YouTube Helps Russia Share How Great It Is in Raw and Subtle Ways.' New Eastern Europe, 15 July 2024. https://neweasterneurope.eu/2024/07/15/how-youtube-helps-russia-share-how-great-it-is-in-raw-and-subtle-ways/.

31 Hawkins, Amy, Geneva Abdul, and Tory Shepherd. 'Sexually Explicit Letters about Exiled Hong Kong Activists Sent to UK and Australian Addresses.' World News. The Guardian, 11 December 2025. https://www.theguardian.com/world/2025/dec/11/sexually-explicit-letters-deepfake-hong-kong-activists-uk-australia.

32 Hille, Kathrin. 'Taiwan Revokes Residency for Chinese TikTok Influencer.' Financial Times, 12 March 2025. https://www.ft.com/content/4891c723-d9a3-4b00-84d6-1cd603c84761.

33 Hou, Isabel. 'Civil Society in East Asia: The Fight against Disinformation.' no date. https://www.goethe.de/ins/kr/en/kul/mkp/kgd.html.

34 Hsiao, Russell. 'Political Warfare Alert: The PRC's Evolving Information Operations Targeting Provincial and Local Media Intermediaries.' Global Taiwan Brief 8, no. 1 (2023). https://globaltaiwan.org/wp-content/uploads/2023/01/GTB-8.1-PDF-v2.pdf.

35 IAEA. 'Fukushima Daiichi ALPS Treated Water Discharge – Reports.' IAEA, 28 April 2022. http://www.iaea.org/topics/response/fukushima-daiichi-nuclear-accident/fukushima-daiichi-alps-treated-water-discharge/reports.

36 Ichihara, Maiko. 'China's 'Malinformation' Comes for Okinawa.' The Diplomat, 20 March 2025. https://thediplomat.com/2025/03/chinas-malinformation-comes-for-okinawa/.

37 Ichihara, Maiko. 'Japan's Upper House Election Reveals How Russian Influence Operations Infecting AI with Flood of Propaganda, Stoking Divisions.' Nippon.Com, 27 October 2025. https://www.nippon.com/en/in-depth/d01170/.

38 Inoue, Yukana. 'Concerns Grow in Japan over Possible Russian Interference in Sunday's Election.' The Japan Times, 18 July 2025. https://www.japantimes.co.jp/news/2025/07/18/japan/politics/russia-influence-japan-election/.

39 Institute for Strategic Dialogue. 'Investigation: How Russia Today Is Evading Sanctions and Spreading pro-Kremlin Propaganda in Italy.' 13 May 2025. https://www.isdglobal.org/digital_dispatches/investigation-how-russia-today-is-evading-sanctions-and-spreading-pro-kremlin-propaganda-in-italy/.

40 Japan Fact-Check Centre. 'Japan Fact-check Center (JFC) Activity Report.' 2025. https://www.factcheckcenter.jp/jfc-activity-report-2024-eng/

41 Kimura, Yuta. 'Protecting Japan's National Security from Information Operations.' ASPI Strategist, 5 July 2024. https://www.aspistrategist.org.au/protecting-japans-national-security-from-information-operations/.

42 Kus, Canan, and Xiaolu Zhang. 'Alice Weidel: Xiaohongshu Star – Rosa-Luxemburg-Stiftung.' 6 June 2025. https://www.rosalux.de/en/news/id/53473/alice-weidel-xiaohongshu-star.

43 Leloup, Damien, and Florian Reynaud. 'The fake YouTube channels working for pro-China influence operations.' Pixels,China. Le Monde, 20 January 2024. https://www.lemonde.fr/en/pixels/article/2024/01/20/the-fake-youtube-channels-working-for-pro-china-influence-operations_6449975_13.html.

44 Lindholm, Rickard. 'Increased Election Interference Activity in Eastern Europe Reveals Difficulties for Democracies to Fight Back. Wilson Center,' 2025. https://www.wilsoncenter.org/article/increased-election-interference-activity-eastern-europe-reveals-difficulties-democracies.

45 Lucas, Edward, Jake Morris, and Corina Rebegea. 'Information Bedlam: Russian and esidency permitormation Operations During the Covid–19 Pandemic.' CEPA, 15 March 2021. https://cepa.org/comprehensive–reports/information–bedlam–russian–and–chinese–information–operations–during–the–covid–19–pandemic/.

46 Mahdawi, Arwa. 'Humour over Rumour? The World Can Learn a Lot from Taiwan's Approach to Fake News.' Opinion. The Guardian, 17 February 2021. https://www.theguardian.com/commentisfree/2021/feb/17/humour–over–rumour–taiwan–fake–news.

47 Marocico, Oana, Seamus Mirodan, and Rowan Ings. 'How Russian–Funded Fake News Network Aims to Disrupt European Election.' BBC News, 21 September 2025. https://www.bbc.co.uk/news/articles/c4g5kl0n5d2o.

48 Matura, Tamás. 'Sino–Russian Convergence in Foreign Information Manipulation and Interference: A Global Threat to the US and Its Allies.' CEPA, 30 June 2025. https://cepa.org/comprehensive–reports/sino–russian–convergence–in–foreign–information–manipulation–and–interference/.

49 Ministry of Foreign Affairs of Japan. 'Japan's Foreign Policy to Promote National and Global Interests.' 2023. https://www.mofa.go.jp/policy/other/bluebook/index.html.

50 Ministry of Foreign Affairs of Japan. 'The Responses to Information Manipulation, Including Spread of Disinformation.' 4 December 2025. https://www.mofa.go.jp/policy/pagewe_000001_00052.html.

51 Ministry of Foreign Affairs of Japan. 'The Signing of the US Japan Memorandum of Cooperation on Countering Foreign Information Manipulation.' 6 December 2023. https://www.mofa.go.jp/press/release/pressite_000001_00027.html.

52 Ministry of Foreign Affairs of Japan. 'Regarding the Inappropriate Remarks by a Chinese Participant to the Munich Security Conference.' 15 February 2026. https://www.mofa.go.jp/a_o/c_m1/cn/pageite_000001_01483.html.

53 Ministry of Internal Affairs and Communications of Japan. 'Hiroshima AI Process.' no date. https://www.soumu.go.jp/hiroshimaaiprocess/en/index.html.

54 Ministry of Internal Affairs and Communications of Japan. 'Launch of DIGITAL POSITIVE ACTION, a Public–Private Partnership Project (Hereinafter Referred to as the 'Project'), to Improve ICT Literacy Comprehensively| Press Release.' MIC ICT Policy, 22 January 2025. https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2025/1/22_2.html.

55 Ministry of Internal Affairs and Communications of Japan. 'Operations Guide for FY2024 Edition.' 2024. https://www.soumu.go.jp/main_content/001013649.pdf.

56 Ministry of Internal Affairs and Communications of Japan. 'Release of 'Existing Practices against Disinformation (EPaD)' at the Internet Governance Forum Kyoto 2023.' MIC ICT Policy, 18 October 2023. https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2023/10/18_3.html.

57 Naing, Hnin Wint. 'China's Repression on German Soil, Transnational Repression.' 2 December 2025. https://www.freiheit.org/southeast–and–east–asia/chinas–repression–german–soil.

58 National Cybersecurity Office. 'Commitment to a Free, Fair and Secure Cyberspace.' no date. https://www.cyber.go.jp/eng/index.html.

59 NHK. 'AI Deepfakes Cloud Japan's Election.' 12 February 2026. https://www3.nhk.or.jp/nhkworld/en/news/backstories/4602/.

60 NHK. 'Japanese Officials Respond to China Military Plane's Intrusion.' August 2024. https://www3.nhk.or.jp/nhkworld/en/news/backstories/3529/.

61 Nikkei Asia. 'Social Media Fuel Pro-Okinawa Independence Disinformation Blitz.' 3 October 2024. https://asia.nikkei.com/spotlight/cybersecurity/social-media-fuel-pro-okinawa-independence-disinformation-blitz.

62 Nimmo, Ben, Nathaniel Gleicher, Margarita Franklin, Lindsay Hundley, and Mike Torrey. 'Meta Quaterly Adversarial Threat Report Q3 2023.' Meta, 2023. https://scontent-man2-1.xx.fbcdn.net/v/t39.8562-6/406961197_3573768156197610_1503341237955279091_n.pdf?_nc_cat=105&ccb=1-7&_nc_sid=b8d81d&_nc_ohc=Rb7RGkhvCiwQ7kNvwFvnvGu&_nc_oc=AdkJPakvp3nOjMSc8eCP7XcWUbCZmjUxHBMJpZmcQdE9lrraWZTSx5C6H9-8c3Y4XfQ1dr4Y_UGFWLn7C4SMqTGw&_nc_zt=14&_nc_ht=scontent-man2-1.xx&_nc_gid=I1ResV_lDF1EyKZW5AguDg&oh=00_AfqNDkqE3QFpA2b1gZySEQb7DMXQMbcaOCFIZwSO9zVSYQ&oe=69670252.

63 Office of the President Republic of China (Taiwan). 'About the Committee.' no date. https://english.president.gov.tw/Page/670.

64 Omelicheva, Mariya. 'Russia's Doxing Campaign: An Expanding Trend in Extraterritorial Repression.' 5 August 2024. https://russiapost.info/society/doxing_campaign.

65 Osthoff, Katharina. 'A look behind the scenes of Chinese espionage in the European Parliament.' 26 April 2024. https://www.freiheit.org/europe/look-behind-scenes-chinese-espionage-european-parliament

66 Our World in Data. 'Democracy Index.' Accessed 9 January 2026. https://ourworldindata.org/grapher/democracy-index-eiu?tab=line&time=2010..2024&country=JPN~TWN~OWID_EUR&mapSelect=JPN~TWN.

67 Padalko, Halyna. 'AI and Information Manipulation: Russia's Interference in the US Elections.' Centre for International Governance Innovation, 22 August 2025. https://www.cigionline.org/publications/ai-and-information-manipulation-russias-interference-in-the-us-elections/.

68 Repnikova, Maria. 'China's Propaganda on the War in Ukraine.' China Leadership Monitor, no. 72 June 2022. https://www.prcleader.org/post/china-s-propaganda-on-the-war-in-ukraine.

69 Reporters Without Borders. 'War in Ukraine: Beware of China's Amplification of Russian Propaganda, RSF Says.' 14 April 2022. https://rsf.org/en/war-ukraine-beware-china-s-amplification-russian-propaganda-rsf-says.

70 Sasakawa USA. "Just Being Born': Assessing and Countering Foreign Information Manipulation and Interference (FIMI) in Japan.' 23 January 2026. https://spfusa.org/publications/just-being-born-assessing-and-countering-foreign-information-manipulation-and-interference-fimi-in-japan/.

71 Seibt, Sébastian. 'Has Germany's Far-Right AfD Become a Gateway for Chinese and Russian Spies?' France 24, 26 April 2024. https://www.france24.com/en/europe/20240426-has-germany-s-far-right-afd-become-a-gateway-for-chinese-and-russian-spies.

72 Tang, Audrey, and Eva-Maria Verfürth. 'Taiwan Is Standing up to Disinformation.' 12 June 2025. https://www.dandc.eu/en/article/how-taiwan-has-reduced-social-polarisation-and-become-more-resilient-disinformation.

73 Taylor, Josh. 'Meta Closes Nearly 9,000 Facebook and Instagram Accounts Linked to Chinese 'Spamouflage' Foreign Influence Campaign.' Technology. The Guardian, 29 August 2023. https://www.theguardian.com/australia-news/2023/aug/30/meta-facebook-instagram-shuts-down-spamouflage-network-china-foreign-influence.

74 Taylor, Josh. 'Twitter Deletes 170,000 Accounts Linked to China Influence Campaign'. Technology. The Guardian, 12 June 2020. https://www.theguardian.com/technology/2020/jun/12/twitter-deletes-170000-accounts-linked-to-china-influence-campaign.

75 The Eastern Herald. 'It Was Terribly Funny.' Dmitry 'Goblin' Puchkov – about Medvedev's Promise to Avenge the Deletion of His YouTube Channel'. 7 July 2023. https://easternherald.com/2023/07/07/it-was-terribly-funny-dmitry-goblin-puchkov-about-medvedevs-promise-to-avenge-the-deletion-of-his-youtube-channel/.

76 The Government of Japan. 'Navigating the Digital Era: The Growing Importance of Fact-Checking'. January 2024. https://www.japan.go.jp/kizuna/2024/01/growing_importance_of_fact-checking.html.

77 The Guardian. 'Ukraine War Briefing: Europe 'No Longer at Peace' with Russia, Says German Chancellor'. World News. The Guardian, 30 September 2025. https://www.theguardian.com/world/2025/sep/30/ukraine-war-briefing-europe-no-longer-at-peace-with-russia-says-german-chancellor.

78 The Guardian. 'YouTube Blocks Russian State-Funded Media Channels Globally'. Technology. 11 March 2022. https://www.theguardian.com/technology/2022/mar/11/youtube-blocks-russian-state-funded-media.

79 Tokyo Shimbun. '＜Q&A＞なぜ原発の処理水を海に放出するの?いつになったら終わるの?'. 25 August 2023. https://www.tokyo-np.co.jp/article/272365.

80 U.S. Defense Intelligence Agency. 'Russia Military Power: Building a Military to Support Great Power Aspirations'. 2017. https://www.dia.mil/Portals/110/Images/News/Military_Powers_Publications/Russia_Military_Power_Report_2017.pdf.

81 Geidel, Vanessa. 'How Germany's Far-Right Politicians Became the Kremlin's Voice'. The Strategist, 8 March 2023. https://www.aspistrategist.org.au/how-germanys-far-right-politicians-became-the-kremlins-voice/.

82 Wu, Huizhong. 'In Taiwan, a Group Is Battling Fake News One Conversation at a Time — with a Focus on Seniors'. AP News, 1 April 2024. https://apnews.com/article/fake-news-disinformation-taiwan-elderly-seniors-19773910ede8cdc39ae0ebc236cd652e.

83 Yu, Chihhao. 'Taiwan Counters FIMI – Governmental and Parliamentary Responses – 台灣資訊環境研究中心 IORG'. 29 October 2024. https://iorg.tw/_en/a/taiwan-counters-fimi-gov-parl.

84 Zack Cooper, Bret Schafer, and Etienne Soula. 'China's State Media and Government Officials Are Backing Russia on Ukraine'. Hamilton Weekly Reports. Alliance For Securing Democracy, 13 March 2022. https://securingdemocracy.gmfus.org/chinas-state-media-and-government-officials-are-backing-russia-on-ukraine-war/.

85 中华人民共和国外交部. '中日双方就福岛第一核电站核污染水排海问题达成共识_中华人民共和国外交部' . 20 September 2024. https://www.mfa.gov.cn/wjbxw_new/202409/t20240920_11493501.shtml.

86 中華民國國防部. 當危機來臨時：臺灣全民安全指引. 2025. https://adma.mnd.gov.tw/files/web/191/file_up/100004/67/%E7%95%B6%E5%8D%B1%E6%A9%9F%E4%BE%86%E8%87%A8%E6%99%82%EF%BC%9A%E8%87%BA%E7%81%A3%E5%85%A8%E6%B0%91%E5%AE%89%E5%85%A8%E6%8C%87%E5%BC%95(%E4%BA%8C%E7%89%88%E4%B8%80%E5%88%B7).pdf.

87 台灣資訊環境研究中心. '2023 台灣資訊環境報告'. 19 January 2024. https://iorg.tw/_en/r/2023.

88 台灣資訊環境研究中心. 'TikTok 上的中共政治宣傳及代理人帳號 – IORG 週報第 99 期 2024.7.1–2024.11.30'. 9 February 2025. https://iorg.tw/_en/da/99#h2–1.

89 蘇貞昌. '蘇貞昌 | Facebook'. 7 February 2020. https://www.facebook.com/photo/?fbid=10157118622901270&set=a.186955736269.

Endnotes

1 European Commission, 'Press Statement by the President on the Defence Package.'

2 The Guardian, 'Ukraine War Briefing: Europe 'No Longer at Peace' with Russia, Says German Chancellor.'

3 Bunde et al., Under Destruction: Munich Security Report 2026, p. 46.

4 The EEAS detected and analysed 540 FIMI incidents over 2025, with 29% attributed to Russia and 6% linked to China. See European Union External Action, 4th EEAS Report on Foreign Information Manipulation and Interference Threats: Dismantling the FIMI House of Cards.

5 Economist Intelligence Unit, Democracy Index 2024. Our World in Data, 'Democracy Index.'

6 Deutsche Welle, 'Faktencheck: Wie Russland versucht, die Wahl zu beeinflussen.'

7 Gershaneck, 'Political Warfare: Strategies for Combating China's Plan to 'Win without Fighting''.

8 U.S. Defense Intelligence Agency, 'Russia Military Power: Building a Military to Support Great Power Aspirations.'

9 Keir Giles, ''Information Troops' – A Russian Cyber Command?.'

10 At a minimum this can be understood by Chinese political strategists as including the US, Canada and Europe, as well as other Anglo–phone countries such as Australia, but could also be extended to include countries broadly supportive of multilateral groupings supported by these countries, such as Japan.

11 Comments from Chinese officials and state media often adopt the term 'strategic autonomy' – a term coined by a number of European leaders – to suggest Europe weaken ties with the US and NATO. The overlap of PRC narratives with European politics is a vivid example of the difficulties of countering FIMI.

12 Matura, 'Sino–Russian Convergence in Foreign Information Manipulation and Interference: A Global Threat to the US and Its Allies.'

13 Naing, 'China's Repression on German Soil, Transnational Repression.'

14 e.g. Davidson, 'China Revives Conspiracy Theory of US Army Link to Covid.'

15 Geidel, 'How Germany's Far–Right Politicians Became the Kremlin's Voice.'

16 European Union External Action, 1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a Framework for Networked Defence.

17 Marocico et al., 'How Russian–Funded Fake News Network Aims to Disrupt European Election.'

18 Lindholm, Increased Election Interference Activity in Eastern Europe Reveals Difficulties for Democracies to Fight Back.

19 Doroshenko, 'Catch Me If EU Can: How RT and Sputnik Evade EU Content Bans.'

20 Alliance For Securing Democracy, Chinese State Media Bolster CCP Narratives to Potentially Unaware Audiences in Germany.

21 BBC News, Wuhan Lab Leak Theory: How Fort Detrick Became a Centre for Chinese Conspiracies.

22 Leloup and Reynaud, 'The fake YouTube channels working for pro-China influence operations.'

23 Gleichgewicht, 'How YouTube Helps Russia Share How Great It Is in Raw and Subtle Ways.'

24 The Guardian, YouTube Blocks Russian State-Funded Media Channels Globally.

25 Al Jazeera, 'Twitter Drops 'State-Affiliated', 'Government-Funded' Labels.'

26 Matura, 'Sino-Russian Convergence in Foreign Information Manipulation and Interference: A Global Threat to the US and Its Allies.'

27 Doublethink Lab, Digital Intelligence Team, and Athena Tong, 'The Rise of AI in PRC Influence Operations: Nine Takeaways from the GoLaxy Documents,' 4 March 2026, https://medium.com/doublethinklab/the-rise-of-ai-in-prc-influence-operations-nine-takeaways-from-the-golaxy-documents-2d6617a753e5.

28 Davidson, 'China Revives Conspiracy Theory of US Army Link to Covid.'

29 Institute for Strategic Dialogue, 'Investigation: How Russia Today Is Evading Sanctions and Spreading pro-Kremlin Propaganda in Italy.'

30 Taylor, 'Twitter Deletes 170,000 Accounts Linked to China Influence Campaign.'

31 Taylor, 'Meta Closes Nearly 9,000 Facebook and Instagram Accounts Linked to Chinese 'Spamouflage' Foreign Influence Campaign.'

32 Nimmo et al., Meta Quaterly Adversarial Threat Report Q3 2023.

33 Alaphilippe et al., 'Doppelganger – Media Clones Serving Russian Propaganda.'

34 Davidson, 'China Using Influencers to Whitewash Human Rights Abuses, Report Finds.'

35 The Eastern Herald, 'It Was Terribly Funny.' Dmitry 'Goblin' Puchkov – about Medvedev's Promise to Avenge the Deletion of His YouTube Channel.

36 Matura, 'Sino-Russian Convergence in Foreign Information Manipulation and Interference: A Global Threat to the US and Its Allies.'

37 BBC Monitoring, 'Analysis: China, Russia Media Narratives on Ukraine War Converge.'

38 Repnikova, 'China's Propaganda on the War in Ukraine.'

39 Omelicheva, 'Russia's Doxing Campaign: An Expanding Trend in Extraterritorial Repression.'

40 Gang and Scott, 'Trolling of Female Asian Journalists on Rise as Beijing Seeks to Discredit Media.'

41 Hawkins et al., 'Sexually Explicit Letters about Exiled Hong Kong Activists Sent to UK and Australian Addresses.'

42 Seibt, 'Has Germany's Far-Right AfD Become a Gateway for Chinese and Russian Spies?'

43 Deutsche Welle, 'Germany: AfD's Krah Faces Probe on Russia, China 'payments''.

44 Osthoff, 'A look behind the scenes of Chinese espionage in the European Parliament'

45 China Global Television Network, 'Workers Party of Britain Leader George Galloway: The West Knows Its Own Democracy Isn't Working.'

46 Kus and Zhang, 'Alice Weidel: Xiaohongshu Star – Rosa-Luxemburg-Stiftung.' AFP Hong Kong, 'Chinese Social Media Posts Falsely Claim German Right-Wing Leader Praises China | Fact Check.'

47 European Union External Action, 4th EEAS Report on Foreign Information Manipulation and Interference Threats: Dismantling the FIMI House of Cards.

48 Zack Cooper et al., 'China's State Media and Government Officials Are Backing Russia on Ukraine.'

49 Reporters Without Borders, 'War in Ukraine: Beware of China's Amplification of Russian Propaganda, RSF Says.'

50 Lucas et al., 'Information Bedlam: Russian and Chinese Information Operations During the Covid-19 Pandemic.'

51 Hsiao, 'Political Warfare Alert: The PRC's Evolving Information Operations Targeting Provincial and Local Media Intermediaries.'

52 Yu, 'Taiwan Counters FIMI – Governmental and Parliamentary Responses – 台灣資訊環境研究中心 IORG.'

53 Office of the President Republic of China (Taiwan), 'About the Committee.'

54 All-out Defense Mobilization Agency, M.N.D., '2025 Urban Resilience (All-Out Defense Mobilization) Exercise of Taipei City Has Been Completed Successfully on July 17 (Thursday).'

55 Hille, 'Taiwan Revokes Residency for Chinese TikTok Influencer.'

56 Yu, 'Taiwan Counters FIMI – Governmental and Parliamentary Responses – 台灣資訊環境研究中心 IORG.'

57 Mahdawi, 'Humour over Rumour? The World Can Learn a Lot from Taiwan's Approach to Fake News.'

58 Tang and Verfürth, 'Taiwan Is Standing up to Disinformation.'

59 中華民國國防部, 當危機來臨時：臺灣全民安全指引.

60 蘇貞昌, '蘇貞昌 | Facebook.'

61 中華民國國防部, 當危機來臨時：臺灣全民安全指引.

62 Hsiao, 'Political Warfare Alert: The PRC's Evolving Information Operations Targeting Provincial and Local Media Intermediaries.'

63 e.g. See Taiwan Fact Check Center https://en.tfc-taiwan.org.tw/ and MyGoPen https://www.mygopen.com/.

64 台灣資訊環境研究中心, 'TikTok 上的中共政治宣傳及代理人帳號 – IORG 週報第 99 期 2024.7.1–2024.11.30.' 台灣資訊環境研究中心, '2023 台灣資訊環境報告.'

65 台灣放伴教育協會, https://pangphuann.tw/.

66 Wu, 'In Taiwan, a Group Is Battling Fake News One Conversation at a Time — with a Focus on Seniors.'

67 Factlink, '日本首相高市早苗「台灣有事說」事件：拆解中國資訊戰與謠言攻勢' .

68 Padalko, 'AI and Information Manipulation: Russia's Interference in the US Elections.'

69 Ichihara, 'Japan's Upper House Election Reveals How Russian Influence Operations Infecting AI with Flood of Propaganda, Stoking Divisions.'

70 Inoue, 'Concerns Grow in Japan over Possible Russian Interference in Sunday's Election.'

71 IAEA, 'Fukushima Daiichi ALPS Treated Water Discharge – Reports.'

72 Cai, 'Fukushima: China's Anger at Japan Is Fuelled by Disinformation.'

73 Ministry of Foreign Affairs of Japan, 'Japan's Foreign Policy to Promote National and Global Interests.'

74 Ministry of Foreign Affairs of Japan, 'The Responses to Information Manipulation, Including Spread of Disinformation.'

75 Ministry of Internal Affairs and Communications of Japan, 'Release of 'Existing Practices against Disinformation (EPaD)' at the Internet Governance Forum Kyoto 2023.'

76 Hou, 'Civil Society in East Asia: The Fight against Disinformation.'

77 Ministry of Internal Affairs and Communications of Japan, Operations Guide for FY2024 Edition.

78 Ministry of Internal Affairs and Communications of Japan, 'Launch of DIGITAL POSITIVE ACTION, a Public–Private Partnership Project (Hereinafter Referred to as the 'Project'), to Improve ICT Literacy Comprehensively| Press Release.'

79 National Cybersecurity Office, 'Commitment to a Free, Fair and Secure Cyberspace.'

80 中华人民共和国外交部, '中日双方就福岛第一核电站核污染水排海问题达成共识_中华人民共和国外交部.'

81 Nikkei Asia, 'Social media fuel pro–Okinawa independence disinformation blitz.'

82 Dreyer, 'The Gloves Come Off.'

83 NHK, 'Japanese officials respond to China military plane's intrusion.'

84 Ministry of Foreign Affairs of Japan, 'Regarding the inappropriate remarks by a Chinese participant to the Munich Security.'

85 Factlink, '日本首相高市早苗「台灣有事說」事件：拆解中國資訊戰與謠言攻勢'

86 Japan Fact–Check Centre, 'Japan Fact–check Center (JFC) Activity Report.'

87 The Government of Japan, 'Navigating the Digital Era: The Growing Importance of Fact–Checking.'

88 Kimura, 'Protecting Japan's national security from information operations.'

89 CSIS, 'Combating Disinformation: A View from Japan.'

90 Ichihara, 'China's 'Malinformation' Comes for Okinawa.'

91 Sasakawa USA, ''Just Being Born': Assessing and Countering Foreign Information Manipulation and Interference (FIMI) in Japan'

92 NHK, 'AI deepfakes cloud Japan's election.'

93 Tokyo Shimbun, '＜Q&A＞なぜ原発の処理水を海に放出するの?いつになったら終わるの?' .

94 Ministry of Foreign Affairs of Japan, 'The Responses to Information Manipulation, Including Spread of Disinformation.'

95 Ministry of Foreign Affairs of Japan, 'The Signing of the US Japan Memorandum of Cooperation on Countering Foreign Information Manipulation.'

96 D'Ambrogio, Japan's Preparedness Strategies: Lessons for the EU.

97 Ministry of Internal Affairs and Communications of Japan, 'Hiroshima AI Process.'

98 Digital Agency, Government of Japan, 'Data Free Flow with Trust (DFFT).'

99 European Commission, 'Communication on the European Democracy Shield.'

100 Bundesministeriums für Bildung, Familie, Senioren, Frauen und Jugend, 'DigitalPakt Schule.'

101 Fakultät für Bildungswissenschaften, 'Demokratie Leben! / Live Democracy!.'