[ADRN Issue Briefing]

The Current Status of Japan’s Countering Digital Influence Operations

Kazuki Ichida (Meiji University)

Introduction

Digital influence operations have the capacity to shape and undermine public perceptions and opinions in targeted countries. The United States National Intelligence Council found that China, Russia, and Iran prioritize digital influence operations over cyber attacks, underscoring their perceived efficacy (National Intelligence Council 2023). Digital influence operations are variously referred to as cognitive warfare and information warfare. For the purposes of this briefing, the term “digital influence operations” will be used.

This briefing describes the current status of countermeasures employed by major actors in Japan. In Japan, entities such as the Ministry of Defense (MOD), the Ministry of Internal Affairs and Communications (MIC), the Ministry of Foreign Affairs (MOFA), and the National Police Agency, and the National Center of Incident readiness and Strategy for Cybersecurity (NISC), have been developing their budgets and organizations. However, efforts by the private sector, including fact-checking organizations, think tanks, and academics, still face limitations in terms of human resources and scale and are far from sufficient. In recent years, there have been signs of expansion due to increased support from the Japanese government.

Three challenges impede Japan’s efforts to counter digital influence operations. First, there is a severe shortage of knowledge and human resources. Second, the measures are primarily focused on countering disinformation, improving literacy, and enhancing strategic communication. Lastly, the attacks leveraging domestic polarization in the target country have not been addressed. This issue is not unique to Japan but also prevalent in Europe and the United States.

Key Actors in Japan’s Digital Influence Operations Countermeasures

The European External Action Service’s recently published “2nd EEAS Report on Foreign Information Manipulation and Interference Threats” listed Governments and other 17 actors (EEAS 2024). In this briefing, the actors are broadly categorized into governments and government agencies, private companies, Fact-Checking Organizations, Think Tanks, and Universities.

The Japanese government and its agencies play a central role in these activities, while other actors are generally less active.

1. Government and Government Agencies

In Japan, the MOD, the Self-Defense Forces, and other security-related organizations are tasked with addressing foreign threats in digital influence operations, while the MIC handles domestic issues, the MOFA manages strategic communications in diplomacy, and the NISC of Cabinet Secretariat leads and coordinates the entire operation. This delineation of responsibilities is explicitly stated in the National Security Strategy released in 2022, and organization development is underway (Cabinet Secretariat 2022).

Criminal matters are handled by the National Police Agency, while intelligence-related tasks are managed by the Cabinet Secretariat, the Ministry of Defense Intelligence Headquarters, Public Safety, and Foreign Affairs. These division of labor among public institutions are described below.

National Security Organizations: The National Security Strategy clearly states that the Ministry of Defense is to deal with digital influence operations. Inside the Ministry, the Defense Intelligence Headquarters (DIH) is primarily responsible for this task (DIH n.d.). The DIH is Japan's largest intelligence organization with more than 2,600 employees (MOD n.d.). According to publicly available documents, the DIH focuses on measures against propaganda and disinformation, including strategic communications. It plans to develop an Artificial Intelligence (AI) system to determine the authenticity of amplified information (MOD n.d.).

Regarding the Self-Defense Forces, notable developments are scarce, except for the JGSDF Training-Evaluation Education Research and Development Command (TERCOM), which has a specialized team for developing new cyber combat systems (TERCOM 2023). Unlike the U.S. CyberCom, preventive measures such as attacking the source do not seem to be contemplated. Primary measures for dealing with propaganda and disinformation mainly occur after the dissemination of information.

The Ministry of Internal Affairs and Communications (MIC): The MIC has been working on this area since 2018 and has conducted a study group with academic experts and platform companies (MIC 2018). Currently, the Advanced Information Systems and Software Division spearheads implementation efforts, focusing primarily on countering disinformation. National security is not within its purview due to division of duties.

As for countering disinformation, the focus is on fact-checking and improving literacy, with a plan already in place.

The Ministry of Foreign Affairs (MOFA): MOFA addressed this issue within the context of strategic communication, aiming to address misinformation about Japan and promote an accurate and positive image of Japan globally. It could be described as the reputation management agency of the Japanese government, with some tasks outsourced to an Israeli reputation management company (Intelligence Online 2023).

The Cabinet Secretariat: The Cabinet Secretariat has several departments working on this issue, including the Cabinet National Security Secretariat, the Cabinet Intelligence and Research Office, and the National Center of Incident Readiness and Strategy for Cybersecurity (NISC). The NISC will become the department overseeing the entire Japanese government's response to cyberspace and will play a similar role in Digital Influence Operations (Cabinet Secretariat 2022). In Japan, cyber attacks and digital influence operations have often been considered separately. In reality, they are sometimes linked, and the organizations responsible for the attacks are often the same. This organizational change will improve the system by centralizing them under NISC.

Others: The National Police Agency handles criminal cases, while the Public Safety and Foreign Affairs departments handle intelligence cases.

As evident, the majority of the Japanese government's countermeasures focus on detecting and addressing disinformation. However, digital influence operations encompass a broader spectrum of activities beyond disinformation, including emotional manipulation, support for narratives from other countries, and perception hacking (Myre 2020; Meta 2023). The Japanese government's response is specialized and narrower compared to other governments like the U.S., which adopt more comprehensive responses from multiple stakeholders. This policy might stem from a lack of knowledge and human resources. For this reason, the government agencies have been engaging private companies that may have knowledge in this area since 2023. Nevertheless, the private sector also faces shortages in expertise and resources. Should the government opt to outsource disinformation countermeasure tasks to private entities, it must develop supervisory and evaluation mechanisms.

2. The Private Sector

Private companies: In Europe and the United State, many cybersecurity, IT, and military companies have departments for digital influence operations and regularly publish reports on their activities. In Japan, few cybersecurity and IT companies engage in such activities, except for foreign-affiliated companies importing reports from their home countries.

Reputation management companies are the primary entities involved in digital influence operations in Japan, although their actual activities remain largely undisclosed. The government agencies commissioning them do not publicly disclose their contents. Based on the general scope of work of reputation management firms, it is presumed that the private sector targets countering disinformation and supporting strategic communications. Strategic communication entails releasing information or signals to strengthen alliances and reveal the values sought, thereby guiding international relations.

As the Japanese government strengthens its budget and systems, inquiries and orders from private firms are expected to increase, leading to business expansion in this area.

Fact-Checking Organizations and Think Tanks: Japan hosts two major fact-checking organizations, namely FactCheck Initiative Japan (https://fij.info) and Japan Fact Check Center (https://www.factcheckcenter.jp/). The number of fact-checking organizations and their activities are small compared to those in the countries concerned, and their sphere of influence is still limited. Fact-checking faces scalability challenges due to the vast amount of disinformation that can be easily produced, and the limited dissemination of fact-checking results compared to disinformation. Similar challenges likely confront fact-checking organizations worldwide.

While several think tanks conduct research on digital influence operations, such as the Japan Institute of International Affairs (https://www.jiia.or.jp) and the Sasakawa Peace Foundation (https://www.spf.org), their number and scope in this area are quite limited. Most reports are based primarily on the compilation of existing materials and surveys.

Universities: Researchers across various fields, including political science, computational sociology, and media theory, mainly from universities, investigate digital influence operations from their unique perspectives. Some of these researchers receive support from the Japanese government.

Ambitious research projects such as "Recommendations for the Revision of the National Security Strategy" and "Toward a Healthy Platform for Discussion" have brought together researchers and practitioners from diverse fields (ROLES 2022; Toriumi and Yamamoto 2023). The former was published before the revision of the National Security Strategy, covering all national security domains. It was groundbreaking in its reference to digital influence operations measures. Unfortunately, the latter lacks transparency regarding funding sources, raising concerns about potential manipulation of public opinion.

Overall, Japan's research community in this area is not as extensive as in Europe and the United States. Increased financial support from the Japanese government may revitalize the related research field in the near future.

Problems with Japan's Digital Influence Operations Measures

Japan's digital influence operations measures have been sluggish so far. Apart from the MIC, which has actively conducted research and studies, only a few citizen groups, researchers, and private companies, including fact-checking organizations, have been involved. In 2023, the Japanese government decided to address this issue seriously, leading to strengthened budgets and organization, which are beginning to yield positive impacts to private companies and research institutions. Although there is currently a lack of immediate knowledge and human resources, it can be said that Japan has reached a starting point.

Three main problems hinder Japan's digital influence operations measures. Firstly, a shortage of knowledge and human resources persists as the most significant obstacle. Secondly, the current focus is primarily on countering disinformation, enhancing literacy, and improving strategic communication. The recently released Carnegie report lists 10 measures for addressing digital influence operations, emphasizing the need for multifaceted measures based on portfolios (Bateman and Jackson 2024).

Finally, similar to digital influence operations measures in Europe and the United States, domestic issues are largely neglected. Foreign digital influence operations often exacerbate domestic polarization in the target country, necessitating interrelated domestic and foreign countermeasures. For example, QAnon, one of the most known conspiracy groups, occasionally coordinated with Russia and China (Kayali and Scott 2022; Soufan Center 2021; Butler and Martin 2022; Graziosi 2022).

Focusing solely on foreign interference fails to address the reality of the threat in two ways. First, the number of countries conducting domestic digital influence operations is greater than the number of countries conducting foreign interference (Martin et al. 2020; Meta 2022; Bradshaw et al. 2020). Domestic digital influence operations pose a more serious threat to democracy. Second, foreign interference often exploits domestic polarization in the target country. In other words, they exploit pre-existing domestic problems in the target country. In terms of protecting democracy, the effectiveness of digital influence operations measures will be limited if they fail to consider the linkage between domestic conditions and external interventions. According to the United States National Intelligence Council, China, Russia, and Iran are primarily exploiting domestic polarization in the United States (National Intelligence Council 2022). Both domestic and foreign interference countermeasures against digital influence operations are essential.

State involvement in digital influence operations is depicted below (Nyst and Monaco 2018; Ichida 2018; Woolley 2023). Currently, Europe, the United States, and Japan address only two of the four patterns. The unaddressed third and fourth patterns, which involve government incitement and support, are particularly challenging to tackle, especially when exploiting domestic polarization.

Pattern 1. Government Execution: The government or its affiliated organizations directly execute the operation.
Pattern 2. Government Support and Coordination: The government devises the plan but delegates implementation to external parties.
Pattern 3. Government Incitement and Support: The government instigates online users to attack individuals and organizations critical of the government to manipulate public opinion, posing the most significant danger.
Pattern 4. Government Approval and Support: The government fosters an atmosphere conducive to attacks through name-calling and criticism.

However, unlike other situations, the Japanese government has a potential advantage in addressing the last problem. Japan's ruling Liberal Democratic Party (LDP) established a team called T2 for online public relations activities after losing power to the Democratic Party of Japan (DPJ) in 2009 (Koguchi 2016). Supported by IT and PR companies, T2's activities resembled contemporary reputation management efforts. This suggests that the Japanese government has a background in conducting domestic digital influence operations. By publicizing its activities, engaging in public debate, and establishing transparency, the government can build a democratic defense posture. ■

References

Bateman, Jon, and Dean Jackson. 2024. "Countering Disinformation Effectively: An Evidence-Based Policy Guide." Carnegie Endowment for International Peace. January 31. https://carnegieendowment.org/2024/01/31/countering-disinformation-effectively-evidence-based-policy-guide-pub-91476 (Accessed February 8, 2024)

Bradshaw, Samantha, Hannah Bailey, and Philip N. Howard. 2021. "Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation." Oxford University Programme on Democracy & Technology. https://demtech.oii.ox.ac.uk/research/posts/industrialized-disinformation/ (Accessed February 8, 2024)

Butler, Josh, and Sarah Martin. 2022. "Australian online anti-vaccine groups switch to Putin praise and Ukraine conspiracies." *The Guardian*. March 1. https://www.theguardian.com/australia-news/2022/mar/02/australias-anti-vaccine-groups-switch-focus-to-putin-praise-and-ukraine-conspiracies (Accessed February 8, 2024)

Cabinet Secretariat. 2022. "National Security Strategy of Japan (Provisional Translation)" December 2022. https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf (Accessed February 8, 2024)

Defense Intelligence Headquarters: DIH. n.d. "情報本部の任務・活動." https://www.mod.go.jp/dih/company.html (Accessed February 8, 2024)

European External Action Service: EEAS. 2024. "2nd EEAS Report on Foreign Information Manipulation and Interference Threats." January 23. https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en (Accessed February 8, 2024)

Graziosi, Graig. 2022. "Anti-vax conspiracy theorists in US turning to antisemitic pro-Putin propaganda, report says." *The Independent*. March 2. https://www.independent.co.uk/news/world/americas/us-politics/putin-propaganda-usa-conspiracy-theorist-b2027230.html (Accessed February 8, 2024)

Ichida, Kazuki. 2018. 『フェイクニュース　新しい戦略的戦争兵器』. Tokyo: Kadokawa Shinsho.

Intelligence Online. 2023. "Japan turns to Israel's 9500 Group to counter Chinese Fukushima disinformation." September 12. https://www.intelligenceonline.com/corporate-intelligence/2023/09/12/japan-turns-to-israel-s-9500-group-to-counter-chinese-fukushima-disinformation,110042325-art (Accessed February 8, 2024)

Kayali, Laura, and Mark Scott. 2022. "Anti-vax conspiracy groups lean into pro-Kremlin propaganda in Ukraine." *POLITICO*. March 17. https://www.politico.eu/article/antivax-conspiracy-lean-pro-kremlin-propaganda-ukraine/ (Accessed February 8, 2024)

Koguchi, Hidehiko. 2016. 『情報参謀』. Tokyo: Kodansha.

Martin, Diego A. Jacob N. Shapiro, and Julia G. Ilhardt. 2020. "Online Political Influence Efforts Dataset." Princeton University Empirical Studies of Conflict Project. Last Updated May 11, 2023. https://esoc.princeton.edu/publications/trends-online-influence-efforts (Accessed February 8, 2024)

Meta. 2022. “Recapping Our 2022 Coordinated Inauthentic Behavior Enforcements, Meta.” December 15. https://about.fb.com/news/2022/12/metas-2022-coordinated-inauthentic-behavior-enforcements/ (Accessed February 8, 2024)

______. 2023. “THIRD QUARTER Adversarial Threat Report.” November 3. https://transparency.fb.com/ja-jp/metasecurity/threat-reporting/ (Accessed February 8, 2024)

Ministry of Internal Affairs and Communications: MIC. 2018. “プラットフォームサービスに関する研究会 (Study Group on Platform Services)”. https://www.soumu.go.jp/main_sosiki/kenkyu/platform_service/index.html (Accessed February 8, 2024)

Ministry of Defense: MOD. n.d. “Integrated Information Warfare with Special Regard to the Cognitive Dimension.” https://www.mod.go.jp/en/d_architecture/infowarfare/index.html (Accessed February 8, 2024)

Myre, Greg. 2020. “A ‘Perception Hack’: When Public Reaction Exceeds The Actual Hack.” *NPR*. November 1. https://www.npr.org/2020/11/01/929101685/a-perception-hack-when-public-reaction-exceeds-the-actual-hack (Accessed February 8, 2024)

National Intelligence Council. 2022. “Foreign Threats to the 2022 US Elections” December 23. https://www.odni.gov/files/ODNI/documents/assessments/NIC-Declassified-ICA-Foreign-Threats-to-the-2022-US-Elections-Dec2023.pdf (Accessed February 8, 2024)

Nyst, Carly, and Nicholas Monaco. 2018. “State-Sponsored Trolling.” July 19. Institute for the Future. https://legacy.iftf.org/statesponsoredtrolling/ (Accessed February 8, 2024)

Research Center for Advanced Science and Technology Open Laboratory for Emergence Strategies: ROLES. 2022. “国家安全保障戦略改訂に向けた提言(Recommendations for the Revision of the National Security Strategy).” October 31. https://roles.rcast.u-tokyo.ac.jp/publication/20221031 (Accessed February 8, 2024)

Soufan Center. 2021. “Quantifying The Q Conspiracy: A Data-Driven Approach to Understanding the Threat Posed by QAnon.” April 21. https://thesoufancenter.org/research/quantifying-the-q-conspiracy-a-data-driven-approach-to-understanding-the-threat-posed-by-qanon/ (Accessed February 8, 2024)

TERCOM (陸上自衛隊の新たな戦い方検討チーム). 2023. “陸上自衛隊の新たな戦い方コンセプトについて” October 3. https://www.mod.go.jp/gsdf/tercom/img/file2320.pdf (Accessed February 8, 2024)

Thomas, Elise. 2022. “QAnon goes to China – via Russia”, Institute for Strategic Dialogue. March 23. https://www.isdglobal.org/digital_dispatches/qanon-goes-to-china-via-russia/ (Accessed February 8, 2024)

Toriumi, Fujio, and Tatsuhiko Yamamoto. 2023. “KGRI Working Papers No.1 健全な言論プラットフォームに向けて ver2.0 (Toward a Healthy Platform for Discussion).” May 2023. https://www.kgri.keio.ac.jp/docs/S0120230529.pdf (Accessed February 8, 2024)

Woolley, Samuel. 2023. *Manufacturing Consensus: Understanding Propaganda in the Era of Automation and Anonymity*. New Haven: Yale University Press.

- **Kazuki Ichida** is a Visiting Researcher at Cyber Security Research Institute, Meiji University.

The East Asia Institute takes no institutional position on policy issues and has no affiliation with the Korean government. All statements of fact and expressions of opinion contained in its publications are the sole responsibility of the author or authors.

This program was funded in part by the National Endowment for Democracy (NED).

"The Current Status of Japan's Countering Digital Influence Operations"

979-11-6617-711-8 95340 Date of Issue: 16 February 2024

Typeset by Hansu Park

For inquiries:
Hansu Park, Research Associate
Tel. 82 2 2277 1683 (ext. 204) hspark@eai.or.kr

The East Asia Institute
1, Sajik-ro 7-gil, Jongno-gu, Seoul 03028, Republic of Korea
Phone 82 2 2277 1683 Fax 82 2 2277 1684
Email eai@eai.or.kr Website www.eai.or.kr