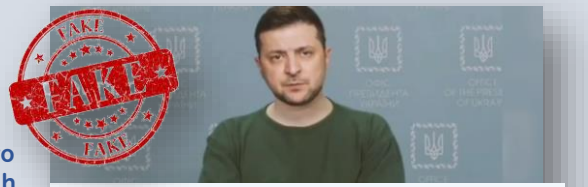
Recent Trends in Information Warfare

- In recent years, concerns regarding information warfare have increased due to the spread of disinformation, efforts to undermine trust in governments, and information activities intended to create social division.
- China and Russia are believed to be conducting information warfare both domestically and internationally in an effort to shape an information environment favorable to their strategic interests.

Taiwan's Ministry of National Defense social media post warning the public about disinformation related to a reported missile launch (Source: Taiwan Ministry of National Defense social media post, April 2023)



Deepfake video falsely showing President Zelenskyy announcing surrender (March 2022)

Pro-Russian media article claiming that "No U.S. assistance can save Ukraine from defeat on the front lines." (Identified as disinformation by SPRAVDI, Ukraine's Center for Strategic Communication and Information Security, May 2024)

Assessments by Western Institutions

【U.S. Department of War】
Annual Report on Military and Security Developments Involving the People's Republic of China

✓ Beijing likely uses official government statements, state-run media, and online disinformation to promote a narrative that Washington seeks to initiate a new Cold War by pressuring Indo-Pacific countries to ally with the United States and strategically encircle the PRC.

Source: U.S. Department of War, Military and Security Developments Involving the People's Republic of China 2024: Annual Report to Congress (December 2024).

✓ Beijing almost certainly considers cognitive domain operations to be a key component of its pressure campaign against Taiwan, intended to weaken Taiwan's will to resist and heighten social divisions in the country. Beijing uses the information space to spread political narratives, influence the Taiwan populace, and emphasize PLA activity around Taiwan.

Source: U.S. Department of War, Military and Security Developments Involving the People's Republic of China 2025: Annual Report to Congress (December 2025).

【Office of the Director of National Intelligence (ODNI)】 Annual Threat Assessment

✓ PRC actors have increased their capabilities to conduct covert influence operations and disseminate disinformation.

Source: Annual Threat Assessment of the U.S. Intelligence Community (ODNI, March 2025)

✓ Russia's gray zone tools include cyber attacks, disinformation and influence operations, energy market manipulation, military intimidation, and sabotage. Russia often hides and denies its role, complicating U.S. efforts to counter it.

Source: Annual Threat Assessment of the U.S. Intelligence Community (ODNI, March 2026).

【NATO】HP

Russia uses conventional, cyber

And hybrid means - including disinformation- against NATO Allies and partners.

[…]

We are strengthening our deterrence and defence, supporting our partners, and enhancing our resilience. This includes calling out Russia's actions and countering disinformation.

Source: NATO, "Setting the Record Straight."

Integrated Information Warfare in the Three Security Documents

【National Security Strategy】

Ⅵ Strategic Approaches Prioritized by Japan

(4) Strengthening Efforts to Seamlessly Protect Japan in All Directions

(v) Strengthening Intelligence Capacities for Japan's National Security

...In addition, from the perspective of **bolstering the ability to respond to information warfare in the cognitive domain, including spread of disinformation**, **a new structure will be established within the Government to aggregate and analyze information on disinformation and others originated abroad, to strengthen external communications, and to enhance cooperation with non-governmental agencies**. Furthermore, **strategic communication will be actively implemented in a coordinated manner within the Government**.

【National Defense Strategy】

IV Key Capabilities for Fundamental Reinforcement of Defense Capabilities

5 Command and control / Intelligence-related functions

...**By FY2027, Japan will develop intelligence capabilities capable of responding to hybrid warfare and integrated information warfare with special regard to the cognitive dimension**.... Moreover, **in order to effectively respond to integrated information warfare, including the spread of disinformation, Japan will fundamentally reinforce the organization and functions of MOD/SDF**, and **conduct information sharing and bilateral/multilateral exercises with its ally and like-minded countries**.

V The Future of Self-Defense Forces

2 Concept of developing SDF architecture

In addition to collecting and analyzing SIGINT, IMINT, HUMINT, OSINT, etc., DIH will assume the central role of responding to integrated information warfare concerning the defense of Japan and fundamentally reinforce the capability to grasp military activities of other countries in a persistent, continuous and accurate manner and analyzing and disseminating them.

【Defense Buildup Program】

II Major Programs Regarding SDF's Capabilities

5 Command-and-Control and Intelligence-related Functions

(3) Responses to Integrated Information Warfare With Special Regard to the Cognitive Dimension

In the international community, **emphasis is being placed on information warfare, which is an attempt to create a favorable security environment by influencing the public opinion and decision-making of other countries through disinformation and strategic communications, etc., and minimizing the impact to one's own decision -making, even when conflict has yet to arise**. MOD/SDF will **establish a system and posture that ensures the capability to cope with information warfare**. To this end, **the DIH, which plays a central role in responding to integrated information warfare, will strengthen the system for information collection, analysis, and communication**. In addition, **the following functions will be developed: automatic collection and analysis of open -source information using artificial intelligence (AI), which will enable continuous collection and analysis of information on trends in each country; automatic collection of information on social networking sites, etc., to determine the authenticity of information communicated by each country; and future forecasting functions for estimating the security situation.**

Integrated Information Warfare: Concept

■ **Integrated information warfare with special regard to the cognitive dimension**, in the context of the defense of Japan, is interpreted as follows:

"In the context of the defense of Japan, from the current point in time as well as during contingency,

I. **Bolster our intelligence-related functions, attaining all-round information collection capabilities;**
II. **Respond to diverse threats, including the dissemination of disinformation by foreign actors, through determining authenticity, intent, etc., and neutralizing harmful actions through various means;**
III. **Utilize every opportunity to swiftly and strategically communicate appropriate information through coordination with the ally and partner countries;**

thus **defending our decision-making process**, while **preventing and responding to unilateral attempts to change the status quo**, and **fostering an advantageous security environment**. On the other hand, **MOD/DIH/SDF will not partake in activities that undermine trust of Japan (ex. dissemination of disinformation, malign influence activities, manipulation)."**

Areas to be Addressed (Examples)

1. Continuous information collection and analysis on the military movements of other countries

Collect

- Attain all-round information collection capabilities
- Collect and share information regarding lessons learned from other countries

2. Determine the authenticity of information communicated by other countries

Expose

- Detect propaganda, disinformation, etc.
- Fact-check disinformation, etc.

3. Foster an advantageous security environment in all situations

Battle

- Strategic communications
- Declassification of secret intelligence
- Maintenance of information communication systems; information security

MOD/DIH/SDF will not partake in activities that undermine trust of Japan (ex. dissemination of disinformation, malign influence activities, manipulation)

Reinforcement of Defense Intelligence Headquarters

Defense Intelligence Headquarters:

- Founded in 1997, DIH is MOD's central intelligence agency and Japan's largest intelligence organization
- Its mission is to gather various intelligence including OSINT and analyze movements related to Japan's national security, such as international military situations
- Authorized strength: 2,698 personnel (Uniformed: 1,936 / Civilian: 762)

(As of April 1, 2026)

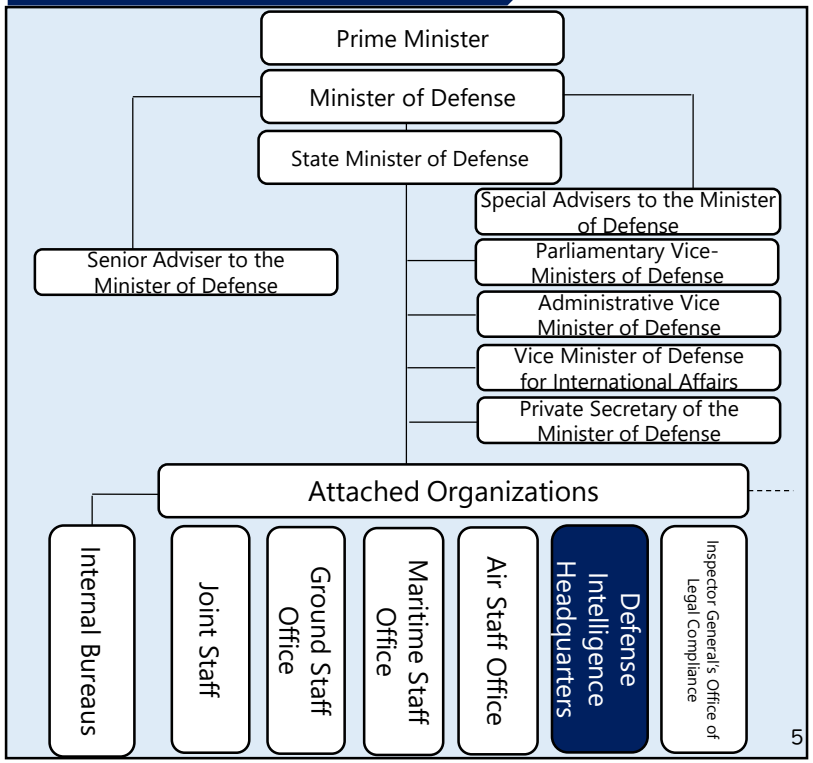
Provide timely and appropriate intelligence products

Policy Decisions

Military Operations

Actively promote information exchange to enhance product quality

MOD Organization



DIH's Intelligence Sources (Examples)

Responding to Integrated Information Warfare

Strengthening Structures for Information Dissemination

- To strengthen societal resilience and secure international support, Japan will **communicate the necessity and legitimacy of its defense policies and related efforts in a proactive and multi-layered manner, both domestically and internationally**, in coordination with allies and like-minded countries.
- **Respond swiftly to the spread of disinformation and other malign information**.
- To achieve these objectives, **enhance communications capabilities for cognitive warfare**, including strategic communications, in coordination with relevant ministries and agencies.
- **Conduct tabletop exercises** to validate effective response procedures for Information Warfare.

Utilization of AI across the Cycle from Information Collection to Information Dissemination

- **Collect large volumes of open-source information widely and efficiently** from social media and other sources. **(OSINT)**
- **While appropriately incorporating the latest technologies and actively leveraging external expertise**, **utilize AI** throughout the entire cycle from information collection to information dissemination.

SDF: Organization of major unit

Ground SDF	Maritime SDF	Air Space SDF
Information Operations Command	Information Warfare Command	(To be established)

Initiatives for Building the Necessary Structure and Posture (1/2)

Strengthening Capabilities for Information Collection, Analysis, and Dissemination

【FY2024】

✓ Establish automatic open source and social media information collection and analysis capabilities utilizing AI (¥2.8 billion)

※Establish automated capabilities for collecting and analyzing open-source information and social media data as part of validating a prototype that consolidated the tools developed in FY2023.

✓ Utilize future forecasting services for estimating the security situation (¥2.1 billion)

【FY2025】

✓ Establishment of automatic open source and social media information collection/analysis capabilities utilizing AI (¥1.2 billion)

※Enhancement of the automated collection and analysis capabilities for publicly available information developed in FY2024

✓ Utilization of future forecasting services for estimating the security situation(¥2.1 billion)

【FY2026】

✓ Establishment of automatic open source and social media information collection/analysis capabilities utilizing AI (¥ 4.5 billion)

※Enhancement of the automatic open source information collection/analysis capabilities developed in FY2025

✓ Utilization of future forecasting services for estimating the security situation(¥ 3.3 billion)

Initiatives for Building the Necessary Structure and Posture (2/2)

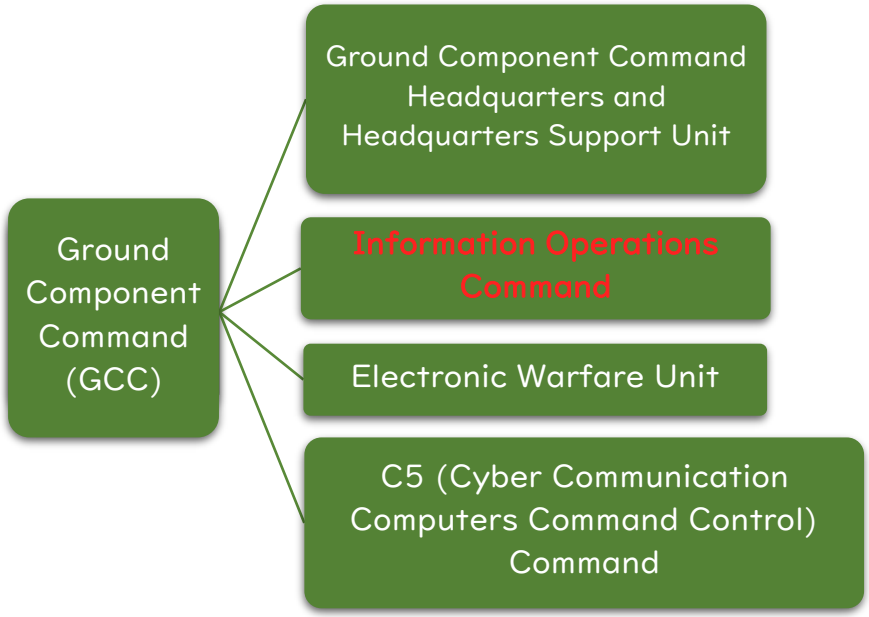
Strengthening the Defense Intelligence Headquarters

To strengthen capabilities for information collection, analysis, and dissemination, the Defense Intelligence Headquarters established a new intelligence officer post and a dedicated office responsible for information warfare.

Review of Core Units within the Services

【 FY2025】

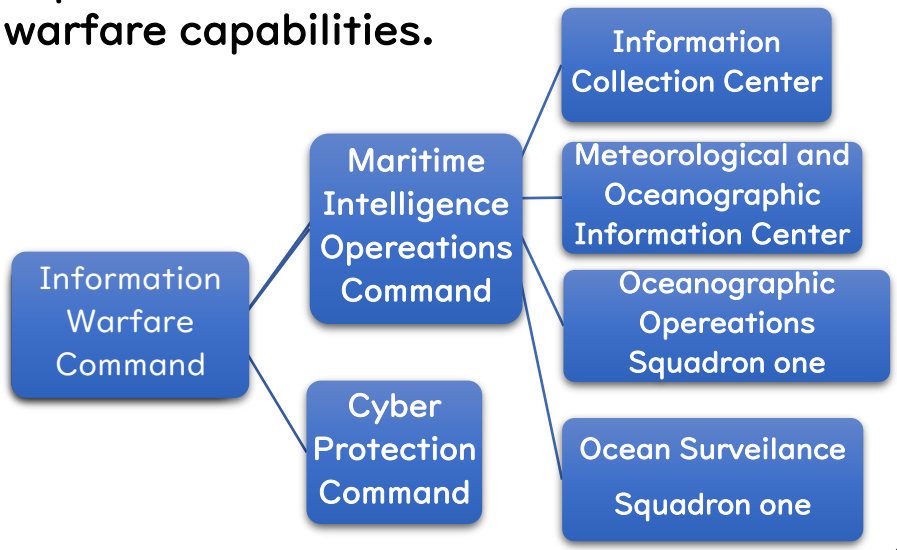
JGSDF Information Operations Command



Strengthen the JGSDF's Information Operations Capabilities

JMSDF Information Warfare Command

Consolidate intelligence, cyber, communications, and meteorological/oceanographic capabilities to enhance information warfare capabilities.



Cooperation with Allies and Like-Minded Partners

- Cooperation with ally and like-minded countries possessing advanced expertise is beneficial for developing information warfare capabilities.
- Deepening relationships with ally and like-minded countries through the sharing of best practices and lessons learned etc.

✓ Japan and the U.S committed to strengthening bilateral coordination on cross-domain operations, including cyber, space, electromagnetic and information warfare, recognizing the importance of all these domains to future concepts of deterrence and response capabilities.

"Excerpt from the Summary of the U.S.-Japan Security Consultative Committee ("2+2") Meeting (July 28, 2024)

✓We welcomed progress in bilateral cooperation on strategic communications to counter foreign information manipulation and interference. We committed to deeper engagement bilaterally and with regional partners to address information threats in the Indo-Pacific, including to support governments, civil society and media to build resilient, open and fact-based information environments.

"Excerpt from the Joint Statement of the 11th Japan-Australia Foreign and Defence Ministerial Consultations ("2+2") (September 5, 2025)

✓ Regarding the Japan-NATO cooperation, Japan intends to promote the following cooperations based on the ITPP.

✓ It is also important to deepen cooperation between the IP4 and NATO, we welcome the IP4-NATO flagship projects: (1) support to Ukraine, (2) Cyber Defense, (3) hostile information, including disinformation, and (4) Technology.

"Prime Minister Kishida' s Participation in the NATO Summit Meeting," Ministry of Foreign Affairs of Japan (MOFA), July 11, 2024