Direction of Defense Capability Transformation (2): Cooperation with Like-minded Countries

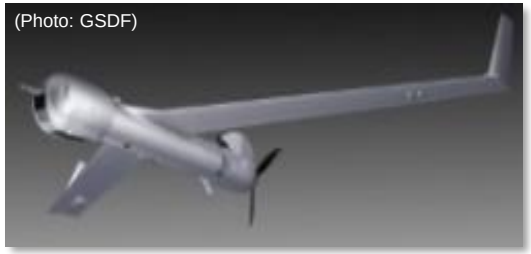
March, 2026

Japan Ministry of Defense

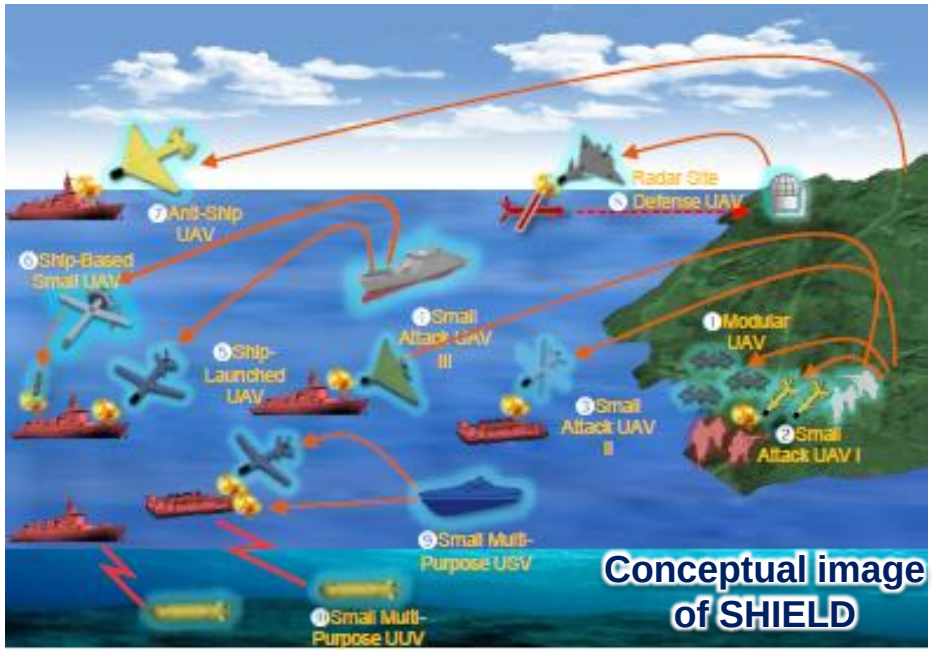
Unmanned Defense Capabilities

Unmanned Defense Capabilities

- Under the current Defense Buildup Program, the Ministry of Defense (MOD) is promoting demonstrations, R&D, and acquisition of unmanned assets used for **intelligence, targeting, attacks, and combat support**.
- The introduction of unmanned assets will be advanced by allocating ¥100.1 billion in the FY2026 budget, aiming to establish **Synchronized, Hybrid, Integrated and Enhanced Littoral Defense (SHIELD) by unmanned assets** in FY2027.
- As Japan's population declines, there is an **urgent need to build up unmanned defense capabilities** to further strengthen the architecture for national defense.



Unmanned assets



Use of Unmanned Assets in the Aggression Against Ukraine

- **Unmanned assets have been used in various ways in the aggression against Ukraine.**
  - ✓ Russia has waged large-scale attack **combining** inexpensive, mass-producible long-range attack and decoy UAVs*1 with **existing ballistic and cruise missiles**.
  - ✓ The massively deployed unmanned assets for ISRT*2 have made troop movements on each other's front lines more transparent.
  - ✓ Ukraine has destroyed high-end Russian assets, such as vessels and bombers, using large quantities of inexpensive, **attritable***3 unmanned assets and imposed asymmetric costs.
  - ✓ The use of unmanned assets helps preserve combat power and **minimizes personnel losses in a protracted war**.
  - ✓ Operational data from unmanned assets obtained by front-line units are fed back to developers, enabling **repeated updates in a very short timeframe**.

*1 UAV: **U**nmanned **A**erial **V**ehicle

*2 ISRT: **I**ntelligence, **S**urveillance, **R**econnaissance and **T**argeting

*3 Attritable: "Designed to be recovered and reused after use but loss is acceptable if required by the mission"

Self-destructive long-range UAV ("Shahed" type UAV)

Attacking the enemy using FPV drones from rear areas, away from the front lines

Image of unmanned surface vehicle (MAGURA V [Ukraine])

Direction of Consideration

- Unmanned defense capabilities **should continue to be regarded as important capabilities** in strengthening defense capabilities.
- Taking into account **the use of unmanned assets in the aggression against Ukraine and other conflicts** and Japan's severe demographic situation caused by **population decline**, and from the perspective of more effectively disrupting attacks against Japan, the following will be given focused consideration.

Main Items for Consideration

- **Considering the military buildup in Japan's surrounding countries and others, it is urgently necessary to transform our force structure into one that can more efficiently disrupt attacks against Japan. In particular, innovative R&D to enable force structure transformation will be critical. As a result of pursuing drastic unmanning and automation, we will aim to become an "organization that makes the most effective use of unmanned assets in the world."**
- **Realizing a rapid innovation cycle to adapt to rapidly changing ways of warfare.**

(Image: ATLA)

Combat-supporting multi-purpose USV

(Photo: MSDF)

Long-endurance UAV (MQ-9B Sea Guardian)

(Photo: ASDF)

UAV designed for collecting target information

Defense Capabilities in the Space Domain

Use of Space for Security

Expanding use of space by the military and civilian sectors

- The use of space, such as for communications, observation, and positioning, navigation and timing (PNT), forms the **very foundation of people's lives**.
- In the field of security, it forms the **core of the command and control/intelligence infrastructure for military operations** in all domains, including ground, maritime, and air (collection of satellite imagery and use of communications satellites).
- **Countries are highly dependent on space for military operations**, and are focusing on strengthening the capabilities and increasing the number of satellites.

Expanding risks and threats in space

- Some countries are **stepping up moves to interfere with and neutralize the satellites of other countries to secure military superiority**.
  - ✓ Technology development contributing to killer satellites, and development and testing of Direct-Ascent Anti-SATellite (DA-ASAT) missiles

Increasing military satellites

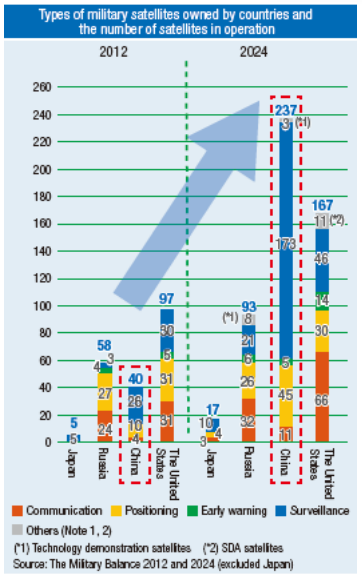
- Pronounced in China, increasing approx. sixfold in 12 years since 2012.

Increasing space debris

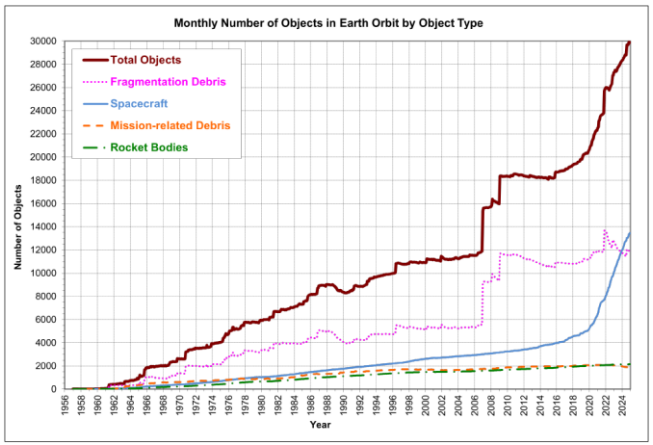
- Number of debris tracked by NASA: over 30,000 objects (approx. 10 cm or larger)

Anti-satellite (ASAT) tests

- China conducted one in 2007 and Russia in 2021.



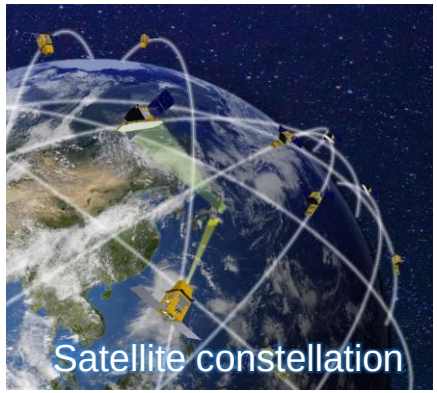
Types of military satellites owned by countries and the number of satellites in operation (2025 Defense White Paper)



Number of objects in the Earth's orbit (NASA)

What Are “Defense Capabilities in the Space Domain”?

Amid expanding threats and risks in space, it is essential that the use of space, which forms the foundation of people’s lives and the core of the Self-Defense Forces’ (SDF) operations, is ensured under all circumstances.

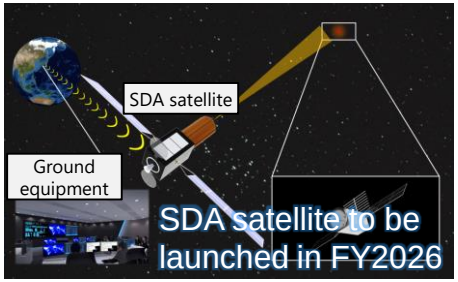

Satellite constellation

Defense capabilities in the space domain

Direction of strengthening defense capabilities in the space domain, as outlined in the Space Domain Defense Guidelines

1 Timely and accurate battlespace awareness

- ✓ Real-time detection/tracking of moving targets to ensure the effectiveness of stand-off defense capabilities
- ✓ Real-time hypersonic glide vehicle (HGV) detection/tracking in its glide phase
- ✓ Real-time monitoring of dynamic information and battlespace in the vicinity of Japan



SDA satellite to be launched in FY2026

2 Satellite communications (SATCOM)

- ✓ Multi-layered and resilient SATCOM network ranging from stratosphere to LEO and GEO
- ✓ Capabilities to accommodate increasing communication needs

3 Mission assurance

- ✓ Further strengthening space domain awareness (SDA) capabilities and building capabilities necessary to protect satellites
- ✓ Strengthening the resilience of the entire space system and considering the establishment of a system to responsively supplement lost functions as necessary


Launch of Kirameki 3 (Tanegashima Space Center)
©JAXA

4 Disrupting command, control, communications, computers and intelligence (C4I) and other capabilities of the opponent

5 Comprehensive initiatives underpinning the policies

- ✓ Strengthening the organizational structure, foundation for personnel, and cooperation with our ally and like-minded countries related to the space domain

Basic Concept Behind "Strengthening Defense Capabilities in the Space Domain"

○ If **Japan's stable use of space is inhibited, it may put Japan in an overwhelmingly disadvantageous position relative to the opponent, particularly in the fields of ISRT*1 and communications, which would seriously interfere with the MOD/SDF's mission execution.**

Securing the SDF's **stable use of space is critically important** for **ensuring "superiority in decision-making,"** which will be key to the SDF's future ways of warfare.

○ If the use of space is inhibited, **Japan's economic and social activities may be adversely affected**.

○ **The space domain facilitates the creation of a virtuous cycle between defense and economy, and this characteristic will be leveraged to the fullest extent.**

Goal to be achieved

◆ **Building a framework that ensures the stable use of space by the SDF, as well as the use of space for people's lives as social infrastructure**

*1 Intelligence, Surveillance, Reconnaissance and Targeting

Direction of Consideration

■ **Defense capabilities in the space domain remain capacities that should be emphasized in strengthening national defense, and efforts will continue to focus in particular on the following matters.**

Main Items for Consideration

- Investing in technological fields where Japan has an advantage and enhancing the capabilities of the SDF while driving corporate growth
- Building a mutually complementary framework with Japan's ally and like-minded countries for capability enhancement and operational cooperation in the space domain
- Securing personnel and raising the level of knowledge related to the space domain
- Ensuring superiority in the space domain through an all-Japan effort

Strengthening Cyber Defense Capabilities

Lessons Learned from Recent Cyber Attacks

Attacks using third countries as proxies (pre-contingency)

- **Third countries** with vulnerable cybersecurity foundations are used as **proxies** to **exfiltrate sensitive military information** of Western countries. Adversaries may also **compromise Japan's defense equipment supply chain** and steal sensitive information.

→ Capacity-building support to improve cybersecurity in third countries (Improving the cyber security environment)

APT attack campaigns (pre-contingency)

- Advanced Persistent Threats (APT), such as Volt Typhoon, compromise **critical infrastructure and military facilities** over an extended period **before a contingency**, aiming to disrupt communications and other core infrastructure during a **future contingency**.
- **Attack campaigns** conducted across **several targets and regions**. **Cyber kill chain** automation using **AI**.
- Protecting the command and control/intelligence systems, which enable the SDF to demonstrate its capabilities, and protecting the **critical infrastructure** base **before a contingency** directly contributes to ensuring mission assurance during a **contingency**.

→
- From peacetime, impose costs on opponents' ability to sustain operations
- Eliminate latent threats prior to detection

Aggression against Ukraine (contingency)

- Following **a long-term compromise of satellite communication networks**, malware was activated immediately before the ground invasion.
- **Simultaneous cyber attacks** put a strain on the defender's resources.
- Ukraine successfully detected and eliminated latent threats at an early stage, with U.S. military **support for threat hunting** prior to the war.

→
- Sustainable operational capability
- A posture that can withstand simultaneous attacks
- Enhancing defensive capabilities before the start of hostilities

Images created using generative AI

Direction for Strengthening Cyber Defense Capabilities

(1) Cyberspace operations capabilities

(4) Cyber ISR
(Intelligence, Surveillance and Reconnaissance)

Public-private partership

Cooperation among relevant ministries and agencies

International cooperation

(2) Cyber resilience

Cyber defense capabilities to be pursued

(5) Cyber unit posture

(3) Real-time SA&IR
(Situational Awareness & Incident Response)

(6) Development/ recruitment of cyber workforce

Images created using generative AI

Specific Way Forward (1)

(1) Cyberspace operations capabilities

- Expand and enhance the JSDF Cyber Defense Command's posture, **including strengthening cyberspace operations capabilities** to counter **simultaneous and high-intensity attack campaigns**.
- To **ensure SDF's mission assurance** in a **contingency**, establish a posture that can deter and respond to an opponent's attack campaign by **implementing remote access and neutralization measures** and **threat hunting** **before a contingency occurs**.
- Consider **capacity-building support for third countries** to counter attacks that use third countries as proxies.

(2) Cyber resilience

- Position the **"protection of MOD Cloud"** as part of cyberspace operations, and develop the posture necessary for the **JSDF Cyber Defense Command to play a central role**.
- Ensure cloud AI security, and with the JSDF Cyber Defense Command playing a central role, develop functions that enable **cyber-AI-data integrated operations**.
- Promote the **installation of edge servers at regional bases** so that **lower-level units can directly process information even in unforeseen circumstances**.

Images created using generative AI

Specific Way Forward (2)

(3) Real-time SA&IR

- To **strengthen real-time cyber SA&IR capabilities** in simultaneous and high-intensity campaigns, establish an **operating model for respective SDF services to coordinate and cooperate in an integrated manner under the command of the JSDF Cyber Defense Command**.

(4) Cyber ISR

- To eliminate latent threats and enhance the effectiveness of IR, **strengthen capabilities in collecting intelligence, from peacetime through contingencies**, and **in developing hypotheses** regarding anticipated threats. **Ensure close coordination with relevant ministries and agencies, foreign organizations, and the defense industry.**
- Share intelligence in cyberspace obtained by the MOD/SDF with relevant ministries and agencies and contribute to government initiatives (**public attribution and information warfare**).

(5) Cyber unit posture

- To ensure **readiness to execute missions** even in simultaneous and high-intensity campaigns, **strengthen the posture of cyber units** under the leadership of the JSDF Cyber Defense Command.

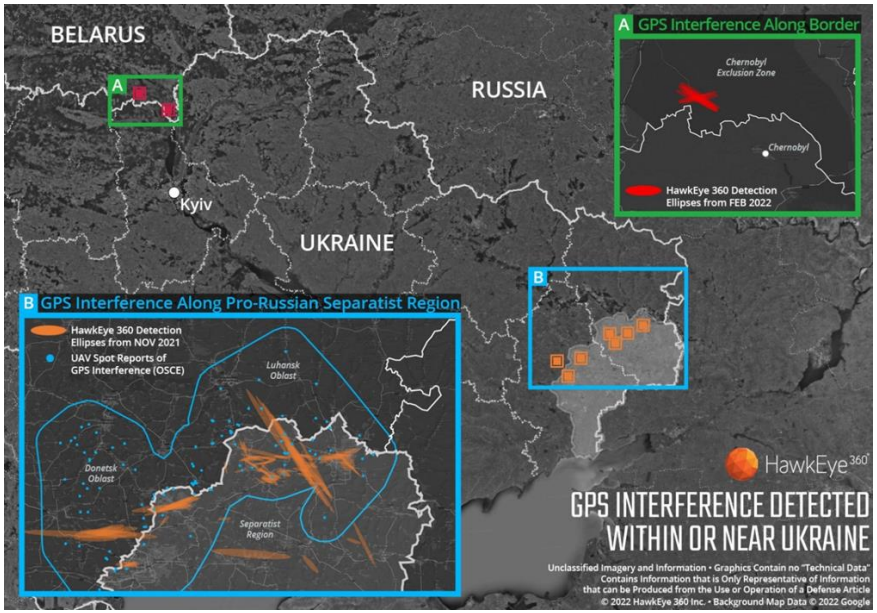
(6) Development/ recruitment of cyber workforce

- Given that the **quantitative targets for cyber units have largely been achieved** under the ongoing Defense Buildup Program, **ensure the quality of the cyber workforce** in the next program, including bringing in talent from outside the MOD/SDF **(especially for AI, data, cloud, etc.)**.

Images created using generative AI

Electromagnetic Domain

- With the **sophistication of electronic warfare** aimed at neutralizing precision strikes and UAVs, it is necessary to further reinforce **electronic jamming capabilities** and **electronic protection capabilities**.
- Due to the increasing use of the electromagnetic spectrum on the battlefield, **electromagnetic spectrum management (ESM)** (managing the electromagnetic environment) to allocate limited frequency bands and avoid fratricide **has become critically important** and must be strengthened with high priority.



Source: HawkEye 360

GPS jamming was observed near the border shortly before the invasion


Source: Petro Poroshenko Foundation
SHATRO 50-1M electronic warfare system


Source: Tochnyi.info
https://tochnyi.info/2024/01/fpv-data-analysis/
Tochnyi


Source: Militarnyi (Photo by Petro Poroshenko Press Service)
https://defencesecurityasia.com/en/fpv-drones-pose-increasing-threat-russia-equips-tanks-with-ew-systems/#google_vignette

Top left: Volnorez (Russia)

Bottom left: SHATRO 50-1M (Ukraine)

Top right: Self-destructive FPV drone

Electronic warfare systems with operational ranges from several hundred meters to appx. 10 km have emerged to protect personnel and equipment as countermeasures against self-destructive UAVs

ESM
Monitoring electromagnetic spectrum usage and appropriately adjusting the frequencies to be used

Electronic Warfare Support
Collecting and analyzing information on electromagnetic waves used by the opponent

Electronic Jamming
Reducing or neutralizing opponent's communications and detection capabilities by radiating electromagnetic waves against their communications equipment and radars

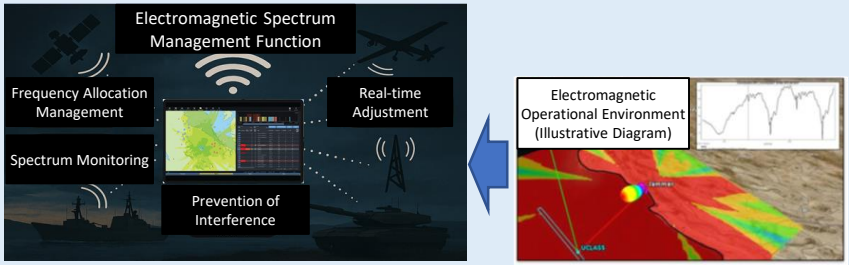
Electronic Protection
Protecting against the opponent's electronic jamming through stealth technology, frequency changes, etc.

Specific Way Forward (1)

ESM

- It is important to **quickly and accurately understand the electromagnetic operating environment** and exercise **command and control** for electronic warfare.
- As the number of UAVs increases, so does the need to **avoid radio interference**.

◆ **Accurately understanding the electromagnetic operational environment**, and strengthening capabilities to **automate the allocation of frequencies** for avoiding radio interference and to exercise **command and control** for electronic warfare



Images created using generative AI

Electronic Warfare Support

- It is important to enhance both the quality and quantity of sensors held by electronic warfare units, which will provide them with **real-time awareness of the electromagnetic environment** for conducting operations.
- The operational tempo on the battlefield is accelerating, making it necessary to **adapt rapidly to changing situations**.

◆ **Expanding, upgrading, extending the range of, and networking sensors** so that electronic warfare units can continuously monitor the electromagnetic operational environment

◆ **Using AI to automate and accelerate** the processing of collected electromagnetic information

Specific Way Forward (2)

Electronic Jamming

- Possess a certain level **of stand-off jammer**-related capabilities.
- Need to **develop and enhance electronic jamming measures** against threats.
- Need to **improve response capabilities** to large numbers of **incoming UAVs**.

- **Diversifying electronic jamming capabilities** by developing **stand-off jammers**, **stand-in jammer** unmanned assets, etc. with high damage tolerance, and **high-power energy systems** for countering UAVs, etc.

Stand-in jammer

High-power microwave system

Images created using generative AI

Electronic Protection

- Existing assets **rely heavily on passive protection** such as stealth technology.
- With the expansion of systems requiring positioning and timing, **the importance of PNT* is becoming more essential**.

*PNT: Positioning, Navigation and Timing

- Creating **multilayered electronic protection** by strengthening active measures, such as frequency hopping, alongside passive protection such as stealth technology
- Creating a **multi-source PNT** by utilizing multiple satellite positioning systems, such as GPS and Michibiki, as well as terrain data matching

Images created using generative AI

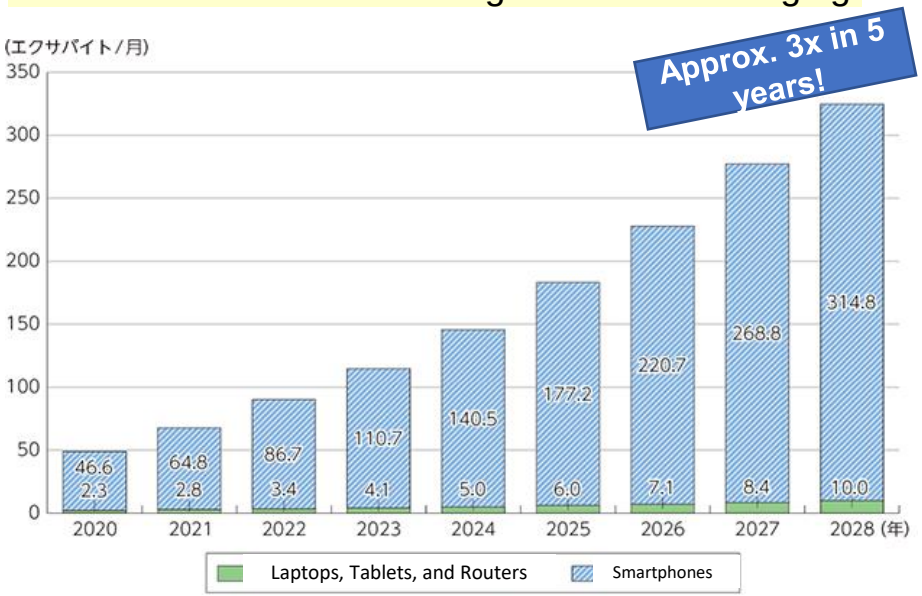
Command and Control, and Communications

Situational Awareness (1): Game-Changing Advanced Technologies

◆ With remarkable technological advances in recent years: (1) the **volume of data** obtained by increasingly high-performance and diversified sensors has **grown dramatically**. (2) These data are **transmitted in real time, at high speed, and in large volumes**. (3) By using AI, it has become possible to **accumulate, process, and analyze data** in a sophisticated and timely manner.

(1) Sensor diversification and sophistication, along with the increasing volume of data

The volume of data circulating worldwide is surging.



Forecast for global mobile data traffic (device-specific)

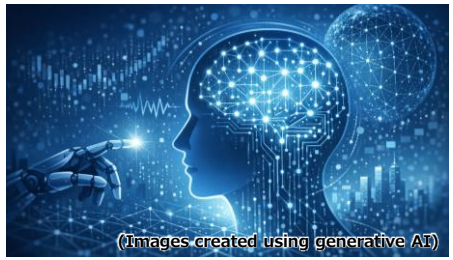
Ever since the Russian aggression began, Ukraine is said to have **collected 2 million hours (= approx. 228 years) of battlefield video from drones by late 2024**.
(Source: Reuters, December 26, 2024)

(2) Realization of real-time, high-capacity communication networks

Progress has been made in developing technologies for **low-power, high-capacity, low-latency, and high-speed transmission**, such as All-Photonics Network (APN) based on photonics-electronics convergence technologies, and in providing **services using LEO satellite constellations**, which enable lower latency communications than GEO.

Images created using generative AI

(3) Rapid evolution of AI



Since big data can be collected and accumulated, countries are focusing on the development and effective use of generative AI, such as ChatGPT, Claude, Gemini (U.S.), and DeepSeek (China), as well as physical AI.

Vast volumes of data that had not been fully utilized can now be used due to technological advances!

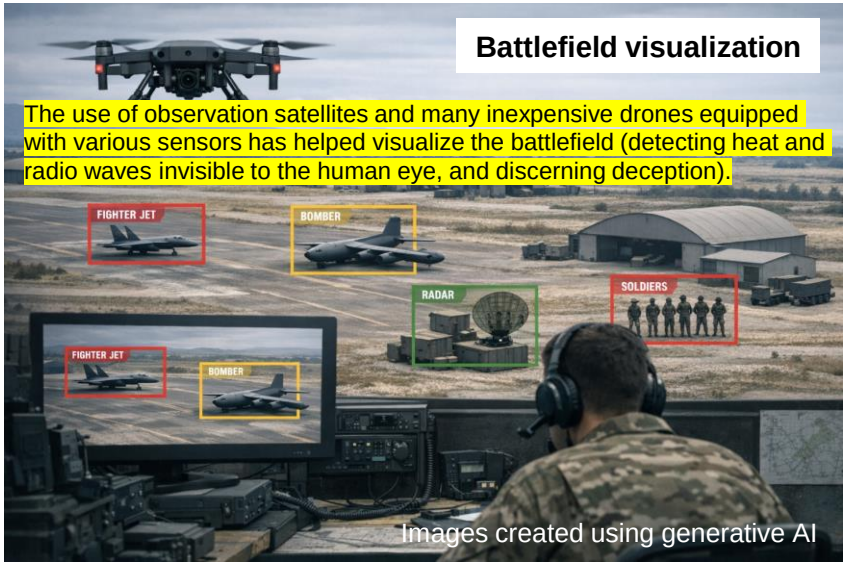
Situational Awareness (2): Accelerated Decision-making Using Advanced Technologies

- In the aggression against Ukraine, **data- and AI-driven warfare** is already unfolding, such as the autonomous operation of UAVs and fire control. **AI is now an indispensable element that influences the outcome of hostilities.**
- Specifically, by integrating data obtained from diverse sensors and utilizing AI, the following have become possible, which contributes to quick, accurate decision-making beyond the limits of human capability:
  (1) **Reducing the "fog of war" and visualizing the battlefield (= previously unseen things have become visible)**
  (2) **Analyzing behavioral patterns from data and making future predictions (= utilizing large-scale data by AI)**
  (3) **Determining the order of priority of targets, allocating forces, and conducting attacks (= supporting human tasks)**

Examples of "New Ways of Warfare" in Ukraine

Battlefield visualization

The use of observation satellites and many inexpensive drones equipped with various sensors has helped visualize the battlefield (detecting heat and radio waves invisible to the human eye, and discerning deception).



Ukraine has pre-trained AI about vulnerabilities in target platforms. Based on this training data, drones autonomously determined the order of priority of targets and attack points. More recently, it has also been suggested that AI-equipped drones have been deployed in combat and have been conducting attacks by autonomous flight.

Decision-making support

Ukraine has developed the Delta data monitoring system, which centrally aggregates various types of information and shares them among the platforms of military services.
Information collected from front-line units, drones, satellites, and other sources is processed by AI and stored in Delta. If target information is entered by touch input, the information is automatically uploaded to Delta, and the optimal firepower is automatically assigned.

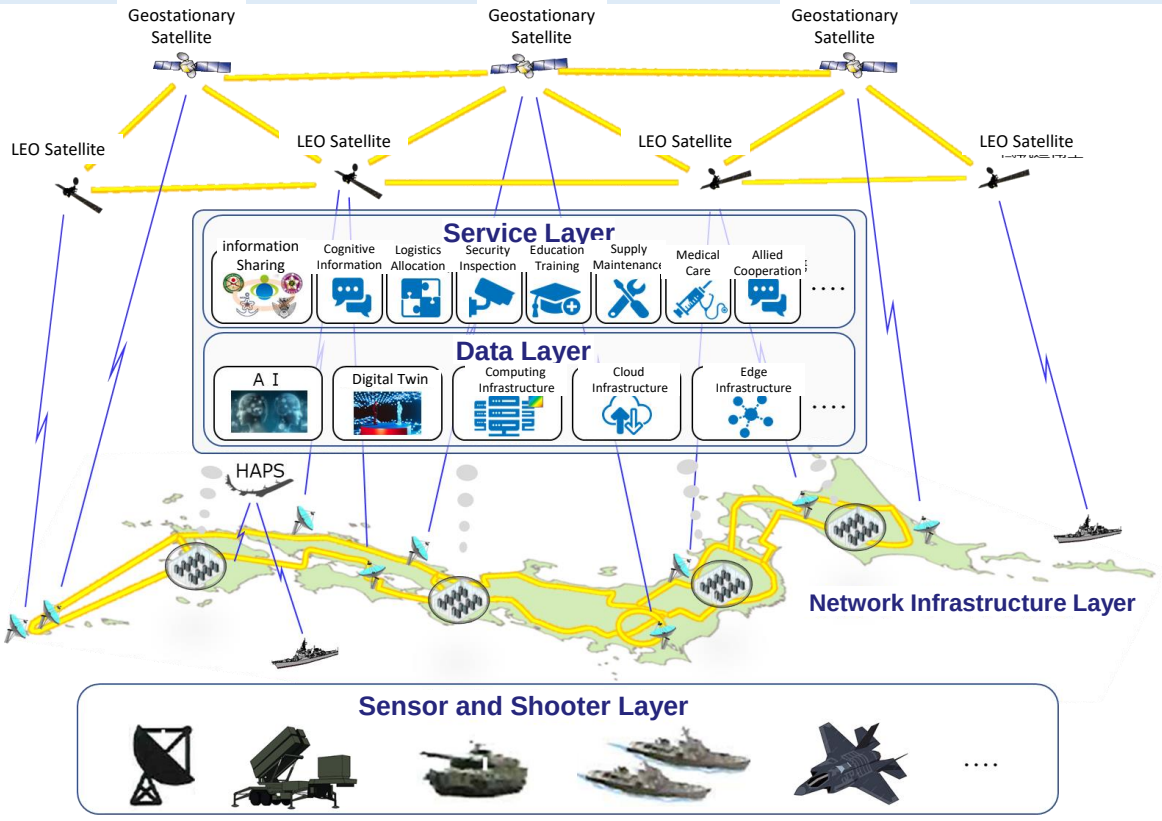
Conceptualization of “New Ways of Warfare”

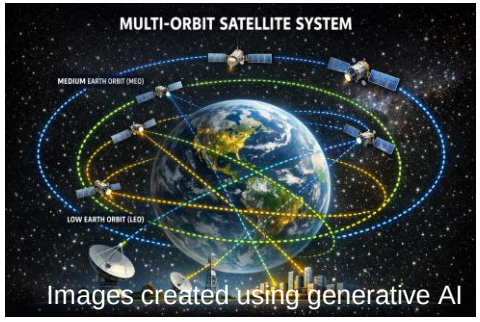
- Various types of data are organically integrated in real time to visualize the combat situation and future predictions using AI, Digital Twin, and other technologies.
- Optimal methods and timing for force employment are recommended using AI.
- Necessary information can be accessed by not only the command center but also field units.
- Mesh networks ensure resilience. Even in the event of disconnection, operations are continued at the front line by using edge AI.

By ensuring communications resilience, maintain *seamless information access* and integrate all data and process them with AI to enable *battlefield visualization* and *future predictions and recommendations*, thereby ensuring *decision-making superiority*.
⇒ Data-centric ways of warfare

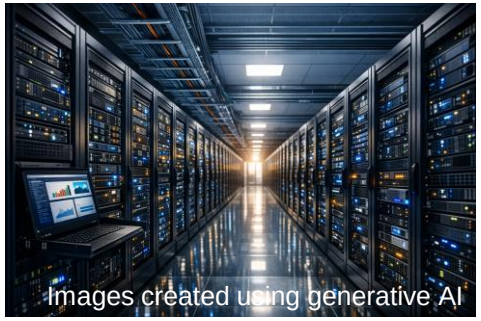
Direction of Consideration

- **The information and communication infrastructure serves as the foundation for all initiatives and is a prerequisite for realizing stand-off missile defense capabilities and the SHIELD concept.**
- **Data-centric ways of warfare will be achieved through the following initiatives.**





Images created using generative AI


Images created using generative AI

<u>Service Layer</u>

⇒ Making maximum use of data and AI

Ex: Command and control, decision support

<u>Data Layer</u>

⇒ Strengthening the data infrastructure (next page)

<u>Network Infrastructure Layer</u>

⇒ Multi-network and high-speed/high-capacity communication

Ex: Multi-orbit satellite systems and HAPS
Optical inter-satellite communications, APN-based terrestrial networks

<u>Common initiatives</u>

⇒ Strengthening the security of infrastructure

✓ Strengthening system risk management
Ex: RMF, Zero Trust

✓ Strengthening and introducing encryption for protecting communications and data
Ex: Post-quantum cryptography, quantum cryptographic communications

Efforts Requiring Particular Focus: Strengthening the Data Infrastructure

- Accelerating decision-making and using AI require **large amounts of AI training data**, making it necessary to establish a cloud-based data integration platform to accumulate data and process it using AI.
- Given the need to **appropriately accumulate and process** the rapidly growing volume of data, the MOD will **shift** from on-premises-type infrastructure **to hybrid cloud** infrastructure that **combines commercial cloud services**
- Ensuring both "security" and "sovereignty" when introducing commercial cloud services

On premises

In-house server environment

Hybrid cloud

◎**Highly customizable**

◎**Easy to manage operational control**

Commercial cloud services

Safe and sovereign large-capacity cloud environment

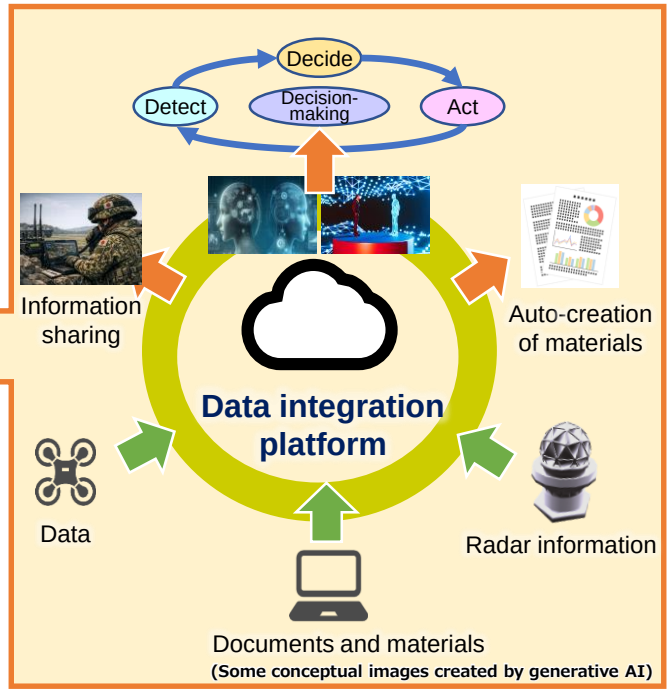
Hybrid cloud

◎**Latest security and other services**

◎**High scalability**
(suitable for high-capacity AI processing)

◎**High data resilience**

◎**Shorter lead time to operational deployment**



Cooperation with Like-minded Countries

Current Situation, Challenges, and Future Direction

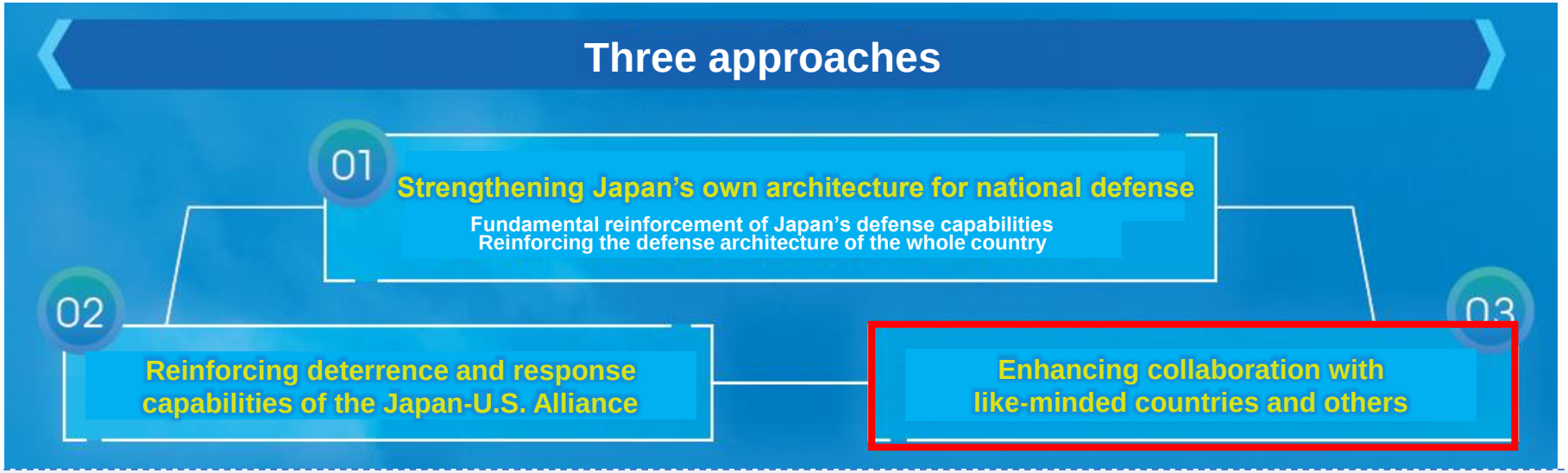
Cooperation with Like-minded Countries: Status under the Three Strategic Documents

- National Security Strategy

  "Maintain and develop a free and open international order and strengthen ties with its (= Japan's) ally, like-minded countries, and others" as part of "efforts centered on diplomacy" (listed first under "strategic approaches prioritized by Japan")

- National Defense Strategy

  Collaboration with like-minded countries identified as one of the three approaches for realizing Japan's defense objectives



[Reference] National Defense Strategy (approved by the Cabinet Decision on December 16, 2022)

III Japan's Basic Defense Policy

3 Collaboration with like-minded countries and others

The third approach is to enhance collaboration with like-minded countries and others. In order to counter unilateral changes to the status quo by force and such attempts and to ensure Japan's security, it is extremely important to reinforce collaboration with not only our ally but also as many countries as possible. From such perspective, Japan will promote efforts to contribute to realizing the vision of a FOIP.

First of all, Japan will, while placing the Japan-U.S. Alliance the key pillar of its security policy, proactively promote multilateral and multilayered defense cooperation and exchanges, taking into account characteristics of the region as well as situation of each country. In doing so, Japan will further promote institutional frameworks such as Reciprocal Access Agreements (RAA), Acquisition and Cross-Servicing Agreements (ACSA), and Agreements concerning the Transfer of Defense Equipment and Technology. (Abridged)

Changes in the Security Environment Following the Formulation of the Three Strategic Documents

○ Need to respond to changes in the strategic environment, including Russia's prolonged aggression against Ukraine

○ Need to secure posture capable of responding to prolonged conflicts.

E.g. 1: Support and cooperation from allies and like-minded countries during the aggression against Ukraine

- The Ukrainian military's operational capabilities and warfighting sustainability have been strengthened through Western countries' provision of large amounts of equipment as well as support in the areas of intelligence and education/training.

  ⇒ In a protracted war, continued support from allies and like-minded countries plays a significant role.

- Ukraine is advancing efforts to co-produce equipment with Western countries, while Russia has also acquired and used weapons from foreign countries.

  ⇒ Bilateral and multilateral initiatives to share production and supply of defense equipment and to secure common maintenance and supply bases also play a significant role in strengthening warfighting sustainability.

E.g. 2: Cooperation with allies and like-minded countries in sea lane defense

- In addition to ensuring the stable use of all sea lanes, maintaining conditions that allow civilian vessels to navigate safely, particularly in the Pacific, is indispensable not only for SDF operations but also for sustaining the daily lives of Japanese citizens.
- Recent examples of armed conflict have also shown that instability in sea lanes can have serious effects on a country's logistics as a whole, including energy and food supplies, and on international logistics overall.

  ⇒ Cooperation with like-minded countries and allies is essential to ensure the stable use of Japan's extensive sea lanes.

Defense assets announced to be provided to Ukraine

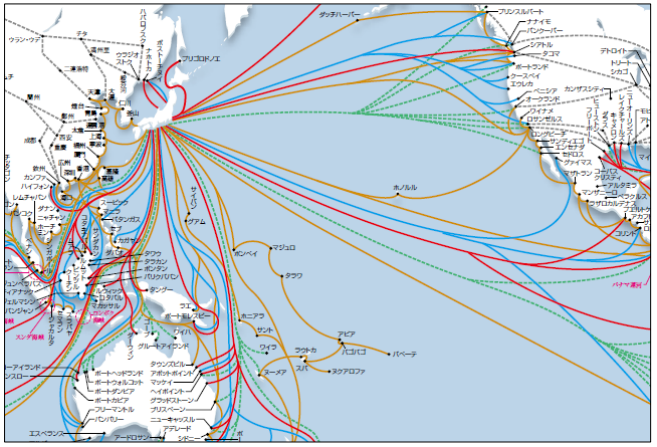
Javelin

HIMARS

PATRIOT

F-16

Maritime routes in the Pacific*



*Source: "Japan's Shipping: SHIPPING NOW 2025-2026," ed. Japan Maritime Public Relations Center. The image has been partially modified for reference.

Cooperation with Like-minded Countries: Approaches

○ Cooperation with like-minded countries has made considerable progress through bilateral and multilateral efforts. Japan has steadily concluded Acquisition and Cross-Servicing Agreements (ACSA), Reciprocal Access Agreements (RAA), Information Security Agreements, and Defense Equipment and Technology Transfer Agreements, which are institutional foundations of defense cooperation and exchanges.

Methodology: Cooperation frameworks

- Build and interconnect a multilayered web of cooperation through bilateral/minilateral cooperation.
  - The Japan-U.S. Alliance as the cornerstone
    ⇒ Japan-U.S.-Australia, Japan-U.S.-Australia-Philippines, Japan-U.S.-ROK, Japan-U.S.- Australia-India
  - Joint development of next-generation fighter aircraft: Japan, U.K., and Italy
- Multilateral cooperation: Japan-ASEAN, JPIDD, NATO-IP4, PIPIR

*Minilateral cooperation: A form of collaboration among three or more but no more than a small number of countries
*IP4: NATO's Indo-Pacific partners (Japan, Australia, New Zealand, Republic of Korea)
*JPIDD: Japan-Pacific Islands Defense Dialogue
*PIPIR: Partnership for Indo-Pacific Industrial Resilience

MOD's approach

- "Spirit of OCEAN" (2025 Shangri-La Dialogue)

A shared determination among defense authorities sharing common values and interests to (1) take a broad and panoramic view of the Indo-Pacific, (2) generate synergy through enhanced cooperation and collaboration, and (3) create new values and benefits for the entire region, grounded in a shared spirit to (1) restore the rules-based international order, (2) strengthen accountability, and (3) advance the international public good through openness, inclusivity, and transparency.

- "Multilayered web of interconnectivity" (2025 ADMM Plus)

Strengthen respective voluntary initiatives, and interconnect various areas of defense cooperation, such as joint exercises, people-to-people exchanges, capacity building assistance, and defense equipment and technology cooperation, layer after layer, creating strong synergies to weave a multilayered web of interconnectivity across the region, thereby fostering a flexible, resilient, and stable regional order.

Cooperation with Like-minded Countries: Tools and Institutional Foundations

Main tools for defense cooperation and exchanges

- People-to-people cooperation and exchanges (Ex: high-level exchanges such as “2+2” and defense ministerial meetings, working-level exchanges, multilateral security dialogues, education and research exchanges)
- Unit-level cooperation and exchanges (Ex: joint training and exercises, reciprocal visits by vessels and aircraft (port calls and air visits), exchange events between units)
- Capacity building (Ex: seminars and practical training in various fields, technical guidance, site visits of education and training, exchanges of views)
- Defense equipment and technology cooperation (Ex: overseas transfer of equipment, joint R&D, participating in international exhibitions, hosting public-private defense industry forums)

Institutional frameworks for defense cooperation and exchanges

- Information Security Agreement (ISA): Establishes measures to appropriately protect classified information exchanged with counterpart governments etc.
- Defense Equipment and Technology Transfer Agreement (ETTA): Establishes the legal framework for joint development and production of defense equipment and technology between governments, as well as for the handling of equipment and technology to be transferred.
- ACSA: Defines settlement procedures to facilitate the provision of supplies and services when conducting activities with foreign militaries.
- RAA: Defines the legal status of forces when they visit the other country and conduct activities, such as joint exercises, and reciprocally simplifies procedures.

	AUS	UK	PHL	IDN	SGP	IND	FRA	GER	ITA	CAN	UKR	ROK	NATO
ISA	○	○				○	○	○	○	○	○	○	○
ETTA	○	○	○	○	○	○	○	○	○				
ACSA	○	○				○	○	○	○	○			
RAA	○	○	○										

*In addition to the above, Japan has concluded ETTAs with Sweden, Malaysia, Vietnam, Thailand, UAE, Mongolia, and Bangladesh.

Direction of Consideration

○ From the perspective of enhancing regional deterrence, the following will be focused in order to consider advancing cooperation with like-minded countries in a more effective manner.

Main Items for Consideration	
	● Ensuring synergies among various areas of cooperation, such as people-to-people exchanges including high-level meetings, operational cooperation including joint exercises, and equipment and technology collaboration ● Ensuring synergies between bilateral cooperation and Japan-U.S./minilateral cooperation ● Cooperation tailored to the individual circumstances of each like-minded country