

R&D Vision

Toward the Realization of a Multi-Domain Defense Force
and Beyond

Explanatory Documentation

Cyber Defense Initiatives

March 31, 2020

**Acquisition, Technology &
Logistics Agency**

What is the "R&D Vision?"

The R&D vision is a document which presents the principles on Research & Development (R&D), technological challenges, and roadmaps of the technologies required to realize our future defense capability for the purpose of strategically conducting advanced R&D from the viewpoint of the mid-to-long term.

The Ministry of Defense (MOD) has formulated *R&D vision concerning Future Fighter Aircraft* in 2010, and *R&D vision of Future Unmanned Vehicles* in 2016 based on *Strategy on Defense Production and Technological Bases and Defense Technology Strategy*. According to the direction shown in *National Defense Program Guidelines for FY 2019 and beyond* (approved by the National Security Council and Cabinet on December 18, 2018), the MOD has formulated the new R&D vision. They are leading to encouragement to acquisition and enhancement of the capabilities required for cross-domain operations such as "Electromagnetic spectrum (EMS) technologies", "Technologies for Persistent ISR including Space", and "Cyber defense technologies" as well as leading to that in traditional domains such as "Underwater warfare technologies" and "Stand-off defense technologies" in order to contribute to realization of Multi-domain Defense Force and to realize technological innovation required for further enhancement of future defense capability.

According to the R&D vision, the MOD will hereafter strategically foster technologies that become necessary in the future and conduct R&D effectively and efficiently.

Remarks: A decision-making whether to initialize a development for a deployment or not is comprehensively done by the perspective of defense program on various then-conditions including progresses of researches conducted depicted on the R&D vision, a latest national security environment, an availability of procuring a foreign weapon system, etc.

Table of Contents

Table of Content Correspondence with the R&D Vision Document	2
Introduction	3
Ministry of Defense and SDF Activities in Cyberspace	4
Issues Concerning the Strengthening of Cyber Defense	5
Technologies Which Should be Acquired by the Ministry of Defense and SDF	6
Necessary Advanced Technologies	7
Classifications of Cyber Defense Technologies	8
Leading Technological Issues Which Should be Addressed (Cyber Defense)	9
Conceptual Diagram of Cyber Defense Functions	12
R&D Roadmap	13
Conclusion	14
Reference	
Previous Initiatives and Foreign and Domestic Trends in Cyberspace	16

Introduction (p. 3)

Ministry of Defense and SDF Activities in Cyberspace (p. 4)

Issues Concerning the Strengthening of Cyber Defense (p. 5)

Previous Initiatives and Foreign and Domestic Trends in Cyberspace (p. 15-17)

Technologies Which Should be Acquired by the Ministry of Defense and the SDF (p. 6)

Necessary Advanced Technologies (p. 7)

Classifications of Cyber Defense Technologies (p. 8)

Leading Technological Issues Which Should be Addressed (p. 9-11)

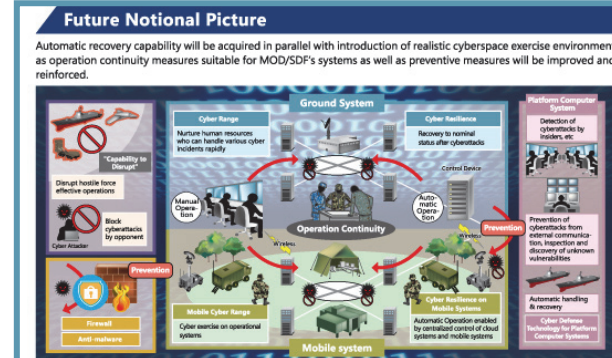
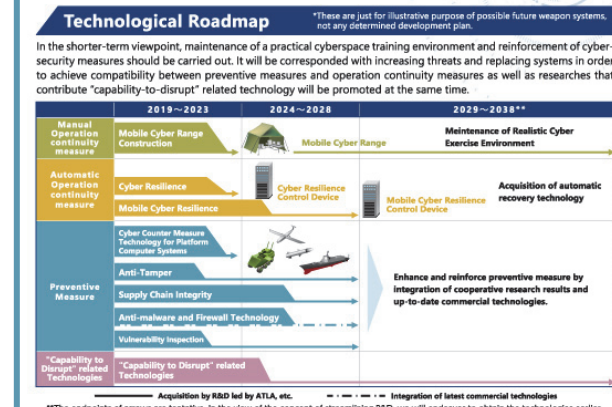
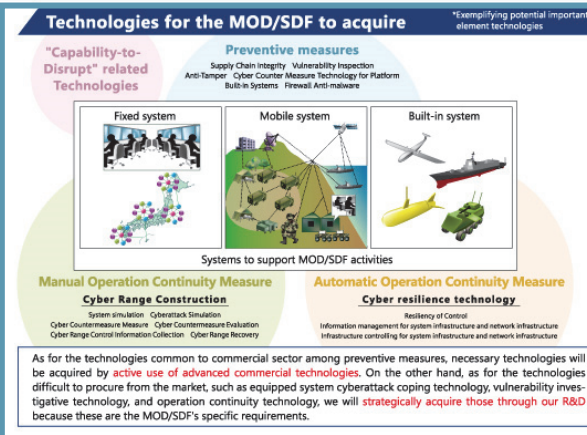
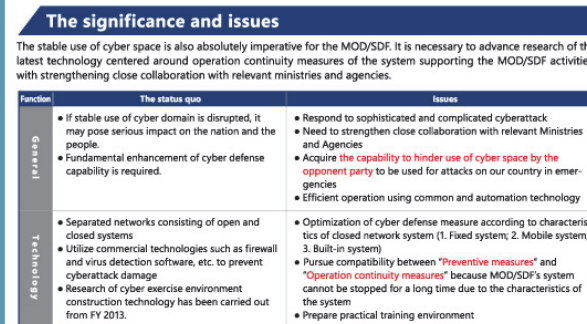
R&D Roadmap (p. 13)

Conclusion (p. 14)



R&D Vision P11-12

Cyber Defense - Compatibility between preventive measures and operation continuity measures



Classifications of Cyber Defense Technologies (p. 8)

Conceptual Diagram of Cyber Defense Functions (p. 12)

National security environment surrounding Japan

Due to the rapid technological innovation in telecommunications and other fields, military technologies have demonstrated remarkable progress. Against the backdrop of these technological advances, the current battle domains combine not only land, sea, and air but also space, **cyberspace**, and the electromagnetic spectrum. To improve their overall military capabilities, each country is pursuing superiority in technologies which support capabilities in new domains. Since space and **cyberspace domains** are also widely used in the civilian sector, impeding the stable use of these domains may have a **significant impact on the safety of the state and its citizens**.

Situation with respect to the cyber domain in surrounding countries

Armed forces rely on various forms of important infrastructure such as electric power to carry out their mission, and cyber attacks against such infrastructure can become a significant hindrance to their mission. Faced with this situation, China is increasing its defense spending to a high level devoid of transparency with the goal of building a "world-class military" by the middle of this century. The country is extensively and rapidly building up the quality and quantity of its military forces and quickly developing its capabilities in the cyber domain, which will enable China to disrupt the chain of command. In addition, North Korea maintains large-scale units in the cyber domain as a type of asymmetric military capability and appears to be pilfering classified military information and developing the capability of attacking important infrastructure targets in other countries.

Direction of capability acquisition in the cyber domain

According to the FY 2018 Guidelines, "Telecommunication networks which utilize the cyber domain are the foundation of SDF activities in various domains, and because attacks against these networks create significant barriers to the organizational activities of the SDF, MOD will continue to strengthen the SDF command communication systems to prevent such attacks in advance, persistent and continuous network monitoring capabilities, and the capabilities to rapidly implement the necessary measures to limit and recover from damage to networks. In addition, MOD will fundamentally strengthen its cyber defense capabilities including the ability in an emergency to disrupt an opponent's use of cyberspace resources to attack when conducting an attack on Japan. In doing so, MOD will significantly increase the number of talented personnel who possess expert knowledge and technical skills."



- (1) In the event that the stable use of the cyber domain is impeded, it would have a significant impact on the safety of the state and its citizens
 - (2) The Ministry of Defense and SDF rely on various forms of important infrastructure, and cyber attacks against such infrastructure are a significant hindrance to their mission
 - (3) Surrounding countries are improving their capabilities in the cyber domain and becoming a realistic threat
 - (4) To continue to strengthen the capabilities in the cyber domain, it is necessary to advance research and development according to the latest technological trends
- Given the reasons stated above, the Ministry of Defense will clarify the technological issues which it should resolve with respect to the technologies required for activities by the Ministry of Defense and SDF in cyberspace and promote various policies by developing an executable roadmap to **steadily ensure Japan's technological superiority**.

Comprehensive Ministry of Defense and SDF policies for handling cyber attacks

In the event that important SDF systems stop functioning due to cyber attacks, problems involving the core of Japan's defense may occur. Therefore, the policies consisting of (1) secure the safety of information systems, (2) counter cyber attacks through specialized units, (3) develop a cyber attack response posture, (4) research the latest technologies, (5) human resources development, and (6) coordination with other institutions are being positioned by the Ministry of Defense and SDF as the "Six Pillars of Cyber Attack Countermeasures" to comprehensively and effectively promote these policies.

1. Secure the safety of information systems

- Introduce firewall and virus detection software
- Separate the networks into DII open and closed
- Implement system auditing, etc.

2. Counter cyber attacks through specialized units

- 24-hour monitoring of networks and information systems via the Cyber Defense Unit (Control), System Protection Unit (Ground), Security and Monitoring Unit (Maritime), and the Systems Monitoring Unit (Air) as well as advanced cyber attack countermeasures (virus analysis)

3. Develop a cyber attack response posture

- Establish criteria for information system security measures
- Establish security measures that staff members should comply with
- Develop a response posture for when cyber attacks occur
- Establish the Cyber Policy Review Committee

4. Research the latest technologies

- Research technologies for constructing cyber training environments

6. Coordination with other institutions

- Share information with the National Center of Incident Readiness and Strategy for Cybersecurity, U.S. Armed Forces, and other relevant nations

5. Human resources development

- Implement study abroad programs at institutions affiliated with Carnegie Mellon University (U.S.) and Japanese graduate schools as well as education through special courses in each SDF branch for the purpose of human resource development
- Implement workplace-based education and professional education at the National Defense Academy to foster an awareness of security issues

Six Pillars of Cyber Attack Countermeasures

Cyber training environments

Simulated attacks

Simulated environment

Defense

Control and evaluation
Research

- Enables counter-cyber attack training in a simulated environment

Issues concerning the strengthening of Ministry of Defense and SDF cyber defenses

[General]

- Through the abuse of infrastructure such as telecommunication networks and information systems, cyber attacks enable unauthorized intrusions via cyberspace, the theft/modification/destruction of information, shutdown or malfunction of information systems, execution of unauthorized programs, and DDoS (Distributed Denial of Service Attack) attacks. In the event that cyber attacks are conducted against Ministry of Defense and SDF networks and systems, they may exert a significant impact on the continuation of SDF operations, and the countermeasure details have become an important issue.
- In addition, as indicated in the FY 2018 Guidelines, the acquisition of the capability in an emergency to disrupt an opponent's use of cyberspace resources to attack when conducting an attack on Japan is an urgent issue.

[Technologies]

- Within the Ministry of Defense and the SDF, systems are divided into open systems which are connected to the Internet and closed systems which are not connected. These systems are continuously monitored and protected by the Cyber Defense Unit and the system protection units of each SDF branch. In the meantime, targeted attacks, zero-day attacks, and other attack methods which evade conventional preventive measures such as firewalls and malware countermeasures have been increasing in recent years. In addition, there have also been reports of successful attacks against systems which are not connected to the Internet.
- Accordingly, in order to avoid long-term shutdowns of systems in use, it has become important for both the Ministry of Defense and the SDF to balance "preventive measures" and "operational continuity measures" to discover and handle attacks even if they do occur to improve system survivability.

* Illustrates potentially important component technologies

Technologies which contribute to "disruptive capabilities"

Preventive measures

Supply chain integrity technologies

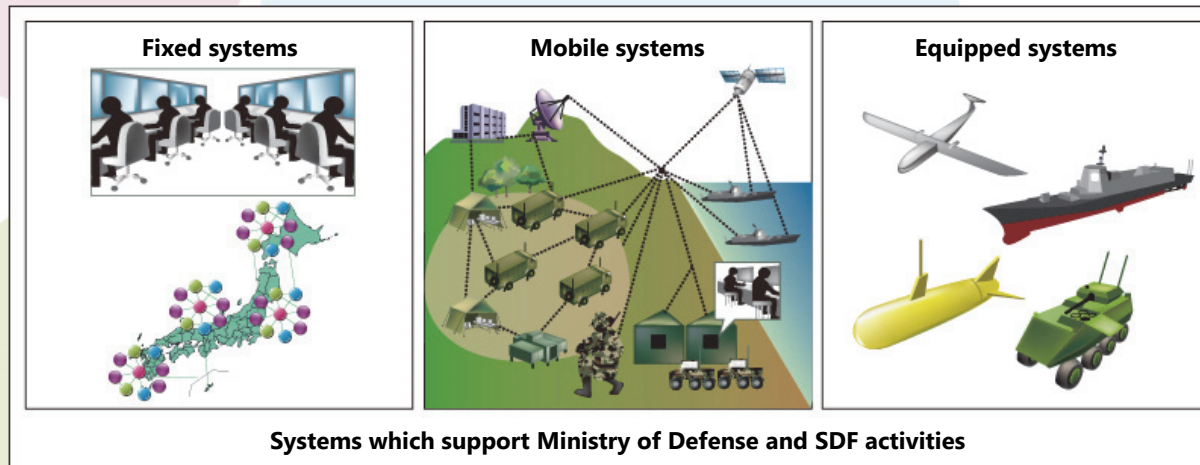
Vulnerability investigation technologies

Tamper-resistant technologies

Cyber attack countermeasure technologies for equipped systems

Firewall technologies

Anti-malware technologies



Manually-implemented operational continuity measures

Technologies for constructing cyber training environments

Technologies for reproducing and controlling cyber attacks
Technologies for gathering cyber training control information
Cyber training environment recovery technologies

Automatically-implemented operational continuity measures

Cyber-resilience technologies

Technologies for control function survivability
System and network infrastructure information management technologies
System and network infrastructure control technologies

Regarding the technologies which are shared with the civilian sector within the preventive measures, acquire the necessary technologies through the **proactive utilization of advanced civilian technologies**. At the same time, cyber attack countermeasure technologies for equipped systems, vulnerability investigation technologies and technologies which contribute to disruptive capabilities, operational continuity measures, and other preventive measures which are difficult to procure from the market will be **strategically acquired through technology research and development**, because the Ministry of Defense and the SDF have specific requirements.

Technological progress in cyber defense

- Anti-malware technologies and other preventive measures are being actively researched in the private sector. On the other hand, tamper-resistant technologies are being researched in the private sector, but there is little public information
- In the area of manually-implemented operational continuity measures, cyber training environments which differ from the actual environments using standard equipment are being practically applied for the training of cyber countermeasure personnel. However, there are not many technologies for building cyber training environments which use actual environments.
- In the area of automatically-implemented operational continuity measures, real-time analysis of security log information and dynamic cyber attack detection using artificial intelligence technologies, etc. are being practically applied. However, there are not many technologies which balance operational continuity with prevention.



Anti-malware technologies



Firewall technologies



Tamper-resistant technologies

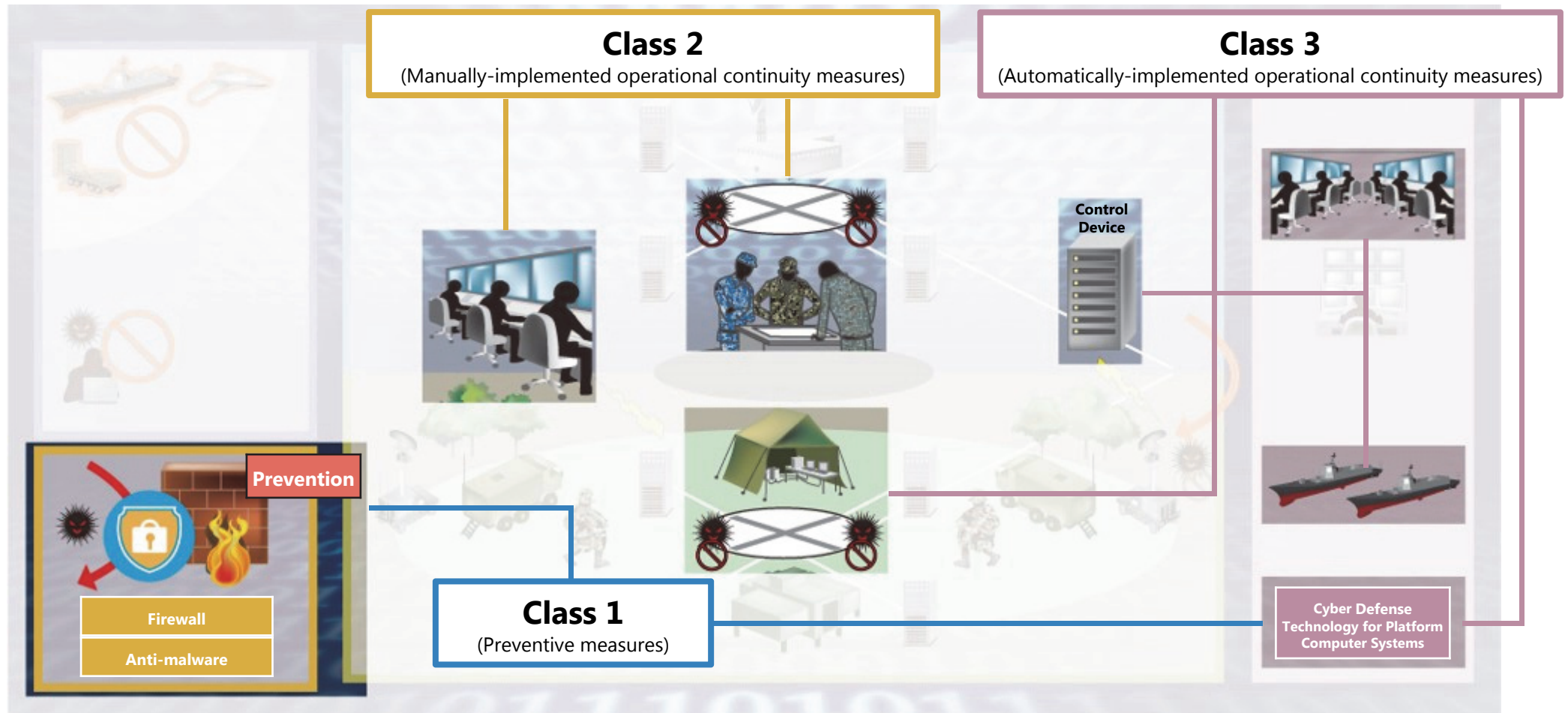
=> Developing with a focus on preventive measures

Direction of future development

- In order to prevent cyber attacks against systems and networks in advance, superior private sector technologies must be incorporated and adapted to Ministry of Defense and SDF systems (closely observing quantum communications, quantum cryptography, and other technologies which may help improve cyber defense capabilities in the future)
- In the area of manually-implemented operational continuity measures, cyber attacks are increasingly sophisticated as security boundaries become vague due to advances in cloud technologies and an explosive increase in the sources of malware infection is expected due to the increase in mobile devices and the application of COTS to mobile systems, which leads to a need for measures to improve the capabilities of cyber countermeasure personnel
- In the area of automatically-implemented operational continuity measures, operational continuity must be rapidly secured and an expansion of the damage caused by cyber attacks against the low-quality and low-speed lines of mobile systems must be prevented. In addition, regarding automatically-implemented operational continuity measures, the utilization of AI and quantum-related technologies must be confirmed and applied with respect to system compatibility
- In equipped systems which require real-time processing, previously cataloged prevention examples and automatically handled operational continuity measures must be adapted to the equipped systems

Advanced technologies which are the key to achieving cyber defense functions

- Technologies which effectively adapt private sector technologies to prevent cyber attacks from an opponent in advance (for example, technologies for preventing internal information leaks and modifications, technologies which are able to investigate vulnerabilities in our systems, and technologies which detect hardware and programs which have been modified in an unauthorized manner)
 - * Future examples include quantum cryptography and quantum communications technologies which may contribute to advanced concealment
- Technologies for constructing cyber training environments which contribute to the development of cyber countermeasure personnel and practice in countermeasure domains (technologies which simulate MOD systems, technologies which autonomously attack based on the skill of the training participants, and technologies which evaluate the responses of the training participants)
- Cyber-resilience technologies are required to automatically ensure the operational continuity of the systems by preventing the cyber attack damage from spreading and ensuring the continuation of operations (technologies which maintain the fundamental control functions of the system infrastructure, technologies which prevent the damage from spreading and continue the operation of important systems, and technologies for managing the operational status of important systems). In addition, AI and other technologies are needed to promote automation and acceleration
- Technologies for preventing cyber attacks on equipped systems in advance and technologies which detect internally-occurring cyber attacks, determine the operational status of the systems, and continue operations



Classification	Description
Class 1 (Preventive measures)	Anti-malware software and firewalls, etc. are present as information security products to prevent cyber attacks in advance
Class 2 (Manually-implemented operational continuity measures)	Training of cyber countermeasure personnel to perform manually-implemented operational continuity measures after cyber attacks. Corresponds to technologies for constructing mobile cyber training environments
Class 3 (Automatically-implemented operational continuity measures)	Implement operational continuity measures to automatically respond via systems, etc. after cyber attacks. Corresponds to cyber-resilience technologies, etc.

Item	Important component technologies		Technology overview	Technological issues	Expected results
Class 1	Tamper-resistant technologies	<u>Hardware tamper-resistant technologies</u>	Technologies for preventing the leak or modification of internal information via hardware	Optimization of Ministry of Defense and SDF systems	In the event that some systems are captured, it will be difficult to perform reverse analysis of programs, etc. from the captured hardware
		<u>Software tamper-resistant technologies</u>	Technologies for preventing the leak or modification of internal information via software	Optimization of Ministry of Defense and SDF systems	
	<u>Vulnerability investigation technologies</u>		Technologies for investigating system vulnerabilities	Optimization of Ministry of Defense and SDF systems	Able to discover unknown system vulnerabilities Able to determine whether hardware is genuine Able to discover unauthorized program modifications
	<u>Supply chain integrity technologies</u>		Technologies for discovering unauthorized hardware modifications and unauthorized programs	Optimization of Ministry of Defense and SDF systems	
	<u>Anti-malware and firewall technologies, etc.</u>		Prevents the execution of unauthorized programs, unauthorized communications, etc.	Optimization of Ministry of Defense and SDF systems	Prevent cyber attacks against Ministry of Defense and SDF systems
	<u>Cyber attack countermeasure technologies for equipped systems</u>		Protects equipped systems from cyber attacks via connected external systems, etc.	Limits the impact on the performance of tactical control systems and provides protection	Prevent cyber attacks against tactical control systems

Red: technologies primarily established through cyber research performed by the Ministry of Defense
Blue: technologies established through non-cyber research performed by the Ministry of Defense (able to apply the results of other research and development)
Gray: technologies acquired through joint research with other institutions
Green: technologies awaiting progress in the civilian sector

Item	Important component technologies		Technology overview	Technological issues	Expected results
Class 2	Technologies for constructing mobile cyber training environments	<u>Technologies for reproducing and controlling cyber attacks</u>	Technologies which attack via autonomous, simulated malware based on the skill of the training participants	Reproduce and control autonomous cyber attacks without control communications from a central source	Enables training which simulates an actual environment for effective human resources development and practice of response procedures
		<u>Technologies for gathering cyber training control information</u>	Information gathering technologies which gather the cyber attack conditions, response conditions, and other information required for training control and reduce the communication timing and volume of information.	Technologies which reduce the communication required for information gathering and gather the information required for training control	
		<u>Cyber training environment recovery technologies</u>	Technologies which rapidly recover only those sections changed due to cyber attacks or countermeasures	Technologies which rapidly restore only those sections changed due to cyber attacks or countermeasures	
Class 3	Cyber-resilience technologies	<u>System and network infrastructure information management technologies</u>	Technologies which centrally manage the cyber attack conditions, system operation information, and the condition of various situations, etc.	Technologies which adapt to dynamic changes in system priority according to various situations. Technologies which are able to adapt even in situations where multiple sites and networks are damaged by cyber attacks and physical attacks, etc.	Detect early signs of cyber attacks through automated analysis of the accumulated logs • Early detection of attacks and damage • Prevent damage from spreading and automate countermeasures • Able to continue operations of important systems when damage occurs
		<u>System and network infrastructure control technologies</u>	Technologies which dynamically control the system and network infrastructure that make up the environment according to the cyber attack conditions, system operation information, and the condition of various situations, etc.	Technologies which adapt to dynamic changes in system priority according to various situations. Technologies which are able to adapt even in situations where multiple sites and networks are damaged by cyber attacks and physical attacks, etc.	
		<u>Technologies for control function survivability</u>	Technologies which maintain the control functions of system and network infrastructure when cyber attacks, etc. occur.	Technologies which are able to adapt even in situations where multiple sites and networks are damaged by cyber attacks and physical attacks, etc.	

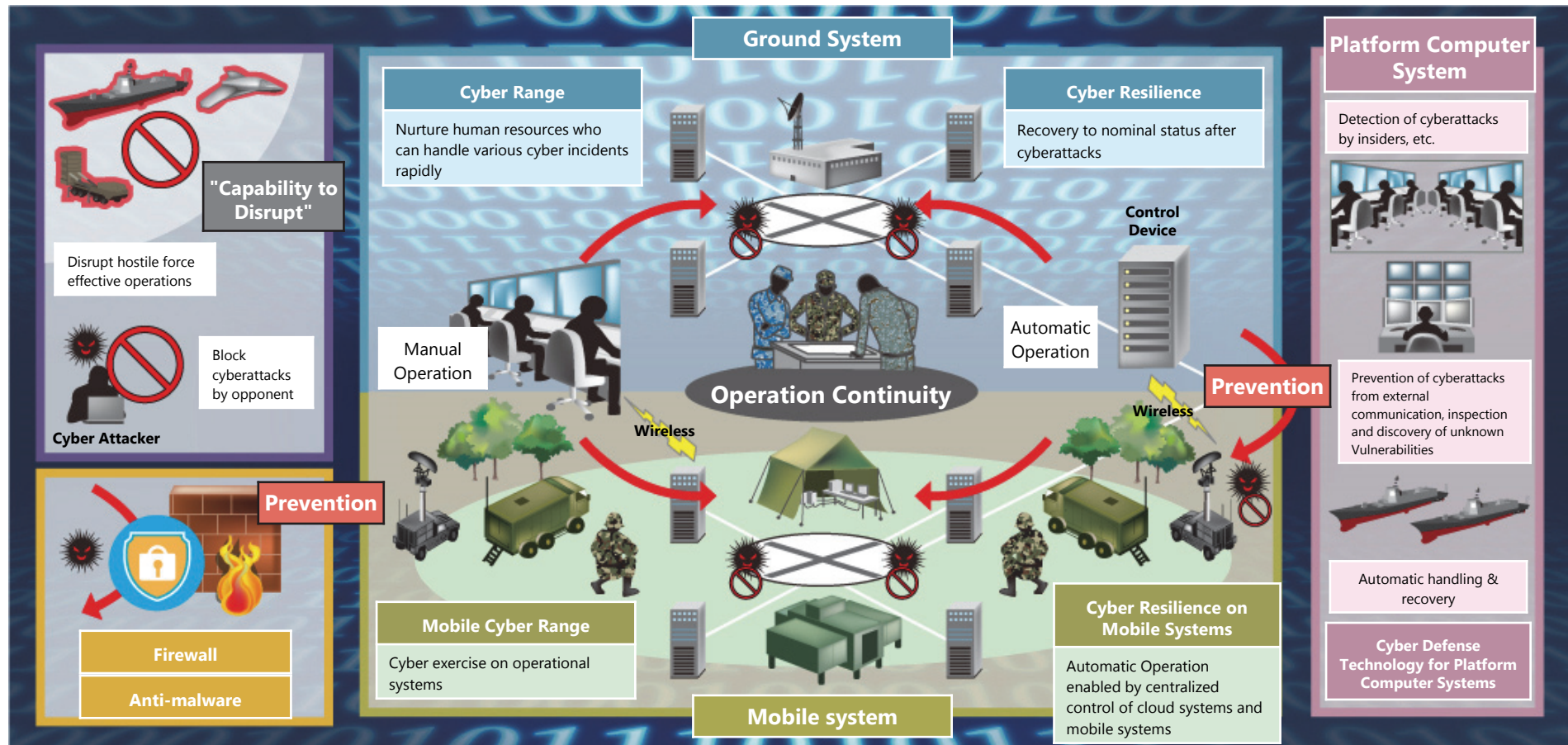
Red: technologies primarily established through cyber research performed by the Ministry of Defense
Blue: technologies established through non-cyber research performed by the Ministry of Defense (able to apply the results of other research and development)
Gray: technologies acquired through joint research with other institutions
Purple: technologies awaiting progress in the civilian sector

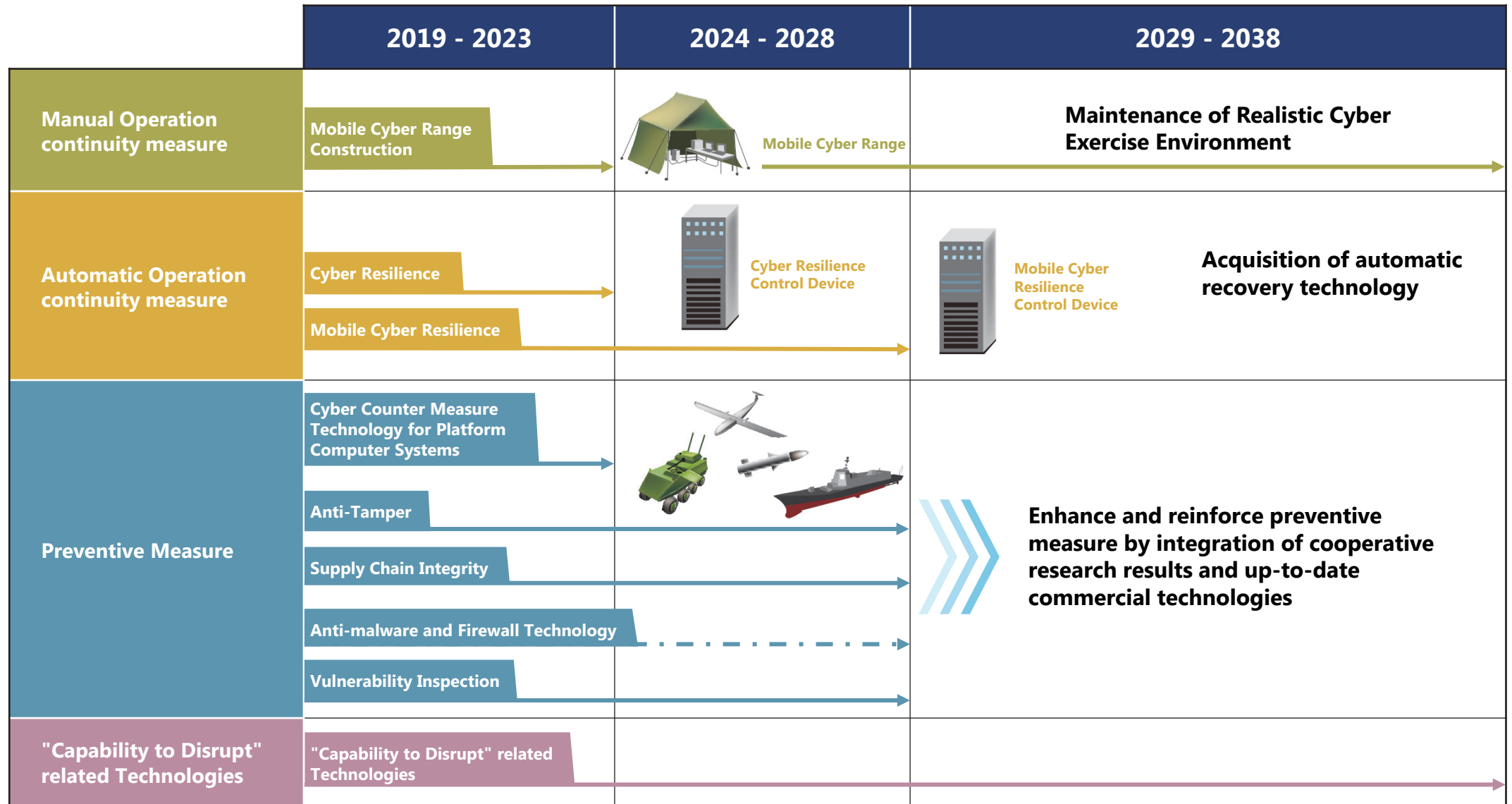
Item	Important component technologies		Technology overview	Technological issues	Expected results
Class 3	Mobile cyber-resilience technologies	<u>Mobile systems information management technologies</u>	Technologies which centrally manage cyber attacks, information, the operating status of important systems, communication path information, etc. on restricted networks	Technologies which adapt to dynamic changes in system priority according to various situations Technologies which are able to adapt even in situations where multiple sites and networks are damaged by cyber attacks and physical attacks, etc.	Detect early signs of cyber attacks through automated analysis of the accumulated logs • Early detection of attacks and damage • Prevent damage from spreading and automate countermeasures • Able to continue operations of important systems when damage occurs
		<u>Mobile systems infrastructure control technologies</u>	Technologies which centrally control the system and network infrastructure which make up the mobile system environment to prevent cyber attacks from spreading and to continue the operation of important systems on restricted networks	Technologies which adapt to dynamic changes in system priority according to various situations Technologies which are able to adapt even in situations where multiple sites and networks are damaged by cyber attacks and physical attacks, etc.	
		<u>Mobile systems Technologies for control function survivability</u>	Technologies which maintain the infrastructure control functions of the system and network infrastructure which make up the mobile system environment on restricted networks when cyber attacks occur	Technologies which are able to adapt even in situations where multiple sites and networks are damaged by cyber attacks and physical attacks, etc.	
	<u>Cyber-resilience technologies for equipped systems</u>		Technologies which detect cyber attacks which occurred within tactical control systems and continue the operation of system functions based on the system operating status and available resource status, etc.	Technologies which limit the impact on the performance of the equipped systems and enable continued operation	



Red: technologies primarily established through cyber research performed by the Ministry of Defense
Blue: technologies established through non-cyber research performed by the Ministry of Defense (able to apply the results of other research and development)
Gray: technologies acquired through joint research with other institutions
Purple: technologies awaiting progress in the civilian sector

In order to implement cyber defenses, carry out preventive measures along with responding through both human and automated responses to support operational continuity measures when cyber attacks occur to improve the system survivability.

- Utilize anti-malware, firewall, anti-tampering, and other civilian technologies to the maximum extent as preventive measures. Also acquire disruptive capabilities to interfere with the opponent's smooth execution of military functions and inhibit cyber attacks in an emergency.
- Construct environments which improve the capabilities of cyber defense personnel through technologies for constructing cyber training environments as part of manually-implemented operational continuity measures.
- Respond automatically through cyber-resilience technologies in a manner which conforms to SDF operations after communication networks and systems operated by the Ministry of Defense and SDF are hit by cyber attacks as part of automatically-implemented operational continuity measures.





 Primarily acquire through research and development
 Acquire through incorporation of new civilian technologies

Note 1 Sufficiently examine the operational, technology, and cost aspects of establishing a specific research and development project.

Note 2 This slide illustrates future equipment which could conceivably be realized and does not indicate a development schedule.

Note 3 The endpoints of the arrows are only tentative. In light of the rapid research and development approach, we will strive for early technology acquisition.

Primary methods of advancing research and development and their outcomes

- The stable use of cyberspace has become essential to both the Ministry of Defense and the SDF, and **preventive measures must be balanced with operational continuity measures** to prevent long-term shutdowns based on the system characteristics.
- Regarding the technologies which are shared with the civilian sector within the preventive measures, acquire the necessary technologies through the proactive utilization of advanced civilian technologies. At the same time, cyber attack countermeasure technologies for equipped systems, vulnerability investigation technologies and technologies which contribute to disruptive capabilities, operational continuity measures, and other preventive measures which are difficult to procure from the market will be **strategically acquired through technology research and development, because the Ministry of Defense and the SDF have specific requirements.**
- Artificial intelligence, quantum computers, sensing, communication, and other quantum technologies which are potentially game-changing technologies in the future are becoming borderless and dual-use. Because the speed of progress in the civilian sector is unusually fast, we will strive for continuous technology improvement and apply the latest technologies according to the progress of domestic and overseas technologies.

Closely observe trends in foreign and domestic rules

- No clear rules pertaining to the application of international law to cyber attack cases exist. The definition of cyberspace also differs by country. **Various discussions** about the relationship between cyber attacks and the right of self-defense **have taken place in international forums.**
- Currently, we are at the stage where various international discussions are being held to determine whether or not cyber attacks alone constitute an "armed attack." So far as the government is concerned, going forward it will have to proceed with an examination of what types of cyber attacks can be assessed on their own as an "armed attack" based on the situation surrounding cyber attacks and international discussions.
- In clarifying the policies and the legal perception of cyber attacks as an organization, **trends in foreign and domestic rules must continue to be closely observed.**
- Advance research and development based on these trends.

Balancing preventive measures and operational continuity measures

- The latest private sector technologies must be efficiently incorporated within the preventive measures
 - The capabilities of cyber countermeasure personnel must be improved within the manually-implemented operational continuity measures
 - Operational continuity must be rapidly secured and the damage caused by cyber attacks must be prevented from spreading within the automatically-implemented operational continuity measures
- Balance preventive measures and operational continuity measures to **improve system survivability**



Reference

Previous Initiatives and Foreign and Domestic Trends in Cyberspace

Class 1 (Preventive measures)

- Research on encryption module mounting technologies and anti-tamper encryption technologies has been conducted since FY 2007.

Class 2 (Manually-implemented operational continuity measures)

- Conducted research into technologies for constructing cyber training environments from FY 2013 to FY 2017. Technology was created which allows effective cyber defense trainings to be carried out according to the level of personnel skill in an environment which simulates Ministry of Defense and SDF systems, and the results were applied to the development of a real-world cyber training implementation system at the general staff headquarters.
- Since FY 2018, MOD has been researching situation assignment and monitoring in narrow band line environments and technologies for constructing cyber training environments in mobile systems composed of non-consumer GOTS (Government Off The Shelf) products.



Research prototypes of technologies for constructing cyber trainings

Class 3 (Automatically-implemented operational continuity measures)

- Conducted research into experimental equipment for handling network cyber attacks from FY 2014 to FY 2016. Methods for securing important communication paths and preventing the spread of damage were researched to enable the stable and effective use of Ministry of Defense and SDF networks when cyber attacks occur so that they may carry out their mission.
- Since FY 2017, MOD has been researching cyber-resilience technologies in the event that system and network infrastructure is damaged to maximize the utilization of the remaining infrastructure and continue the operation of important systems during that time

- ✓ Research results have been achieved for some Class 1 component technologies.
- ✓ Research results have been achieved in the area of Class 2 technologies for constructing training environments in fixed systems. Mobile systems are currently being researched.
- ✓ Research results have been achieved for Class 3 cyber-resilience technologies in fixed systems.

Class 1 (Preventive measures)

- In addition to web single sign-on and other conventional forms of access control, more advanced approaches such as integrated authentication management, integrated access control, administration, auditing report functions, and high-reliability configurations are appearing in Japan.
- OS products with discretionary access control functions and firewall products are being released by private companies and gaining popularity.
- Private security vendors within Japan are minimizing the damage of cyber attacks and also playing a role where possible in helping to identify attackers.

Class 2 (Manually-implemented operational continuity measures)

- The United States has been advancing the NCR (National Cyber Range) to test cyber warfare strategies since 2009, and the Department of Defense can now implement full-scale cyber warfare tests and exercises having completed the testing period.
- In 2016, ENISA (European Network and Information Security Agency) launched Cyber Europe 2016 to conduct European cyber exercises.
- According to reports from the Russian state-run news agency, the Russian military appears to be considering the establishment of a cyber warfare unit.

Class 3 (Automatically-implemented operational continuity measures)

- According to the "Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Roadmap," the US military has been expanding previous optimizations since 2010 and is advancing a large-scale system consolidation based on cloud technologies in accordance with the "Department of Defense Chief Information Officer, Cloud Computing Strategy" and other initiatives.

- ✓ Private companies and security vendors both in Japan and overseas possess Class 1 products and technologies.
- ✓ Various countries are engaged in constructing Class 2 cyber training environments and creating organizations.
- ✓ While it is believed that various countries are engaged in researching Class 3 technologies, the details are unknown with some exceptions.