Overview of the “Cybersecurity Strategy”

○ Based on the “**National Security Strategy**” and initiatives such as the **Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts**, this strategy presents the objectives and policies necessary to promote coordinated efforts to respond to threats in cyberspace from a medium- to long-term perspective and **with the next five years in mind**.

Fundamental Concept

○ Cyberspace serves as a foundation supporting the sustainable development of the economy and society, as well as liberalism, democracy, and cultural advancement.
○ The international order based on universal values such as the rule of law and respect for fundamental human rights is facing a serious crisis, and cyber threats are heightening concerns over people’s daily lives, economic activities, and ultimately, national security.

By continuing to uphold the “five principles”* as its basic principles, the government will take a more proactive role and strengthen its measures to respond to the increasingly challenging situation in cyberspace, thereby clarifying its commitment to the realization of a “free, fair and secure cyberspace.”

*The five principles guiding the formulation and implementation of measures are: “Assurance of the free flow of information,” “The rule of law,” “Openness,” “Autonomy” and “Collaboration among multi-stakeholders.”

Situational awareness

- Increasingly challenging situation in cyberspace and growing state-sponsored cyber threats
- Advancement in digitalization across society and the escalation of cyber threats
- Emerging technological innovations, such as AI and quantum technology, and their impact on cybersecurity

Direction of measures

1. Defense and Deterrence Against Intensifying Cyber Threats

- To address the increasingly severe security environment in cyberspace, the government will combine a range of measures including active cyber defense, with existing measures such as incident responses, within a framework of public–private collaboration and international cooperation, thereby imposing costs on adversaries and strengthening defense and deterrence against intensified cyber threats.
- The government will proactively share information with the private sector

Defense and deterrence with the government playing pivotal roles

Formation of a public–private collaboration ecosystem

Promotion and strengthening of international cooperation

2. Enhancement of Cybersecurity and Resilience Across Society by Broad Participation

- Clarify and implement measures required of various stakeholders, along with approaches to ensure their effectiveness (government agencies and related organizations taking the lead as role models.)
- Promote digitalization and cybersecurity in parallel

Strengthening measures for government agencies and related entities

Strengthening measures for critical infrastructure operators and local governments

Ensuring resilience across the entire supply chain (SMEs and vendors, etc.)

Promoting cybersecurity improvement by full participation

Ensuring safety and security through countermeasures against cybercrime

3. Formation of an Ecosystem for Human Resources and Technologies Supporting Japan’s Cyber Response Capabilities

- Securing and developing cybersecurity talent through collaboration among industry, academia, and government
- Creating new technologies and services centered on domestically developed innovations

Efficient and effective development and retention of cyber workforce

Formation of an ecosystem for emerging technologies and services

Response and initiatives for advanced technologies such as AI and quantum technology

**Based on public–private and international collaboration, the government will take the pivotal role in cybersecurity measures, promoting Japan’s cybersecurity efforts through a whole-of-nation approach that earns the understanding and cooperation of citizens and stakeholders.
Through these efforts, Japan aims to become a nation with world-class resilience, capable of responding seamlessly and continuously to the increasingly severe conditions in cyberspace.**