Reality of China's information warfare and cognitive warfare against Japan

M.S. Aoki Masao
Senior Research fellow of SSRI, Japan

Abstruct

The information space has long since been structured by Internet technology and spread not only to companies and research institutions, but also to government agencies and the public at large.

It can be said that information operations by other countries have been supported by information transmission technologies such as typography, telegraph, telephone, radio, and television broadcasting since before the age of the Internet, as well as the development of technologies that spread national sovereignty to other countries since the Age of Exploration, but especially in the age of the Internet, such activities are interactive and information transmission volume, It is no exaggeration to say that in the age of the Internet, the propagation and influence of threats have accelerated as a result of the interactive nature, volume of information transmission, and speed of information transfer.

On the other hand, in the case of information operations from countries that use languages other than one's own, there is first of all a language barrier, and such a language barrier has been an effective part of the defense wall even in the age of the Internet, but recent technologies such as generative AI and deep fakes as expressive power are easily overcoming even that barrier, and the growing threat of other countries' information activities supported by such cyberspace technologies is remarkable.

In the midst of all this, not only state-sponsored cyber espionage such as technology theft and policy theft, but also psychological operations in the cognitive domain to influence public opinion and intervention in elections, the basis of democracy, have been reported in the world.

In order to grasp the reality of China's information and cognitive warfare, it is not difficult to imagine that organizing and analyzing events across multiple domains in Japan and analyzing the threat picture together with Taiwan, which shares a common threat, will lead to security in multiple domains such as cyber space, physical space, and cognitive domain space in both countries, and ultimately contribute to the security of not only Asian countries but the world.

In understanding threats, especially in the cyber domain, by other countries, it is important to collaborate in Track 1.5, especially from the perspective of national cybersecurity, with an awareness of the following events close to the government.

1. technology theft cyber espionage
2. policy theft cyber espionage
3. public safety activities in the cyber domain in the territory of other countries
4. activities in the cognitive domain involving other countries
5. cybercrimes considered as state-ignored cybercrimes