NPI 中曽根平和研究所

July 16, 2024

China's Information Warfare
China's Cyberattacks, Information and Cognitive Warfare in Cyberspace, and the Use of Generative AI Technology
Research Project for Risk in the Information Sphere
Implementation Report

On July 16, 2024, the Research Project for Risk in the Information Sphere at Nakasone Peace Institute held a discussion based on reports by Research Project Chairperson Mr. Osawa Jun, Senior Research Fellow at NPI, and Dr. Tsuchiya Takahiro, Associate Professor at Kyoto University of Advanced Science. The summary is as follows.

Osawa presented a report, entitled "Information Warfare by China." First, as an aspect of hybrid warfare, he outlined the current situation in Japan, where the authorities responsible for information/cognitive warfare and cyber warfare are separate, and attacks from China and Russia are conducted through a combination of both methods of warfare. In addition, he pointed out that it is necessary to look not only at information warfare but also at cyber warfare, and that the importance of cyber situation awareness (CSA) is increasing in light of the recent cyberattacks.

Next, he gave an overview of the battle in the cognitive domain waged by China. Since the emergence of the concept of "control of the brain," Chinese Communist Party (CCP)-related actors, for example, have been using bot accounts on X (formerly Twitter) disguised as U.S. citizens to spread disinformation about domestic issues, including U.S. political and social problems, in an effort to destabilize the United States. However, it is only in the past two to three years that Western countries have begun to counter this situation, and it can be said that their response has been slow. The United States Department of State report on information warfare by China, entitled "How the People's Republic of China Seeks to Reshape the Global Information Environment," released in September 2023, presents analysis that China is attempting to exert control over the narratives in the global information space and that its information manipulation spans the use of propaganda, disinformation, censorship, and so on. In addition, during the war in Ukraine, China has been engaged in activities to amplify Russia's disinformation in the information sphere. The Publicity Department of the Central

Committee of the Chinese Communist Party (CCPPD) and the United Front Work Department (UFWD) are named as the main actors in this kind of information manipulation. In particular, the CCPPD contributes to the spread of disinformation seen in peacetime in other countries, including Japan, and it is suspected that the controversy over the 2023 discharge of treated water at Fukushima was provoked due to a campaign by the CCPPD.

He also explained that the campaign was developed not simply through disinformation dissemination but disinformation was combined with cyberattacks in the campaign. In the Russian-style complex information warfare (cyberattacks and disinformation dissemination), in addition to disinformation dissemination using Russian trolls, cyberattack methods such as distributed denial-of-service (DDoS) attacks and hacking leaks are also used. An example citing a specific use of complex information warfare by China was an increase in DDoS attacks and message tampering by hacking that occurred in conjunction with the visit of the Speaker of the U.S. House of Representatives Nancy Pelosi to Taiwan in 2022. Furthermore, during the Taiwan presidential election, disinformation that included narratives attempting to discredit allies and fracture alliance relations was disseminated. Messages asserted, for example, that U.S. forces would not come to Taiwan's defense and that the U.S. had asked Taiwan to develop biological warfare agents. This kind of disinformation has been confirmed not only in Taiwan but also in South Korea and Japan. For example, a news aggregator operated by a Chinese company in South Korea published an article containing disinformation about COVID-19, to the effect that Washington uses its allies as a testing ground. An investigation by the University of Toronto in Canada pointed out that similar news aggregators are operated in Japan as well. In order to address such information warfare, it is important to analyze the social media sphere with an awareness of cyberattacker's narratives, pay attention to the current topics that are the source of narratives, and observe the tools and routes of dissemination carefully.

The report also pointed out the use of artificial intelligence (AI) for influence operations. According to a Microsoft Corporation report released in April 2024, China's cyberattackers use AI-generated and AI-enhanced content for influence operations. These influence operations amplify AI-generated content (video, audio, memes, etc.) in the U.S., Japan, South Korea, and Taiwan to propagate China's strategic narratives. Specifically, a CCP-affiliated actor known as Storm 1376 deployed AI-based influence operations targeting Taiwan's presidential and legislative elections around winter 2023. This operation can be said to be the first time a state actor has used AI content to influence an election outside its own state.

Next, Dr. Tsuchiya presented a report entitled “China’s Cyberattacks, Information and Cognitive Warfare in Cyberspace, and the Use of Generative AI Technology.” At the beginning of the presentation, he described the current situation of frequent cyberattacks. He noted that as cyberattacks involving state actors have become more apparent, with almost all companies being the target of cyberattacks, attack methods have become more sophisticated, and that security falls behind due to the dominance of cyberattackers.

First, regarding the organizations in China’s cyberattacks and information and cognitive warfare, the Ministry of State Security of China and the People’s Liberation Army’s (PLA) cyberspace unit, PLA Unit 61486, are considered to be the main actors for cyberattacks. For information and cognitive warfare, the Ministry of Public Security, the Ministry of State Security, and the PLA’s Information Support Force are considered to be the key actors. However, due to the organizational restructuring of the PLA’s Strategic Support Force, there are many aspects that are currently unclear. Examples in which these organizations are believed to have been involved include intervention in the Taiwan presidential election, use of cyberspace in conjunction with the One Belt, One Road initiative, and propaganda activities in cyberspace. Such operations have been used to strongly shape China’s narratives.

Information and cognitive warfare using generative AI technologies has also been identified. For example, around the time of the military exercises conducted by China after Speaker Pelosi’s visit to Taiwan in 2022, new methods began to be used, utilizing new technologies such as deepfake and other generative AI, as well as various channels of new online community platforms. Deepfake videos have been observed to have spread not only within China but also to the West. However, due to the current level of accuracy, it is possible to distinguish real from fake videos. In fact, in the case identified during the Taiwan presidential election, debunking was quickly accomplished. However, it was pointed out that, without the use of AI or similar tools, technological advances may make it impossible to distinguish between real and fake content in the near future.

AI-based avatars are also being put to practical use. AI reporters have already appeared on 20 to 30 platforms in China, and a 2023 report by the Australian Strategic Policy Institute confirms attempts to spread disinformation more widely by using foreign avatars. Propaganda and disinformation dissemination using these AI-generated figures is not limited to Japan, the U.S., and Taiwan, but also extends to Europe via YouTube accounts and other means. In addition, videos with deepfakes of avatars imitating Russian military personnel were spread on TikTok to influence public opinion in

China.

Another example is “Spamouflage,” which is deployed across platforms using a variety of accounts. This activity has been confirmed to continue even after the 2019 pro-democracy movement in Hong Kong. In addition, according to a CNN report, a deepfake video using a Ukrainian woman’s face was used to influence public opinion in China. In response to this report, a case was introduced in which the Chinese side sent out a rebuttal video claiming that the alleged AI-generated Chinese avatar represented a real person.

In the Q&A session following the above reports, the panelists and participants exchanged comments on such issues as common elements of strategic communication and cybersecurity, China-Russia coordination and mutual learning situation, possible narratives created by China against Japan in the future, roles and mechanisms of information operations in China and who controls them, the relationship between online space and local narratives and local-level events, and the role of mass media and how information is reported, given the fact that information on social media is further spread by mass media coverage.