February 16, 2024

“Information Warfare” by Russia: Focus on its Strategies, Objectives, and Case Studies

Research Project for the Risks in Information Sphere Implementation Report

On February 16, 2024, the Research Project for the Risks in Information Sphere at Nakasone Peace Institute held a discussion based on a report by Mr. Sasaki Takahiro, former Defense Attaché at the Embassy of Japan in Russia (retired rear admiral, Maritime Self-Defense Force). The summary is as follows.

The word “safe” in the strict sense of the word does not exist in the Russian language, and the closest equivalent is said to be a word implying “a state of being free from danger.” The Russian nation is very sensitive to the state of “no danger” in its relations with other countries. This sensitivity has led to an excessive sense of defensiveness toward other countries, an expansion of buffer zones, and expansionism. The current war against Ukraine is “all-domain warfare (hybrid warfare),” which includes information warfare and cyber warfare.

Besides Russia, there are various “information spheres” in other countries around the world that disseminate propaganda that favors their own nation or agenda to their citizens and the world. Therefore, it is important to compare conflicting “information spheres” to discern the truth.

Taking the Russia-Ukraine war as an example, information and news reports originating from Ukraine are visible primarily in Western countries. In these reports, Russia is shown as the evil aggressor, while the West supports an invaded Ukraine and protects democracy from authoritarianism. On the other hand, information and news reports originating from Russia cannot be viewed in Western countries. These reports portray Ukraine as well as the U.S. and NATO, which support Ukraine, as evil, while Russia is shown as having legitimacy. These reports label the actions of the West as a double standard. Because most Russian citizens belong to the “Russian information sphere” the problem is that most Russian citizens believe such information disseminated by the Kremlin without questioning.

Information warfare can be broadly divided into two categories: “strategic information warfare,” which is conducted to influence national policies, decision-making of state and military leaders, and to manipulate public opinion on the one hand; and “operational and tactical information warfare,” which is conducted to understand the enemy’s situation from an operational and tactical standpoint and to obscure its own actions during a contingency, on the other.

In Russia, President Vladimir Putin said in February 2012 that he recognized the effectiveness of information warfare as comparable to nuclear weapons, and Chief of the General Staff General Valery Vasilyevich Gerasimov, in his February 2013 speech entitled “The Value of Science Is in the Foresight,” recognized that information warfare as the mainstream of modern warfare. Former Chief of the General Staff Yury Baluevsky also stated in February 2017 that information warfare can paralyze all the enemy state’s power

structures.

Russia's emphasis on information warfare in terms of security is evident in a number of strategic documents, such as the " Information Security Doctrine of the Russian Federation" and the "Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space." Russia views information warfare not only as a battle for information security but also as a battle targeting political, economic, and social systems by broadly using the information spheres, and thereby as a "battle in the cognitive domain" involving the psychological manipulation of state decision makers.

In the war against Ukraine, Russia conducted influence operations within Russia, in Ukraine, the West, and the international community in a battle in the cognitive domain. However, compared to the annexation of Crimea in 2014, influence operations in 2022 can be said to have largely failed, except for those conducted within Russia.

By spreading a large amount of disinformation prior to the outbreak of the war, Russia sought to emphasize the legitimacy of its military action against Ukraine and to create public opinion favorable to Russia. After the war began, a large amount of disinformation intended to demoralize the Ukrainian people and incite anxiety was confirmed. In addition, influence operations aimed at dividing Ukraine from its allies were conducted in order to hasten the end of the war.

What is distinctive compared to 2014 is that in 2022 Russia focused on domestic propaganda to consolidate domestic public opinion in favor of the regime. This is, so to speak, an information warfare campaign with the goal of impressing upon the Russian public that information other than that issued by the Russian authorities cannot be trusted. However, as was seen in the broadcast of a female staff member of the state-run TV Channel One holding up a placard calling for opposition to the war shortly after its outbreak, there are signs of a breakdown in the control of information in Russia, and this could become a future risk factor for the Putin regime.

Currently, Russia is not only fighting an information war by spreading disinformation but is also conducting a battle of narrative proliferation.

Information warfare using disinformation spreads and utilizes "false information" that is convenient to the state. Therefore, it is possible to respond to this by fact-checking. On the other hand, narrative-based information warfare combines "facts" that are convenient for the state to shape and then utilizes a narrative of "national ideals" as an interpretation of the facts. The result of this process cannot be addressed by fact-checking. Therefore, an approach that is distinct from the response to disinformation and that has a different dimension from just fact-checking will be required in the future.

In response to this information warfare by Russia, Ukraine has been able to gain support not only from the Ukrainian people but also from the Western countries supporting Ukraine and the international community through strategic dissemination of information using factual information. In addition to identifying Russian forces through its own intelligence in the current war, the Ukrainian military has also been able to locate Russian forces by fusing information collected from civilians to utilize this information in its attacks. Meanwhile, like Russia, Ukraine is conducting media control not only toward its own citizens but also toward foreign countries. In fact, there are facilities called "media centers" in Lviv and Kyiv cities, where military-

related interviews are allegedly possible for those with government-issued press cards. However, there are opinions voiced that "Conversely, this means that Ukraine can show what it wants to show and not show what it does not want to show." It is also true that some have said that they felt they are being taken advantage of. Further, it can be said that Russia and Ukraine are the same in that they both conduct domestic surveillance for the purpose of maintaining national security and public order.

Regarding Russian information warfare against Japan, it is possible that Russia will further engage in influence operations to divide Japan and the U.S. by shaping public opinion in Russia's favor, such as by creating negative public opinion about U.S. forces in Japan and suggesting that a peace treaty can never be concluded with Japan if it continues its support for Ukraine. In fact, there are already cases in which Russian government-affiliated media outlets have been conducting information operations aiming to solidify public opinion against Japan in Russia, such as adding to and altering the comments section of Yahoo Japan's "Yahoo News" when translating it into Russian. In addition, there have been several confirmed cases of Japanese nationals leaking classified information to officials of the Main Intelligence Directorate of the General Staff and the Foreign Intelligence Service of Russia.

Countermeasures to respond to Russian information warfare include (1) halting dissemination of information from state-sponsored sources, (2) responsible response from platforms, (3) promoting fact-checking and fostering information literacy, (4) strategic dissemination of information, and (5) Hunt Forward Operations (HFO) by the United States to neutralize Russia's influence operations (since 2018, the U.S. has been sending cyber operations experts to allied countries to probe adversaries' intelligence and strategically expose malicious behavior), all of which face a variety of challenges that must be overcome.