Democratic Elections Under Challenge in Digital Age —How to Confront Social Divisions and Disinformation—

Osawa Jun
Senior Research Fellow
Nakasone Peace Institute

Elections and information warfare: From analog to digital

I have a white ballpoint pen in my hand. It was given to me by a local non-profit organization staff when I went to Belgrade, the capital of Serbia, to conduct research in December 2000, almost a quarter of a century ago, when I was still a young, fledgling researcher. On the pen, there is a message in Serbian, calling for participation in an election rally of the then opposition coalition Democratic Opposition of Serbia (DOS), ahead of the December 23, 2000 Serbian parliamentary elections. In that year, Serbia experienced massive demonstrations over the September presidential election against the pro-Russian Slobodan Milošević government, which did not recognize the election results, and President Milošević was forced to step down. In the December parliamentary election, the DOS won 64% of the overall vote, controlling 70% of the seats, bringing about a peaceful change to a government that took a cooperative line with the West.

After 2000, in Eastern Europe and the Commonwealth of Independent States (CIS) region, authoritarian pro-Russian regimes were successively overthrown during elections in Georgia in 2003, in Ukraine in 2004, and in Kyrgyzstan in 2005 to create pro-European democratic governments, and, in addition to these regime changes, anti-government movements were active in Moldova and Belarus. This series of democratic movements is called “color revolutions” because the anti-government movements in each country used distinctive “colors” as symbols of resistance. Some claim that behind these color revolutions was the influence of US foreign policy of assisting democratization around the world. It was said in Belgrade that the ballpoint pen introduced at the beginning of this article was also made with the support of the United States.

Some readers may wonder what this quarter-century-old ballpoint pen has to do with the “Democratic Elections Under Challenge in Digital Age,” but the realization of regime change through non-military means of US support for democratization has shaken Russia and triggered a major shift in the Russian military’s concept of modern warfare, leading to the information warfare currently taking place in the digital space. A quarter of a century ago, there were no smartphones and the means of message transmission was analog, but today, with the development of the Internet and smartphones, information is transmitted in seconds in the social networking service (SNS) social media space. Not only in elections, but also in the digital space, the progression of events is becoming ever faster in cycle, and the situation can change drastically in just a few hours.

Battle in the cognitive domain waged in peacetime by Russia and China

Nakasone Peace Institute
The views expressed in this work are solely those of the author and do not necessarily reflect the views of Nakasone Peace Institute.

The Russia-Ukraine War drew attention to the term "hybrid warfare." Hybrid warfare, which is said to be a characteristic of modern warfare, is characterized by the parallel use of non-military and military means, the blurring of the boundary between peacetime and wartime, the beginning of information warfare and cyber warfare in the peacetime phase, and the increasing intensity of the methods used as the crisis progresses.

To begin with, Russia does not distinguish between peacetime and contingency, and peacetime and the gray zone itself is considered to be a sphere of contemporary interstate conflicts. Russia has developed a unified operation with continuity between military and non-military means to achieve its strategic objectives. The modern warfare concept presented by General Valery Vasilyevich Gerasimov, Chief of the General Staff of the Armed Forces of the Russian Federation, is characterized, among other things, by attacks on the cognitive domain of the enemy country's civilian population, known as information warfare (IW), and on the enemy's information space, known as cyber warfare.

What comes to mind when we think of information warfare operations is the use of disinformation to disrupt an opponent, but Russian information warfare is different from what we generally assume. Russian information warfare focuses on the historical fissures that exist in the society of the target country, and, based on the uniquely Russian concept of "reflexive control," it seeks to elicit a cognitive response from the people of the target country in order to widen these fissures and undermine the stability of the society. This reflexive control is an attempt to evoke memories of the past that are deeply rooted in the society of the target country, influence the people's interpretation of reality, and bring about the result of social division by embedding disinformation in narratives, rather than inputting disinformation only into the direct senses such as sight and hearing. This is an attempt to draw out the divisive results of the target country's society. Thus, Russian information warfare targeting elections does not directly disseminate disinformation about the elections themselves. Rather, it is fought in the cognitive domain to undermine the target country's society over the years by cultivating distrust and suspicion toward the electoral system and democracy in the target country's society.

Like Russia, China makes no distinction between peacetime and wartime, and it is safe to assume that it has been waging information warfare against its neighbors even during peacetime. Based on the Thirty-Six Stratagems to "stir up the water to catch a fish," or confusing the opponent to achieve one's goal, the People's Liberation Army's political maneuvering regulations include what are called "three types of warfare: psychological warfare, public opinion warfare, and legal warfare." In the digital age, this concept is changing into a form of securing "cognitive dominance." In other words, the concept involves undermining and causing the opponent to lose situational awareness, disseminating disinformation to frustrate their will, and tampering with the target's decision-making mechanisms.

Before elections in the Indo-Pacific region, information warfare has been conducted in favor of China. Even in the last decade, there have already been reports of Chinese information warfare observed during elections in Taiwan, Cambodia, Australia, and the United States. In 2023, in the US, disinformation was spread on SNS social media that a large fire in Hawaii was caused by a US military weapon, clearly indicating China's attempt to spread disinformation to destabilize US society even during peacetime and not just during elections. In August 2023, the US social media company Meta Platforms Inc. deleted 7,700 SNS social media accounts believed to be of Chinese origin, claiming that accounts impersonating US citizens were manipulating information and further closed over

Nakasone Peace Institute
The views expressed in this work are solely those of the author and do not necessarily reflect the views of Nakasone Peace Institute.

4,800 accounts in November 2023. There is a growing sense of alarm in the US government that China is learning from Russian information warfare and is building a foundation, including bot account networks on SNS social media, to influence the politics of the US and other countries.

A wide variety of information warfare methods

When we hear the words "information warfare" and "cognitive warfare," we tend to think of the dissemination of disinformation on SNS social media. However, information warfare methods are not limited to the dissemination of disinformation but also involve a combination of cyberattacks and other methods. For that reason, the author chooses to refer to it as "information manipulation type of cyberattack."

Russian information warfare methods aimed at democratic elections such as the 2016 US presidential election and the Brexit referendum in the UK included (1) spreading fake news on SNS social media using troll forces, (2) spreading fake news disguised as neutral media such as Russia Today (RT) and Sputnik Media sites, and (3) cyberattack intrusion into the election system (with the goal of discrediting the election rather than interfering with it), which seems to be done mainly through disinformation in the SNS social media space. However, according to "International Security and Estonia 2021," an annual report by the Estonian Foreign Intelligence Service that analyzes Russian information warfare, Russian information warfare methods are diverse, including (4) hijacking media sites and spreading fake news through cyberattacks, (5) hacking and leaking of confidential information through cyberattacks, (6) disruption of information dissemination through distributed denial of service (DDoS) attacks on media and government websites, and (7) disruption of accurate information dissemination and loss of credibility of public institutions by defacing government and other public websites, and these methods are used in a combined manner.

In fact, the method described in (5) above was used in the 2016 US presidential election, when two cyberattack groups, APT28, which was associated with the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (commonly known by the previous abbreviation GRU), and APT29, which was associated with the Foreign Intelligence Service of the Russian Federation (FSB) or Foreign Intelligence Service (SVR), separately penetrated the US Democratic National Committee (DNC) network via cyberattack and stole DNC executives' emails, confidential records, and donor lists. The cyberattack groups disclosed the vast amount of information they stole through WikiLeaks, including Democratic Party officials' emails suggesting obstruction of Hillary Clinton's opponent, Bernie Sanders, which had a major impact on the Democratic Party's election campaign, including the resignation of DNC Chairman Debbie Wasserman Schultz.

Although it was not an attack directly targeting the election, an information manipulation type cyberattack using the method described in (6) above was conducted in Japan on September 6, 2022, in parallel with the large scale Russian military exercises in the Far East, Vostok. A cyberattack, which was considered to be a DDoS attack, occurred against the Japanese government portal site, e-Gov Japan, managed by the Digital Agency, and caused access failures. Other access disruptions also occurred on websites of government entities such as the Ministry of Internal Affairs and Communications (local tax portal), the Ministry of Education, Culture, Sports, Science and Technology, the Imperial Household Agency, and others. Further, access problems that appear to be caused by DDoS attacks were observed on the websites of regional banks, credit card companies, transportation systems such as

Nakasone Peace Institute
The views expressed in this work are solely those of the author and do not necessarily reflect the views of Nakasone Peace Institute.

subways, and some SNS social media sites.

Not only Russia, but also China, which recognizes the cognitive domain as a battlefield, has been waging information/cognitive warfare during peacetime for the purpose of forming a situation favorable to China. The 2021 National Defense Report of the Republic of China (ROC, Taiwan) Ministry of National Defense assesses the information warfare methods used by China as (1) external propaganda using official media under control by investment, (2) public opinion control through mass postings by collaborators with nationalist tendencies, (3) influence operations using content farms, and (4) information dissemination by local collaborators targeting specific objectives. Analysis shows that a complex mix of methods are used.

Some of these methods were used in Taiwan's past elections. In the 2016 presidential election, cyberattacks through hacking and leaks were observed, in the 2018 local elections, there was mass dissemination of positive opinions about pro-China candidates through method (2) above, and in the 2020 presidential election, there were combined influence operations using (1), (2), and (3). Additionally, in parallel with military exercises conducted during U.S. Speaker of the House Nancy Pelosi's visit to Taiwan in 2022, information manipulation type cyberattacks were also conducted, including DDoS attacks against public institution websites to obstruct information transmission, hacking to alter messages on digital signage (billboards), and hijacking of commercial broadcasters to broadcast fake video images.

Therefore, the methods of information warfare are not only the dissemination of disinformation but are also combined with cyberattacks and other methods. It is necessary to be careful not to look merely at disinformation, as this may lead to a misperception of the overall picture of information warfare operations.

Information manipulation type cyberattacks and measures to be wary of in 2024, the global election year

The year 2024 will be a global election year. National elections will be held in about 40 countries and regions around the world, including presidential elections in the United States and Russia. To name a few of the major elections, presidential and parliamentary elections are scheduled in the US, Russia, India, the UK, and other major countries, as shown in the table below, while the Liberal Democratic Party (LDP) presidential election is scheduled in Japan in September 2024.

Table 1: National Elections in Major Countries and Regions in 2024

Date	Country, Region / Election Details
January 13	Taiwan presidential election
March 5	US presidential primary election "Super Tuesday"
March 17	Russia presidential election
April 10	South Korea legislative election
April to end of May	India general election
June 6 to 9	European Parliament election
November 5	US presidential and congressional elections

Nakasone Peace Institute
The views expressed in this work are solely those of the author and do not necessarily reflect the views of Nakasone Peace Institute.

Date undecided (May or later)	South Africa general election
Date undecided	UK general election

Source: Compiled by the author from JETRO World Political and Economic Schedule and other sources.

Of these, in Taiwan's presidential election, disinformation dissemination, presumably from China, aimed at influencing the election, has been observed since 2023. According to an investigation by Taiwan FactCheck Center, a non-profit organization established in 2018 to combat disinformation, such disinformation dissemination is magnified in several narratives. One of these is a series of narratives about a military crisis in the Taiwan Strait that directly affects Taiwan's security. Specifically, these narratives include: "The Taiwan government will expand conscription in preparation for the Taiwan Strait crisis," "Taiwan's military is weak, while the People's Liberation Army is strong," "The United States will not come to Taiwan's defense," and "Taiwan's politicians are already preparing to flee Taiwan."

In the "Taiwan's military is weak" narrative, disinformation was circulated on TikTok, Facebook, LINE, and other Chinese-language social media sites that "a missile was fired over Taiwan's airspace but the Taiwan military could not detect it" during a Chinese military exercise held in response to President Tsai Ing-wen's visit to the US in April 2023. A narrative also circulated about the same Chinese military exercise said that "the US will not come to Taiwan's defense" and that "on the day the Chinese navy carrier *Sandong* entered the waters of eastern Taiwan, the US ordered the *Nimitz*-class aircraft carrier strike group to immediately retreat toward Japan at full speed," which was blatant disinformation posted on Facebook claiming to be a quote from an Australian news website.

Such a narrative is likely intended to influence the outcome of the election by strongly suggesting that a Democratic Progressive Party (DPP) presidency would bring the crisis of military conflict, while an opposition presidency would continue the status quo of peace.

What also cannot be overlooked by Japan is that some of these narratives are designed to discredit the United States. Specifically, there is disinformation circulating in Taiwan, such as "US forces will not come to assist Taiwan due to the revision of the Taiwan Relations Act," "the US has established a biological weapons laboratory in Taiwan," and "U.S. Treasury Secretary Janet Yellen has said she will destroy Taiwan Semiconductor Manufacturing Company, Ltd., (TSMC)." It is believed that these are intended to discredit the US as an ally and put a wedge in the alliance.

Similar disinformation has also been observed in South Korea. In a November 2023 report, the National Intelligence Service of South Korea noted that 38 fake news sites operated by Chinese companies, with names such as *Seoul Press*, *Busan Online*, *Daegu Journal*, and *Chungcheongdo Times*, were found to be disguised as legitimate South Korean media, and that disinformation that "the US is testing coronavirus in South Korea" was being disseminated from these sites. At the same time, the report also pointed out that these fake news sites were disseminating disinformation that "the release of treated water from Japan's Fukushima nuclear power plant will cause a devastating blow to the food distribution network in South Korea." This suggests an attempt to both disrupt the alliance with the United States as well as undermine the improving relations between Japan and South Korea.

How should Japan deal with this kind of information manipulation type cyberattack? The prescription is summarized in the report on the project the author worked on that was published in 2022 by The Sasakawa Peace Foundation. The proposal was entitled, "*gaikoku kara no disuinfomeshon ni sonaeru* [prepare for disinformation

Nakasone Peace Institute
The views expressed in this work are solely those of the author and do not necessarily reflect the views of Nakasone Peace Institute.

from foreign countries]" (in Japanese). To add just one point, in order to deal with information warfare involving a nation-state, proactive cyber defense is required in the same way as it necessary for general cyberattacks. This is a series of operations that includes situational awareness of information warfare, discernment of the cyberattacker's intentions, identification of the cyberattacker, and implementation of countermeasures to thwart the cyberattacker's intentions. All of these operations need to be carried out 365 days a year, 24 hours a day to protect elections and democratic systems in the digital age.

Acknowledgement

This article is an English translation of the article that was first published in the Japanese-language journal *Gaiko (Diplomacy)*, published by Toshi Shuppan, Vol.83 Jan./Feb. 2024.

The views expressed in this work are solely those of the author and do not necessarily reflect the views of Nakasone Peace Institute.