Lessons from the War in Ukraine applied to Taiwan

BLURB: Cybersecurity has become a key component of national security, and the government has a critical role to play to protect citizens and private property.

Soon after Russia invaded Ukraine in February 2022, countries including Japan and the United States rapidly began learning hybrid warfare lessons from the war. As a result, many countries have been actively enhancing their cybersecurity capabilities across multiple operational domains including cyber, electromagnetic, and space.

How Japan and the United States Responded Quickly

Public information sources indicate that the Japan Ground Self-Defense Force (JGSDF) was the first armed force to host a global, multilateral cyber exercise covering hybrid warfare following the initiation of war between Russia and Ukraine. On March 1, the JGSDF invited cyber-related units from six countries, namely the United States, France, Australia, the Philippines, Indonesia, and Vietnam, to join the Japan Ground, Maritime, and Air Self-Defense Forces in a "Multinational Cyber Defense Competition."

According to Kyodo News, the cyber exercise aimed to strengthen each participating country's capabilities to

counter hybrid attacks. This JGSDF-hosted event was designed to offer a dedicated forum for sharing concerns and expertise detailing responses to various attack scenarios, notably including cyber warfare and communication disruption.

In April 2022, the US Army held a two-week exercise in California for just under 6,000 soldiers to train them on comprehensive multi-domain attack response capabilities. The training scenarios entailed an adversary that was not only launching rockets and missiles into a target city, but also utilizing information warfare via the spread of disinformation across social media channels, and also conducting electronic warfare by jamming legitimate communication channels.

Two months later in June 2022, the US National Guard conducted a large-scale, two week-cyber defense exercise dubbed “Cyber Shield,” in Arkansas. This set of exercises involved not only defending against enemy nation state cyberattacks, but also providing countermeasures against the spread of disinformation through social media. The purpose was to train soldiers to concentrate on their missions and minimize the chance to be misled, misinformed, or distracted by illegitimate news.

The National Guard also welcomed experts from key private-sector companies. Such public-private partnerships are proving to be crucial as damage caused by cyber and information warfare will not be isolated to one organization or market sector. These widespread preparations demonstrate a strong commitment by the United States to prepare for multi-faceted emergency scenarios and proactively improve its response capabilities through

public-private partnerships, even during peacetime.

Space, Cyber and Electromagnetic Domains

From the very onset of the conflict, Ukraine has been relentlessly countering disinformation campaigns by Russia and continuing to share their own narratives with its soldiers, citizens and international partners, crucially relying on the US company SpaceX's "Starlink" satellite internet network for internet-based communications. Given the prominence of Starlink for the Ukrainian Government, Starlink is in a continuous state of defense against a barrage of ongoing cyberattacks and signal jamming attempts.

In April, Dave Tremper, Director of Electronic Warfare in the Office of the Secretary of Defense, within the US Department of Defense, praised the speedy response of SpaceX that took place the day after a Russian attempt at jamming Starlink was reported. The quick response by SpaceX prevented disruption and damage to the satellite service. He stressed that the US government should follow suit in preparing for swift defensive actions.

The US Army recognizes the importance in preparing for multi-domain enemy operations. Which is why they announced in August recent significant improvements in battlefield coordination between its Special Operations Command, Space and Missile Defense Command, and Cyber Command. These improvements are in response to the fact that adversaries can now conduct hostile operations simultaneously across multiple domains.

The Indian Army has also been paying close attention to

multi-domain operations, studying the effectiveness of the multi-pronged attacks, targeting both electromagnetic and internet-based communication channels, which were utilized by Russia against Ukraine. Furthermore, the Indian army also conducted a communication exercise in late July to confirm the operational readiness and response of their space-related equipment, using the satellite services of the Indian Space Research Organization.

Applying Lessons in Hybrid Warfare to Taiwan

Not all countries will apply the expertise gleaned from the war in Ukraine for strictly defense purposes. At an international cybersecurity conference, CYBERUK, in May, Lindy Cameron, Chief Executive of the UK National Cyber Security Center, expressed her concerns regarding the danger of countries to misuse such knowledge in the Indo-Pacific.

FBI Director Christopher Wray, during a speech given in Boston in June, indicated that China was intensely studying the war in Ukraine with a strong emphasis on the cyberwarfare aspect. In connection with a potential Taiwan conflict, he further warned that China was seeking to improve its cyber capabilities to “deter or hurt” the United States. However, it is worth noting that Wray was not simply sounding an alarm but was also offering strong support for private companies so they can coordinate to form a strong overall defense of the US across public and private sectors.

Wray, along with Ken McCallum, Director General of the British Security Service (MI5), called attention to China's

activities at a joint press conference in London. They also called on corporate executives to work with the FBI and MI5 to obtain relevant intelligence.

Companies must continue to work to strengthen their cyber defenses and protect the personal information of their employees and customers and hard-earned and valuable intellectual property. However, as cybersecurity has become a key component of national security, the government has a critical role to play to protect citizens and private property.

Citizens and industry are keen to learn about details on cyberattacks and information warfare the government observed and documented in Ukraine and Taiwan, and what of course recommended proactive countermeasures that companies and individuals can take. Also, the government should clarify regarding what kind of support it will provide for citizens and private companies in a national crisis.

In summary, in preparation for potential widescale hybrid attacks, multi-domain exercises are indispensable and should cover countermeasures across space, cyber, and electronic communication channels. Such exercises not only offer a sense of security to both the general public and industry, but they would also serve as a deterrent to potential adversaries who would seek to harm Japan, the United States, or their allies.

RELATED:

- *[Asia's Next Page] Japan's Planning on Taiwan: Mitigating Beijing's Gray-Zone Warfare*
- *No Criticism Allowed: Xi and Putin Tighten their Sphere of Influence and Grasp on the Media*
- *Misperceptions Regarding Japan's Cybersecurity Capabilities*

(This was first published as a Sankei Seiron column. Read the column in Japanese at this link.)

Author: Mihoko Matsubara, Chief Cybersecurity Strategist, NTT Corporation

Keywords: Mihoko Matsubara, NTT Corporation, cybersecurity, national security, Ukraine, cyber warfare, hybrid warfare, SpaceX Starlink, cyber defense, multi-domain exercises, Taiwan, US Japan, Japan Ground Self-Defense Force, multilateral cyber exercise,