Conducting Hybrid Warfare in the Russia-Ukraine War

Siong-Ui Tsiam
Policy Analyst

Division of Cyber Security and Decision-Making Simulation

Topic: cyber warfare, cognitive warfare, patterns of warfare

1. News Highlights

Since the annexation of Crimea by Russia through militia combined with local forces, the confrontation between Russia versus Ukraine and Western democratic nations has persisted. With Russian support, pro-Russian separatists in Eastern Ukraine further established the Donetsk People’s Republic and Luhansk People’s Republic, accepting military aid from Russia in the ongoing conflict with Kyiv.[1] Russia has repeatedly warned NATO against “expanding east” and deem it the line that cannot be crossed. The United States as the main leader of NATO, on the other hand, refused to make such a guarantee and emphasized that it will honor the will of member states and follow the democratic system in reviewing new applications. Hybrid warfare has been the primary method of attack by Russia in the major battles throughout the crises, including the annexation of Crimea in 2014, the conflict between the Ukrainian government and the Donbas militia, and the ongoing invasion of Ukraine. This article analyzes the hybrid warfare methods employed in the events, and how they might be of reference to Taiwan in terms of security implications.

2. Security Implications

1. Military warfare actions in hybrid warfare

In terms of the actual military

[1] Andrew E. Kramer, “Fighting Escalates in Eastern Ukraine, Signaling the End to Another Cease-Fire,” *The New York Times*, March 30, 2021, https://nyti.ms/3gyC30v.

actions in this invasion, Russia first began deploying troops in the name of "military exercise", but instead of returning to defend their base after the military exercise, the troops lingered along the Ukraine border to garrison and build a camp.[2] By continuing to build up its military forces as well as making diplomatic announcements and shaping public opinion,[3] Russia openly accuses Ukraine of violating Russia's national interest. While Russia works on its military deployment and makes diplomatic accusations, its cyber warfare and propaganda warfare persists. Even amidst its large-scale military mobilization and deployment, the Kremlin continues to accuse the West of irresponsibly escalating the situation with its warning of Russia's imminent invasion of Ukraine.[4]

On February 21, the day after the closing of the Beijing Winter Olympics, Putin announced to the world through television broadcast that he will be signing the order approved by the State Duma to acknowledge the sovereignty of the two republics of Donetsk and Luhansk. On February 24, Putin instructed the Ministry of Defense to send troops into Ukraine to assist the "peacekeeping operation" in the two regions, then followed by air raiding significant sites in Ukraine to neutralize air defense forces of Ukraine. Finally, hybrid tactical camps adopting blitzkrieg with tank-based mechanized troops struck Ukrainian forces with large-scale suppressive fire from the above-deployed regions including from the directions of Belarus, Sumy, Kharkiv, the two occupied regions in Eastern Ukraine, Crimea, and Odessa, attempting to surround and takedown Kyiv via the Dnieper River. In the meantime, Russia, or rather pro-Russian separatists, sabotaged and infiltrated major cities including Kyiv.[5]

[2] 2 Eugene Rumer, "Even a Major Military Exercise Like Zapad Can't Fix Some of the Biggest Security Challenges Facing Russia," *Carnegie Endowment for International Peace*, September 21, 2021, https://bit.ly/3IRPZPO.

[3] "Satellite Images Show Russia Still Building up Forces Near Ukraine," *Reuters*, December 24, 2021, https://reut.rs/3CnmQta.

[4] "Vladimir Kuznetsov, Nancy Cook, U.S. Ramps Up Ukraine Warnings as Russia Denies Invasion Plans," *Bloomberg*, February 17, 2022, https://bloom.bg/3pLBiWM.

[5] Lily Hyde, "Saboteurs Spark Suspicion and Solidarity in Kyiv," *Politico*, February 26, 2022, https://politi.co/3CoXriH.

2. Cyber warfare actions in hybrid warfare

Russia has deployed hybrid warfare in Ukraine against Eastern Ukraine and other regions since the annexation of Crimea in 2014. It may be difficult to determine the actors behind the cyberattacks as a state, a group, or an individual, but after the attacks, many countries pieced together enough clues to point to Moscow. The actual actions included using Mimikatz to gain administrative access via Windows and steal network administrator credentials, then hack the power company system on a large scale; or using NotPetya, which masquerades as ransomware but actually takes out the system, severely impacting post offices, banks, the metro, payment systems, and even power systems in Ukraine. NotPetya masquerades as ransomware, but it operates differently in that no contact information or bank transfer details are provided as hackers generally do to receive ransom, and that paying the ransom still leads to permanent and irreversible damage to the data. Since 60% of the victims are infrastructures in Ukraine, experts point to Moscow as the source, naming it an act of cyber warfare which is a wiper disguised as ransomware.[6]

Russia initiated a new round of cyberattacks early during its military deployment in early 2022, attacking government organizations and banks in Ukraine through DDoS in an attempt to cause social unrest from within. Following the first wave of DDoS attacks was a data-wiping malware dubbed HermeticWiper, which data security companies believed had been attacking Ukraine for some time.[7] Used alongside the HermeticWiper was PartyTicket, a poorly coded malware believed to have been used to tie up resources in the victim's system, so that the attack of HermeticWiper could perform more efficiently.[8] In terms of cyber operations, there has yet to be a hard kill on a larger scale, for example, the

[6] Iain Thomson, "Everything you Need to Know about the Petya, er, NotPetya Nasty Trashing PCs Worldwide," *The Register*, June 28, 2017, https://bit.ly/3HDkTtI.

[7] HermeticWiper, "New Data-wiping Malware Hits Ukraine," *Editor of WeLiveSecurity*, February 24, 2022, https://bit.ly/3Kc3Osn.

[8] Juan Andrés Guerrero-Saade, "HermeticWiper | New Destructive Malware Used In Cyber Attacks on Ukraine," *Sentinel Labs*, February 23, 2022, https://bit.ly/35HJkc7.

previous attack on the power plant or other key infrastructures, and this may have to do with the fact that the Russian forces intend to conduct propaganda warfare at the same time. On the other hand, Ukraine is creating an IT Army, openly calling for volunteers around the world to join them and Russian targets will be regularly announced for cyberattacks.[9]

3. Public opinion and propaganda warfare in hybrid warfare

The Kremlin has repeatedly declared to the world since 2015 that Ukraine is becoming the breeding ground for Neo-Nazism,[10] and accused the Azov Battalion stationed in Mariupol in 2014 to be the fortress of ultranationalism, white supremacy, and Neo-Nazism, with the two regions of special historical, cultural, and identity connections to Russia as main targets of the propaganda warfare. After invading the aforementioned two regions, Russia shut down the local Ukrainian language media, leaving only the Russian channel to control the source of information for residents, making sure that their viewpoints are aligned to Moscow.[11] Furthermore, separatists in St. Petersburg and Eastern Ukraine produced a series of videos that were considered fake, with the main purpose to echo the accusations made by Moscow that pro-Ukrainian protesters have committed various extreme crimes and crimes against race and humanity. Such information was spread through media and hackers.[12] Under the threat of Anti-West, Kyiv Threat, and Extremism, Russia did not face much resistance within Russia or the two regions when advancing into Crimea and Eastern Ukraine.

[9] "Ukraine Creates 'IT Army'–Says 'Hack these Russian Companies'," *The Stack*, February 26. 2022. https://bit.ly/3vOeObu.

[10] "В МИД РФ назвали Украину «полигоном неонацизма»," *NTV Russia*, December 17, 2015, https://bit.ly/3hDvY3o.

[11] Tsung Han Wu, "Emotions in Politics and Asymmetric Warfare: With 2014 Ukraine Crisis as Example," *Defense Situation: Special Edition on Asymmetric Defense Thinking and Application*, p. 62.

[12] Andrei Soshnikov, "Inside a Pro-Russia Propaganda Machine in Ukraine," *BBC*, November 13, 2017, https://bbc.in/3vHqLQf.

Prior to invading Ukraine in 2022, Russia adopted the same method of public opinion warfare to manipulate the public opinion on Ukraine in Russia. When Russia was ready to invade, the favorable impression of Ukraine in Russia was significantly lower. In addition to the above accusation of extremism, Russia condemned Ukraine for repeated violation of the Minsk Protocol and creating bloody confrontations in Eastern Ukraine. A Russian far-right talk show host had many times advocated in the show that Moscow should not hesitate to use military force should Ukraine seek accession to NATO,[13] which was obviously trying to influence the public opinion through entertainment. In this invasion, the Kremlin reinforced its control of the language used by the public opinion and the media. All statements must be aligned with Putin, calling it "special military operations", and words such as war, invasion, and attack are considered a violation of Moscow policy and thus controlled.[14]

During the Russian invasion this time, large amounts of fake accounts appeared on various social media, and Telegram, a Russian-based messaging platform, falsely claiming the collapse of the Ukraine government, the President fleeing the country, Russia surrounding Kyiv, the Ukraine government conducting genocide of civilians in Eastern Ukraine, or that Russia is attacking the radicals and not Ukrainians;[15] all of which, on the one hand, justifies the "peacekeeping operation" of Russia in Ukraine, and on the other, dismantling the resistance of Ukrainian civilians and troops. However, with assistance from the international community, various non-governmental fact-checking organizations have appeared on the internet, educating the public on how to spot disinformation.[16]

Meanwhile, the Ukrainian President

[13] Roman Goncharenko, "How Russian Media Outlets are Preparing an Attack on Ukraine," *Deutsche Welle*, February 16, 2022, https://bit.ly/3KxH8Dp.

[14] Andrew Roth, "'Don't Call it a War' – Propaganda Filters the Truth about Ukraine on Russian Media," *The Guardian*, February 26, 2022, https://bit.ly/3sEgHp9.

[15] Rebecca Kern, Mark Scott, and Clothilde Goujard, "Social Media Platforms on the Defensive as Russian-based Disinformation about Ukraine Spreads," *Politico*, February 24. 2022, https://politi.co/35rYD97.

[16] Melissa De Witte, "Seven Tips for Spotting Disinformation Related to the Russia-Ukraine Conflict," *Stanford News*, March 3, 2022, https://stanford.io/3sCuXim; Alan Yuhas, "Russian Propaganda over Crimea and the Ukraine: How Does it Work?," *The Guardian*, March 17, 2014, https://bit.ly/3sHZyv6.

and other top officials used a mobile phone to film a simple yet real video, sending fearless images of Ukrainians through Western media or platforms,[17] and their Ministry of Defense and agency on national security used words, pictures, and videos on social media including Facebook and Twitter to document and share with the world the heroic resistance by Ukraine, the brutal indiscriminate attacks of Russia, and how the Russian forces continue to crumble and be defeated, all of which can be seen as anti-public opinion warfare practiced by Ukraine against Russia and the world. While some of which are also suspected of false claims and pending fact-checking, the main purpose is to largely cancel what the Russian propaganda and public opinion warfare is trying to achieve.

3. Trend Observation

1. Cyber and public opinion warfares may suffer from military setback

Since the internet knows no boundary and given the fact that it is difficult to clearly determine the public and private domains, the aforementioned cyber attacks may have been targeted at Ukraine but have also caused billions of economic losses in USD around the world. Facing the war, it is presumed that the reason Russia has yet to conduct a large-scale cyberattack or shut down the internet in Ukraine is mainly due to the following three factors: Russia is over-confident in its military operations and wants to use the internet to share quickly with Ukraine and the rest of the world how incredibly easy it is for them military-wise, block the possibilities of other nations intervening, and breakdown the mental barrier of the Ukrainian resistance.

According to intelligence provided by Ukraine, Putin had originally planned to take down four major cities in Ukraine within 48 hours, including Kyiv, and further pressure Volodymyr Zelenskyy into signing a surrender agreement followed by the establishment of a pro-

[17] Vera Bergengruen, "How Putin Is Losing at His Own Disinformation Game in Ukraine," *TIME*, February 25, 2022, https://bit.ly/3hLRNO7.

Russian regime.[18] According to this plan, the Russian forces obviously aimed to replicate the air raid on Iraq by the US forces widely covered by the media during the Gulf War, which followed with a blitzkrieg of tanks taking down Baghdad, and achieve the above purpose by having the media and social networks showing off the Russian attacks.

Secondly, having suffered extensive cyberattacks after 2014 with some key infrastructure destroyed, Ukraine has worked on reinforcing the ability to protect their core network while working with NATO or technological exchange and support with the West to improve its capability and joint defense to effectively defend against Russian cyber operations, but also give it the ability to strike attacks. When the actual military actions taken by Russia face repeated setbacks, public opinion and propaganda warfare naturally fail to be effective with the loss of samples and materials to use. Furthermore, Ukraine is creating an IT Army in the name of defending Europe and the Free World, providing targets so hackers outside Ukraine can attack Russia, which on a certain level has also impacted Russia.

As the attacker, the Russian forces need to establish communication among troops in joint combat even more than the Ukrainian forces. Even though the ability for overall joint combat in this battle has been questioned throughout, the liaison between troops and even the logistic pipeline can determine the success of the battle. When Russia undergoes large-scale electronic or spectrum countermeasures, forces fighting on the front line will also suffer and lose communication behind the front. Therefore, due to actual operational requirement, Russia has yet to shut down the power or internet on a large scale. Without substantial progress in military operations, cyber or public opinion warfare is thwarted due to lack of substantial material, thus unable to support the military operation.

2. Social media and messaging platforms become another variable

Hybrid warfare is a supplementary method to regular warfare, aimed at stepping up the harm that can be caused

[18] Larisa Brown, “Ukraine Resistance Shatters Putin’s Plan for Victory in 48 Hours,” *The Times*, February 28, 2022, https://bit.ly/3sUpWBZ.

by regular warfare and putting the enemy in a tactical environment of further disadvantage, or it can be used to improve the advantage of one's own tactical environment. Be it the hybrid warfare by Russia against Ukraine or China against Taiwan, with regulations and monitoring becoming more strict, we are seeing less of TV stations or state-owned media disseminating news of specific political stances. Instead, social media, messaging, and internet platforms that cannot be fully monitored by the public authority are on the rise to become the breeding ground for cognitive warfare initiation and cultivation. During the Russian invasion, social networks including Facebook, Twitter, Instagram, content farms, messaging platforms including LINE and Telegram, and even video-sharing platform YouTube, have seen a significant increase in fake accounts and bot accounts to accelerate the spread of information. It has become very easy for the general public to be influenced in real-time by the cognitive warfare with their smartphones. The mixture of real information also makes it difficult to spot disinformation.

As the owner of the above-mentioned media outlets, the authority of these large transnational enterprises is similar to that of the government yet cannot really be monitored by the government or traditional media. When complicated algorithms and correlating cash flows are involved in the operations of these media outlets, it can be rather easy to pay off domestic actors with RMB or rubles. Just like Ukraine, in terms of the potential attacks against Taiwan by China, once war starts, we can anticipate an overwhelming attack of hybrid warfare to shake the public morale and create social chaos. Therefore, we should continue to pay attention to and review the manipulation of social media and messaging platforms in the hybrid warfare used in the Russia-Ukraine war.

(Originally published in the 51th "National Defense and Security Biweekly", April 8, 2022, by the Institute for National Defense and Security Research.)

(The contents and advice in the assessments are the personal opinions of the authors, and do not represent the position of the Institute for National Defense and Security Research.)