Study

Information Operations in the Russia-Ukraine War

24 Jan. 2023

Dr. Ahmed Daifullah Algarni
Vice President of the International Institute for Iranian Studies (Rasanah)

RASANAH
المعهد الدولي للدراسات الإيرانية
International Institute for Iranian Studies

Contents

The Russian military operation on Ukrainian territory is continuing, as is the media blitz involving the two parties. The latter encompasses all media outlets and social media platforms. The Russia-Ukraine war has shown that a single-worded piece of news, a picture or even a figure can prove to be an effective weapon that supports the battle on the ground. They impact the psychological state of both civilian and military personnel. We have seen how data has been seized, distorted and manipulated in this war to portray the adversaries in the worst possible light, to destroy their psychological resilience, and to erode their sense of patriotism. Furthermore, history, religion and the patriotic spirit have been used in psychological warfare against adversaries.

Information operations are regarded as one of the tools of modern warfare; "influence operations" or "information warfare" (IW) are other terms for them. These operations include gathering information on the foe, managing it, re-analyzing it and publishing it in the media in a hazy and distorted manner to negatively impact the foe's public image and build a public consensus at home and abroad that opposes its orientations and interests. In the Russia-Ukraine war, we have observed cyber operations and the dumping of uncorroborated information into cyberspace by actors involved in the crisis with the purpose of delivering certain messages to influence global public opinion in a way that serves the internal and external interests of the parties involved in the war.

This war has shown us that the concept of information warfare is expanding and being used in unprecedented ways. The concept of information warfare can be used defensively or offensively. Electronic warfare, command and control warfare, information piracy warfare, psychological operations warfare and economic information warfare all fall under this umbrella of "information warfare." As a result, information warfare now has multiple levels, tools, objectives and domains and requires strategies similar to war strategies.

We will look at how the information operations associated with the Russia-Ukraine war since its inception have been more complicated than we can imagine. We will look closely at how the Russians have made significant efforts to use information and cyberwarfare alongside military operations. On the other hand, we will investigate how the Ukrainians have mobilized their information warfare capabilities and used them to counter the Russian narrative. Finally, we will dis-

cuss how the Western media discourse appears to be quasi-unified in the face of the Russian narrative and in support of Ukraine.

Russian Information Operations

For decades, going as far back as the Soviet era, delusive information, or what can be called "active measures," has been an essential part of the Russian foreign policy strategy. Russian actors are among the most powerful in instrumentalizing psychological operations and the dissemination of propaganda and disinformation via social media, which the Russians refer to as "reflexive control."

Back to the Cold War and as part of the psychological warfare activities between the East and West, Russia's Committee for State Security, most famously known as the Komitet Gosudarstvennoy Bezopasnosti (KGB), was a key player in disinformation campaigns during Operation Secondary Infektion. For example, in the mid-1980s, Russians popularized the idea that HIV/AIDS was a genetically modified virus created by the Pentagon as part of its alleged biological weapons research at the US Army Medical Research Institute for Infectious Diseases in Fort Detrick, Maryland. They claimed that the virus had escaped and had spread throughout the world.

Between 2014 and 2018, Russia conducted a slew of Infektion operations on social media platforms. Russia ran the operations through a centralized entity; for example, the operations included forging, intervention, and attacks on Kremlin critics. According to multiple reports, the campaign used fabricated reports and accounts to incite conflict among Western countries. In the majority of cases, they targeted Ukraine. Only nine months into Russia's war on Ukraine, at least 2,500 pieces of content in seven languages were published across more than 300 platforms.

Objectives of Russian Information Warfare

By analyzing the pro-Russia narratives on the war and its propagation of disinformation, it is obvious that Moscow is attempting to shape perceptions regarding the invasion and the wider geopolitical context surrounding it to achieve all or part of the following objectives:

- **Dampening the Ukrainian population's morale:** Several Russian narratives have been identified that appear to be aimed at dampening

Ukrainian morale, inciting tensions within Ukraine, and sowing division between Ukrainian society's currents and its leadership. Among these stories are claims, later proven false, that the Ukrainian government and army had surrendered. Ukraine allegedly announced its surrender to Russia in a video posted on Ukrainian websites in March. The news even appeared on the Ukraine 24 channel's news bar, indicating Russia's success in hacking the Ukrainian channel.

According to CNN, pro-Russian internet operatives claimed last March that Ukrainian President Volodymyr Zelenskyy committed suicide in a military bunker in Kyiv where he was leading the fight against the invasion. They claimed he was considering suicide as a result of Ukraine's military failures. It was later revealed that this was misinformation.

Another operation in April claimed that the Azov Regiment, also known as the Azov Gang in Russia, had sought vengeance on Zelenskyy after he abandoned their fighters to die in Mariupol. It also claimed that Azov commanders attempted to flee the city by disguising themselves as civilians. It is worth noting that the Azov Regiment of Ukraine is an extremist nationalist movement that believes in white supremacy. It includes Nazi sympathizers from more than 22 different European countries, as well as the United States. This has aided the Russians in their efforts to portray the Ukrainian government and Ukrainians who do not wholeheartedly support Russia as Nazis.

- **Distancing Ukraine from its Western supporters**: The Russians also strive to sow discord among Ukraine, its Western allies, and the rest of the world. For example, Russia targeted the relationship between Ukraine and Poland by publishing opinion articles written by ghostwriters who claimed to be members of The Democratic Party of Russia (DPR).

These articles spread the story that a Polish criminal gang was trafficking Ukrainian refugees and that senior Polish officials were involved in the operation. This story also sought to portray the refugees as imposing an undue burden on Poland's economy and healthcare system, and that the immigrants were neo-Nazis who were using collective crossings to carry out attacks on Polish soil. Meanwhile, an early February information operation revealed that the Ukrainian and Polish governments were seeking to allow Polish forces to be deployed in western Ukraine. A map indicating where the Polish armed forces would be deployed was published, alleging that the forces would annex vast areas

of Ukraine and stay for years. As a result, Russia recreated historical conditions that Poland and Ukraine previously experienced.

Russian propaganda has magnified the European countries' disagreements over how to deal with Russia diplomatically, as well as blowing up the disagreements over the imposition of economic sanctions on Russia, and extensively covered the announcement by Hungary and some other countries of their willingness to pay the price of Russian gas in rubles — a departure from the position of European Union (EU) member countries. Russia is attempting to sow discord, particularly between France and Germany, which continue to maintain diplomatic contacts with Russia, on the one hand, and Eastern European countries, which are opposed to this diplomatic rapprochement and refuse to engage in dialogue with Moscow, on the other.

Russia organized a special disinformation campaign highlighting the failure of the March European Summit in the Belgian capital of Brussels to reach an agreement on imposing additional sanctions on Russia. It also emphasized the divergent positions of EU member countries, which have become increasingly concerned about the implications of additional sanctions on their own economies. Narratives seen on Telegram channels included predictions that the West will soon forget and abandon Ukraine. This is partly due to the United States shifting its focus to other impending conflicts, such as a war with Iran, or pivoting to the Indo-Pacific region.

• **Promoting positive perceptions about Russia and countering the Western narrative:** It appears that the various Russian narratives aim to bolster positive perceptions of Russia and polish its public image by demonstrating that its military operations are just, legitimate, and justified. Russia, for its part, denies allegations of war crimes committed by the Russian army in Ukraine, but accuses Ukrainian forces of the same crimes. For example, the Cyber Front Z Telegram channel claimed that "Nazi" Ukrainians forced civilians into a Mariupol theater and then blew it up, alleging that Ukrainian forces used chemical weapons. Similarly, Russia accused Ukraine of initiating a plan to use a "dirty bomb," which Ukraine and its Western allies dismissed as a pretext for escalation. The latter claimed that the sole purpose of this accusation was to justify Russia's use of tactical nuclear weapons by claiming that Ukraine was the first to pull the trigger.

The pro-Russian information campaign is being translated into nearly six languages, with audiences in China, Latin America, and the Middle

East. True and fake accounts are being used in the campaign. It can be argued that the majority of the world's population is either neutral or supports Russia's position in the war. While 141 UN member countries voted to condemn Russia's aggression in Ukraine, no country in Asia, Africa or the Middle East imposed sanctions on Russia. The reason for this is that Russia has recently targeted the virtual sphere in the mentioned regions, allowing it to disseminate its own narrative to the point where peoples in these regions do not view the war in the same way that the West does. The Middle East and North Africa has long been a target for Russian information operations. Since 2007, the Kremlin has used the Russia Today satellite channel to communicate with the peoples of the Arab world. The Arab Spring and Russia's intervention in Syria in 2015 were both watershed moments for Russian media outlets and Kremlin narratives in the region.

For example, on Twitter Russia Today and Sputnik Arabia produce far more content than BBC Arabic. While the two Russian channels have averaged 180 and 87 tweets per day since their inception, BBC Arabic has only averaged 32. Overall, the two channels present the case that the United States and Europe are to blame for the Middle East's instability, while cementing Moscow's image as a stabilizing force. Given the resentment many in the Middle East have for Western policies in the region, this narrative has a strong resonance with them. There appears to be large segments of the population who believe in the Russian narrative — not because they love Russia, but because they despise the United States and the West.

On the other side, Russia has designed a strategy based on countering the Western narratives on Ukraine through establishing a host of verification programs and organizations to undermine any newsfeeds that contradict its authorized narrative. Russia's Channel One, the country's largest official channel, has launched a program called "AntiFake" to debunk what they call false stories about the Russia-Ukraine conflict. It uses fact-checking tools such as statistics, forensic analysis and black-and-white videos to demonstrate that claims about Russian violence are false, and it includes short videos debunking Western claims about the Russian military campaign.

Western media outlets have called into question the Russian army's military victories, providing figures about Russian losses. Meanwhile, Russia's Channel One refutes Western statistics, portraying Russian

operations as successful. According to this channel's news reports, more than 1,100 Ukrainian military infrastructure facilities have been disabled, and hundreds of pieces of equipment have been destroyed. The channel has not mentioned the number of Russian casualties. The Russian Ministry of Defense published maps of the Kharkiv region that showed a significant withdrawal of the Russian army from this region, where a large-scale Ukrainian counterattack occurred, with Moscow refusing to acknowledge the magnitude of the losses that Kyiv has referred to. Yet, despite the Russian army's retreat in the lands east of the Kharkiv region behind the Oskol River, the Russian army spokesman only mentioned the "withdrawal" of forces in the Balakliya and Izyum regions (eastern Ukraine). The Russian goal is to "regroup" forces near Donetsk (one of the capitals of pro-Russian separatists) to mislead the public into believing that there was no military defeat.

Prior to that — by the time the Russian military operations were being launched — and in order to create a pretext and justification for the invasion, Russian President Vladimir Putin addressed the Russian nation on the morning of the operation, February 24, 2022, saying that the West holds full responsibility for the tragic events that occurred in the Donbas region of eastern Ukraine over the previous years. He went on to say that he made the decision to invade because he was forced to by the West and that there was no other option now.

Putin believes that irresponsible Western politicians have sought to force Russia into this option in recent years by expanding the North Atlantic Treaty Organization (NATO) eastwards, bringing their armies and infrastructure ever closer to Russian borders. "It is a fact that over the past 30 years we have been patiently trying to come to an agreement with the leading NATO countries regarding the principles of equal and indivisible security in Europe," Putin said. However, NATO's response to Russia has been "cynical deception and lies or attempts at pressure and blackmail." He provided a detailed account of the historical circumstances leading up to the present moment.

The most important battle for the Kremlin right now is to win the sympathy and support of the Russian people, as well as to confuse or even silence opponents. To control media content, the Russian authorities have imposed hefty fines on any media outlet or journalist who publishes reports on the war relying on resources other than the Kremlin or the Russian Ministry of Defense or depicting the war as an invasion not merely as a military operation. Any media outlet or

journalist who breaches Russia's media policy or guidelines can also face a 15-year jail sentence.

Reports published by the Digital Threat Analysis Center (formerly Miburo) show that 85 percent of Russians obtain the majority of their information from Russian state media. Meanwhile, according to the Levada-Center in Russia, an independent pollster, more than half of Russians see NATO and the United States as the primary cause of the war in Ukraine, while only 7 percent blame the Kremlin.

The West seeks to discredit Putin through influencing the media and relying on Russian opposition to the war, and hoping that this opposition, with the help of Western economic sanctions, could lead to the overthrow of Putin's rule in Russia. However, polls show that Putin's popularity has grown since the military operation began, and that more Russians support the state's operations in Ukraine. Furthermore, polls show that the Russian protests are still insignificant and powerless to influence or withstand the government.

- **Distorting the United States' and the West's image globally:** Russian influence campaigns have also sought to weaken the global standing of the United States and the West, as well as to manage global perceptions so that global public opinion is favorable toward Russia's intervention and cause. This intent was echoed by Russia's Foreign Minister Sergei Lavrov during a meeting of GCC and Russian foreign ministers for strategic dialogue. "We are working to limit Western hegemony over the world," he said.

To accomplish this, Russia has engineered disinformation campaigns run by Russian, Belarusian and pro-Russian actors, employing a variety of tactics, techniques and procedures to support tactical and strategic objectives directly related to the conflict itself.

Many Russian reports and images on social media and on Russian satellite channels in multiple languages, for example, have promoted narratives such as the allegation that laboratories linked to the Pentagon were conducting biological weapons research in Ukraine. On March 6, Russian Defense Ministry Spokesperson Igor Konashenkov stated that Russia's military operation in Ukraine led to the discovery of evidence of Pentagon-linked laboratories conducting biological weapons research in Ukraine. Accounts linked to Russia later expanded on this claim, alleging that the biological laboratories were funded by the United States and that they exist not only in Ukraine but around the world. Russia is still conducting investigations into this matter and

claims to be in the process of providing additional evidence. However, no evidence confirming the Russian claim has emerged thus far.

Themes of a pro-Chinese campaign known as DRAGONBRIDGE (as called by Google) on Russia's war appear to target Washington's foreign policy. The campaign promotes claims that the United States pursues only its own interests, is an unreliable partner and seeks to fan the flames of conflict everywhere in the world to increase weapon sales. This Russian propaganda campaign has also questioned the perceived US and European harmony when it comes to sanctions on Russia. It claims that the United States intimidated and forced Europe to impose the sanctions despite the continent's worsening energy problems.

Observers of the Russian campaign targeting Arabic-speaking audiences will also notice that Russia promotes the claim that the United States fled Afghanistan in 2021, that it has now abandoned Ukraine, which deserves its fate because of its alliance with the "American axis of evil," and that NATO has sacrificed Ukraine to avoid a war with Russia. The Russian campaign also accuses the West of hypocrisy in dealing with Saudi Arabia in comparison to Moscow by failing to put the war in Ukraine on the same level as the war in Yemen. It also cites Western accusations of racism against Arabs and Muslims. Even Israel has been mentioned in Russian media outlets, with accusations that Israeli intelligence is supporting Ukraine against Russia in the ongoing crisis, and that Israel has supported the Ukrainian colored revolutions in collaboration with the CIA. Because of the West's superiority in the realm of information technology, Putin may not fully succeed in the information war against the United States and Europe. However, he is having success in the Middle East and Africa, as well as in the world's two most populous countries, China and India. China, Iran and India have taken advantage of the Russia-Ukraine war to advance their long-term strategic goals. It was discovered that a large number of Chinese, Iranian and Indian state media outlets amplified Russian propaganda by producing mostly pro-Russian media content. In China, a media campaign involving mostly fake accounts was launched across multiple social media platforms, websites, and forums. The campaign shifted its focus to create content in English and Chinese that mirrored the narratives promoted by Russia's state-run media. The Chinese Communist Party-affiliated paper adopted the narrative that the Bucha massacre was a sham. It is worth noting that the Russians have launched a propaganda campaign to refute Western

accusations that the attacking Russian forces committed a massacre in which dozens of civilians were killed in Bucha, a small town north of the Ukrainian capital Kyiv.
On May 24, 2022, Russian authorities focused on spreading information on the Chinese website Weibo, which featured a post by a Ukrainian soldier wearing a badge of the US flag and a Nazi tattoo. Later, the same website published photos of the same soldier participating in anti-China protests in Hong Kong. Following that, Chinese media outlets and senior members of Weibo accused Ukrainian soldier Serhii Fedorovych Filimonov of being a Nazi backed by the West in order to incite protests in Hong Kong.
It was discovered that the China Internet Network, which accounts for one-fifth of all internet users worldwide, is pro-Russian, and the majority of its users identify with the Kremlin's narrative. The "not free internet" users get a lot of their information about the war from Russian state media, which glorifies the "noble" Russian soldiers.
Additionally, it has been observed that the BRICS bloc, which includes Brazil, India, China, South Africa and Russia as well as the countries in Southeast Asia, tend to believe the Russian narrative.

Russian Information Warfare Tools

Before and during the invasion, Russia used all of its conventional and digital media outlets, both internal and external, to launch campaigns to influence public opinion with multiple narratives, some of which are true and some of which are fabricated. Throughout the Russia-Ukraine war, the Russians were active with their strategic messaging through information operations that ran concurrently with disruptive cyber threat activities. Cyber-enabled operations, established assets and hack-and-leak operations are among the Russian and Belarusian information operations associated with the invasion. They have done so by utilizing sophisticated campaign infrastructure as well as a set of vectors that have been leveraged by selected actors allied with Russia.
Mandiant, a threat intelligence website, has been tracking Russia's digital moves for years and has released a comprehensive overview of its latest findings. These include troll farms and fake news portals linked to the Russian intelligence service as part of a "disinformation

campaign promoted by a slew of actors," according to the report's authors. Mandiant identified the following as key tools in Russia's misinformation campaign:

- **APT28**: A Russian nation-state group known as APT28 (aka Fancy Bear, Sofacy, or Strontium). The group was discovered by the Ukrainian Security Service as well as the governments of the United States and the UK, and was described as information operations media of the Main Directorate of the General Staff of the Russian Federation (GRU). The activity of these channels includes promoting content that is intended to undermine Ukrainian trust in their government and its response to the invasion. The content also appears to be intended to undermine Western support for Ukraine. It also includes some non-political posts or accurate news reports to lend credibility to the content. The GRU-backed Telegram channels have highlighted alleged corruption and incompetence on the part of the Ukrainian government, such as claims that Ukraine is not prepared for conflict and that Ukrainian oligarchs are pressuring Zelenskyy to leave the country. Russia Today and Sputnik were able to get around the Western ban by broadcasting on Telegram rather than on Twitter and Facebook.
- **Ghostwriters**: Russia has enlisted the help of a group of writers to write for hacked websites and suspected social media accounts. In April of this year, fabricated content was published to promote a narrative that appeared to be intended to sow discord between Ukrainians and the Polish government. These ghostwriters also continued to publish and promote opinion pieces critical of NATO and its presence in the Baltic, with increasing references to Ukraine in this context. Mandiant determined that Belarus, specifically the Belarusian spy group UNC1151, was at least partially responsible for the ghostwriter campaign. The group had also conducted similar campaigns targeting European countries.
- **Hacking hostile platforms**: Russia has enlisted the help of "cyber forces" to counter the Ukrainian war narrative. According to the Russian newspaper Fontanka, one of its reporters infiltrated a Ukrainian cyberattack platform called "Cyber Front Z," where he met the "cyber forces" and explored how they operate across social media platforms such as YouTube, TikTok, and Twitter. According to the Fontanka reporter, Russia gathered a large number of reporters, commentators, content analysts, designers and coders to form an online front against

Western-backed Ukrainian websites, writing comments on all of these platforms refuting the Ukrainian narrative of the war.

- **Internet**: Since 2018, the Australian Strategic Policy Institute (ASPI) has examined Russia-related information operations on the internet. It was noted that the majority of the hashtags and tweets were heavily focused on criticizing and stirring up hot political issues in the United States, as well as defaming candidates in US and European elections. The tweets also attempted to discredit NATO in the eyes of Europeans, denigrate Ukrainian leaders, and promote Russian foreign and military policies in Syria. In terms of public participation in information operations, Twitter is currently the most influential social media platform.
- **Cyberattacks**: According to Cybercrime Magazine, hacker attacks and other forms of cybercrime will cost the global economy more than $6 trillion in 2021. By 2025, these crimes are expected to cost the global economy approximately $10.5 trillion per year. Every 11 seconds, somewhere in the world, a cyberattack occurs.

It is worth noting that Russia's cyber capabilities are ranked lower than those of the United States, China and the UK in the US National Cyber Power Index, which is compiled by the Belfer Center in the United States. Nonetheless, Russia has used cyberattacks in recent conflicts, including its invasions of Georgia in 2008 and Crimea in 2014. Ukraine has since become a "training ground" for Russian cyberwarfare operations. However, when Russia invaded Ukraine, many security analysts predicted unprecedented levels of cyberwarfare by Russia, owing to Moscow's history of such attacks. And this has yet to materialize effectively.

However, just hours before the invasion, a type of malware known as Wiper hacked into the Ukrainian government's computer systems, corrupting its data. A week before the invasion, a massive campaign of distributed denial-of-service (DDoS) attacks, many of which were blamed on Russia, flooded Ukrainian bank websites with data and signals, rendering them inaccessible. These attacks were unsurprising as Ukraine has been subjected to a barrage of cyberattacks since the conflict with Russia erupted in 2014. Despite the numerous low-level cyberattacks, Ukraine's basic infrastructure such as phone lines, internet, electricity and healthcare systems, is still intact.

So, why did Russia not use cyberattacks as expected, and why are Russian cyberattacks officially labeled as acts of espionage or sabotage

rather than acts of war? This can be explained by Russia's continued belief in its ability to control Ukraine. It may be in its best interests to preserve parts of Ukraine's infrastructure rather than destroy it and then be forced to rebuild it. However, another plausible hypothesis is that Russia is not fighting with all of its cyber power in order to avoid any escalation or repercussions outside of Ukraine, which could prompt the West to respond. Any cyberattack may trigger Article 5 of NATO, which states that an attack on any member country is considered as an attack on all of them. Nonetheless, Russia may retain its most powerful cyber weapons and increase the frequency of its cyberattacks if the ground war falters or is hampered by financial sanctions. The current conflict in Ukraine has demonstrated how quickly Russian hacking groups and information warfare executors can twist facts and alter information about daily events. Mandiant conducted an analysis of information operations consistent with Russian political interests that occurred in conjunction with Russian-sponsored disruptive and destructive cyberthreat activity in the weeks leading up to and following the invasion. It also discovered cyber operations involving the dissemination of Wiper malware masquerading as ransomware.

Ukrainian Information Operations

Ukrainian Campaigns of Influence

We have also seen the Ukrainian cyber army wage an information war against the Russian narrative, carry out cyberattacks on Russian targets and achieve tangible success in the online war since the outbreak of the war in Ukraine on February 24. The Ukrainian communication and information strategy has been widely successful in attracting an outpouring of Western sympathy and support. Since Russia's annexation of Crimea in 2014, Washington and the European capitals have supported this strategy. The heroic stories and military resistance of Ukrainian army soldiers in the face of Russian attacks, as well as the human stories of civilians fleeing their homes and cities, made headlines in the Western media. As a result, Western public opinion sympathized with the Ukrainian people.

According to The Washington Post, Ukraine has won the information war by launching an aggressive communications campaign that has resulted in large Western arms donations and widespread support for unprecedented economic sanctions against Russia. Zelenskyy's

speech to the US Congress was powerful. To win over US lawmakers, he focused on clarifying facts and affirming common Ukrainian values with the West. He also warned that the consequences of the war would affect everyone if they did not pay attention to the outcomes. Zelenskyy focused on cultivating a sense of shared identity between Americans and Ukrainians, at least in part, in response to some criticism that Ukraine is a corrupt country that does not share the same values as the United States. The first point brought up was his emphasis on democracy, independence, and freedom. He compared the Russian invasion to Nazi aggression during World War II.
Indeed, his influence was successful in obtaining the US government's approval to provide Ukraine with various weapons worth $800 million until May. The package includes surface-to-air missiles and drones, which the Biden administration previously refused to supply. Zelenskyy's remarks may have resonated with some in Washington who lean toward the Russian line, convincing them that the Ukraine situation ultimately poses a greater risk to the United States if it does not respond (to the Russian aggression).

Tools of the Russian Information War

- **Encrypted Telegram** has emerged as the primary digital battleground in the information war between Ukrainians and Russians. Zelenskyy has a Telegram channel where he speaks directly to Russian people in Russian. The fact that Facebook, Twitter and YouTube abandoned neutrality and took the Ukrainian side by banning Russian messages and official Russian media such as Russia Today and Sputnik has aided the Ukrainian media campaigns.
- **Cyber Hunta**: This is a pro-Ukrainian hacking group that is comprised of several volunteers with the goal of exposing Moscow's involvement in the Russia-Ukraine conflict. It claims to be unconnected to the Ukrainian government. This hacking group's goal is to remove pro-Russian trolls from Ukrainian websites while also protecting Ukrainian websites from pro-Russian hackers. This hacking group has previously hacked Russian government websites such as the Russian Presidential Administration, the Russian Parliament and the Ministry of Foreign Affairs as well as emails associated with one of President Putin's advisors Vladislav Yuryevich Surkov.
- **Cyber Hundred8**: This hacking group's goals include removing pro-Russian trolls from Ukrainian websites and protecting Ukrainian

websites from pro-Russian hackers. It also teaches Ukrainians how to combat trolls and respond to cyberattacks. However, little is known about its composition or structure.

- **Null Sector:** This hacking group was formed following the February 2014 demise of former Ukrainian President Viktor Yanukovych. It mostly uses DDoS attacks against Russian websites, flooding servers with illegitimate requests and overloading server infrastructure, causing them to go down.

- **Ukrainian Cyber Troops/Army:** This hacking group, founded by Eugene Dukokin, a former cybersecurity consultant and programmer, targets pro-Russian separatists and Russian forces in Ukraine. It reports pro-Russian officials' accounts to various banking and payment sites as well as social media platform accounts, in order to close them down.

Anti-Russia Western Propaganda Campaigns

The Western Media's Authority

It is widely acknowledged that the West and Europe command an unrivaled media machine, which has been instrumentalized in the information war against Russia. A Western media campaign opposing the Russian invasion has been launched since the start of the Russian military attack on Ukraine. Russian messages have been essentially blocked on Facebook, YouTube, Twitter, and Google. Access to official Russian information channels is restricted on these platforms. Analyzing the Western media campaign against Russia reveals significant exaggeration in describing events as well as selectivity in shedding light on certain incidents while ignoring others, frequently avoiding impartiality and objectivity in analysis. Western propaganda has attempted to portray Russian operations as an "unprovoked invasion," to highlight any manifestations of internal Russian opposition to the invasion of Ukraine, and to exaggerate the "devastating" impact of Western economic sanctions on Russia. The West insists that the "economic disaster" will destroy and paralyze Russia' s economy. It ignores the fact that Russia has precautionary measures in place, even in the banking sector. Russia and China are attempting to set up two transfer networks between banks that are independent of the Western network. This is in addition to Moscow's adoption of the "equal deals"

system, the sale of oil in Russian rubles and other protectionist measures that appear to have been planned far in advance.
Western media reports quickly painted a particular picture of the current conflict's origins. It is entirely based on the narrative that there was a group of people who gained independence in 1991, following the collapse of the Soviet Union, and the majority of them spoke Ukrainian (in the western part of the former Soviet Union), and wanted to break away from their historical relationship with the eastern part (Russia) and reorient toward the West, Europe in particular, and NATO. According to Western discourse, the conflict on the ground is between a Ukrainian "nation" struggling to preserve its culture, independence and unity and a Russian desire to dominate Kyiv and bring back the "specter" of the Soviet Union's past. The Western propaganda campaign is centered on refuting everything Russian President Vladimir Putin has said about the reasons for the military operation in Ukraine. This was done to arrive at the only possible conclusion: the military operation is an "unprovoked invasion" of a country that poses no threat to Russia. On the contrary, the narrative insists that Russia is a threat to this country and to other former Soviet Union countries. According to Western media discourse, NATO did not expand eastward except because the former Soviet Union countries knocked on its door and asked for protection from Russia (the fearsome neighbor that threatens their security).

A Unified Anti-Russia Western Media Discourse

The unity of the Western propaganda media discourse is apparent when analyzed. There are no narratives being promoted outside the bounds of this discourse. Therefore, Lebanese academic Asa'd AbuKhalil, professor of political science at California State University Stanislaus, said in an article in the Lebanese newspaper Al-Akhbar, "The articles on national security and foreign policy in Western newspapers are nothing but platforms for Western intelligence circles. They are part of the Western war machine against its enemies, especially when Western media reports the same narrative with almost no variations." He provides numerous examples of how the Western media operates, ranging from the Crimean crisis to Middle East wars, and from Palestine to Iraq and Syria. He believes that the media has been preparing for the current conflict, which could not have happened without coordination with Western security and intelligence agencies.

In fact, there is widespread agreement in the Western media that the Russian military operation failed to achieve its goals, and there is little coverage in the Western press that is not biased in this regard. One of the most prominent aspects of the Western media's biased coverage is the exaggeration of the Ukrainian resistance, which they claim has confronted the "Russian invasion" and has been far more effective than expected. They claim that this resistance is what is thwarting Russian plans and that it will undoubtedly succeed in the end.
Western media analyses also emphasize the Russian army's lack of combat efficiency and exaggerate its logistical problems due to a lack of spare parts, food and fuel supplies, in reference to the difficulties encountered by the large military convoys that attempted to enter Kyiv. We rarely see objective media coverage of the Russian army's significant successes, particularly in southern Ukraine, in the Western media. Furthermore, Western sources claim that the Russian army's morale is extremely low for a variety of reasons, the most important of which is that the Russian soldiers may not have known exactly what needed to be done in Ukraine, or that they did not anticipate all of the Ukrainian resistance. Their commanders may have told them that the Ukrainians would surrender quickly and Kyiv would fall within days, which has not yet occurred. Of course, the Western media does not ignore the military assistance provided to Ukraine, which, according to Western propaganda, helped to effectively repel the Russian attack. Nonetheless, independent perspectives that contradict the Western narrative of events can be found in some Western media outlets. For example, a retired US Army officer and history lecturer at the Marine Corps University Dr. Edward Erickson laid out his point of view, "The Western media coverage focuses exclusively on the tactical level of the war. They only see the Ukrainian side of the war, with correspondents sympathizing with them." He does not believe that the Russian army is performing as poorly as the Western media portrays. On the operational level, Erickson believes the Russians are conducting a coordinated campaign. Despite recent withdrawals, Russia's performance appears to be positive so far. The US expert also confirms that the Russian army has not yet fully utilized its firepower and intensity, particularly its powerful artillery. "We have not seen the Russian Air Force conduct large-scale operations so far."

Conclusion

The military adage "in war, truth is the first casualty" will continue to apply. Information warfare will continue to be a key tool in future conflicts. Information, propaganda and counter-propaganda operations are central to the ongoing Russia-Ukraine war. They reveal a fierce struggle over narratives between Russia on the one hand and Ukraine and other Western powers on the other. These actors have attempted to shape the Ukrainian crisis' narrative in a manner that is consistent with their respective interests and visions. We anticipate that such operations, including cyber threat activity and potentially disruptive and other destructive attacks will continue as the war progresses. Furthermore, future wars will increasingly be "hybrid wars," a combination of firepower and information warfare. The information war in the Russia-Ukraine conflict is not limited to traditional media outlets, but also includes digital media and cyber warfare.

This war has demonstrated that social media platforms will play a significant role in future information wars, particularly because they are regarded as an important field for disseminating information without verification and at a low cost. Anyone with a fictitious persona or a pseudonym can say and post anything. The results are a mash-up of fact and fiction that evolve so quickly that it is nearly impossible for even professionals to verify and know what is right and wrong amid all the commotion. Then there is chaos, doubt and uncertainty as fact and fiction merge.

Similarly, cyberwarfare, as one type of information warfare, has played an important role in this conflict. It will almost certainly be a tragic part of future wars. It will entail fighting enemies from afar with new categories of weapons such as viruses, malware and programs that target system operations or even completely shut them down. Cyberattacks will be the new invisible and unpredictable battlefield. Hackers and coders from various countries will compete to disrupt the target country's economy and various aspects of life. Nothing prevents this, as anyone with a home computer and sufficient technological expertise can launch such attacks. Damage can be devastating at times because this individual has the ability to disrupt entire networks, including those supporting critical infrastructure.

One of the most significant aspects of cyberwarfare is that no one can predict it. Its methods are renewable and open to creativity, innova-

tion and the generation of new ideas. It is certain that we are in the midst of a new form of warfare without precedent in history, and that we are at the start of a new era in which there will be no place except for those who research and innovate in the field of cyberspace, either to defend information structures and cyberspace, or to attack potential enemies when necessary.

Many countries have begun to consider establishing an information technology army (cyber armies) by training the greatest number of creative cadres in this vast arena. It is the creative minds that will be able to change the rules of future wars and extract victory at a lower cost than conventional weapons and weapons of mass destruction. Only they can deal with the invisible damage to potential foes. Perhaps in the future, the military balance of power will shift. A country with insufficient hard (military) power can outperform its adversaries by utilizing its skill and creativity in information technology and cyberspace.

Nonetheless, international legislation to control cyber operations is required. This is because a cyberwar could bring the entire world to its knees, set it back hundreds of years, and spark new conflicts that are more dangerous than all previous conflicts.