Toda Peace Institute

Policy Brief No. 158 **May 2023**

Digital Warfare and Peace:
Learning from Ukraine's Response to the Russian Invasion

Anna Romandash

Abstract

Before launching a full-scale invasion of Ukraine on February 24, 2022, Russia had maintained a low-scale war with Ukraine since early 2014. That conflict, which culminated in the annexation of the Crimean peninsula and the ongoing Donbas war, received less international attention than the 2022 full-scale invasion. Due to the Kremlin's propaganda channels, troll armies, and "useful idiots" in the West and beyond, Russia was able to control the narrative on the situation in Donbas and Crimea and significantly diminish both support and interest toward Ukraine throughout 2014–2022. Yet, things changed after the start of the full-scale war in 2022. In 2022, Ukraine shifted international views on the Russian invasion. Ukraine's efforts significantly contributed to Russia's digital isolation and mainstreamed Ukraine's counter-narratives using open-source data, digital allies, and successful communication campaigns.

Keywords: Ukraine, Russia, hybrid warfare, information, propaganda, cyberattacks, trolls, elves.

Introduction

States wage war not only with tanks and guns, but through various non-military means as well. There are trade and economic wars, cultural and history wars, and information wars, aka infowars. The latter includes all kinds of media to inform the larger public, and the ability to shape a narrative around a specific event, figure, or dispute to achieve a political goal. This is also known as "cognitive warfare" – an attempt to shape how people think and feel about political issues (Backes & Swab, 2019).

Infowars require resources such as influential media channels, various digital platforms, and a large number of real or artificial followers spreading specific messages across the infospace. Digitalization means that cognitive warfare is expanding its outreach while its goal remains the same: waging infowars through various media to win the hearts and minds of the target audience. Cyberattacks, data, and digital vulnerabilities of the opponent are key in this process (Jankowicz, 2020).

Russia is a global leader in waging infowarfare. Since Vladimir Putin came to power on the eve of the 21st century, he quickly spread his control over all Russian state media. Russian information space, which was relatively free throughout the nineties, soon became heavily censored and regulated. Thanks to the tight grip over television, newspapers, and radio, the Russian president and his allies were able to shape the domestic and international narrative in Russia. Russians still have independent media options as alternatives to the state channels although many have been shut down after the start of the full-scale war, and the remaining ones went into exile (Yablokov, 2022).

In the two decades before Russia's 2022 invasion of Ukraine, the Kremlin managed to create an influential information system to shape the narrative outside of Russia. Primarily with the investment in its foreign media outlets such as Russia Today (RT) and Sputnik, it was able to reach diverse audiences across the globe and provide a Kremlin-friendly view of the world in people's native languages (Omelicheva, 2022). The Russian state expanded its media production by heavily investing in digital armies of bots and trolls who filled social media with Kremlin-dictated messages. The aim of this digital army was not only to reinforce Russia's standing in the world by destabilizing its potential rivals; another objective was to justify Russia's imperialism and wars of aggression by creating a parallel reality where nobody could be trusted (Van Herpen, 2015; Polianska, 2022).

Cyberwarfare became one of the most important tools for undermining people's trust in public institutions and authorities across the West. The Kremlin also used its hackers to retrieve sensitive information from foreign states, disrupt public services, and blackmail foreign governments using the stolen information. It meddled in the elections by massively spreading fake news and releasing its bots during the Brexit referendum and the US Presidential Elections of 2016 and 2020, among others (Hall Jamielson, 2020).

Russia's investment into information had been successful, yet things changed in 2022. As it launched a full-scale invasion of Ukraine, it experienced difficulties not only waging a conventional war, but also controlling the information space outside of Russia (Treverton, 2022). While Russian cyberwarfare remains a strong force and keeps targeting different

organisations and institutions via malware and other tools, Ukraine's approach to the cyberwar is unprecedented given that it relies strongly on volunteers and horizontal networks of digital experts from across the world who cooperate with the Ukrainian government while also leading independent information campaigns.

Russia's Hybrid Warfare Against Ukraine

Ukraine has been a target of Russian unconventional warfare since at least the early 2000s. it has been targeted in the religious sphere by the Russian Orthodox Church and economically through trade wars with Russia. As early as in 2000s, after Ukrainians elected a pro-EU and pro-NATO President, Russia stopped sending its gas through the pipeline in Ukraine which delivered energy to Europe. Russian media and authorities immediately accused Ukraine of stealing gas. Despite rebuffs from the Ukrainian side, the Russian narrative was largely accepted in Europe (Nuryyev et al., 2021). Russia also banned Ukrainian imports, openly supported pro-Russian political candidates, and funded pro-Russian groups within Ukraine. Similar activities followed throughout the 2000s until Ukrainians elected a pro-Russian candidate as President in 2010.

Cyberattacks

Russia has been using cyberattacks against various governments in order to disrupt their activities or prevent them from going forward with the policies that the Russian authorities considered anti-Russian. It carried out cyberattacks in combination with conventional military force – as in cases of Georgia and Ukraine, and as stand-alone practices against other countries during peacetime. The aim of the cyberattacks is to disrupt the information systems and manipulate or steal data using computer networks as a main weapon (Burkadze, 2022).

In 2007, for instance, Russia launched a mass cyberattack on Estonia when the Estonian government decided to move a Soviet-era monument from the city centre to a less prominent place (Odoh, 2021). The attack targeted websites of state organisations, media, and banks, generating a mass denial of service for the users. Alongside this, spamming campaigns were carried out such as flooding news websites with pro-Russian commentaries. Russia also interfered in the US 2016 and 2020 presidential elections by supporting Russia-friendly candidate Donald Trump and undermining his opponents in both the Republican and Democrat parties. Russia's troll farms—a hired army of social media influencers—discredited Trump's rival candidates on social media and promoted conspiracy theories related to the election (Lee, 2018). Russia also launched cyberattacks and surveillance campaigns across the EU member states to track government officials and cause disruption. For example, Russian hackers with links to the military infiltrated and spied on energy and military organisations across the EU (Lyngaas, 2023).

Ukraine has been a key target of Russia's cyberattacks since 2014 as a part of Russia's hybrid warfare. On March 13, 2014, Russia launched its major Distributed Denial of Service (DDoS) cyberattack on Ukraine's communications infrastructure only three days before Russia's so-called referendum for illegal annexation of Crimean peninsula. The attack attempted to

overwhelm Ukraine's digital platforms with fake traffic. Two months later, Russian hackers launched cyberattacks against Ukraine's election committee in the wake of Ukraine's presidential elections. The attempt failed, and the hackers were not able to change the election results, but they slowed down the counting process. Russia continued with regular cyberattacks on Ukraine's power grid, call centres, and energy infrastructure companies. For instance, more than 230,000 residents of Western Ukraine were without power for up to six hours on December 23, 2015 as a result of a Russian cyberattack on energy infrastructure. Russians continued with cyberattacks on electrical substations provoking short-term power outages across the country although they could not disable the equipment or generate a lasting impact (Przetacznik & Tarpova, 2022).

In June 2017, Ukraine experienced its most severe cyberattack. Russia's malware targeted Chernobyl nuclear plant and managed to shut down around 13 thousand devices of Ukraine's transport, financial, and communication infrastructure. The cyberattack also prompted the destruction of all the data on the affected devices; the data could not be restored afterward. The cyberattack went beyond Ukraine; it targeted companies in the EU and the US such as FedEx and Maersk causing damages of more than $10 billion (Armour et al., 2022). In 2021, Russia also targeted Ukraine's security services and government digital platforms; the cyberattack had limited success in causing temporary damage to the systems.

Prior to the full-scale invasion, Russia intensified its cyberattacks. In mid-January of 2022, hackers gained temporary control over the websites of Ukraine's Cabinet of Ministers, Ministries of Foreign Affairs, Education and Science, and Defense in addition to about 60 more state-run websites. A week before the invasion, Russia carried out another attack against government websites, media, and financial institutions. It did that again on February 23, a day before the full-scale invasion, while also attempting to destroy data of about 100 organisations in finance, IT, and aviation (Serpanos & Komninos, 2022).

The attacks continued throughout the full-scale invasion with a similar strategy of targeting state-led digital platforms, wiping data, and attacking infrastructure to cause communication and energy outages. Russia also increased its reliance on fake news and deep fakes; for instance, it circulated a deep fake video of Ukraine's President Volodymyr Zelenskyi announcing Ukraine's surrender (Scott, 2022). Other activities included phishing emails, surveillance, and hacking citizens' banking and other personal data from government platforms. Power stations, postal services, and other infrastructure elements were also targeted. Often, cyberattacks matched in time with military attacks such as massive missile attacks on Ukraine (Schroeder & Dack, 2023).

"Useful Idiots" in information warfare

A key feature of Russia's information warfare is its use of so-called "useful idiots." The term "useful idiots" describes a person spreading false propaganda without understanding how they are being deceived and used by a political actor. Russia uses marginalized or extremist voices in Western societies to repeat Russian propaganda and tailor it for domestic audiences based on the public sentiments in different countries. Relevant investigations across Europe showcased that Russia financed groups of journalists, politicians, and political analysts to promote Russia-friendly theories and messages for European audiences

(Hall Jamieson, 2020). Similarly, Russia has been investing heavily into the pro-Russian lobby in the US. In regions like Latin America and Africa, Russian media narratives and overall Russian information presence have emphasised anti-European or anti-imperialist sentiments (Van Herpen, 2015; Jankowicz, 2020).

Russian troll factories are active across the globe. Russian agents create profiles that imitate real people and post Russia-friendly comments and stories in various local languages. These trolls use a common tactic. They craft narratives that aim to "divide and conquer" by emphasising the divisions within target societies and creating more social tensions and conflicts. This strategy intends to diminish support for national authorities and change public perceptions toward Russia. A recent example of Russia's information warfare is the use of trolls and fake news during the US mid-terms elections as well as spreading pro-Kremlin rhetoric through extreme left and right channels in the US, thus presenting Ukraine as a warmongering state (Dutkiewicz & Stecula, 2022).

Ukraine's Response After February 24, 2022

Framing the invasion

Prior to Russia's full-scale invasion, Ukraine-Russia relations were mostly framed through the Russian perspective. For instance, Russia's "narrative warfare" has been used to justify the Crimean annexation and war in Donbas in 2014. Russia's narrative of this invasion emphasised false claims that Ukrainians were part of the Russian nation (Aleksejeva, 2022). Given that Russian media channels were well-known across the world, Russia used assertive and often aggressive rhetoric to push fake news and conspiracy theories about Ukraine; these messages were often repeated without due verification by Western and other international outlets.

Ukraine opted for communicating its message with a different strategy. It reached out to a few Western journalists and organised several public events in the EU and beyond. The approach brought limited successes given that the Russian view on the Donbas war, Crimea, and Ukraine was still more widely cited abroad.

In 2022, Ukraine increased its attention to strategic communications to ensure its message reached other countries. The first key step Ukraine took was to shift the narrative from the Russian messaging to Ukraine's perspective through emotionally-charged, empathic language strategically communicated via social media.

As Russia prepared and carried out a military invasion of Ukraine, Russian propaganda attempted to portray Ukraine as a corrupt, failed state, ruled by a Nazi-friendly government in an attempt to justify its invasion. Ukraine's communication strategy countered that narrative to show Ukraine as a democratic, modern, and free country. Ukraine's President Volodymyr Zelenskyi, a Jewish Ukrainian who grew up in a Russian-speaking household, used social media to communicate with live, people-oriented, emphatic appeals that gathered sympathy and humanized Ukraine and Ukrainians. A former actor, Zelenskyi amassed a massive following on Instagram, Telegram, and Twitter, and used his personal

communication channels to update followers across the world on the situation in Ukraine and present his country as a resilient nation.

Instead of traditional formal messages by the government officials, Zelenskyi recorded public messages in a military bunker in Kyiv, visiting the frontlines in the East, or standing next to destroyed Russian missiles. He aimed his messages at Ukrainians and also the world, with pleas for the need to help Ukraine. His messages combined verified information and explanations with highly emotional, personalized language and were successful in gathering large audiences from different parts of the world (Butler, 2022). Unlike Russian propaganda, Zelenskyi and Ukraine's communication campaign was able to humanize the messages presented on the war and turn the leadership of Ukraine into digital influencers carrying out strategic communication campaigns. For instance, Zelenskyi has been appealing to influential people across different sectors by having online appearances during cultural and sports events such as Golden Globes or Cannes Film Festival. He also simplified his language and used humour such as suggesting that Russian soldiers can steal all the toilets they want in Ukraine as long as they leave the country.

Ukraine's peace messaging

Ukraine was able to use its new powers in the digital space to push for peace-related narratives that countered Russian messaging. Ukraine's main message is that peace is only possible when Ukraine is represented and listened to, and when Russia complies with humanitarian and human rights law, pays reparations, and is significantly punished for its illegal invasion. This messaging differs greatly from the narrative pushed by the Kremlin that peace is possible when Ukraine gives up more of its territories and agrees to the demands set by the Russian government (McInnis et al., 2022).

Ukraine used digital spaces to successful debunk Russian disinformation that Ukrainians are Nazis and the government is corrupt and a failed state. Ukraine communicated to both Western and domestic audiences to showcase how Russia's view on peace and ceasefire was doomed to fail as it did not guarantee any justice or any sustainable end to the hostilities. More importantly, Ukraine's success in digital warfare enabled it to become a subject in the discussions instead of being a mere object as it was during the 2014 War in Donbas negotiations when Russia also employed information warfare to undermine trust in Ukraine and justify its aggression (Osadchuk, 2022).

Another aspect of Russian propaganda argues that the Russian full-scale war is not against Ukraine, but NATO. Ukraine debunked this messaging by tracking arm sales and demonstrating how the arms were used. Foreign analysts found no evidence of arms misuse ("US finds …", 2022).

To debunk Nazi myths, Ukraine intensified many diverse voices within the country such as Ukraine's Jewish community, other ethnic and religious groups, and the Russian-speaking population. Further, Ukraine did not only debunk the statements from the Russian side, but started building its own messaging and mythology regarding the war and Ukraine's identity. These include the international communication campaigns United 24, digital and offline exhibits, classes, and events on Ukraine's history, language, culture, and present realities;

promotion of Ukraine-specific imagery and slogans such as "Be brave like Ukraine" or "Freedom is our Religion" and so on. By investing and encouraging more online discussions on Ukraine in the digital space, Ukraine was able to keep the momentum going as well as attract a significant number of pro-Ukrainian voices who inform about the country in a transparent way which is critical of the Kremlin.

Ukraine created emphatic messaging to counter the top-to-bottom Russian state media narrative. Similarly, Ukraine's state social media pages—such as pages of the Ministry of Defense, the state of Ukraine, or prominent Ukrainian politicians—are heavily reliant on direct communication, humour, and pointing out the fallacies in Russian messaging to showcase how the Russian view of the invasion is false and manipulative (Scott, 2022).

Digital warfare, ironically, allowed Ukraine to decolonize online spaces by becoming more present, effectively countering Russian-led misinformation and attacks, and creating its own image and narrative. Furthermore, Ukraine's successful hybrid warfare allowed it to minimise the impact of Russian propaganda and manipulations although Russia still remains a major player in cyberattacks and hybrid warfare.

Isolating Russia

An important step in isolating Russia's propaganda was uncovering the networks of Russia-funded lobbyists and politicians in such countries as Italy, Bulgaria, and Austria among others (Nabozhniak, 2022; von Daniels et al., 2022). While investigations into the illicit financing helped decrease the influence of "useful idiots", Ukraine also attempted to undermine Russian influence in the digital world by isolating and cutting Russian tech from the rest of the world. In the beginning of the full-scale invasion, Ukraine's Minister of Digital Transformation, Mykhaylo Fedorov, launched a campaign to facilitate Russia's "digital blockade" and encourage Western companies to leave Russia (Scott, 2022). Such companies as Juniper Networks, Apple, Visa, MasterCard, and Netflix have exited the country although major companies remained (Goode, 2022). For example, Google is still operational in Russia although heavily censored by the Russian state (Sauer, 2022). In 2022, Russia banned some companies such as Meta's social media platforms Facebook and Instagram (Sauer, 2022).

Ukraine continues to encourage Western companies to cut ties with Russia. In addition to the direct economic impact, another goal of this campaign is to limit Russia's access to Western technologies by discouraging Western communication and tech companies from operating, investing, or doing research and development in Russia. More than 1300 companies have exited Russia so far. Major Russian communication companies and media such as RT and Sputnik have been banned in different regions of the world thanks to Ukraine's efforts (Linnane, 2022). Due to Western sanctions, Russia's ability to get a hold of Western technology is also limited.

Some tech companies have been reluctant to leave Russia; they include Siemens, Vimeo, Patreon, and Microsoft (Pylypenko, 2022; Rogers, 2023). This has limited Ukraine's ability to isolate Russia in the cyber space. At the same time, a government-initiated campaign has created a precedent of mass boycott of Russia by Western companies. While some companies chose to stay and still operate within Russia, they significantly reduced their

investment, cut advertisements, and no longer provide updates to customers in Russia (Linnane, 2022). Ukraine's lobbying campaign to isolate Russia continues, and more companies such as Siemens, SAP, and Lumen have joined in the last few months.

Ukraine's IT Army hacktivism and open-source investigations

As a follow up to his "digital blockade" strategy, Ukrainian Minister Fedorov also launched an IT Army, a digital volunteer movement that now consists of approximately 100,000 people ("Ukraine's 'IT Army'…", 2022). These are digital volunteers, computer scientists and hackers from Ukraine and abroad, whose job is to help Ukraine win the war with Russia through digital means. The IT Army launches cyberattacks against Russian state media and other websites run by the Kremlin. In addition, the hackers and investigative journalists have been able to retrieve sensitive data on Russian soldiers fighting in Ukraine and share it with the rest of the world. This allows for further investigation of the activities of the soldiers many of which are linked to war crimes; these practices violate international practices of data protection. This data may be used for future investigations and international war tribunals. Furthermore, Ukraine's IT Army is working toward strengthening Ukraine's capacity for protecting itself from Russian cyberattacks and increasing the security of Ukraine's digital infrastructure. According to Western military experts, Ukraine significantly improved its resistance to Russian cyber threats and has undergone "a real revolution by moving upmarket in its defensive cyber fight" (Basso, 2023).

In addition, Ukraine has partnered with tech companies such as Clearview and Palantir which provide AI-driven solutions to the issues of identification and decision-making on the ground at the front line (Scott, 2022). Through the partnership with these companies, Ukraine's Armed Forces use facial recognition software and can access large amounts of social media data from images taken from Russia's social media platform that purports to identify soldiers from Russia as well as to match criminals with their identities which can be further used for war tribunals (Lonas, 2022). Once the identities of fallen soldiers are confirmed, Ukraine's IT Army informs the soldiers' relatives about the death of the soldier. The rationale for using this technology is twofold. First, Ukraine asserts that the Russian Ministry of Defense was hiding information related to soldier deaths from families. Second, the goal was to diminish the morale of Russian troops on the ground and Russians within Russia. It should be noted that Western civil rights organisations opposed to the use of any facial recognition criticised Ukraine's adoption of Clearview, citing the possibility of misidentification (Paresh, 2022).

Ukraine's Armed Forces also established digital initiatives to encourage Russian soldiers to surrender. There are Ukrainian drones on the front line that can be used by Russian soldiers to ask for surrender and receive the protections guaranteed by the Geneva Convention relative to the Treatment of Prisoners of War. In addition, Ukraine established digital platforms and chatbots to provide simple ways for Russian soldiers to surrender (Rashid, 2022; Jankowicz, 2022).

Furthermore, open-source data has been instrumental in debunking Russia's fake news and strengthening Ukraine's narrative on the ongoing war. For example, open-source data allowed investigative journalists to debunk various statements from the Russian Ministry of

Defense claiming they destroyed Ukraine's ammunition depots, soldiers' barracks, or killed a significant number of Ukrainian troops (Melkozerova, 2023). In addition, using open-source data allowed researchers to gather evidence of Russians being trained by Iranian instructors on how to operate Iran-made drones; and then, thanks to open-source videos, investigators were able to reveal the identities of Russian operators. Open-source data has been crucial in providing evidence to document allegations of the crimes committed by the Russian army in Bucha, Borodyanka, and other liberated territories of Ukraine. It is being actively employed now as the war continues to help geolocate Russian troops, confirm statements on the important battles, and discover the locations from which missiles are being launched against Ukraine.

Digital elves and the NAFO movement

In addition to Ukraine's IT army, it also has its own army of elves. Elves are pro-Ukrainian digital users who fight Russian trolls, politicians, and media personalities in the online space. Online elves is an international phenomenon which originated in Lithuania as digital activists organised themselves to debunk Russia's narratives and oppose Russian trolls in the digital space (Nordstrom, 2022). The 2022 Russian invasion of Ukraine strengthened the movement and led to the formation of more digital communities fighting the Kremlin narratives. The most prominent group is called NAFO, or the North Atlantic Fellas Organization, which consists of volunteers mocking Russian propaganda online and raising awareness of Russian crimes in Ukraine. While there is no official estimate of the number of NAFO members, the number can vary from tens of thousands to hundreds of thousands (Braun, 2022). According to Tobias Fella, a German political scientist working with soldiers on the usage of social media, NAFO is a Western civil society response to Russian campaigns that is participating in a "battle for sovereignty of interpretation" in digital spaces (Neuhann, 2022). NAFO has a loose horizontal structure with its members located across the world. The NAFO movement uses English and delivers content that is easily understood by users in the US, Europe, and other parts of the Western world and beyond.

NAFO volunteers directly engage with government officials, civil society, and the media to increase the momentum for support to Ukraine. NAFO uses memes, jokes, and other creative means to generate discussions on topics related to Ukraine. Some battle "whataboutism" which diverts attention away from the Russian invasion by asking questions such as "What about the US invasion of Iraq?" so that Russia's role as an aggressor is minimised. Other NAFO fellows mock fallacies and illogical arguments of the Russian and pro-Russian commentators. For instance, NAFO volunteers have been able to engage in Twitter discussions with some Russian ambassadors and mock their propaganda (Braun, 2022; Smart, 2022). The NAFO movement also raised a few million US dollars for humanitarian aid and weapons to Ukraine, and remains an active digital force (McInnis et al., 2022).The movement has been recognised by Ukraine's Minister of Defense Oleksiy Reznikov, leaders in the West such as United States Representative Adam Kinzinger, United States Army Major General Patrick J. Donahoe, former Estonian President Toomas Hendrik Ilves, current Estonian Prime Minister Kaja Kallas, and Lithuanian Minister of Foreign Affairs Gabrielius Landsbergis (Michaels, 2022).

In addition to NAFO, Ukrainian voices on Twitter received significant support from Western followers. Media personalities, journalists, and influencers are creating shared Ukrainian spaces where they explain Russian colonialism, Ukraine's history, and crucial aspects of the invasion that could be misunderstood by the people who lack significant background knowledge on Ukraine or Russia. Ukraine's state organisations such as the Ministry of Defense or Ministry of Digital Transformation are also sharing easy-to-follow content with visuals, explainers, and memes in English and other languages to appeal to other audiences thus creating direct channels for communication with foreign audiences.

Ways Forward

Ukraine's digital response to the 2022 Russian full-scale invasion and hybrid warfare has been well-received domestically and internationally. Unlike the 2014 Russian war in Donbas when Ukraine's messaging was largely overlooked, Ukraine's communication approach in the 2022 war allowed the country to improve its digital media representation and use Russia's tactics against the opponent. In many Western countries, Ukraine has been able to control the narrative and frame the invasion according to Ukraine's perspective thus significantly reducing the influence of Russian propaganda. Through the usage of social movements, digital volunteers, and IT experts' contributions, Ukraine was also able to achieve significant representation in the digital space as well as target Russia and pro-Russian fake news channels and psyops using its own methods.

This, however, does not mean that Ukraine's efforts in the digital space have fully achieved their purpose. While Ukraine's narrative dominates the Western media space, it has not reached the same level of publicity and support in African, Latin American, and Asian countries where the Russian media presence is still dominant (Brands, 2022). In addition, Ukraine remains vulnerable to Russian cyberattacks even though it now has the capacity to launch attacks in response (Rashid, 2022). Furthermore, when it comes to counternarratives from the Russian side, these are constantly supported by various extreme groups across the world; this means that Ukraine's information campaigns need to continue to counteract these actions.

Thus, an important step forward is to expand Ukraine's communication outreach to the audiences and regions where Russian propaganda remains dominant. This would require allocating more resources such as messaging in local languages, creating content that would appeal to the locals, and researching historical, cultural, and political parallels that could be used to humanize and simplify the Russo-Ukrainian war and Ukraine in general to new foreign audiences. This would also mean looking for digital influencers and activists who can appeal to the locals.

Another crucial step is protecting Ukraine domestically from cyberwarfare as well as information warfare. This can be done by strengthening cooperation that the Ukrainian government has already established with technological companies and other governments in the cyber space. Ukraine needs to increase its data sharing with other international agencies while also reinforcing the security of its state platforms and critical infrastructure from Russian cyberattacks. Additionally, Ukraine needs to increase its outreach to

Ukrainians under Russian occupation as they have limited access to Ukraine's media. Russia is blocking access to non-Russian information sources in every region they occupy. This is especially important for places that have been in an information vacuum, and where the locals lack verified information on the reality in Ukraine.

Further, Ukraine needs to monitor and respond to the feedback it receives from foreign audiences regarding its messaging. While empathy and support for Ukraine were very high in the beginning of the full-scale invasion, there is an increased risk of "Ukrainian fatigue" as foreigners tire of news about Ukraine. Therefore, messaging needs to be balanced and strategic, and appear in digital and offline spaces to reach key audiences.

Supporting Ukrainian narratives for democracy and self-determination requires a robust digital presence to reach groups which have lacked representation in the past, and which have found their space through meaningful online participation (Jankowicz, 2020). Digital presence requires a large number of volunteers with different types of skills; but it showcases that even organisations and communities which lack major resources can pose a significant threat to autocracies when they use digital media and tools to promote democracy and liberal values. To further strengthen this strategy, Ukraine needs to keep on involving diverse and marginalized voices that represent the country, and that often originate from grassroots initiatives. For example, it can encourage citizen-led digital archives or platforms that talk about Ukraine's diversity, ethnicities, and perceptions on race to debunk propaganda, create a more positive and multidimensional image of itself, and raise awareness on the current events and of Ukraine as a whole.

Ukraine's IT army of supporters both within the country and outside of it, shows that through direct communication, use of popular language, and horizontal networks of volunteers, it is possible to challenge the digital Goliath and become a major force in the hybrid warfare – yet use it for promotion of peace, sovereignty, and international rule of law. Ukraine's Ministry of Digital Infrastructure should continue its cooperation with Ukraine's IT Army, encourage more volunteers to join, and push for more sanctions on Russia's tech sector to decrease its capacity to cause Ukraine and the rest of the world digital harm.

Ukraine should continue to use the digital sphere to advance understanding about Ukraine. This is an important element in its defence against Russian information warfare. The country has already started launching digital content—cartoons, shows, online exhibitions, and virtual meetups—to attract more attention to Ukraine and promote a positive image of Ukraine as well as explain what Ukraine is and what it is not. If Ukraine manages to keep the momentum, better protect its digital infrastructure, and reach new audiences, it may be able to win the information war and spread its message on peace and the end of the invasion for greater impact.

References

Aleksejeva, N. (2022). Narrative Warfare. *Atlantic Council.* Retrieved from https://www.atlanticcouncil.org/in-depth-research-reports/report/narrative-warfare/

Armour, P.G., Berghel, H., Charette, R.N., and King, J.L. (2022). Ukraine Aftershocks. *Computer,* 55 (11), 85-93.

Backes, O., and Swab, A. (2019). Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States. *Belfer Center for Science and International Affairs.* Retrieved from https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states

Basso, D. (January 13, 2023). French army hails Ukraine's cyber defence 'revolution'. *Euractiv.* Retrieved from https://www.euractiv.com/section/politics/news/french-army-hails-ukraines-cyber-defence-revolution/

Braun, S. (September 17, 2022). Ukraine's info warriors battling Russian trolls. *DW.* Retrieved from https://www.dw.com/en/nafo-ukraines-info-warriors-battling-russian-trolls/a-63124443

Burkadze, K. (2022). International legal definition of a cyberattack. *Journal Iusticia*, 2 (2), 74-82.

Butler, M. (May 12, 2022). Ukraine's information war is winning hearts and minds in the West. *The Conversation.* Retrieved from https://theconversation.com/ukraines-information-war-is-winning-hearts-and-minds-in-the-west-181892

Dutkiewicz, J., and Stecula, D. (July 4, 2022). Why America's Far Right and Far Left Have Aligned Against Helping Ukraine. *Foreign Policy.* Retrieved from https://foreignpolicy.com/2022/07/04/us-politics-ukraine-russia-far-right-left-progressive-horseshoe-theory/

Goode, L. (March 1, 2022). Apple Stops Sales in Russia—and Takes a Rare Stand. *Wired.* Retrieved from https://www.wired.com/story/apple-russia-iphone-ukraine-traffic-maps-rt-sputnik-app-store/

Hall Jamieson, K. (2020). *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know.* Oxford University Press.

Lee, David. (February 18, 2018). The Tactics of a Russian Troll Farm. *BBC*. Retrieved from https://www.bbc.com/news/technology-43093390

Linnane, C. (June 8, 2022). Companies that exited Russia after its invasion of Ukraine are being rewarded with outsize stock-market returns, Yale study finds — and those that stayed are not. *Market Watch*. Retrieved from https://www.marketwatch.com/story/companies-that-exited-russia-after-its-invasion-of-ukraine-are-being-rewarded-with-outsize-stock-market-returns-and-those-that-stayed-are-not-11654258241

Lonas, L. (April 15, 2022). Ukraine has used facial recognition tech to notify hundreds of Russian families of dead soldiers: report. *The Hill.* Retrieved from https://thehill.com/policy/international/3269911-ukraine-has-used-facial-recognition-tech-to-notify-hundreds-of-russian-families-of-dead-soldiers-report/

Lyngaas, S. (March 15, 2023). Russian hackers targeted European military and transport organizations in newly discovered spying campaign. *CNN.* Retrieved from https://edition.cnn.com/2023/03/15/politics/russian-hackers-europe-military-organizations-microsoft/index.html

McInnis, K., Jones, S.G., and Harding, E. (October 5, 2022). NAFO and Winning the Information War: Lessons Learned from Ukraine. *CSIS.* Retrieved from

https://www.csis.org/analysis/nafo-and-winning-information-war-lessons-learned-ukraine

Melkozerova, V. (January 9, 2023). Russian claims of revenge attack on Ukraine debunked. *Politico.* Retrieved from https://www.politico.eu/article/russian-claims-of-revenge-attack-on-ukraine-kramatorsk-debunked-war/

Michaels, D. (September 22, 2022). Ukraine's Internet Army of 'NAFO Fellas' Fights Russian Trolls and Rewards Donors With Dogs. *The Wall Street Journal.* Retrieved from https://www.wsj.com/articles/ukraines-internet-army-of-nafo-fellas-fights-russian-trolls-and-rewards-donors-with-dogs-11664271002

Min-seok, K. (December 11, 2022). Learning from Ukraine's cyber defense. *Korea Daily.* Retrieved from https://koreajoongangdaily.joins.com/2022/12/11/opinion/columns/Ukraine-Russia-cyberwarfare/20221211194959487.html

Nabozhniak, O. (December 1, 2022). The germs of the Russian world. *Texty.* Retrieved from https://texty.org.ua/projects/108323/germs-russian-world-who-supports-russia-europe/

Neuhann, F. (September 4, 2022). Die westliche Antwort auf Putin-Trolle. *ZDF.* Retrieved from https://www.zdf.de/nachrichten/politik/nafo-meme-internet-trolle-ukraine-krieg-russland-100.html

Nordstrom, L. (January 23, 2022). 'We're at war': The 'Lithuanian Elves' who take on Russian trolls online. *France24.* Retrieved from https://www.france24.com/en/europe/20220123-we-re-at-war-the-lithuanian-elves-who-take-on-russian-trolls-online

Nuryyev G, Korol T, and Tetin I. (2021). Hold-Up Problems in International Gas Trade: A Case Study. *Energies,* 14(16), 1-16.

Odoh, E. M. (2021). Cyber Attack as a Tool to Influence Foreign Policy: A Comparative Study of Russia's Cyber-Attacks on Estonia and Georgia. *University of Nigeria Journal of Political Economy*, 11(1), 1-13.

Omelicheva, M. (November 14, 2022). United We Stand (With Russia)? How Moscow's Soft Power Shaped Views on the War. *PONARS Eurasia.* Retrieved from https://www.ponarseurasia.org/united-we-stand-with-russia-how-moscows-soft-power-shaped-views-on-the-war/

Osadchuk, R. (2022). Undermining Ukraine. *Atlantic Council.* Retrieved from https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine/

Paresh, Dave. (March 24, 2022). Ukraine uses facial recognition to identify dead Russian soldiers, minister says. *Reuters.* Retrieved from https://www.reuters.com/technology/ukraine-uses-facial-recognition-identify-dead-russian-soldiers-minister-says-2022-03-23/

Polianska, I. (September 2, 2022). A history of defamation: Key Russian narratives on Ukrainian sovereignty. *EU vs. Disinfo.* Retrieved from https://euvsdisinfo.eu/a-history-of-defamation-key-russian-narratives-on-ukrainian-sovereignty-2/

Przetacznik, J., and Tarpova, S. (2022). Russia's war on Ukraine: Timeline of cyber-attacks. *European Parliamentary Research Service*. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

Pylypenko, Y. (October 13, 2022). International Businesses Leaving Russian Market: Is There Progress? *Vox Ukraine.* Retrieved from https://voxukraine.org/en/international-businesses-leaving-russian-market-is-there-progress/

Rashid, H. (December 7, 2022). IT Army of Ukraine Hit Russian Banking Giant with Crippling DDoS Attack. *Hack Read.* Retrieved from https://www.hackread.com/it-army-of-ukraine-russia-bank-ddos-attack/

Rogers, J. (January 7, 2023). Moral Rating Agency slams Western companies, including Microsoft and Nestlé, over alleged supply of products to Russia. *Market Watch.* Retrieved from https://www.marketwatch.com/story/moral-rating-agency-slams-western-companies-including-microsoft-and-nestle-over-alleged-supply-of-products-to-russia-11673016382

Sauer, P. (March 21, 2022). Russia bans Facebook and Instagram under 'extremism' law. *The Guardian.* Retrieved from https://www.theguardian.com/world/2022/mar/21/russia-bans-facebook-and-instagram-under-extremism-law

Scott, M. (August 24, 2022). How Ukraine used Russia's digital playbook against the Kremlin. *Politico.* Retrieved from https://www.politico.eu/article/ukraine-russia-digital-playbook-war/

Schroeder, E., and Dack, S. (2023). A parallel terrain: Public-private defense of the Ukrainian information environment. *Atlantic Council.* Retrieved from https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment/

Serpanos, D., and Komninos, T. (2022). The Cyberwarfare in Ukraine. *Computer*, 55 (7), 88-91.

Smart, J.J. (Novembr 14, 2022). Founder of NAFO Reveals Identity, Discusses Raison D'être. *Kyiv Post.* Retrieved from https://www.kyivpost.com/russias-war/founder-of-nafo-reveals-identity-discusses-raison-detre.html

Treverton, G.E. (2022). Will the Ukraine War Reshape the Internet? *CSIS.* Retrieved from https://www.csis.org/analysis/will-ukraine-war-reshape-internet

"Ukraine's 'IT Army' Stops 1,300 Cyberattacks in 8 Months of War" (November 16, 2022). *Dark Reading*. Retrived from https://www.darkreading.com/endpoint/ukraine-it-army-stops-1300-cyberattacks-war

"US finds no signs of weapons falling into wrong hands in Ukraine" (December 13, 2022). *Ukrayinska Pravda.* Retrieved from https://www.pravda.com.ua/eng/news/2022/12/13/7380625/

Van Herpen, M. H. (2015). *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy.* Rowman & Littlefield.

Von Daniels, J., Joeres, A., and Richter, F. (2022). The Gazprom Lobby. *Correctiv.* Retrieved from https://correctiv.org/en/latest-stories/2022/10/07/gazprom-lobby-germany/

Jankowicz, M. (December 13, 2022). Ukrainian army issues instructional video telling Russians how to surrender to a drone. *Insider.* Retrieved from https://www.businessinsider.com/ukraine-army-video-tells-russians-how-to-surrender-to-drone-2022-12

Jankowicz, N. (2020). *How to Lose the Information War: Russia, Fake News, and the Future of Conflict.* Bloomberg Publishing.

Yablokov, I. (December 6, 2022). Russia's recently exiled media learn hard lessons abroad.*Open Democracy.* Retrieved from https://www.opendemocracy.net/en/odr/russia-independent-media-exile-problems-tvrain/

The Author

Anna Romandash is a multi-award-winning journalist and researcher from Ukraine. She has extensive experience working across Eastern Europe and Central Asia where she studies democratization processes, freedom movements, and human rights policymaking. Romandash has written substantially on Belarus and Russia's dictatorships, Ukraine-EU relations, and Europe's security architecture. Her areas of interest include international security and media development in fragile contexts. Romandash is the Fourth Freedom Forum's first Howard S. Brembeck Fellow, a Research Affiliate at the Mgrublian Center for Human Rights at Claremont McKenna College, and a digital scholar at Vassar College. She holds an MGA degree from the Keough School of Global Affairs at the University of Notre Dame, and a MA in Communications from Ukrainian Catholic University.

Toda Peace Institute

The **Toda Peace Institute** is an independent, nonpartisan institute committed to advancing a more just and peaceful world through policy-oriented peace research and practice. The Institute commissions evidence-based research, convenes multi-track and multi-disciplinary problem-solving workshops and seminars, and promotes dialogue across ethnic, cultural, religious and political divides. It catalyses practical, policy-oriented conversations between theoretical experts, practitioners, policymakers and civil society leaders in order to discern innovative and creative solutions to the major problems confronting the world in the twenty-first century (see www.toda.org for more information).

Contact Us
Toda Peace Institute
Samon Eleven Bldg. 5th Floor
3-1 Samon-cho, Shinjuku-ku, Tokyo 160-0017, Japan
Email: contact@toda.org

Sign up for the Toda Peace Institute mailing list:
https://toda.org/policy-briefs-and-resources/email-newsletter.html

Connect with us on the following media.
YouTube:@todapeaceinstitute3917
Twitter: https://twitter.com/TodaInstitute
Facebook: https://www.facebook.com/TodaInstitute/