

The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine

 [mandiant.com/resources/information-operations-surrounding-ukraine](https://www.mandiant.com/resources/information-operations-surrounding-ukraine)

The recent phase of Russian aggression toward Ukraine, manifested by Russia’s full-scale invasion, has flooded the information environment with disinformation promoted by a full spectrum of actors. Concerted information operations have proliferated, ranging from cyber-enabled information operations, including those that coincided with disruptive and destructive cyber threat activity, to campaigns leveraging coordinated and inauthentic networks of accounts to promote fabricated content and desired narratives across various social media platforms, websites, and forums.

While the full extent of this activity has yet to be seen, more than two months after the start of the invasion, Mandiant has identified activity that we attributed to information operations campaigns conducted by actors we judge to be operating in support of the political interests of nation-states such as Russia, Belarus, China, and Iran, including ongoing campaigns that we have tracked for years. This report examines a slice of this activity, highlighting significant information operations Mandiant has observed in our work responding to the invasion and presenting our early analysis of those events.

Information Operations Aligned with Russian Interests Concurrent with Disruptive and Destructive Cyber Threat Activity

Mandiant identified information operations aligned with Russian political interests that occurred concurrently with disruptive and destructive, likely Russian sponsored cyber threat activity in the weeks immediately preceding and following the start of the invasion, including incidents involving the deployment of wiper malware disguised as ransomware (Table 1). Cyber-enabled information operations by nature require access to diverse skillsets to support different operational components, which varies based on the complexity of the operation. While we cannot link these operations to the concurrent disruptive and destructive activity, this limited pattern of overlap may suggest that some of the actors behind information operations observed in this conflict are linked to groups with extensive capabilities.

Date	Information Operation	Concurrent Disruptive and Destructive Activity
-------------	------------------------------	---




Jan. 14, 2022	Multiple Ukrainian government websites, including that of the Ministry of Foreign Affairs, were defaced with a message in Russian, Ukrainian, and Polish claiming that data had been deleted from government servers and would be released.	The defacements likely coincided with the January deployment of destructive tools <u>PAYWIPE</u> , an MBR wiper disguised as ransomware, and the <u>SHADYLOOK</u> file corrupter against Ukrainian government and other targets.
Feb. 23, 2022	Dozens of Ukrainian government websites were defaced with the same image displayed in the Jan. 14 incident.	This incident coincided with destructive attacks against Ukrainian government targets using the <u>NEARMISS</u> master boot record (MBR) wiper and <u>PARTYTICKET</u> wiper disguised as ransomware.
March 16, 2022	An information operation targeting Ukraine promoted a fabricated message alleging Ukraine's surrender to Russia via the suspected compromise and defacement of the Ukraine 24 website and news ticker in a Ukraine 24 TV broadcast with a written message, as well as via an artificial intelligence (AI)-generated "deepfake" video impersonating Ukrainian President Zelenskyy delivering that same text.	On the same day, Mandiant identified the <u>JUNKMAIL</u> wiper targeting a Ukrainian organization. The malware was configured via a scheduled task to execute approximately three hours before Zelenskyy was scheduled to deliver a speech to the U.S. Congress.

Table 1: Significant information operations that occurred concurrent with other disruptive or destructive cyber threat activity

Russian and Belarusian Information Operations Include Cyber-Enabled Operations, Use of Established Assets

Russian and Belarusian information operations actors and campaigns, including those that have historically been linked to cyber threat activity such as hack-and-leak operations, have engaged in activity surrounding the invasion that is consistent with their previously established motives. Their use of developed campaign infrastructure, including in some instances the refocusing of established assets, demonstrates how years-long efforts of Russian, pro-Russian, and Belarusian information operations targeting Ukraine and the broader region have been leveraged to address emerging security interests. In addition to known campaigns, we have also identified information operations activity promoting pro-Russian content on the invasion that we have not attributed to a previously observed campaign or actor.

OBSERVED RUSSIA-ALIGNED IO ACTIVITY SURROUNDING THE INVASION OF UKRAINE

	Networks and Personas	Secondary Infektion	NDP	Ghostwriter	IRA (Cyber Front Z, alleged)
	"News Outlets"	NDP	Covert News Outlets Operated by SVR, GRU & FSB		
	Telegram	GRU-Run Telegram Channels	IRA (Cyber Front Z)	Russia-aligned Hactivist Groups	NDP
	Cyber-Enabled IO	UNC1151/Ghostwriter	Russia-aligned Hactivist Groups		

MANDIANT

Figure 1: Vectors leveraged by identified Russia-aligned actors and campaigns in observed information operations surrounding the Russian invasion of Ukraine. "Russia-aligned" refers to Russian, Belarusian, and pro-Russia activity; this graphic does not reflect activity pre-dating this conflict

APT28: Telegram channels that the Security Service of Ukraine (SBU) has attributed as information operations assets of the 85th Main Special Service Center of the Russian General Staff's Main Intelligence Directorate (GRU), the same organization to which the U.S. and UK governments attributed APT28 activity, have continued to post content pertaining to the current conflict. These channels were active prior to the invasion, and while we were unable to independently confirm the SBU's attribution, we note that the channels' activity includes promoting content that appears intended to weaken Ukrainians' confidence in their government and its response to the invasion. The content also appears intended to undermine support for Ukraine from its Western partners, interspersed with more seemingly benign posts relaying apolitical content or news reporting.

APT28 has an extensive history of involvement in information operations, ranging from hack-and-leak operations to disruptive activity. Prominent operations involving APT28 have included compromises of the U.S. Democratic National Committee (DNC) and U.S. Democratic Congressional Campaign Committee (DCCC) in 2016, documents from which were subsequently leaked by the false hactivist persona Guccifer 2.0, and the 2014 compromise, defacement, data leak, and data destruction of the Ukrainian Central Election Commission's network and website.

Ghostwriter: A suspected Ghostwriter operation in April leveraged a suspected compromised website and multiple suspected compromised or otherwise actor-controlled social media accounts to publish fabricated content to promote a narrative that appeared intended to foment distrust between Ukrainians and the Polish government. Inauthentic personas we attributed to the Ghostwriter campaign have also continued to publish and promote opinion articles criticizing NATO and its presence in the Baltic States, with increased references to Ukraine in that context. We have assessed with moderate confidence that Belarus is likely at least partially responsible for the Ghostwriter campaign.

In the weeks leading up to the invasion and subsequent weeks thereafter, we observed multiple campaigns conducted by Belarusian espionage group UNC1151 targeting European countries, including a recent spear-phishing campaign targeting Lithuania. Observed targeting associated with UNC1151 threat activity is notable, given the group's technical support to information operations attributed to Ghostwriter.

Niezależny Dziennik Polityczny (NDP): Immediately following Russia's invasion of Ukraine, we observed assets associated with NDP, an information operations campaign centered around an online journal of the same name, shift toward an aggressive defense of Russian strategic interests. During this period, we observed the campaign's concerted promotion of narratives seeded by both overt and covert sources within Russia's propaganda and disinformation ecosystem. We do not attribute the NDP campaign to a specific actor. However, we have observed overlaps between NDP and the Ghostwriter campaign that may suggest some degree of coordination or advanced shared knowledge of operational planning between the two campaigns.

Secondary Infektion: Both prior to and during the invasion, the ongoing suspected Russian influence campaign referred to as "Secondary Infektion" has continued its operations, targeting audiences with fabricated narratives that are often supported by falsified source materials, such as forged documents, correspondence, pamphlets, and screenshots, as well as counterfeit petitions and interviews. All specific Secondary Infektion activity referenced in this blog are operations that we are sharing our attribution of publicly for the first time.

Internet Research Agency (IRA): Reporting from the Russian newspaper Fontanka.ru suggested the existence of covert influence operations related to the Telegram channel "Cyber Front Z." The channel is overtly dedicated to organizing the coordinated promotion of pro-Russia content pertaining to the invasion to audiences in Russia, Ukraine, and the West on social media (Figure 2). The Fontanka.ru report claimed that Cyber Front Z may be run by individuals linked to entities sanctioned by the U.S. as related to the IRA, and that the paid positions promoted by this Telegram channel are part of a "troll factory" that uses inauthentic personas to promote pro-Russia content on multiple platforms. We are unable to independently confirm these claims, but note that such activity is aligned with what we have previously observed from known IRA assets.



Figure 2: Example of content posted to the Cyber Front Z Telegram channel, which it encourages its followers to post on the social media accounts of specified targets. Provided content often includes crude or offensive imagery; featured here is a meme of Ukrainian forces trapped at the Azovstal steel plant in Mariupol while a cartoon Russian soldier calls in an airstrike

Russian Intelligence-Linked Covert Media Outlets: We observed outlets that self-present as independent entities, but have been publicly reported to be linked to Russian intelligence entities, engaged in the publication and amplification of pro-Russia narratives related to the invasion. These include outlets with reported links to the Foreign Intelligence

Service of the Russian Federation (SVR), Federal Security Service of the Russian Federation (FSB), and Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU).

Russia-Aligned “Hactivist” Groups: Established hactivist personas JokerDNR and Beregini have remained active in their targeting of Ukraine in the leadup to and since Russia’s invasion, including through their publication of allegedly leaked documents featuring possible personally identifiable information (PII) of Ukrainian military members. Additionally, newly established “hactivist” groups, whose degrees of affiliation to the Russian state are yet unknown, like Killnet, Xaknet, and RahDit, have engaged in hactivist-style threat activity in support of Russia, including distributed denial-of-service (DDoS) attacks, hack-and-leak operations, and defacements.

Observed Pro-Russia Narratives Seek to Demoralize Ukrainians, Sow Division Between Ukraine and Western Allies, Bolster Public Perception of Russia

Disinformation narratives promoted through concerted information operations have made an array of claims attempting to shape perceptions of the invasion and the larger geopolitical context surrounding it. Many of the narratives we have observed promoted appear intended to serve at least one of these three functions: demoralizing Ukrainians and fomenting internal unrest; dividing Ukraine from its allies; and bolstering perceptions of Russia (Figure 3). Much of this activity has targeted audiences in Ukraine and Europe. However, we have also identified information operations assets promoting messaging that we judge to be aimed at Russian domestic audiences, underscoring Russia’s need to sell the war to its own people.

[OBSERVED RUSSIA-ALIGNED NARRATIVE THEMES ON RUSSIA’S INVASION OF UKRAINE]



Figure 3: Observed Russia-aligned narrative themes related to Russia’s invasion of Ukraine

Demoralize the Ukrainian Population

We have identified multiple narratives that appeared intended to demoralize Ukrainians and incite internal unrest within Ukraine, including false claims of the surrender of the Ukrainian government or military.

- An information operation in March disseminated an artificial intelligence (AI)-generated “deepfake” video of Zelenskyy stating that Ukraine had surrendered to Russia, and defaced the Ukraine 24 website and news ticker in a Ukraine 24 TV broadcast with an identical message or screenshot from the deepfake video (Figure 4). Since the start of the war, other Ukrainian websites have also been defaced with messages alleging Ukraine’s surrender.
- A Secondary Infektion operation in March falsely claimed that Zelenskyy had committed suicide in the military bunker in Kyiv where he had been leading the fight against the invasion, alleging that he had been contemplating suicide due to Ukraine’s military failures.
- Another Secondary Infektion operation from April alleged that the Azov “gang” sought vengeance against Zelenskyy for abandoning their fighters to die in Mariupol, and claimed that Azov commanders had attempted to escape the city by pretending to be civilians. (The narrative here specifically refers to Ukraine’s Azov Regiment, a special operations detachment within the Ukrainian National Guard, which is itself part of a broader ultranationalist movement—segments of which have been known to espouse white nationalist rhetoric; Azov has frequently appeared in pro-Russia narratives seeking to cast the Ukrainian government, and Ukrainians more broadly, as Nazis.)
- Telegram channels attributed by Ukraine to the GRU highlighted alleged corruption and incompetence on the part of the Ukrainian government, such as claims that Ukraine was unprepared for the conflict, and that Ukrainian oligarchs had “paid Zelenskyy for the right to leave the country.”

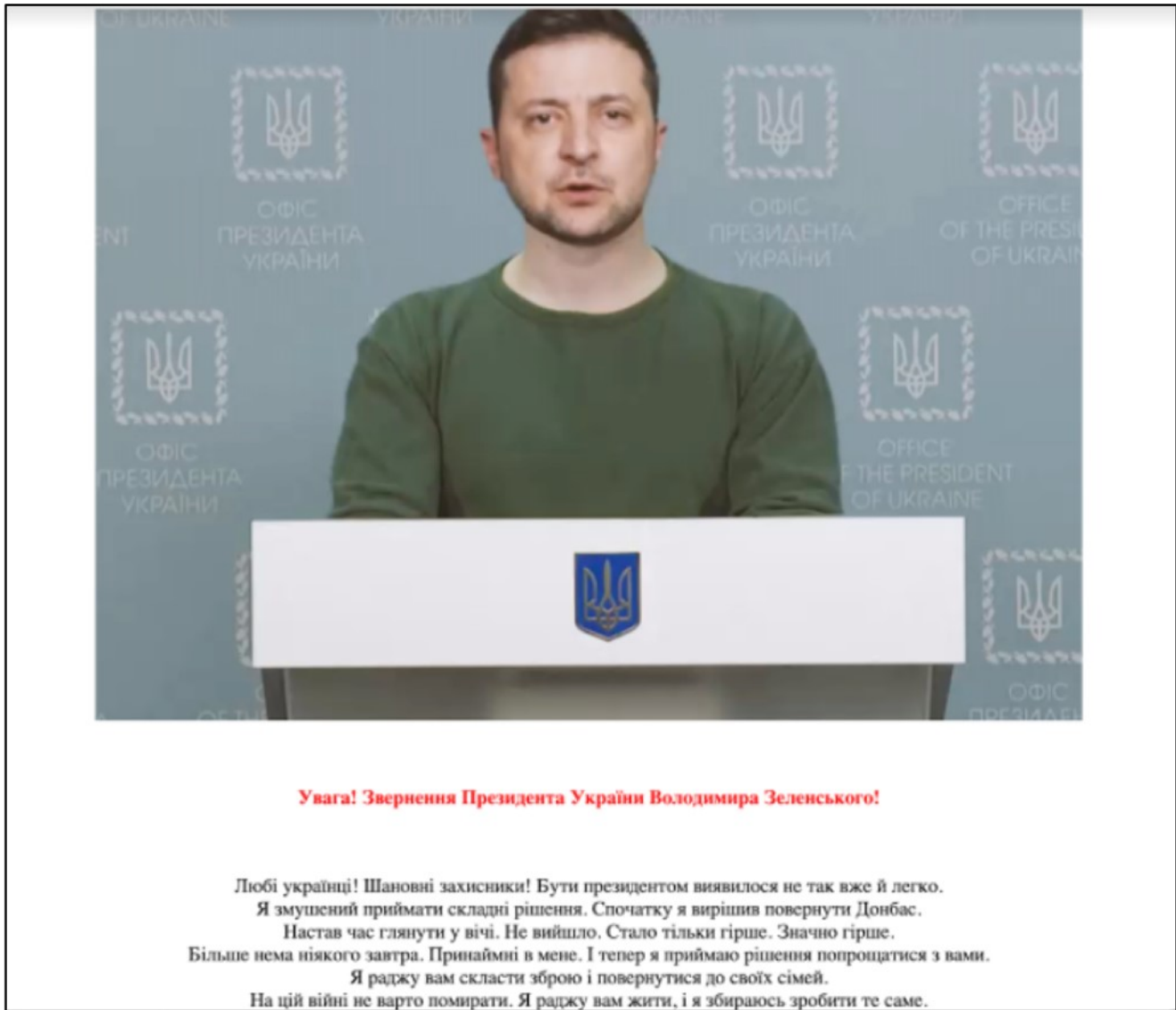


Figure 4: Screenshot from an artificial intelligence (AI)-generated “deepfake” video of Zelenskyy stating that Ukraine would surrender to Russia

Divide Ukraine from Its Allies

- A recent Ghostwriter operation, which we are making our attribution of public for the first time, leveraged compromised assets to publish fabricated content promoting the narrative that a Polish criminal ring was harvesting organs from Ukrainian refugees to illegally traffic in the European Union, and that Poland’s Internal Security Agency was investigating the criminal enterprise, which was said to involve “high-ranking Polish officials.”

- Opinion articles published by suspected inauthentic personas associated with NDP promoted narratives seemingly intended to damage Polish-Ukrainian relations by creating fear, uncertainty, and doubt (FUD) surrounding Poland’s acceptance of Ukrainian refugees. These narratives included falsehoods that sought to portray the refugees as overly burdening Poland’s economy and healthcare system and to stoke fears among Polish citizens that “neo-Nazis”, or other undesirable immigrants, would begin exploiting mass border crossings to carry out attacks on Polish soil.
- The Jan. 14 and Feb. 23 defacements of Ukrainian government websites referenced war crimes committed by the "Ukrainian Insurgent Army" (UPA) against ethnic Poles during World War II, a theme previously observed in Russian and Belarusian information operations. For example, a November 2021 Ghostwriter operation featured a fabricated account from a retired Polish general, stating that the alleged presence of Ukrainian volunteers with far-right political leanings in Poland was “an insult” to the victims of the same war crimes.
- Recent Ukrainian- and Russian-language Secondary Infektion operations claimed that the Ukrainian and Polish governments sought to enable Polish troops to deploy in western Ukraine, a move they portrayed as anathema to the Ukrainian people. One operation in early April claimed that Poland attempted to use an alleged “provocation,” staged by Ukraine, showing Russian troops committing atrocities in Bucha to justify stationing troops in the country, while an operation in early February involved the dissemination of a map showing specific locations where Polish troops would be located, with the suggestion that those troops would occupy large swaths of Ukraine for years (Figure 5).
- Observed narratives from Telegram channels Ukraine attributed to the GRU included suggestions that the West would soon forget about and abandon Ukraine, due in part to the diversion of its attention to impending conflicts elsewhere, such as a potential war launched by the U.S. against Iran.

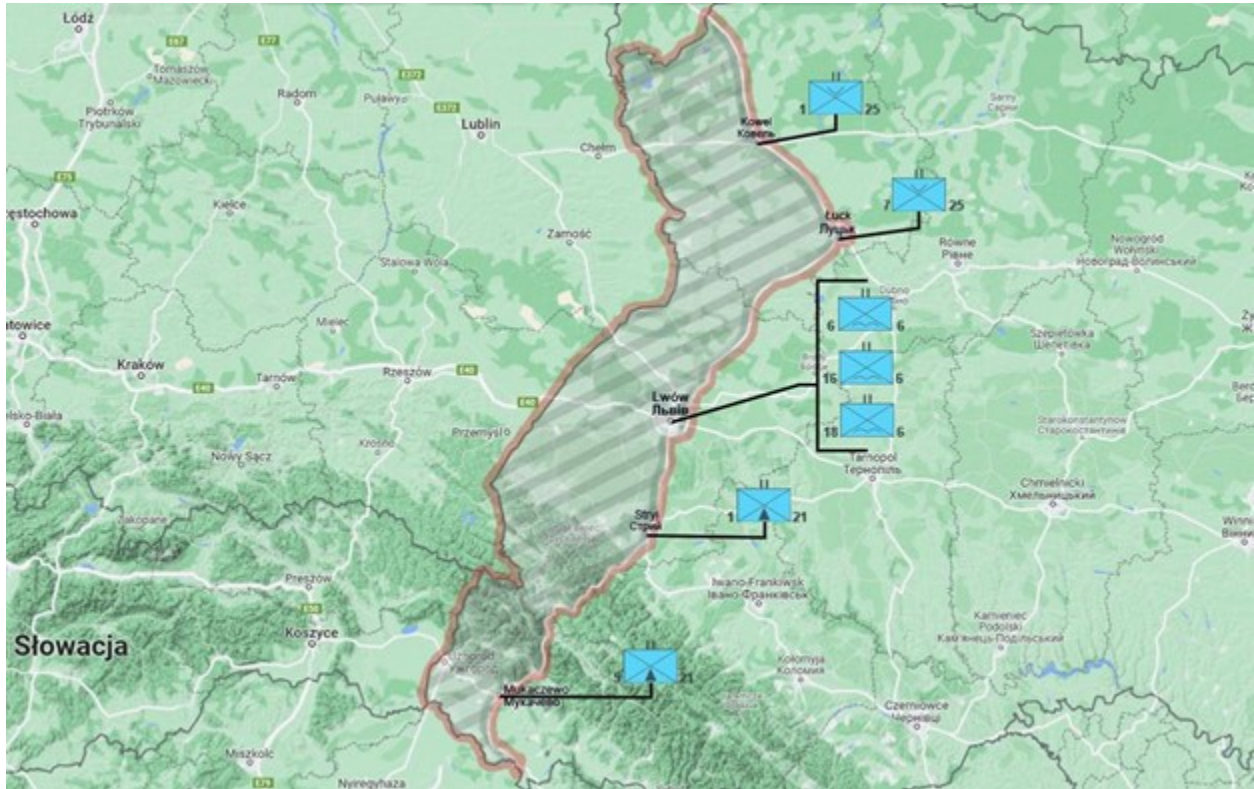


Figure 5: A map disseminated in a suspected Secondary Infektion operation claimed to show specific locations where Polish troops would be stationed in western Ukraine

Bolster Perceptions of Russia

Multiple identified narratives have appeared intended to bolster perceptions of Russia through denial and deflection, including by refuting Russian war crimes in Ukraine and making counter-allegations against Ukrainian forces.

- Cyber Front Z, in its coordinated promotion of pro-Russia commentary, called on social media users to claim that Ukrainian “Nazis” forced civilians into a theater in Mariupol, which they then detonated.
- We identified a coordinated and inauthentic network of social media accounts that promoted Russian-language messaging, including assertions that Ukrainian forces had used chemical weapons.
- These accounts also denied the effects of the West’s response to Russia’s invasion of Ukraine, such as sanctions on Russia, and claimed that such measures had negative consequences for the West.

Pro-PRC Information Operations Campaign DRAGONBRIDGE Messaging Includes Echoes of Russian State-Promoted Narratives

DRAGONBRIDGE, a pro-PRC campaign which comprises a network of thousands of inauthentic accounts across numerous social media platforms, websites, and forums that we first reported to customers in 2019, has shifted its messaging in response to the Ukraine

crisis and subsequent invasion. DRAGONBRIDGE content in English and Chinese has included echoing narratives promoted by Russian state media and influence campaigns, such as alleging the existence of Pentagon-linked laboratories conducting biological weapons research in Ukraine. Notably, such echoing of narratives is not unusual, and charging the U.S. with malfeasance and interference in other countries is likewise in line with PRC political interests; we have previously observed both pro-PRC and pro-Russia information operations promoting content on the alleged involvement of U.S. biolabs in hazardous research. The campaign’s leveraging of Russia-aligned narratives on Ukraine may constitute a form of political opportunism in its continued attempts to target the U.S. and the West’s global standing.

- On March 6, Russian Defense Ministry spokesperson Igor Konashenkov claimed that Russia’s military operation in Ukraine had uncovered evidence of Pentagon-linked laboratories in Ukraine conducting bioweapons research. DRAGONBRIDGE accounts subsequently amplified this claim, including allegations that U.S.-funded biolabs existed not only in Ukraine, but also around the world.
- DRAGONBRIDGE accounts also insinuated that the alleged biolabs in Ukraine were responsible for “mysterious outbreaks,” the nature of which went unexplained, and that biolabs elsewhere in the world were likewise harming local populations (Figure 6).



Figure 6: Screenshot from DRAGONBRIDGE video insinuating a connection between the presence of a U.S. biolab in Ukraine and the occurrence of multiple “mysterious outbreaks”

DRAGONBRIDGE messaging on the invasion also appeared to take aim at U.S. foreign policy and its relations with other countries through claims that the U.S. is self-serving in its actions and that it is an unreliable partner in its alliances. Some accounts alleged that the U.S. sought

to fan the flames of the conflict as it stood to benefit the most, citing its arms sales to Ukraine, while others cast doubt on the U.S. and Europe's seeming policy alignment on sanction measures against Russia, suggesting that the U.S. had bullied Europe into enacting those sanctions, despite deepening energy woes on the continent.

Pro-Iran Information Operations Denigrate Western Response to Conflict, Take Aim at Russia-Israel Relationship

Similarly, Mandiant has observed Iranian and pro-Iran information operations leveraging narratives pertaining to the invasion to take aim at the West, Saudi Arabia, and Israel. Involved campaigns have included the [Liberty Front Press \(LFP\) campaign](#), as well as activity from a pro-Iran campaign we have not previously named that we are dubbing “Roaming Mayfly”, due to its potential links to the Iran-aligned Endless Mayfly influence campaign that [Citizen Lab reported on](#) in 2019.

- Messaging directed at Arabic-language audiences asserted that the U.S. fled from Afghanistan in 2021, and had now abandoned Ukraine, which deserved its fate due to its alliance with the “American axis of evil.” Similarly, English-language content averred that NATO had sacrificed Ukraine to avoid engaging in a war with Russia.
- Pro-Iran information operations assets also declared that Ukraine should not have surrendered its nuclear weapons, implying that such a concession had left it vulnerable to the subsequent invasion.
- Pro-Iran information operations have also leveraged the conflict to accuse the West of hypocrisy in its dealings with Saudi Arabia compared to Russia, by juxtaposing the war in Ukraine against the war in Yemen. Tangentially, assets leveled accusations of racism on the part of the West against Arabs and Muslims, noting alleged differences in its response to the conflict in Ukraine in comparison to conflicts in the Middle East.

We also observed Roaming Mayfly target Russian audiences on the eve of the war in what appeared to be an attempt to use the crisis in order to drive tensions between Russia and Israel. Namely, the campaign leveraged a (now-suspended) impersonator of the Russian journalist and foreign policy thinker, Fyodor Lukyanov, to publish tweets suggesting that Israeli intelligence was supporting Ukraine against Russia in the current crisis, and that Israel had supported the “Ukrainian color [revolutions]” of 2000, 2004, and 2014 (Figure 7).



Figure 7: Tweets by suspected Fyodor Lukyanov impersonator suggesting that Israeli intelligence was supporting Ukraine against Russia in the current crisis and that Israel had supported the “Ukrainian color [revolutions]” of 2000, 2004, and 2014

Outlook

Information operations observed in the context of Russia’s invasion of Ukraine have exhibited both tactical aims responding to, or seeking to shape, events on the ground and strategic objectives attempting to influence the shifting geopolitical landscape. While these operations have presented an outsized threat to Ukraine, they have also threatened the U.S. and other Western countries. As a result, we anticipate that such operations, including those involving cyber threat activity and potentially other disruptive and destructive attacks, will continue as the conflict progresses.

One notable feature of operations attributed to known actors thus far is their apparent consistency with the respective campaign’s established motives. Russia-aligned operations, including those attributed to Russian, Belarusian, and pro-Russia actors, have thus far employed the widest array of tactics, techniques, and procedures (TTPs) to support tactical and strategic objectives, directly linked to the conflict itself. This is especially beneficial when the facts on the ground shape Russia’s need to influence events in Ukraine, marshal domestic Russian support, and manage global perceptions of Russia’s actions. Meanwhile, pro-PRC and pro-Iran campaigns have leveraged the Russian invasion opportunistically to further progress long-held strategic objectives. We likewise expect this dynamic to continue, and are actively monitoring for expansions in their scope of information operations activity surrounding the conflict.