FLASHPOINT

The Role of OSINT in Russia's Invasion of Ukraine

Leveraging Open-Source Intelligence to Understand Organizational Risk Across Cyber, Physical, and Informational Battlefields

Table of Contents

Introduction

MODERN WARFARE

On February 24, 2022, Russian President Vladimir Putin announced on state television a "special military operation" against Ukraine. With that, after years of low-intensity warfare, Russia's full-scale invasion of Ukraine began in earnest.

From the Ukrainian standpoint, this is a war for existence—for the opportunity to be called Ukrainians, to speak their own language, and to live in a democratic state. It is not a war over a long-disputed territory, NATO membership, or Nazis, as is Russia's claim.

While this is far from the first conflict between the two countries, it is certainly one of the most complicated. Today, Russian and Ukrainian forces are fighting across cyber and physical battlefields, which often overlap. Furthermore, an information war is afoot—a fight for public opinion and influence. Finally, economic warfare exists in the form of sanctions, although this battle is mostly being fought between Ukraine's Western allies and Russia.

This report is written by members of Flashpoint's Intelligence Team, whose collective expertise bridges everything from Russian-language cybercrime to the politics and culture of Russia and eastern Europe. It is not exhaustive; rather, it is intended to provide readers with a deeper understanding of the increasingly vital role of open-source intelligence (OSINT) in Russia's ongoing invasion of Ukraine.

To be clear, Ukrainians and organizations that are active in Ukraine face the biggest, most serious risks. But this war is also actively impacting even those who are not physically present or financially and operationally involved in Ukraine, including commercial entities or world governments. For these organizations, it is an immense challenge to gain a proactive, intelligence-driven understanding of the various (and frequently intertwined) elements of this modern military engagement, and make decisions based on this data.

In a theater of war that is materially digital and physical, gaining reliable, timely, and actionable intelligence is a daily test. By highlighting a unique set of real-life use cases in this report, we aim to showcase how organizations are leveraging the intelligence cycle to learn about the conflict, which has included large amounts of OSINT sourced from publicly available information (PAI). This can help organizations across the public and private sectors drive situational awareness, build risk assessments, prevent disruption, implement counterterrorism and crisis response efforts and, ultimately, make decisions that help protect from harm what they value most.

In March 2014, Russia began a hybrid war against Ukraine, which included direct support to pro-Russian militias in the Donetsk and Luhansk regions of eastern Ukraine (which border Russia) as well as disinformation campaigns and cyberattacks, and the annexation of the Crimean peninsula on March 18, 2014 following a special forces operation and a staged referendum.

Russia has supported separatist leaders in eastern Ukraine both financially and militarily, including with military personnel on the ground, although the Russian government has denied this. The United Nations estimates that more than 13,000 people were killed in the conflict between 2014 and 2022. In spite of international mediation, the war remained frozen until late February 2022, when Russia began its full-scale invasion of Ukraine.

Recruitment on the Frontlines

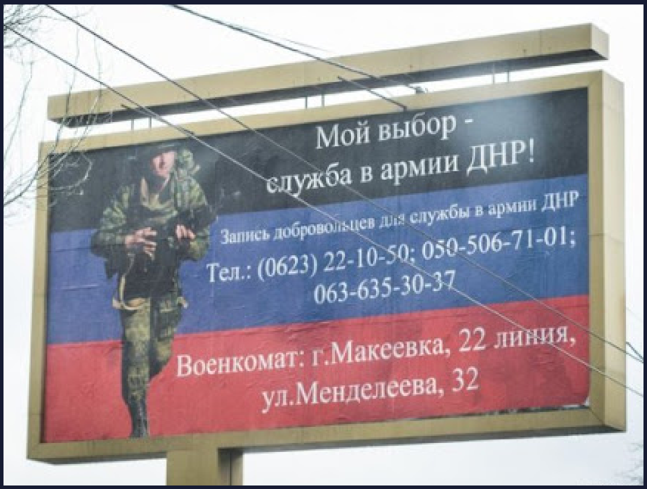
Recruiting soldiers has been a vital part of Russia's efforts, from the very beginning of the invasion of Ukraine in 2014. Initially, the Russian Federation mostly relied on word-of-mouth and occasional advertisements on Russian social media platforms like VK and OK, with the goal of primarily recruiting outcasts into pro-Russia militias fighting in the self-proclaimed Donetsk and Luhansk People's Republics (DPR and LPR).

In 2015, the "people's militias" were transformed into armies and recruitment reached a new level. Billboards encouraging young men to join the ranks of the armed forces of DPR and LPR could be seen everywhere across the occupied territories of Ukraine. Gradually, recruitment has become more open.

For years, the Wagner Group, a Russian private military company, used covert ways to recruit people, while the Russian state and Wagner's owner, Yevgeny Prigozhin, both denied links to the company. But over the course of 2022, it started to openly recruit people in prisons and then on billboards across Russia. Similarly, Russian governors were first trying to organize "volunteer battalions," and since September recruitment has been completely open in the framework of mobilization. But this has not diminished the role of Telegram channels completely. For instance, in Wagner's case, they serve advertisement purposes.

However, technological progress and more specifically the rise of social media and chat platforms allowed recruiters to shift their efforts to various groups and channels. Chat services allow for wider reach and can bring recruits from outside of the self-proclaimed republics. The shift to chat services also allowed researchers and analysts to closely track the increase or decrease in these efforts.

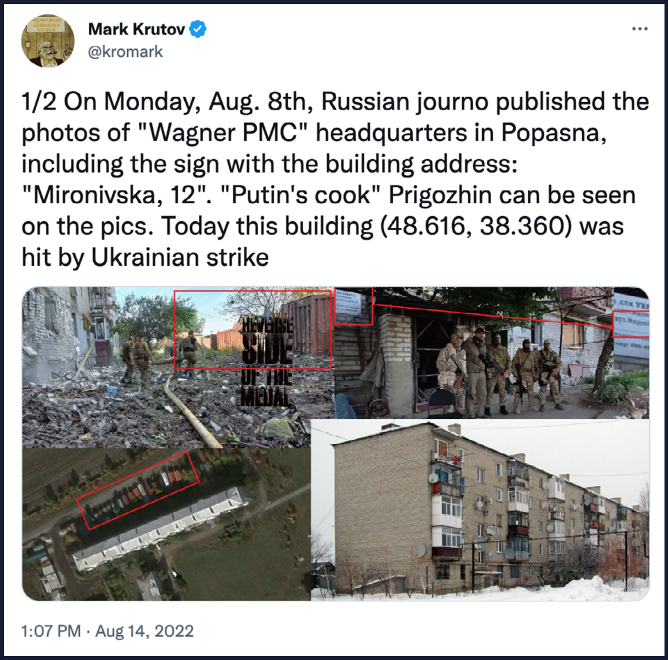
For instance, in February prior to Russia's full-scale invasion, Flashpoint reported on an observed increase in DPR and LPR recruitment and fundraising efforts on various Russian-language social media and chat platforms.


Мой выбор -
служба в армии ДНР!
Запись добровольцев для службы в армии ДНР
Тел.: (0623) 22-10-50; 050-506-71-01;
063-635-30-37
Военкомат: г.Макеевка, 22 линия,
ул.Менделеева, 32

A billboard seeking volunteers to serve in the DPR Army: "My choice: service in the DPR Army!" (Image: Flashpoint)

(It is important to note that Ukrainian recruitment and fundraising efforts have also been present since 2014, which is why we chose to focus on the more recent recruitment and fundraising activities of DPR and LPR.)

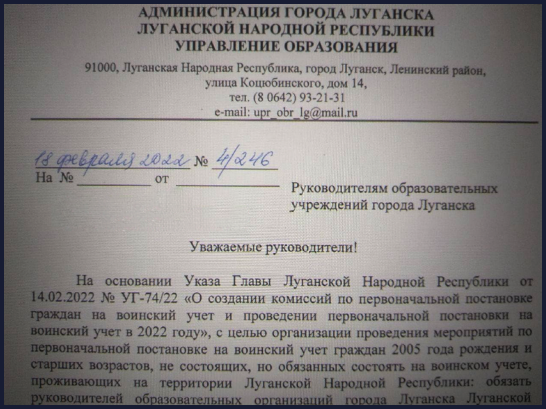
Our reporting highlights the importance of converged cyber and physical intelligence—where internet-driven communication and funding influence and enable kinetic movement and warfare. In fact, Flashpoint was able to match the contact information these groups provided in their VK posts to data from our collections, which proved that the same pro-Russian separatist groups recruiting on VK in February were also recruiting on Telegram in January, prior to the start of the full-scale invasion.



Mark Krutov
@kromark

1/2 On Monday, Aug. 8th, Russian journo published the photos of "Wagner PMC" headquarters in Popasna, including the sign with the building address: "Mironivska, 12". "Putin's cook" Prigozhin can be seen on the pics. Today this building (48.616, 38.360) was hit by Ukrainian strike

1:07 PM · Aug 14, 2022



АДМИНИСТРАЦИЯ ГОРОДА ЛУГАНСКА
ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ
УПРАВЛЕНИЕ ОБРАЗОВАНИЯ

91000, Луганская Народная Республика, город Луганск, Ленинский район,
улица Коцюбинского, дом 14,
тел. (8 0642) 93-21-31
e-mail: upr_obr_lg@mail.ru

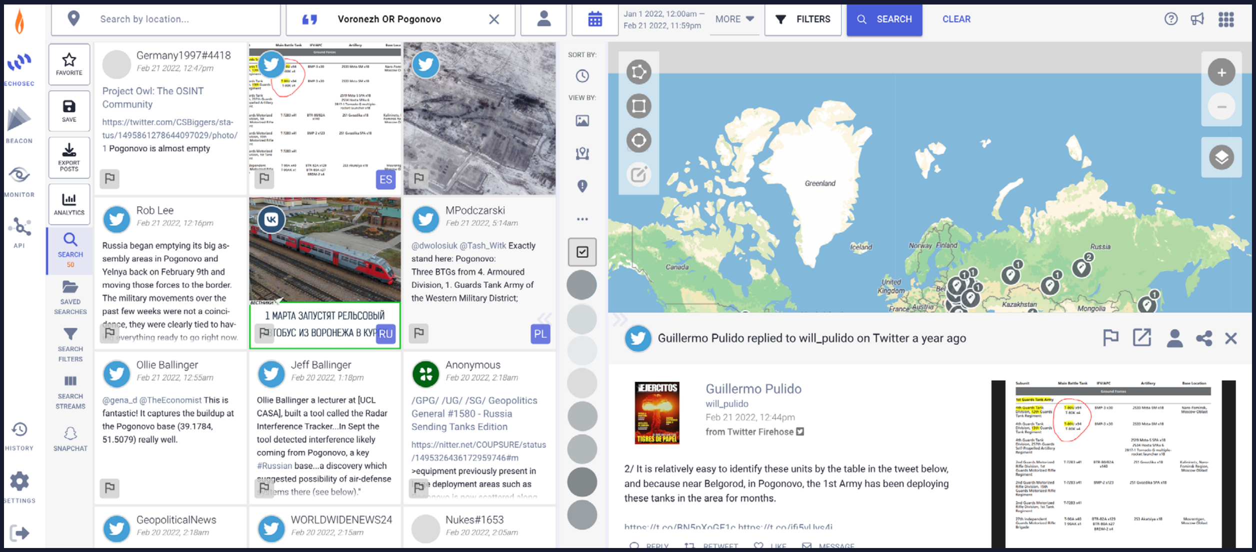
18 февраля 2022 № 4/246
На № __________ от ______________

Руководителям образовательных
учреждений города Луганска

Уважаемые руководители!

На основании Указа Главы Луганской Народной Республики от 14.02.2022 № УГ-74/22 «О создании комиссий по первоначальной постановке граждан на воинский учет и проведении первоначальной постановки на воинский учет в 2022 году», с целью организации проведения мероприятий по первоначальной постановке на воинский учет граждан 2005 года рождения и старших возрастов, не состоящих, но обязанных состоять на воинском учете, проживающих на территории Луганской Народной Республики: обязать руководителей образовательных организаций города Луганска Луганской

ABOVE: Screen capture from a Wagner Group Telegram channel showing what is apparently an official document from the Lukansk People's Republic for military recruitment. This image was shared during a discussion about the withdrawal of mercenaries from the Wagner Group from various Central Africa Regions in order to be redeployed to a special operation in Ukraine. (Image: Flashpoint)



Voronezh OR Pogonovo

Jan 1 2022, 12:00am –
Feb 21 2022, 11:59pm

Germany1997#4418
Feb 21 2022, 12:47pm
Project Owl: The OSINT Community
https://twitter.com/CSBiggers/status/1495861278644097029/photo/1 Pogonovo is almost empty

Rob Lee
Feb 21 2022, 12:16pm
Russia began emptying its big assembly areas in Pogonovo and Yelnya back on February 9th and moving those forces to the border. The military movements over the past few weeks were not a coincidence, they were clearly tied to having everything ready to go right now.

ВЕСТНИКИ
1 МАРТА ЗАПУСТЯТ РЕЛЬСОВЫЙ АВТОБУС ИЗ ВОРОНЕЖА В КУР

MPodczarski
Feb 21 2022, 5:14am
@dwolosiuk @Tash_Witk Exactly stand here: Pogonovo:
Three BTGs from 4. Armoured Division, 1. Guards Tank Army of the Western Military District;

Ollie Ballinger
Feb 21 2022, 12:55am
@gena_d @TheEconomist This is fantastic! It captures the buildup at the Pogonovo base (39.1784, 51.5079) really well.

Jeff Ballinger
Feb 20 2022, 1:18pm
Ollie Ballinger a lecturer at [UCL CASA], built a tool called the Radar Interference Tracker...In Sept the tool detected interference likely coming from Pogonovo, a key #Russian base...a discovery which suggested possibility of air-defense systems there (see below)."

Anonymous
Feb 20 2022, 2:18am
/GPG/ /UG/ /SG/ Geopolitics General #1580 - Russia Sending Tanks Edition
https://nitter.net/COUPSURE/status/1495326436172959746#m
>equipment previously present in large deployment areas such as Pogonovo is now scattered along

GeopoliticalNews
Feb 20 2022, 2:18am

WORLDWIDENEWS24
Feb 20 2022, 2:15am

Nukes#1653
Feb 20 2022, 2:05am

Guillermo Pulido replied to will_pulido on Twitter a year ago

Guillermo Pulido
will_pulido
Feb 21 2022, 12:44pm
from Twitter Firehose

2/ It is relatively easy to identify these units by the table in the tweet below, and because near Belgorod, in Pogonovo, the 1st Army has been deploying these tanks in the area for months.

https://t.co/BN5nXoGF1c https://t.co/ifi5vLlvs4i

Subunit	Main Battle Tank	IFV/APC	Artillery	Base Location
Ground Forces				
1st Guards Tank Army				
4th Guards Tank Division, 12th Guards Tank Regiment	T-80U x94 T-80K x4	BMP-3 x30	2S33 Msta-SM x18	Naro-Fominsk, Moscow Oblast
4th Guards Tank Division, 13th Guards Tank Regiment	T-80U x94 T-80K x4	BMP-3 x30	2S33 Msta-SM x18	
4th Guards Tank Division, 257th Guards Self-Propelled Artillery Regiment			2S19 Msta-S SPA x18 2S34 Hosta SPA x6 2B17-1 Tornado-G multiple-rocket launcher x18	
2nd Guards Motorized Rifle Division, 1st Guards Motorized Rifle Regiment	T-72B3 x41	BTR-80/82A x140	2S1 Gvozdika x18	Kalininets, Naro-Fominsk Region, Moscow Oblast
2nd Guards Motorized Rifle Division, 15th Guards Motorized Rifle Regiment	T-72B3 x41	BMP-2 x123	2S1 Gvozdika SPA x18	
2nd Guards Motorized Rifle Division, 1st Tank Regiment	T-72B3 x41			
27th Independent Guards Motorized Rifle Brigade	T-90A x40 T-90AK x1	BTR-82A x129 BTR-80A x27 BRDM-2 x4	2S3 Akatsiya x18	Mosrentgen, Moscow Oblast

ABOVE: A screenshot of Echosec showing social media intelligence, gathered between January 1 - February 21, tracking physical evidence (video, images, chatter) of Russian military mobilization to strategic Ukrainian border locations, suggesting an invasion was imminent. (Image: Flashpoint)

Cryptocurrency and Illicit Financing

Fundraising for both Ukrainian and Russian causes has primarily focused on bank transfers and fiat currency that is available in each country. Since the beginning of the full-scale invasion, Flashpoint has also observed an increase in the use of cryptocurrency. Cryptocurrency-based transacting allows for a wider geographical reach of fundraising efforts, which means that people and entities outside of Ukraine or Russia can securely and anonymously transfer money to pro-Ukrainian or pro-Russian causes, or organizations whose mission aligns with their values.

However, the fact that the money is being transferred via blockchain technology still allows the tracing of funds via clustering techniques. A lot depends on the operational security of the receiving party. For example, Flashpoint reported in March on 262 cryptocurrency addresses used in advertisements that asked for donations to either Ukrainian or Russian causes related to the war.

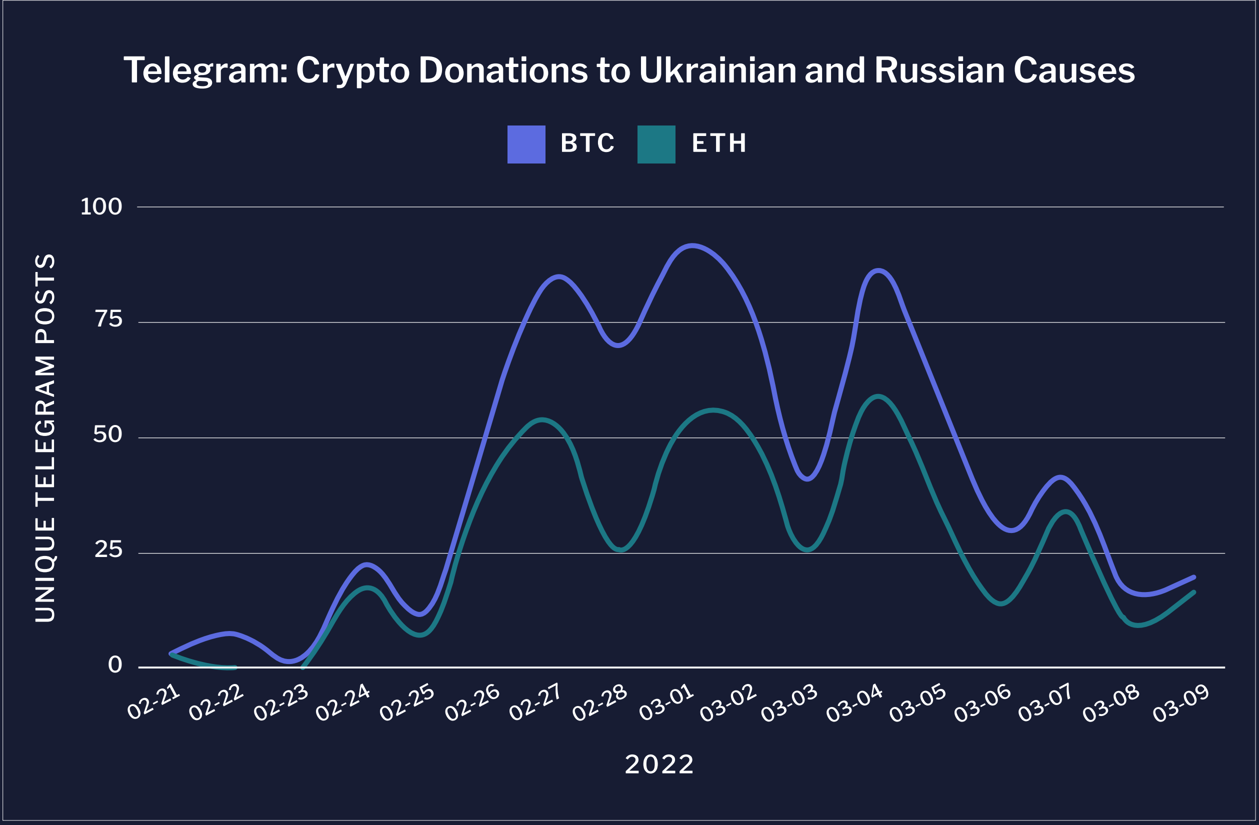


Chart shows the total number of unique Telegram posts containing Bitcoin and Ethereum wallet addresses that claim to be fundraising for, or donating to, Ukrainian or Russian humanitarian or war efforts. (Graphic: Flashpoint)

As Russia's invasion faltered and its regular troops faced growing criticism domestically, attention shifted to mercenary groups and private military companies operating in Ukraine, including the Russian Imperial Movement (RIM), the Wagner Group, and Task Force Rusich. Flashpoint—which includes support for anti-money laundering (AML), counter-terrorist financing (CTF), and know-your-customer (KYC) compliance programs—has looked at Task Force Rusich's illicit funding efforts since the beginning of the full-scale invasion.

By triangulating blockchain and threat intelligence related to mercenary groups like Task Force Rusich, as well as regional subject matter expertise, Flashpoint provided insight into on-the-ground operations, including troop movement; communication and transaction methods; and arms, supply, and infrastructure needs to organizations that are active in Ukraine and intent on avoiding falling afoul of sanctions on Russia's agents in the war.

Destructive Malware Wipers

Throughout 2022, Flashpoint tracked multiple new wiper strains deployed against Ukrainian and Western networks.

Before Russia's full-scale invasion of Ukraine in February, the "WhisperGate" campaign, which first appeared on January 13, 2022, used wiper malware against Ukrainian government networks, IT firms, and nonprofits. The malware included a fake ransomware note, likely to disguise its nature as destructive malware. According to Microsoft's analysis, WhisperGate issues a ransom note by overwriting the Master Boot Record. However, it lacks a ransom recovery mechanism. Thus, its purpose appears to be to render data unrecoverable. This has made researchers liken it to the 2017 worm "NotPetya," which was attributed to the Russian APT "Sandworm."

Another impactful campaign that used wiper malware occurred on the day of the invasion when KA-SAT, a satellite telecommunications service used by the Ukrainian military, was targeted by the wiper "AcidRain." Researchers at SentinelOne noted that AcidRain had possible overlap with the malware "VPNFilter," which, again, had been linked to Sandworm. Other wipers observed during the war have included "CaddyWiper," "DoubleZero," "HermeticWiper," and "IsaacWiper."

While many of these wipers were deployed against Ukrainian and Western networks, late 2022 saw a wiper deployed against Russian networks. In December 2022, researchers at Kaspersky reported that "CryWiper," a new strain of wiper malware, had been deployed against various Russian government networks, including courts and local governments. CryWiper provides a note asking for a ransom while wiping data.

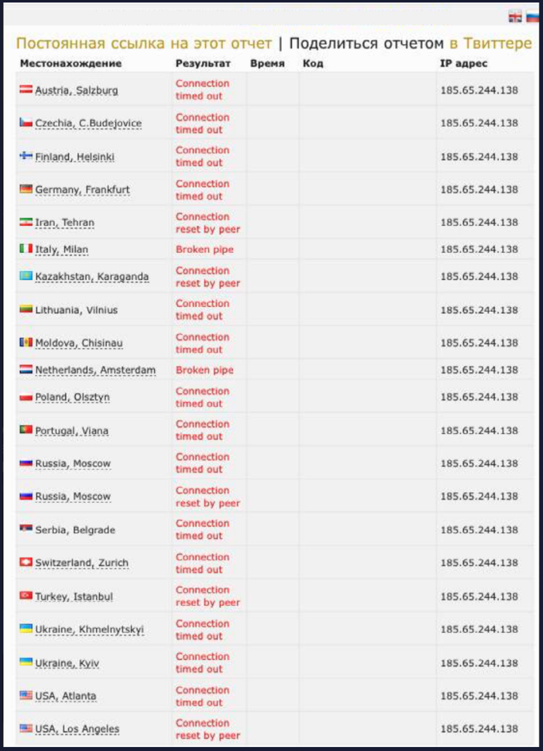
Flashpoint has been collecting indicators of compromise and information on the targeting of these campaigns throughout 2022. We are continuously assessing the risk of such wipers being used against critical infrastructure systems in countries in addition to Ukraine, considering the potential exposure of Western systems to Ukrainian targets and the increasing propensity of attackers to use wiper malware against industrial targets.

Apart from the newly identified malware strains, it is worth keeping an eye on the increasingly blurred lines between state-backed groups and threat actors peddling tools that would normally be used by financially motivated actors. Russian APT groups have used third-party tools several times to cover their tracks and make attribution more difficult. In the 2022 WhisperGate campaign, the attackers used a crypter that was identified as one purchased from a third-party service. Flashpoint is aware of several sellers peddling such crypters in illicit communities.

Killnet: Russia's Favorite DDoS Hacktivists

Russia's full-scale invasion of Ukraine also laid the groundwork for previously unnoticed or unknown cyber collectives, including the hacktivist group Killnet. Throughout the war, Killnet—a self-proclaimed "army of cyber partisans" allegedly motivated by pro-Russian, anti-Western sentiments—has conducted distributed denial-of-service (DDoS) attacks on various public and private entities it deems to be supportive of Ukraine.

On June 18, Killnet attacked Lithuanian networks after the Baltic government announced that it would close routes between Lithuania and Russia's Kaliningrad region in order to fulfill the obligations of European Union sanctions against Russia. The attack was, at that point, Killnet's largest coordinated attack, in which numerous other pro-Kremlin hacktivist groups participated, and was sustained over several days. Later, Killnet claimed responsibility for an attack on the US Congress website as well as other US government entities. The role and impact of Killnet and other similar groups is the "shock and awe" form of information warfare, suggesting to primarily an audience in the Russian Federation—and to a lesser extent in the West—that the websites and networks are vulnerable and will be attacked if their countries continue to support Ukraine or express anti-Russian sentiment. The hacktivist groups also play an important role in Russia's domestic propaganda, as evidenced by the frequent appearances of some of them in Kremlin-connected media.



Постоянная ссылка на этот отчет | Поделиться отчетом в Твиттере

Местонахождение	Результат	Время	Код	IP адрес
Austria, Salzburg	Connection timed out			185.65.244.138
Czechia, C.Budejovice	Connection timed out			185.65.244.138
Finland, Helsinki	Connection timed out			185.65.244.138
Germany, Frankfurt	Connection timed out			185.65.244.138
Iran, Tehran	Connection reset by peer			185.65.244.138
Italy, Milan	Broken pipe			185.65.244.138
Kazakhstan, Karaganda	Connection reset by peer			185.65.244.138
Lithuania, Vilnius	Connection timed out			185.65.244.138
Moldova, Chisinau	Connection timed out			185.65.244.138
Netherlands, Amsterdam	Broken pipe			185.65.244.138
Poland, Olsztyn	Connection timed out			185.65.244.138
Portugal, Viana	Connection timed out			185.65.244.138
Russia, Moscow	Connection timed out			185.65.244.138
Russia, Moscow	Connection reset by peer			185.65.244.138
Serbia, Belgrade	Connection timed out			185.65.244.138
Switzerland, Zurich	Connection timed out			185.65.244.138
Turkey, Istanbul	Connection reset by peer			185.65.244.138
Ukraine, Khmelnytskyi	Connection timed out			185.65.244.138
Ukraine, Kyiv	Connection timed out			185.65.244.138
USA, Atlanta	Connection timed out			185.65.244.138
USA, Los Angeles	Connection reset by peer			185.65.244.138

Screenshot showing the results of an apparent Killnet DDoS attack. (Image: Flashpoint)

Prior to the war (and very likely also post-invasion) the group was preoccupied with commercial work, particularly DDoS-for-hire attacks. The group openly pledged allegiance to Russia, particularly in the context of the war, and stated its disdain for NATO and Western weapons shipments to Ukraine. It is unclear how many individuals are involved with Killnet, which is supposedly a decentralized and volunteer-run-and-operated organization, meaning that anyone could conceivably join its cause. In late 2022 Killnet announced the creation of an umbrella organization, which would unite pro-Kremlin hacktivist groups, if not organizationally, then at least in purpose and coordination.

While it has attracted the attention of global media, the effectiveness of Killnet's attack remains relatively unclear. Despite Killnet's loud claims of being an ideologically motivated collective, the group still accepts commercial orders. Its "loudness" and ability to make headlines could also be viewed strictly from a marketing lens. All of those mentions of Killnet in the world's top publications have likely brought new DDoS customers to the table.

Notably, Killnet's recruitment of new members and fundraising efforts, as well as its planning and execution of attacks, take place in dedicated Telegram chat groups. The ability to actively monitor these groups allows analysts and researchers to stay on top of Killnet's potential cyber activities and, potentially, plan their own defensive measures.

The Battle for the Russian-Language Darknet

One of the ongoing processes that Russia's February invasion has accelerated is the fragmentation of the Russian-speaking cyber underground. Cracks first appeared after the early years of the war. From 2015 to 2017, attacks on Ukraine's critical infrastructure and major companies attributed to Russian advanced persistent threat (APT) groups led to Ukraine seeking closer ties with Western countries in the field of cyberdefense while aligning itself with the legal foundations of the international framework to fight cybercrime. This led to increased cybersecurity information sharing and cooperation on arrests and investigations.

As a consequence, while cross-border cooperation between cybercriminals in Ukraine and Russia continued, the participants in these schemes increasingly found Ukraine to be an unsafe operating environment. This especially became clear following the 2019 takedown of Whost, a bulletproof hosting provider, and the arrest of ransomware operators. These splits have widened since the February invasion, as the effective cross-border cooperation requiring the movement of goods and finances to Russia has become more complicated. While most threat actors in the Russian-speaking cyber underground remained financially motivated, some—such as the now-defunct ransomware group Conti—took sides in the war, and many have welcomed the breakdown of incipient cooperation between Russian and Western law enforcement.

One major development that was impacted by the narrative of the war was the aftermath of the takedown of the underground marketplace Hydra by US and German law enforcement in April 2022, which led to a "war of underground marketplaces." While Hydra primarily focused on narcotics, in recent years it had increasingly offered cybercrime and crucially money laundering tools, as Flashpoint analysts pointed out in our 2021 white paper with Chainalysis, *Hydra Market: Where The Crypto Money Laundering Trail Goes Dark*. Its demise predictably resulted in seismic shifts in the Russian-language cyber underground. Following Hydra's demise, several new marketplaces sprung up, trying to attract vendors and customers that used to rely on Hydra.

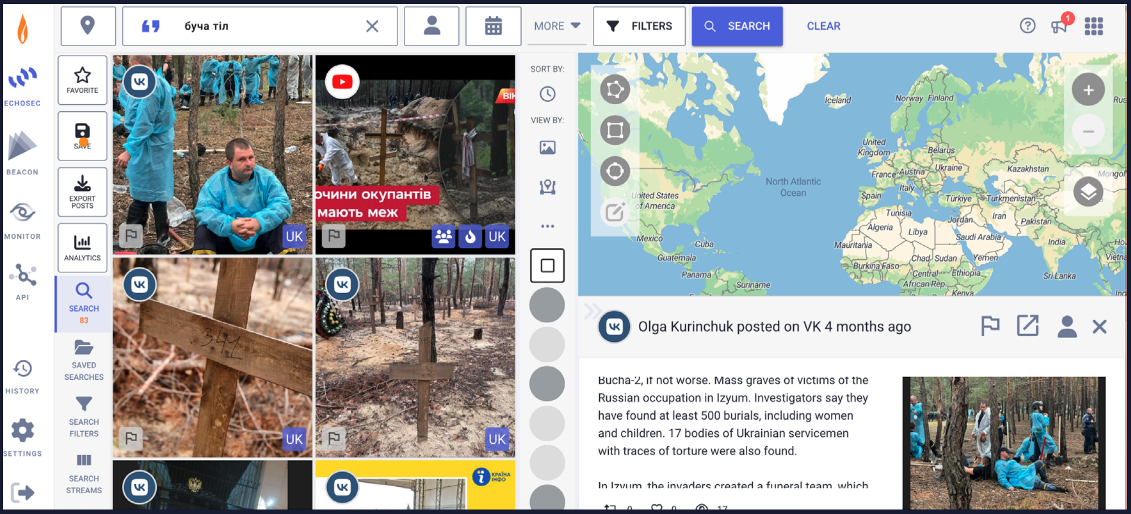
Vendors and customers initially congregated on RuTor, a long-standing darknet hangout. In May and June, however, activity once associated with Hydra started breaking down into various competing marketplaces, which led to rumormongering, DDoS attacks, and data leaks between the marketplaces. The rivalry between two of the leading competitors that emerged over the summer, RuTor/OMGOMG and WayAWay/Kraken, came to mirror the war in Ukraine when rumors started circulating that RuTor had come under the control of the Security Service of Ukraine (SBU).

Regardless of whether there were any grounds for this story considering it aligned with accusations voiced in the Russian Security Council that the SBU is spreading narcotics in Russia, it was quickly picked up and used by RuTor's opponents, including Killnet. Killnet also aligned itself with WayAWay and Solaris, another emerging Hydra successor, in the second half of the year. Flashpoint reported these developments on several occasions, including in our intelligence report: Release the Kraken: The Battle for the Russian-Language Darknet.
As of the end of 2022, the war of marketplaces has continued and the cyber theater of the war in Ukraine is still evolving. Even if the arguments referencing an ideological split between Russia and Ukraine are only a cover for a rivalry that is driven primarily by financial interests, the widening of splits started before February and is unlikely to stop in the foreseeable future. It now appears that parallel, mutually hostile ecosystems are emerging in a previously much more cooperative space. Monitoring such developments will be vital to understanding the changing threat landscape that organizations face.

Documenting Violence

Throughout the war, and especially since the February 2022 invasion, Telegram has become a vital source of first-hand information from the battlefield and the occupied regions (as well as integral to the spread of propaganda and disinformation). This is partly due to the fact that Telegram has not been blocked by the Russian authorities, even as Russia attempted to block channels encouraging Russians to desert from the army. It is also partly due to Telegram's lax moderation policies, which allow a very wide range of explicit or disturbing imagery to be posted on the platform, even as mainstream social media networks have tightened up their regulations in recent years.

For the duration of the war, eyewitnesses, military bloggers, correspondents, soldiers, and mercenaries alike have shared both textual information and visual media on Telegram and other social media platforms. These have been used as material for open-source investigations of the placement, activities, and identities of invading troops, as well as the atrocities committed by them. In future court proceedings on war crimes, this Telegram data could be crucial evidence.

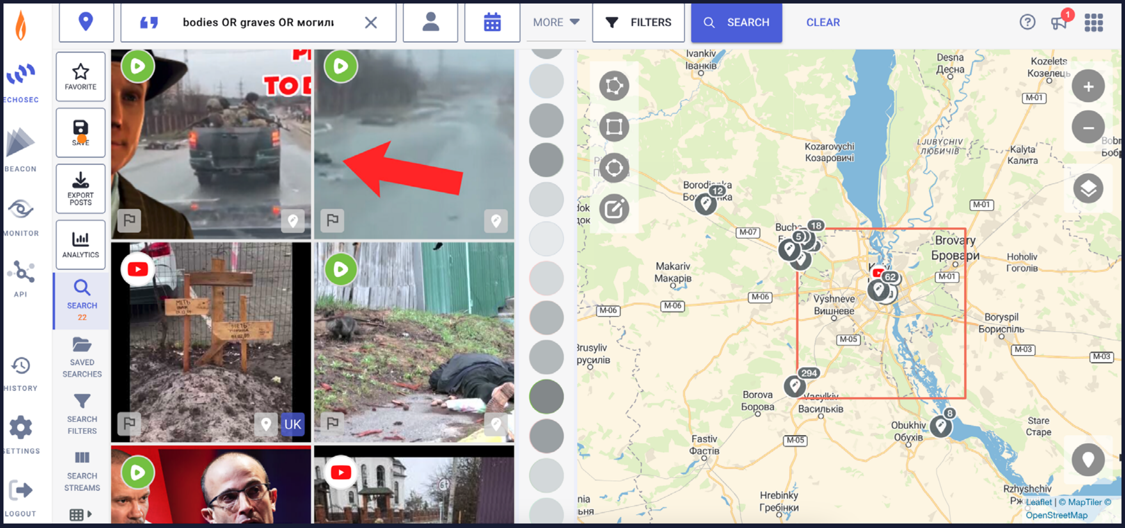


Olga Kurinchuk posted on VK 4 months ago

Bucha-2, if not worse. Mass graves of victims of the Russian occupation in Izyum. Investigators say they have found at least 500 burials, including women and children. 17 bodies of Ukrainian servicemen with traces of torture were also found.

In Izyum, the invaders created a funeral team, which

ABOVE: In March 2022, Russian paratroopers systematically killed more than 450 Ukrainian civilians and prisoners of war, including children, in the Ukrainian village of Bucha. After the liberation of the town, images and videos depicting the victims of the massacre spread via social media and messaging platforms. Despite the evidence, Russian officials denied the events, calling it a "provocation." Echosec allows users to export and store post content, including video and image content of eyewitness accounts of violence shared on social media, to be used for investigations into human rights violations and proceedings over potential war crimes. (Image: Flashpoint)



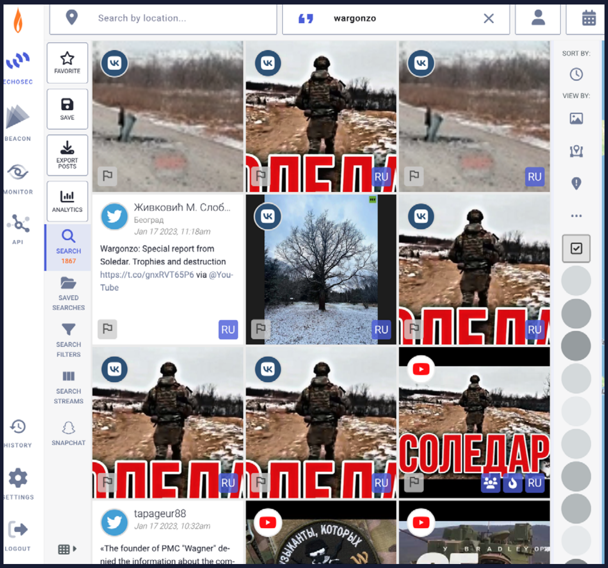
ABOVE: Echosec screenshot showing results for the terms "bodies," "graves," or "Irpin," following the March 28 conclusion of the Battle of Irpin. (Image: Flashpoint)

However, Telegram channels and groups can be erased, and the content within them can be changed or removed. The importance of preserving such evidence has been highlighted by projects such as OSINT Ukraine, a public archive of Telegram content related to the war, which has stored archived posts from over 150 conflict-related channels, including photos and videos. Such archives, however well curated, nonetheless only allow the archival of a fairly limited number of channels and contents.

Since the beginning of the February invasion, Flashpoint has prioritized identifying and contextualizing the maximum possible number of messaging groups and channels sharing information (or disinformation) about the war. Our capabilities make it possible to run targeted searches not only in text archives but also in the media shared by these groups and channels. These media can also be cross-referenced with mainstream social media posts that can be accessed via the Flashpoint platform.

War Bloggers and Policy

Since the beginning of the February invasion, a wide range of pro-Kremlin channels emerged on Telegram. They are run by war correspondents of state-backed media, military bloggers, and mercenary groups, as well as domestic politicians and propagandists. By collecting hundreds of thousands of followers on Telegram, they have come to shape the domestic image of the war. Moreover, their audiences and posts have observable overlaps with those of Russia-aligned hacktivist channels. Some of the most popular voices have included Semyon Pegov, aka "WarGonzo"; Yury Podolyak; "Correspondents of the Russian Spring"; and "Rybar," who has been identified as Mikhail Zvinchuk, a former Russia Ministry of Defense official.



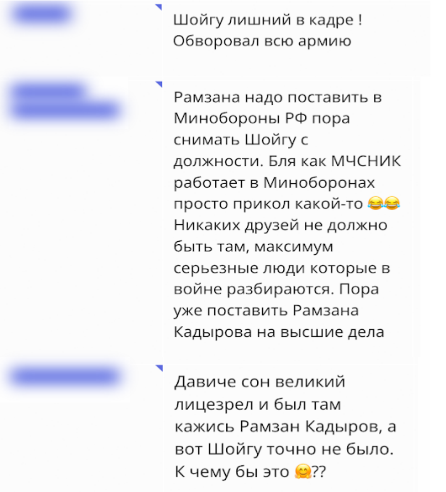
Живковић М. Слоб...
Београд
Jan 17 2023, 11:18am
Wargonzo: Special report from Soledar. Trophies and destruction https://t.co/gnxRVT65P6 via @YouTube

tapageur88
Jan 17 2023, 10:32am
«The founder of PMC "Wagner" denied the information about the com-

An Echosec search showing results for "wargonzo," a Russian military blogger whose content has notably been reshared and propagated across the world via social media and other platforms.
(Image: Flashpoint)

While the narratives promoted by them have often aligned with the Kremlin's preferred narratives, at times they have been markedly critical of Russia's leaders. For instance, after Ukraine's successful counter-offensive in the Kharkiv region in September, several channels and users of nationalist groups criticized Russia's military leadership, attacked Defense Minister Sergey Shoigu, and called for an escalation in Ukraine and military mobilization in Russia even before the Kremlin took the decision to order it. Domestic political actors such as Yevgeny Prigozhin, the head of the Wagner Group, and Ramzan Kadyrov, the head of Chechnya and Russia's most followed Telegram influencer, both cheered these attacks.

The Kremlin acknowledged the rising importance of these Telegram channels by simultaneously trying to rein them in and co-opt them. In October, Russian law enforcement reportedly checked the channels for "discrediting" and "posting fakes" about the Russian army, which can carry long prison sentences in Russia. Russian President Putin's spokesperson warned the operators of the channels against criticizing the Kremlin. In December, the Kremlin included four military bloggers in a newly formed "Mobilization Council." Nonetheless, as of January 2023, the Kremlin is still struggling to control the narratives shared by these channels. Though it did not actually take place, a "Christmas ceasefire" announced by Putin for the Orthodox Christmas period in January received heavy criticism from several military bloggers.



[redacted]

Шойгу лишний в кадре !
Обворовал всю армию

[redacted]

Рамзана надо поставить в Минобороны РФ пора снимать Шойгу с должности. Бля как МЧСНИК работает в Миноборонах просто прикол какой-то 😂😂 Никаких друзей не должно быть там, максимум серьезные люди которые в войне разбираются. Пора уже поставить Рамзана Кадырова на высшие дела

[redacted]

Давиче сон великий лицезрел и был там кажись Рамзан Кадыров, а вот Шойгу точно не было. К чему бы это 🤗??

Examples of members of pro-war Russian Telegram groups criticizing Shoigu in early October:

"Shoigu is redundant! He robbed the whole army!"

"Ramzan [Kadyrov] needs to be appointed to [head] the Defense Ministry and Shoigu should be dismissed."

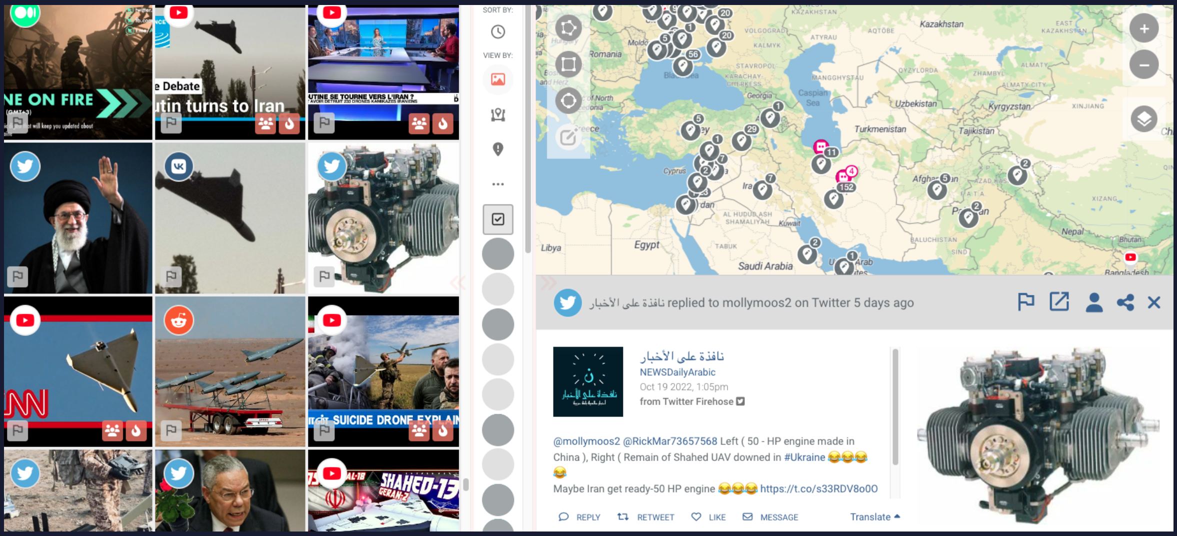
"A while ago I had a great dream, Ramzan Kadyrov was in it, but Shoigu definitely wasn't. What does it mean?" (Image: Flashpoint)

Flashpoint has been monitoring several dozens of these channels since February and worked to identify the most important and most influential ones, based on their presence in pro-Kremlin media, mainstream social media, and our own collections. As Russia faces further battlefield setbacks as of late 2022, following and understanding the narratives that these continuously popular Telegram channels promote will be essential to understand how the war is domestically understood and how Russia's failures and successes are used by domestic power brokers jockeying for influence.

Iranian UAVs Bring Strength to Russian Military

Open-source intelligence is critical to understanding the full spectrum of any physical threat environment. This has proven true concerning the continuous influx of Iranian kamikaze uncrewed aerial vehicles (UAVs) into the Ukrainian theater, which has enabled President Putin to conserve Russian arsenals.

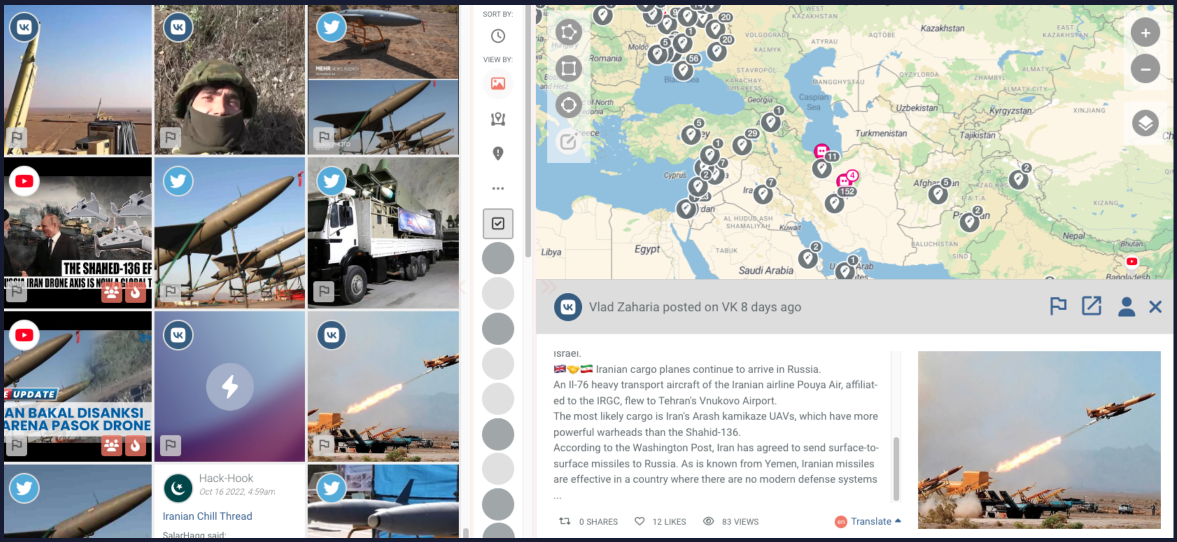
Flashpoint heeded early warnings from the US National Security Council (NSC). In July 2021, for instance, the NSC indicated that Russia was intending to purchase UAVs from Iran to supplement its inventory. In addition, the NSC became aware of several Iranian UAV types being used by Russian forces in Ukraine in near real-time through those on the ground who shared images and videos of the first evidence of Iranian UAV implementation in Iran.



نافذة على الأخبار replied to mollymoos2 on Twitter 5 days ago

نافذة على الأخبار
NEWSDailyArabic
Oct 19 2022, 1:05pm
from Twitter Firehose

@mollymoos2 @RickMar73657568 Left (50 - HP engine made in China), Right (Remain of Shahed UAV downed in #Ukraine 😂😂😂😂
Maybe Iran get ready-50 HP engine 😂😂😂 https://t.co/s33RDV8o0O



Vlad Zaharia posted on VK 8 days ago

Israel.
🇬🇧🤝🇮🇷 Iranian cargo planes continue to arrive in Russia.
An Il-76 heavy transport aircraft of the Iranian airline Pouya Air, affiliated to the IRGC, flew to Tehran's Vnukovo Airport.
The most likely cargo is Iran's Arash kamikaze UAVs, which have more powerful warheads than the Shahid-136.
According to the Washington Post, Iran has agreed to send surface-to-surface missiles to Russia. As is known from Yemen, Iranian missiles are effective in a country where there are no modern defense systems
...

ABOVE: Screenshots of the Echosec searches tracking heavy aircraft activity from Iran to Russia that were suspected of delivering UAVs for use against Ukraine, as well as Chinese parts used in the drone engines. (Image: Flashpoint)

The vast amount of images and footage related to Iranian UAVs in use in Ukraine enabled Flashpoint to monitor the types of UAVs in use by Russian forces. It also painted a clearer picture as to how these UAVs fit into Russia's war strategy, as well as how Ukrainian forces were confronting the threat.

Flashpoint was keenly aware of the challenge Iranian UAVs pose to the Ukrainian military; Iran's UAV technology had already widely proliferated to Iran's armed proxies throughout the Middle East and had been used in attacks against coalition forces and vessels in the region. Iran saw the potential for UAVs as a gamechanger in the Middle East battlespace (Syria, Iraq, Yemen, e.g.) early on. Thus, Flashpoint's intelligence on Iran's UAV tactics in the Middle East assisted Flashpoint's analysis on how they might be implemented in Ukraine. Open-source intelligence is continuously proving to be vital to fully assessing any given threat landscape, and in Ukraine, it is more critical than ever.

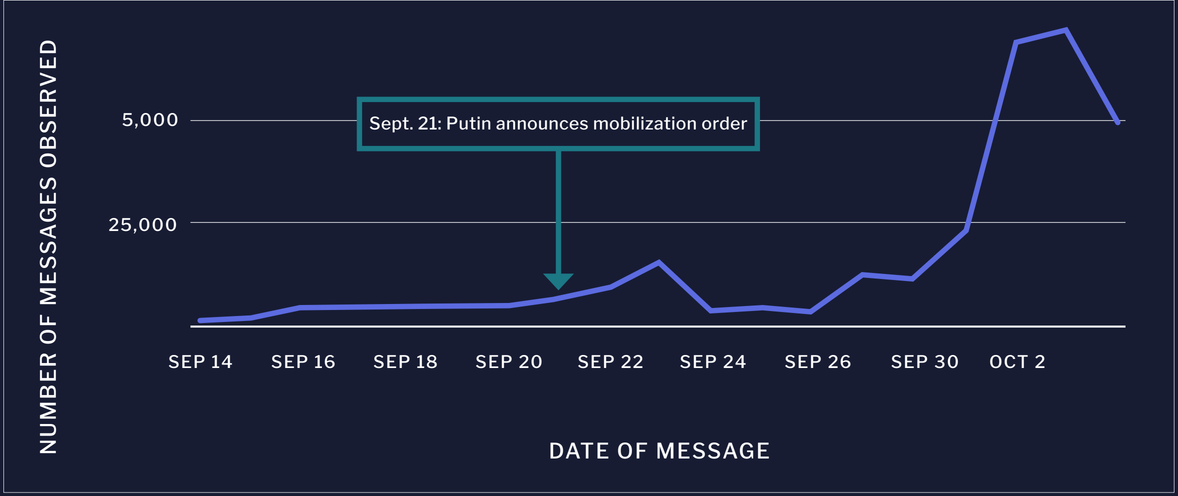
Mobilization Protests in Russia

In light of Ukraine's successful counteroffensive in the Kharkiv region, Russian President Putin issued a decree announcing a "partial" mobilization in Russia. The announcement caused an immediate shock among Russians. In the following days, hundreds of thousands of Russian citizens fled abroad as protests against the draft started in several regions.

The protests against mobilization failed to stop the process. Later, however, many mobilized men protested against abuses, a lack of proper equipment and training, and missing payments to themselves and their families promised in Putin's decree. It is unclear how many people the authorities managed to mobilize, or even whether the mobilization has ended. However, estimates range from around 200,000 to 500,000 men, and it appears that they were separated into two groups. Some draftees received more substantial training, while others were sent to the frontlines almost immediately, with only basic training and faulty equipment.

Monitoring events like this helps to understand the domestic reaction of Russian society to the ongoing war and to track the presence of protest potential or its impact on an internal coup in Russia. Notably, a coup depends on much more than protests, including the potential costs of plotting, the potential payout, and the alternative to Putin and his policies.

The announcement of the mobilization also affected cyberspace trends. After Putin's mobilization order was first announced, Flashpoint observed a growing number of chatter and advertisements on Russian-language illicit communities and social media platforms, offering methods or access to avoid the draft. This included fake employment certifications, fake illness documentation, manual name removal, and fake education certificates. Some of these offers, it is worth noting, were likely scams and contributed to the rise of panic. On Russian mainstream social media, Flashpoint analysts also saw a steady increase in the number of posts mentioning the protests in the northern Caucasus and the situation at border crossings.



Graph showing the number of posts that contain words associated with services to dodge the draft, including certificates, help with mobilization, arrangement, and deferment. (Graphic: Flashpoint)

Disinformation, Conspiracy Theories, and Justification Narratives

Disinformation narratives have become very closely woven into the events of this war, lasting from Russia’s annexation of Crimea in 2014 to today’s ongoing invasion of Ukraine. These narratives have the power to shape political and kinetic decision-making; they are also an effective tool for psychological influence. Perhaps the most well-known disinformation narrative is Russian propaganda about the so-called “denazification and demilitarization” of Ukraine, which was (and still stands as) the Kremlin’s official reason for launching a full-scale war against Ukraine.

One Russia-spun disinformation narrative, which the Russian Defense Ministry also promoted, claimed that the US is financing Ukrainian “biolaboratories producing bioweapons” to help covertly spread “deadly pathogens,” including COVID-19 and “African swine fever and anthrax.” Part of this pro-war disinformation campaign highlights the use of “bird killers” and then mosquitoes that “target only ethnic Russians” via “bioweapons.” There were also unsubstantiated claims that Ukraine is building a “dirty bomb,” a conventional explosive combined with radioactive material, and that its authorities are spreading narcotics in Russia.

Some of Russia’s disinformation narratives have been adopted into the discourse of Western extremists and conspiracy theorists. The “secret biolabs” narrative, for example, likely resonated with audiences primed to imagine the existence of such establishments during the COVID-19 pandemic. Research has shown, however, that Russia’s disinformation narratives were particularly successful in developing countries, e.g. certain African countries and India.

While the Kremlin keeps the editorial policies of Russia's pro-Kremlin media outlets under close control, disinformation narratives do not always originate from officials. In fact, what is perhaps most important is not necessarily how these disinformation narratives begin but how they spread and influence major events. Throughout the war, Flashpoint has observed how various disinformation narratives were then taken up by pro-Russia Telegram channels and pro-Kremlin mainstream media, and tweaked until being reprinted in Russian mainstream media. One such instance occurred when Russia-connected accounts amplified unverified information by a French social media user, who suggested that French howitzers in Ukraine were being resold for profit. This is not a unique case. Russian state propaganda created and pushed false stories accusing Ukraine of selling US-donated weapons on darknet marketplaces. Often this news is spread in conjunction with threats that weapons will find their way into criminal communities and may lead to highly armed banditry. The main goal of such narratives is to force partner countries to stop supplying weapons to Ukraine.

The chat groups in which these conversations occur are extremely important to track because they can often result in cyber or physical attacks against Ukrainian refugees, organizations, and politicians who openly support Ukraine, and may lead to extremist actions against Ukrainian diplomats or delegations at international events.

Conclusion

PREPARING FOR THE LONG RUN

It is not yet clear how long Russia's invasion of Ukraine will last. It is, by all accounts, an open-ended war. President Putin is preparing Russians for a long-term war effort. Ukraine and its supporters in the West seem to show no immediate exhaustion despite Russia's efforts to wear them down. In Ukraine, most citizens want to continue fighting until the full liberation of the occupied territories. Europe is learning to live without Russian energy.

In addition to the unknowable length of this war, another factor security and intelligence professionals need to consider is the constantly changing face of the war itself. To date, we have seen a quick Russian assault, which Ukrainians repelled; a veritable war of attrition; numerous counter-offensives; political crises and economic problems in Russia; disruptions to the global economy; changes to the Russian-language cybercrime landscape; the blurring of the lines between financially motivated and state cyber threat actors; data leaks from Russia; and more. In late 2022, Russia, which initially prepared for a short war, changed its tactics yet again by hitting critical infrastructure in Ukraine. Both sides seem to be preparing for offensives in 2023. In short, we will likely still see changes in how the war is fought, by what means, and at which targets. When it makes more sense to attack Western entities, Russia may very well shift tactics—major cyberattacks take time. When it makes strategic sense, the face of war will change again.

As a result, it has become a near imperative for just about every government and commercial organization in the world to be able to acknowledge and calculate their risk profiles in relation to the war. Today, in this context and many others, timely intelligence and rock-solid analysis are must-haves to protect critical assets, infrastructure, and stakeholders from security risks.

To learn more about Flashpoint, sign up for a free trial today.

FREE TRIAL ➔