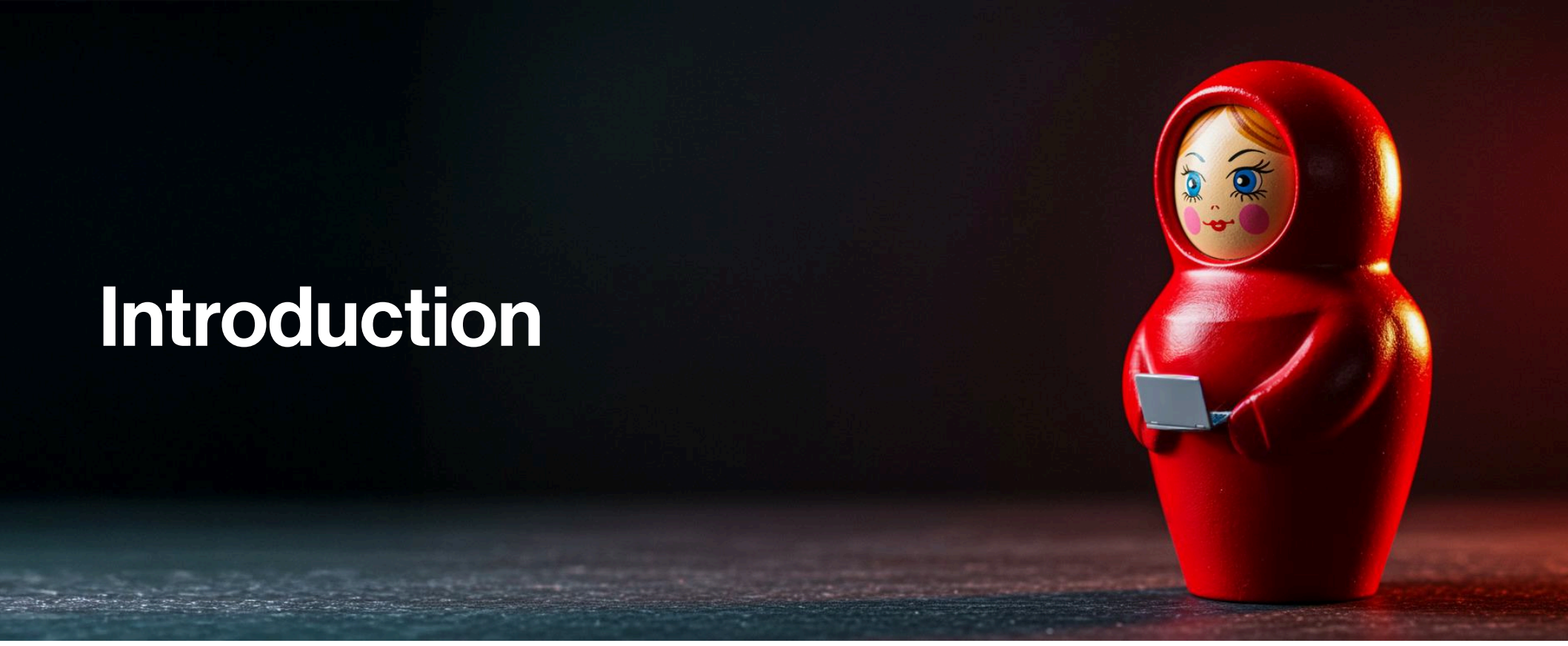
Russian Cybercrime & State Militarization:

Marching Together in the Digital Age

by Anastasia Sentsova

Introduction



Over the past three years, the number of pro-Russian hacktivist groups has grown significantly, with the surge picking up after Russia's full-scale invasion of Ukraine in February 2022. They are not the only actors online; pro-Ukrainian, pro-Belarusian, and other state-aligned groups also operate, creating a crowded, contested digital battlefield where cyberattacks and information operations are routine tools of coercion and psychological pressure.

Cyber operations are now a core element of Russia's hybrid warfare, but they only scale when enough people join, which means mass recruitment of "digital soldiers." That raises a hard question: are "independent" pro-Russian hacktivists truly freelance, or do they work with, for, or alongside the state?

Claims of direct state involvement require the highest level of confidence and must be assessed carefully. At the same time, we can and should consider the potential indirect influence of the state probabilistically. That means examining the domestic political landscape, relevant laws and incentives, and the social dynamics that make alignment more or less likely. We measure that by analyzing messaging signals, explicit slogans, references to geopolitical events, patriotic calls to action, and deliberate targeting of proclaimed states' enemies to estimate state influence, whether direct or indirect.

In addition, Russia's reputation as a safe haven for cybercriminals complicates the analysis of potential state involvement and must be taken into account. Many ransomware actors, for instance, operate openly within Russia's borders, and Moscow's reluctance to act decisively sends implicit signals to these groups, effectively shaping and reinforcing their behavior. Furthermore, several documented cases over the years have revealed the participation of government officials in cyber operations that intersect with conventional cybercrime. This pattern will be examined in greater detail in the analysis.

At the core of the observed influence on hacktivist groups is the Russian state's long-running push to militarize society. Built on wartime memories of the Second World War and reinforced during Vladimir Putin's presidency, this project gained visible legal and institutional force starting in the 2010s. The Foreign Agents law (early 2010s) and the 2014 annexation of Crimea accelerated the effort: patriotic education, military youth programs, and legal pressure on NGOs and independent media became central tools. The trend intensified after February 2022, when emergency censorship laws and mass propaganda turned administrative control into broad social coercion.

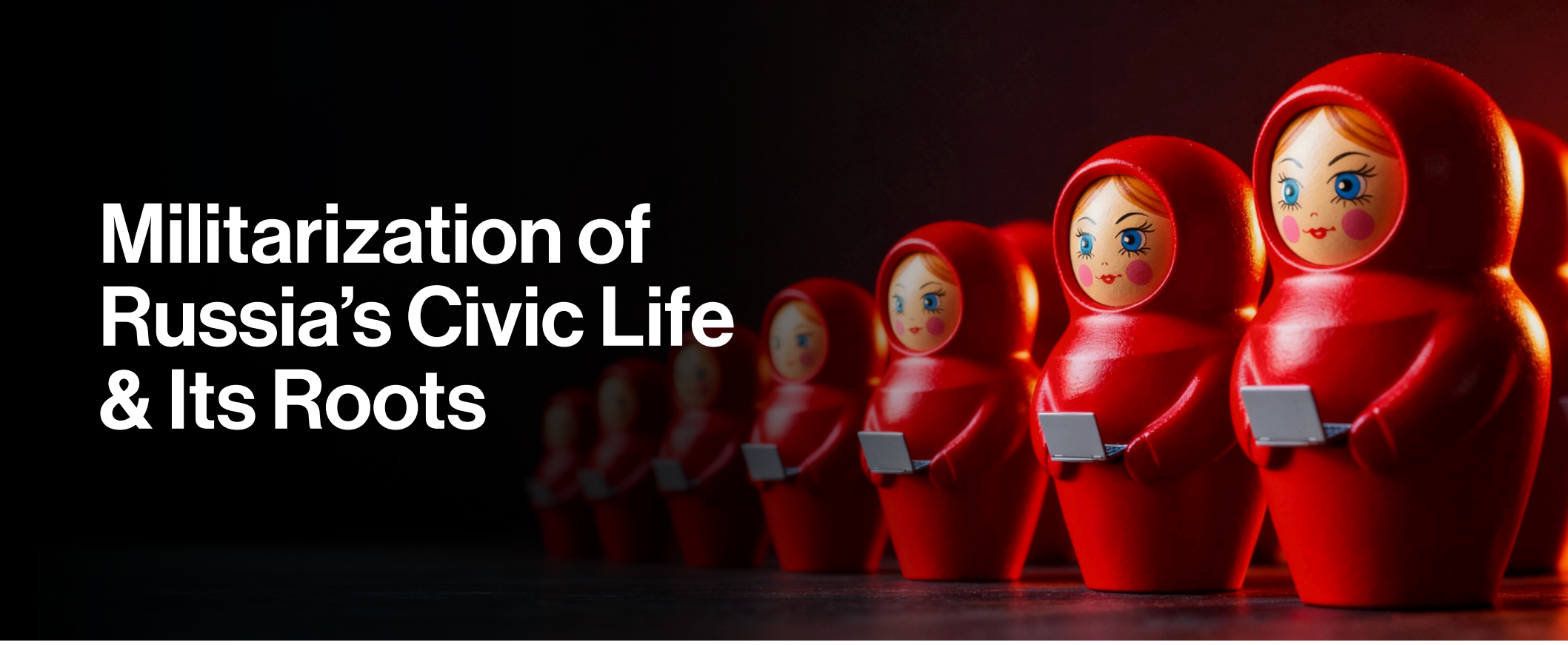
One central vehicle for militarization efforts is the All-Russia People's Front, and a subject of our research, a public movement launched at Putin's initiative in 2011. The movement has a strong physical presence and many local initiatives, as well as in the digital sphere. In April 2023, the All-Russia People's Front launched CyberSquad. This volunteer network recruits civilians to monitor online spaces for "Rusophobic" or "hostile" content, file complaints, and amplify pro-state narratives.

The emergence of hacktivist groups alongside official programs creates a crowded, informal ecosystem of politically motivated cyber actors that furthers the militarization strategy and actively participates in a hybrid war. Institutional differences aside, official movements and informal groups often pursue the same goals, recruitment, legitimacy, and mass influence. Under state militarization, their playbooks converge: heroification and militarized language, “people’s army” framing, human-interest stories that normalize participation, appeals to revenge or duty, and coordinated amplification across platforms and media.

This research examines that convergence. By analyzing Russia’s militarization strategy alongside official volunteer programs and Russian cybercrime, we aim to map how “digital soldiers” are recruited and assess the likely effects on public opinion and escalation risk in the information environment. It’s a journey through the state’s digital fingerprints — its language, slogans, and familiar symbols — where its presence quietly reveals itself. Because even when cyber operations try to appear “independent,” the state’s voice inevitably slips through.

In our attempt to answer whether Russian cybercriminals are marching in step with the state, we’ll lay out the evidence. Think of it as building a conspiracy board: we’ll keep the tone analytical, with a light sprinkle of sarcasm at the author’s discretion to keep readers engaged. Consider it an occupational hazard: when the state speaks half in bureaucracy and half in slogans, sometimes the only accurate translation is irony.

Militarization of Russia's Civic Life & Its Roots



The shift to a modern, militarized civic order in Russia didn't happen overnight. It unfolded over more than a decade through laws, institutions, and public rituals that reshaped everyday life. Start with cultural memory. The Second World War (WWII) or the Great Patriotic War, as it's known in Russia, is a central pillar of public identity. Public discourse in Russia emphasizes the country's role and sacrifice in defeating Nazi Germany; that narrative is repeatedly rehearsed in parades, memorials, school lessons, and a politics of remembrance that prizes duty, sacrifice, and military glory.

Military parades are perhaps the ultimate flex of the Russian state, spectacles that carry their own history, a lineage of power staged in public. The modern Victory Day parade traces back to June 24, 1945, when Soviet troops marched through Red Square and cast down captured Nazi standards before the Kremlin walls. What began as a singular act of triumph became, under Leonid Brezhnev, a cyclical ritual: May 9 transformed from a day of remembrance into an annual affirmation of the state's strength and continuity. After the Soviet collapse, Boris Yeltsin's 1995 parade reasserted the tradition, and in 2008, Vladimir Putin restored tanks and missiles to Red Square, merging commemoration with demonstration. Each iteration has redefined what loyalty means, and over time, these narratives have been repurposed to justify modern military policy and to normalize a civic culture in which readiness, obedience, and patriotic duty are everyday values. In short, militarization has deep roots in Russian society.

May 9 parades are also a tool of foreign policy, used to project Russia's global influence and to reinforce external relationships with friendly states. Attendance serves as a soft signal of alignment: governments that send leaders or military contingents are, at a minimum, willing to be seen endorsing Moscow's narrative of victory and contemporary resilience.

In 2025, marking the 80th anniversary of Victory Day, Russia hosted one of its most extensive guest lists since 2022, with 29 foreign leaders expected. Among them were Xi Jinping (China), Luiz Inácio Lula da Silva (Brazil), Aleksandar Vučić (Serbia), and Nicolás Maduro (Venezuela). China also sent a People's Liberation Army (PLA) honor guard that marched on Red Square. Other attendees reportedly included leaders from Zimbabwe, Cuba, Laos, Mongolia, Equatorial Guinea, Ethiopia, South Ossetia, Myanmar, Palestine, and Slovakia.

"Russia has been and will continue to be an indestructible obstacle to **Nazism**, **Russophobia**, and **anti-Semitism**, and will stand in the way of the violence perpetrated by the champions of these aggressive and destructive ideas," said Putin in his speech marking the 80th anniversary of Victory Day during the parade.

The symbolism of the event is carefully orchestrated, consistent with the broader propaganda playbook. Visiting leaders appear alongside Putin during the ceremony and often wear the St. George's ribbon, the black-and-orange badge of wartime commemoration that, since 2014, has also become a marker of modern pro-war identity. The ribbon thus performs a dual role: honoring the memory of WWII while simultaneously signaling acceptance or at least tolerance of Russia's current military policy.

How the war is presented inside Russia matters; it shapes what people expect from the state and what they come to accept as normal. These rituals and symbols are not neutral. For the careful reader, keep an eye on how these symbols evolve, slipping into cybercrime narratives and revealing their intersection with the state's broader information operations.

Figure 1: Chinese President Xi Jinping and Russian President Vladimir Putin during the Victory Day parade, both wearing the black-and-orange St. George's ribbon, a symbol traditionally associated with Russia's wartime commemoration and, in recent years, its modern military campaigns.
Source: CNN

Vladimir Putin himself has become a symbol of Russia and plays a central role in this analysis. Over nearly twenty-five years of his rule, the Kremlin has carefully engineered his image. War leader and defender, patron of tradition and memory, and everyman patriot are among the key archetypes deliberately embedded into his public persona. Central to this construction is the widely adopted belief that "**Russia has risen from its knees**" (Rus: **Россия поднялась с колен**) under Putin's leadership. It functions both as an official slogan actively promoted by the state and as a worldview internalized by much of society. The phrase transforms post-Soviet humiliation and instability into a story of recovery, discipline, and renewed strength, an emotional foundation for the militarized civic order. Within this frame, every reform, military campaign, or confrontation with the West becomes proof of restored sovereignty and historical justice. It also provides moral justification for ongoing military actions, which are often portrayed and widely accepted within Russian society as the rightful reclamation of territories that "belong" to Russia.

Putin thus stands as a living emblem of continuity and control. His appearances and statements are carefully choreographed; when he endorses an initiative, it carries enormous symbolic weight, signaling institutional approval from the highest level. The longevity of Putin's rule also carries a paradoxical benefit for analysis. His twenty-five years in power have produced a remarkably stable political ecosystem, rigid, hierarchical, and deeply structured, which makes it easier to trace how the state's agenda operates and replicates itself across different domains, including the cyber sphere. The system functions through vertical transmission: rules, slogans, and symbols are crafted at the top, then diffused downward through ministries, media networks, educational programs, and civic organizations.

One of the most illustrative examples of this top-down diffusion is the All-Russia People's Front. This Kremlin-backed civic movement operationalizes the state's ideological directives and mirrors its narratives across social, cultural, and digital domains, a structure we examine in the next section.

The All-Russia People's Front Movement
(Patriotism with a Project Manager)

The All-Russia People's Front (ONF) (Rus: **Народный фронт**, **ОНФ**) is a Kremlin-backed civic movement launched at Vladimir Putin's initiative in 2011 and is a clear case study not only of how the state's push toward militarization but also what narratives, tactics, and symbols it exploits to communicate with the masses in pursuing its agenda.

Presented as a coalition of local groups, NGOs, and public figures, it functions as a high-reach platform to legitimize and mobilize support for state priorities. ONF runs extensive on-the-ground activity to build local legitimacy and recruit supporters. Its main initiatives include regional project sessions and public forums; infrastructure and urban improvements; awards and prestige campaigns; humanitarian drives and fundraising for conflict zones; monitoring public projects and anti-waste work (corruption checks); fundraising drives, volunteer mobilization, and youth engagement.

The movement's online presence includes an official website and a Telegram channel launched on January 19, 2017, with nearly 89,000 subscribers as of October 22, 2025. Both reflect ONF's activity but serve different purposes: the website serves as the formal record, including program pages, reports, and official statements, while the Telegram is a higher-reach, more engaging public channel with a slightly different tone and greater audience interaction.

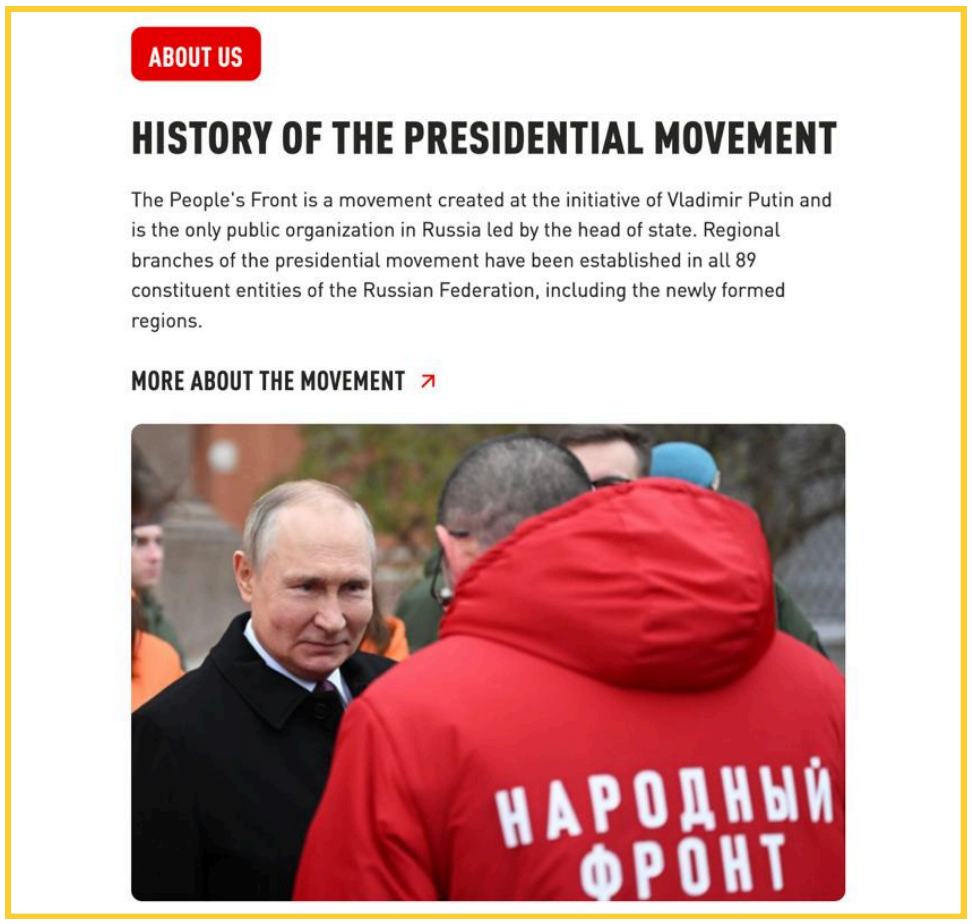


Figure 2: Screenshot of the People's Front website homepage showing Vladimir Putin shaking hands with a man wearing a jacket bearing the inscription "All-Russia People's Front" (Rus: **Народный фронт**).
Source: ONF Website

ONF activity perfectly illustrates what narratives emerged as part of Russia's militarization strategy and, more importantly, how they are integrated into civic life. Both the website and Telegram are useful for analysis, but in this section, we focus on the ONF Telegram channel. We aim to surface the methods and tactics that advance the state's militarization agenda, how they shape the general public, and how they spill into the cyber sphere as our research progresses. To uncover these methods and the narratives pushed by the state, we read ONF's online activity alongside historical and legislative context, capturing both the movement's physical and digital initiatives.

We concentrate on three main pillars that expose both the policy and its delivery mechanisms: **Forming an External Enemy, Justifying Military Actions & Occupation, and Youth Militarization**. Across these, we identify the influence strategies and techniques used to deliver the message to the public.

Forming of an External Enemy

The creation of ONF ran in parallel with an intensifying militarization that became much more visible in the early 2010s. The state leaned on historical memory, the trauma and victory narratives of WWII, and recycled that rhetoric through a Cold War frame to cast the West, especially the United States and the broader Anglosphere, as a persistent external threat. These sentiments were pushed to the masses in part because NATO enlargement and Western support for democratizing movements were framed as threats to Russia's security and influence. Over time, the term "**The Collective West**" (Rus: Коллективный Запад) emerged. The result was a steady drumbeat: Russia is surrounded by enemies and must always be ready.

This narrative found constant reinforcement in the public sphere. Television hosts, historians, and senior officials framed post–Cold War politics as unfinished business, a betrayal of promises made to Moscow, an era where "Russophobia" replaced anti-communism. Victory Day commemorations began to feature not just remembrance of 1945 but warnings about the "resurgence of fascism" in modern forms: NATO troops near Russian borders, color revolutions, and Western sanctions. By the mid-2010s, these narratives had fused with state ideology: patriotism, sovereignty, and vigilance were moral obligations. The civic order became one of permanent mobilization, not against a single enemy, but against a newly formed threat—the West.

The state frames harsh measures as protecting national sovereignty, and the law-making follows that story. To lock that narrative in, the state cleared unwanted voices from the information space and limited foreign influence. In 2012, it passed **the Foreign Agents law**: any NGO that accepted foreign funding and did vaguely defined "political" work had to register, wear a public "foreign agent" label, and file intrusive reports. Human rights groups warned that the law would choke civil society, and it did. Hundreds of organizations were designated, fined, pressured to scale back or close, and in some cases, activists (both Russian and foreign) were criminally prosecuted. The label worked like reputational poison: once branded a "foreign agent," a group was treated as suspect by officials and the public.

Additionally, **the Undesirable Organizations** law adopted by the Duma in 2015 gave prosecutors sweeping powers to ban foreign and international groups deemed a threat. If you weren't already a "foreign agent," you could still be declared "undesirable" and pushed out of civic space. Later in 2017, the foreign-agent rules were extended to media, then to individuals and informal groups. Independent outlets were smeared, audited, shut out of advertising, and in many cases driven offline.

In practice, "foreign" usually meant Western governments, EU agencies, American foundations, and other Western donors. The label drew a sharp "**us vs them**" line: anyone who worked with Western organizations could be framed as doing foreign business inside Russia. That made it easier to delegitimize critics, cut funding channels, and justify tighter oversight, all framed as protecting national sovereignty and security.

In a post dated October 7, 2023, the ONF Telegram channel reposted a message from the State Duma deputy Denis Maidanov, accompanied by a video in which he congratulated Vladimir Putin on his birthday. Maidanov, a popular singer, songwriter, and prominent cultural figure who later became a politician, repeated familiar state narratives, praising Russia for having "**successfully demonstrated to the collective West its ability to resist its hegemonic agenda**". The post reinforced the fusion of politics, patriotism, and popular culture, using Maidanov's celebrity status to amplify a message of loyalty and national strength.

Influence strategy and techniques: Involving famous public figures is a deliberate strategy. The ONF frequently uses well-known personalities to present awards and lend prestige to its initiatives. Regional and national ceremonies feature athletes, actors, and other celebrities who often become ONF members themselves and serve as cultural ambassadors at events. Their participation adds visibility and emotional appeal, blurring the line between entertainment and civic mobilization. These ceremonies are also attended by regional governors and officials, reinforcing the movement's legitimacy and political alignment. Larger Kremlin-area events, such as teacher and volunteer awards, are staged in prominent venues, underscoring the state's endorsement and turning civic recognition into a spectacle of loyalty.

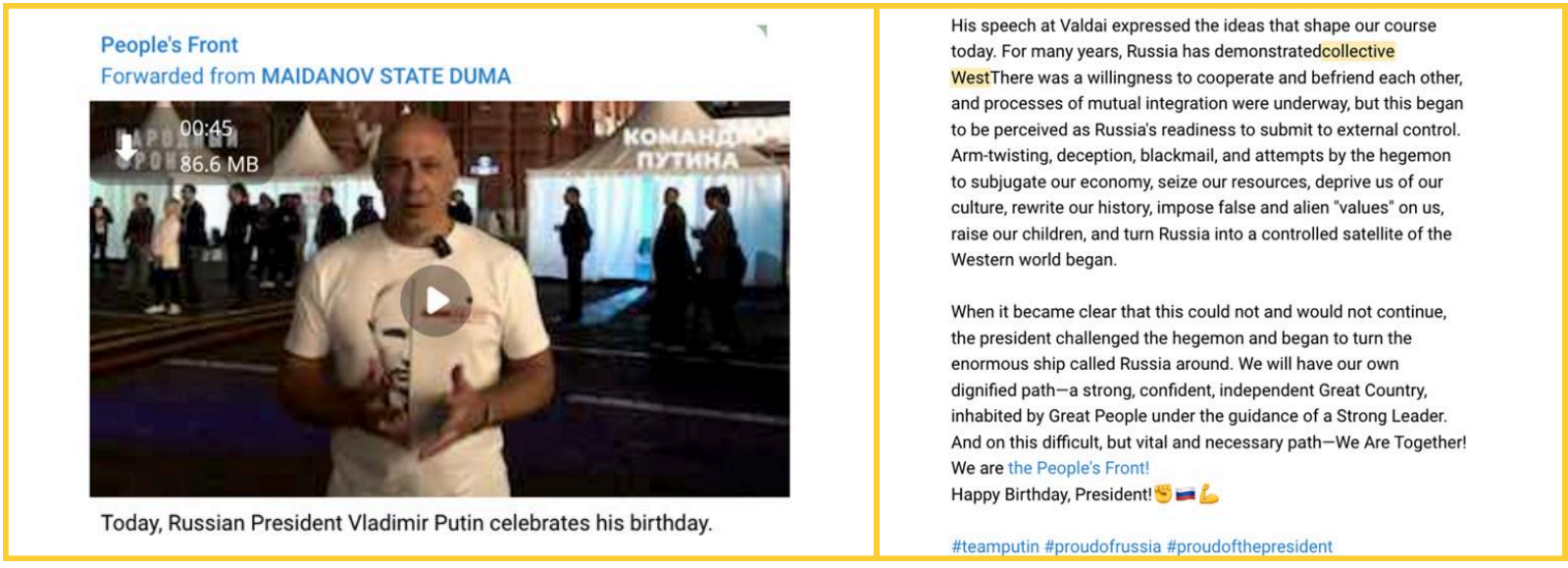


Figure 3: Denis Maidanov, an ONF member and State Duma deputy, featured in a video congratulating Vladimir Putin on his birthday, reiterating the "Collective West" narrative.
Source: ONF Telegram

Justifying Military Actions & Occupation

The escalation of the militarization strategy became overtly physical after 2014: Russia seized Crimea that year, and armed conflict erupted in the Luhansk and Donetsk regions. Moscow moved quickly to implement administrative changes: shortening the path to Russian citizenship, rapid registration of residents, and the wholesale transfer of municipal and legal systems into Russian hands. That bureaucratic push did more than simplify paperwork; it erased legal separation and gave the occupation an ordinary, day-to-day logic.

A dominant theme since then has been legitimizing Russia's takeover of Ukrainian territories. Many early ONF posts focused on civic campaigns and local services following the 2014 annexation of Crimea. Telegram updates about Crimea were part of a coordinated political-communications and governance playbook built around consolidation and legitimation. Once annexation occurred, claims needed social foundations: seizing territory could not remain a purely military or diplomatic act; it had to be made ordinary in daily life. Schools, local administrations, and public spaces became the frontlines of normalization. ONF functioned as an instrument for translating central political claims into local institutional practice, from curriculum changes to urban improvement programs.

Two illustrative posts reveal this approach. On **March 13, 2017**, ONF announced a project session in Crimea's Sevastopol, Bakhchisaray, and Simferopol to upgrade residential courtyards and solicit local input on urban improvement. The post informed readers about upcoming ONF sessions in Crimea dedicated to addressing these issues.

Influence strategy and techniques: The environmental program framed public service as state care. ONF organized sessions, listened to residents, and used the activity to project an image of the state as caretaker rather than occupier. Such performative engagement softens resistance and produces gradual acceptance when amplified by media coverage and local PR operations.

A second post, dated **July 20, 2017**, reported Ministry of Education plans to introduce lessons on Crimea and Sevastopol's "reunification" with Russia. ONF working-group head Lyubov Dukhanina called for a mechanism to rapidly update history curricula.

Influence strategy and techniques: Education operates as a force multiplier for legitimacy. Promoting history lessons and fast-tracking curriculum changes is a deliberate long-term investment: textbooks and classroom activities shape the next generation's perception of Crimea as inherently Russian territory, aligning local memory with state policy.

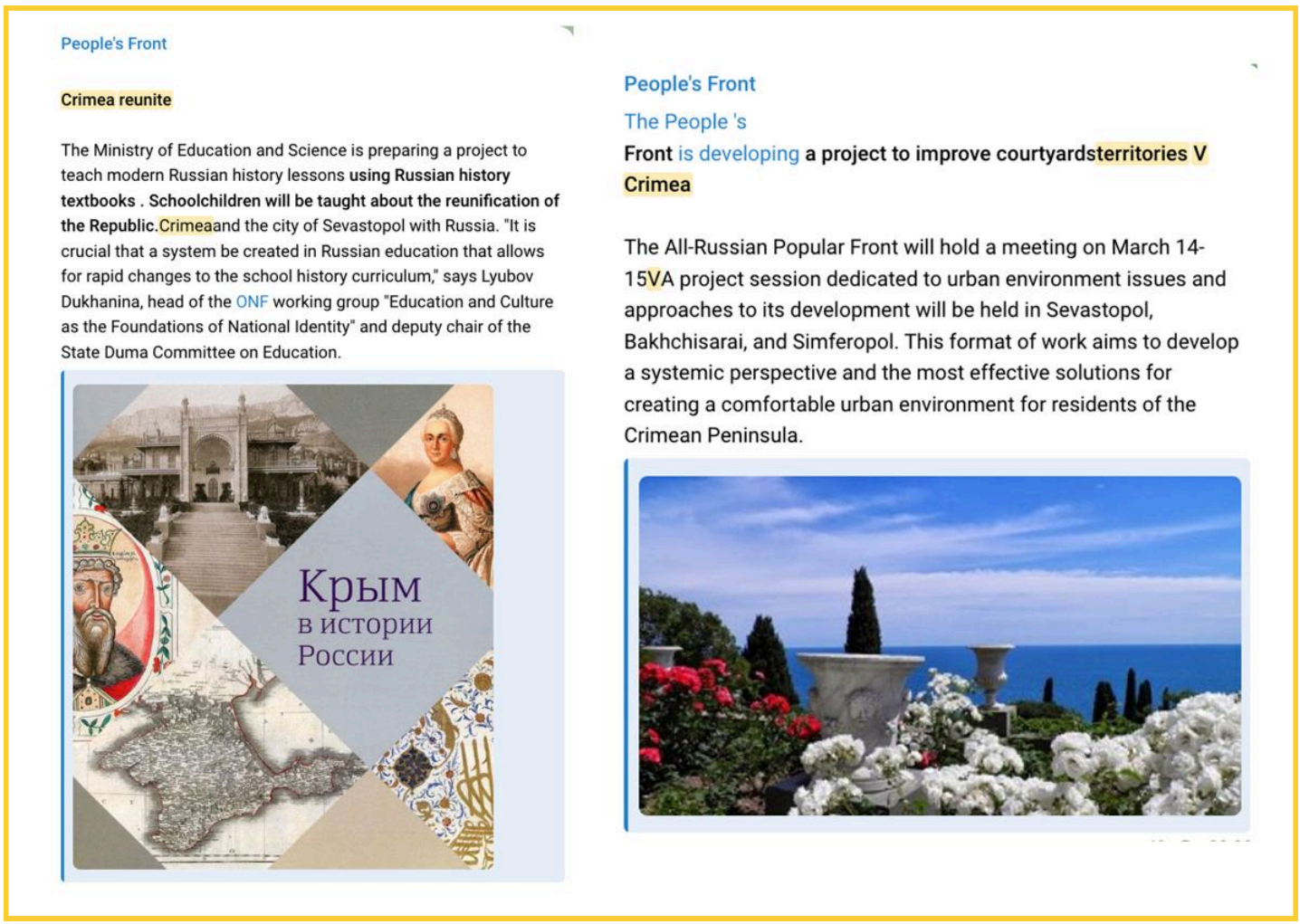


Figure 4: Screenshots of posts (left to right): one announcing upcoming curriculum changes in education, and another showing an ONF session overseeing urban improvement projects in Crimea.
Source: ONF Telegram Channel

Meanwhile, in occupied Donetsk and Luhansk, the conflict that began as street protests and armed takeovers hardened into a war. The self-proclaimed Donetsk People's Republic (DNR) evolved into a hybrid entity, part local militia, part Russian proxy sustained by a steady flow of weapons, advisors, and propaganda. Over time, what emerged was less an occupation than a gradual absorption. Administrative systems, currencies, education, and media were aligned with Russian standards, blurring the boundary between occupied and domestic space. When Russia formally recognized the "republics" in February 2022 and launched a full-scale invasion days later, it marked the culmination of a process long in motion, a war normalized through bureaucracy, rhetoric, and the quiet machinery of everyday governance.

With the start of the full-scale invasion of Ukraine in 2022, Russia's social and political landscape shifted dramatically, accelerating the long-term drift toward militarization. The state moved quickly to tighten control, not only over actions but over language itself. Efforts to dominate the information space intensified to fit the "new reality": laws and narratives were introduced to enforce the official line and suppress dissent. Journalists, citizens, and outlets that referred to the conflict as a "**war**" rather than the sanctioned term "**Special Military Operation**" or **SV**) (Rus: **Специальная Военная Операция**, **СВО**) faced prosecution. In addition, emergency legislation criminalized so-called "fake" reporting about the armed forces and broadly outlawed "discrediting" the military. Overnight, administrative pressure turned into criminal liability.

The ONF's language evolved in parallel. Its tone grew more coercive and overtly militarized, reflecting the state's wartime posture. Messaging shifted toward mobilization, fundraising, recruitment drives, and the legitimization of military actions as a civic duty. The campaign to normalize newly occupied territories continued, framed as humanitarian support and administrative inclusion. ONF communications began highlighting the government's "assistance" to regions newly "added" to Russia. On its homepage (see Figure 2), ONF emphasizes that it now has representatives in all 89 federal subject regions in Russia's count. Internationally, however, Russia is recognized as having 83 federal subjects; the six additional territories include Crimea and Sevastopol (annexed in 2014) and the four regions claimed in 2022: Donetsk, Luhansk, Zaporizhzhia, and Kherson.

In a post dated **November 14, 2024**, the ONF reported that dozens of volunteers from across Russia — Tatars, Buryats, Kalmyks, Ossetians, and Russians — and activists from Dagestan had arrived in the Donetsk People's Republic to support the organization's work in 12 newly "liberated" settlements. The message emphasizes ethnic and regional diversity, framing the mission as a united, multiethnic national effort.

The ONF lists the supplies delivered, food, hygiene kits, clothing, medicine, water, fuel, heaters, and generators, and promotes the "**Everything for Victory!**" (Rus: **Всё для Победы**!) fundraising campaign, urging readers to contribute via donation links. Notably, over time, the "Everything for Victory!" slogan has moved beyond a single initiative. Reinforced by ONF and echoed across state and social media, it has become a national brand, a shorthand for the wartime mood and a vehicle for everyday mobilization.

Influence strategy and techniques: This post exemplifies how ONF communication fuses humanitarian rhetoric with militarized normalization. The language of relief evacuation, medical aid, and reconstruction is paired with militarized slogans, "Everything for Victory!" and patriotic inclusivity listing Russia's ethnic groups. Such framing serves two purposes. First, it embeds the occupation within a civic-moral framework: the "front" becomes not only a military line but a space of collective care and service. Second, it broadens participation, transforming the war into a nationwide project of unity and duty. In addition, fundraising campaign drives serve a dual purpose: they not only gather resources for military and logistical support but also cultivate a sense of belonging and participation among citizens.

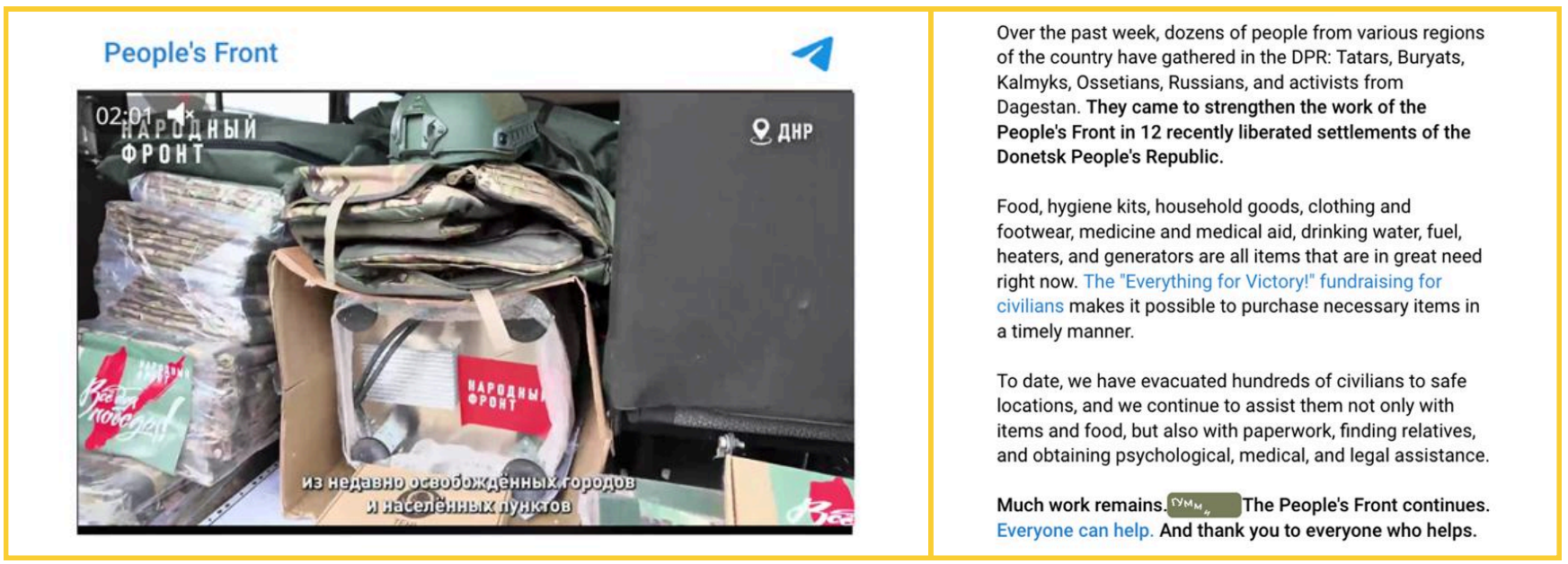


Figure 5: ONF post promoting volunteering and fundraising campaigns aimed at uniting and solidifying society.
Source: ONF Telegram Channel

Youth Militarization

The country's youth play a central role in the Russian state's militarization agenda. It represents not only the future nation but also the future army, a generation the state already envisions as its fighters. The process of youth militarization officially began in 2001, when Vladimir Putin approved **the State Program on Patriotic Education of Citizens of the Russian Federation**, and it intensified throughout the early 2010s.

With the start of the Russia–Ukraine war in 2014, youth programs were visibly recalibrated to serve new political and military objectives, extending even into the newly occupied territories. Within months, schools in both Russia and these regions adopted Russian curricula. History and civics lessons were rewritten so that Crimea's "reunification" was presented as an unquestionable fact. Textbooks, classroom activities, and school ceremonies became instruments for shaping collective memory, a deliberate, long-term effort to embed a new national narrative in children's minds.

The militarization of youth moved quickly from classroom rhetoric to physical practice, a shift from soft patriotism to explicit military preparation. From 2016, **the Young Army** (Rus: **Юнармия**) and similar programs rolled out nationwide: uniformed clubs, drills, camps, and military sports turned civic youth activities into pre-military training. That was no accident; it created a recruitment pipeline and made readiness a normal part of youth life. According to reports, Yunarmiya is expected to receive 1 billion rubles (approximately $11 million USD) in funding in 2025. The BBC produced an excellent documentary on this subject, which readers are encouraged to watch for a deeper understanding.

Figure 6: Screenshots (left to right): an image from a BBC documentary, and a photograph from an article covering Yunarmiya reporting on its current state, budget, and rollout.
Source: The Moscow Times & BBC

An analysis of the ONF Telegram channel reveals a consistent emphasis on youth militarization. A post from **July 18, 2021**, described an ONF-backed event in Yaroslavl called "**Army Move**" for mothers of special-needs children, where participants were issued camouflage and Kalashnikovs, tried drill practice, shooting, and basic parachute elements, and experienced mock special-forces scenarios.

Influence strategy and techniques: In the broader strategy of militarization, events like this offer a playful, low-risk introduction to "war reality." They convert local social programs into visible demonstrations of state care and create soft recruitment pathways through family ties, youth groups, and veteran networks. At the same time, such activities can desensitize participants to violence and blur the line between humanitarian outreach and mobilization, especially when vulnerable groups (mothers of special-needs children) are used as the public face of the program.

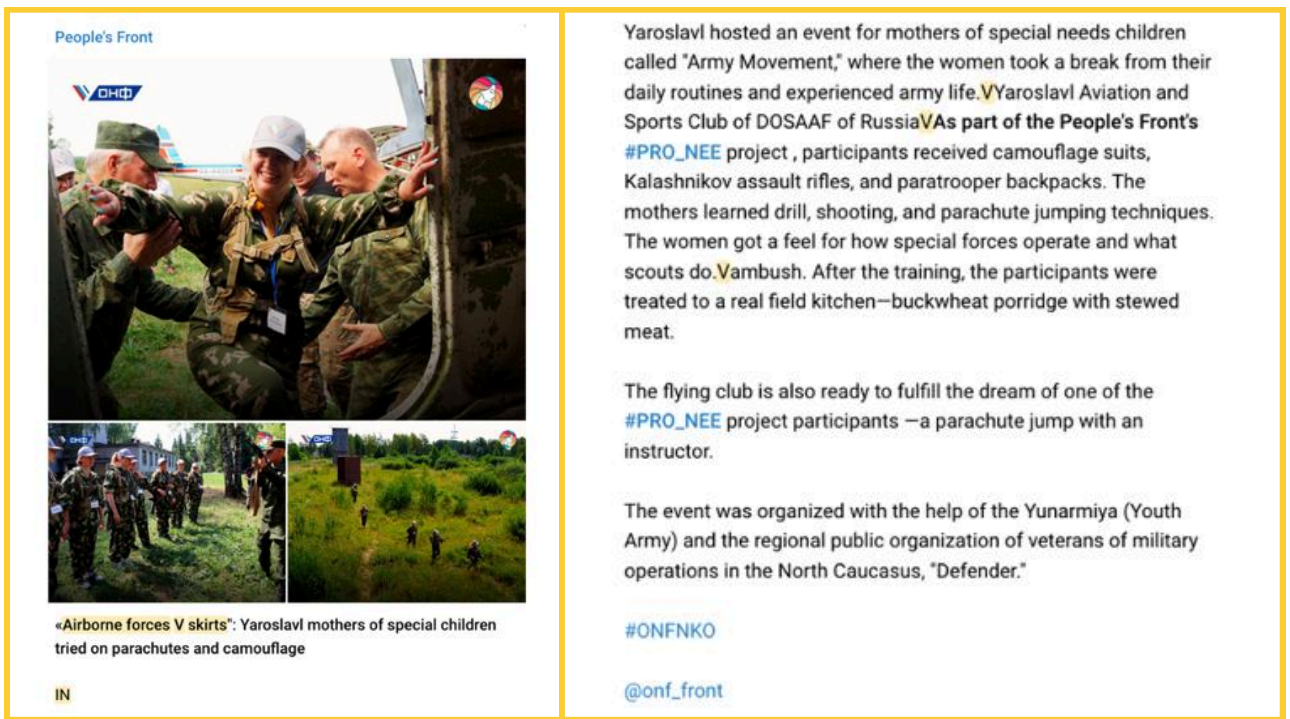


Figure 7: ONF post promoting an event for mothers of special-needs children as part of its youth programs. Source: ONF Telegram Channel

The review of ONF's activity across the three dimensions examined above provides a clear answer to how the narratives of militarization are integrated into civic life. Through campaigns such as "Everything for Victory!" and public rituals of recognition, the organization translates central state narratives into forms of everyday participation, from school programs and volunteer drives to public ceremonies and media storytelling. These mechanisms not only sustain domestic cohesion but also prepare society to function within a permanent wartime framework.

Yet the architecture of this system, its hierarchy, symbolism, and incentives, doesn't stop at the physical level. The same structures now replicate in the digital sphere. With the creation of CyberSquad, which we will analyze in the next section, the state extends its mobilization logic into online life, transforming regular people into "digital soldiers" tasked with defending Mother Russia's information space.

Mobilizing the Motherboard: ONF's CyberSquad

Moving into the digital space was a logical step for ONF. In April 2023, it introduced a new initiative, CyberSquad (Rus: **Кибердружина**), described as a volunteer network tasked with identifying "Russophobic" or otherwise hostile content, encouraging CyberSquad members to file complaints with social media platforms and regulators, and coordinating takedown.

The emergence of CyberSquad fits seamlessly into the broader state agenda of extending narrative control over the information space, an effort that has only intensified since 2022. The expanding legal framework around speech, media, and online behavior has transformed the wartime narrative into law, embedding ideological conformity into everyday life. A series of legislative acts criminalizing "discrediting" the army, defunding organizations labeled as "foreign agents," outlawing "undesirable" groups, and policing language has systematically tightened public expression and institutionalized a new civic order.

However, the state has gone even further from silencing dissenting voices to prohibiting interaction with disapproved content altogether. On July 22, 2025, the State Duma passed a law imposing fines of 3,000 to 5,000 rubles for searching for or accessing materials on the federal list of extremist content. This law criminalized not just speech, but curiosity itself.

Russia's list of banned extremist materials, maintained by the Ministry of Justice of the Russian Federation (Rus: **Минюст России**), functions not only as a legal registry but also as a mirror of the state's political fears and priorities. Per our analysis, as of October 21, 2025, the list contained 5,484 entries, ranging from religious pamphlets and nationalist songs to blog posts.

In essence, the Russian government's classification of extremism is not about objective threat assessment, but about narrative management. Across religion, politics, and culture, the "extremist" label operates as a flexible boundary around acceptable thought and speech. This is not a war on extremism; it is governance by suppression, a system in which the definition of "extremist material" matches the state's political needs and criminalizes dissent, even symbolic or artistic form.

The CyberSquad's activities serve the broader agenda of controlling the information space, effectively reinforcing the state's efforts to regulate speech and shape the public narrative. In addition, it shows the state's attempt to enlist citizens in a form of digital conscription, transforming online participation into a civic duty.

Moreover, as explored further, CyberSquad's behavior mirrors pro-Russian hacktivist groups in its effort to serve as a counterforce to other hacktivist movements, including pro-Ukrainian ones, extending the "information war" into a cyber one. The digital underground, much like the physical battlefield, is divided. Pro-Russian and pro-Ukrainian collectives engage in a continuous cycle of attacks and public taunts, becoming their own form of trench warfare. In our previous research, we documented one such episode: a joint attack by pro-Ukrainian and pro-Belarusian hacktivist groups against Russia's Aeroflot, illustrating how digital operations often echo real-world geopolitical conflicts.

To begin with our analysis, let's take a look at the CyberSquad's volunteer cyber patrol ecosystem and its structure. To clarify, all of the CyberSquad messages are originally in Russian and were translated by an analyst into English. According to the ONF website, anyone can join CyberSquad by following the registration link, becoming a member, and immediately receiving digital assignments. The work combines both promotion and policing: volunteers are encouraged to "support your own" by amplifying content from pro-Russian bloggers and channels to expand their reach, while simultaneously engaging in moderation, identifying and reporting material across popular platforms for removal or restriction.

Figure 8: Homepage of CyberSquad, displaying its description and links to its two primary Telegram sources.
Source: ONF Website

As promoted on the ONF's official website, the initiative directs users to two primary Telegram sources: the CyberSquadBot and the "Russian Truth" (Rus: **Русская Правда**) channel.

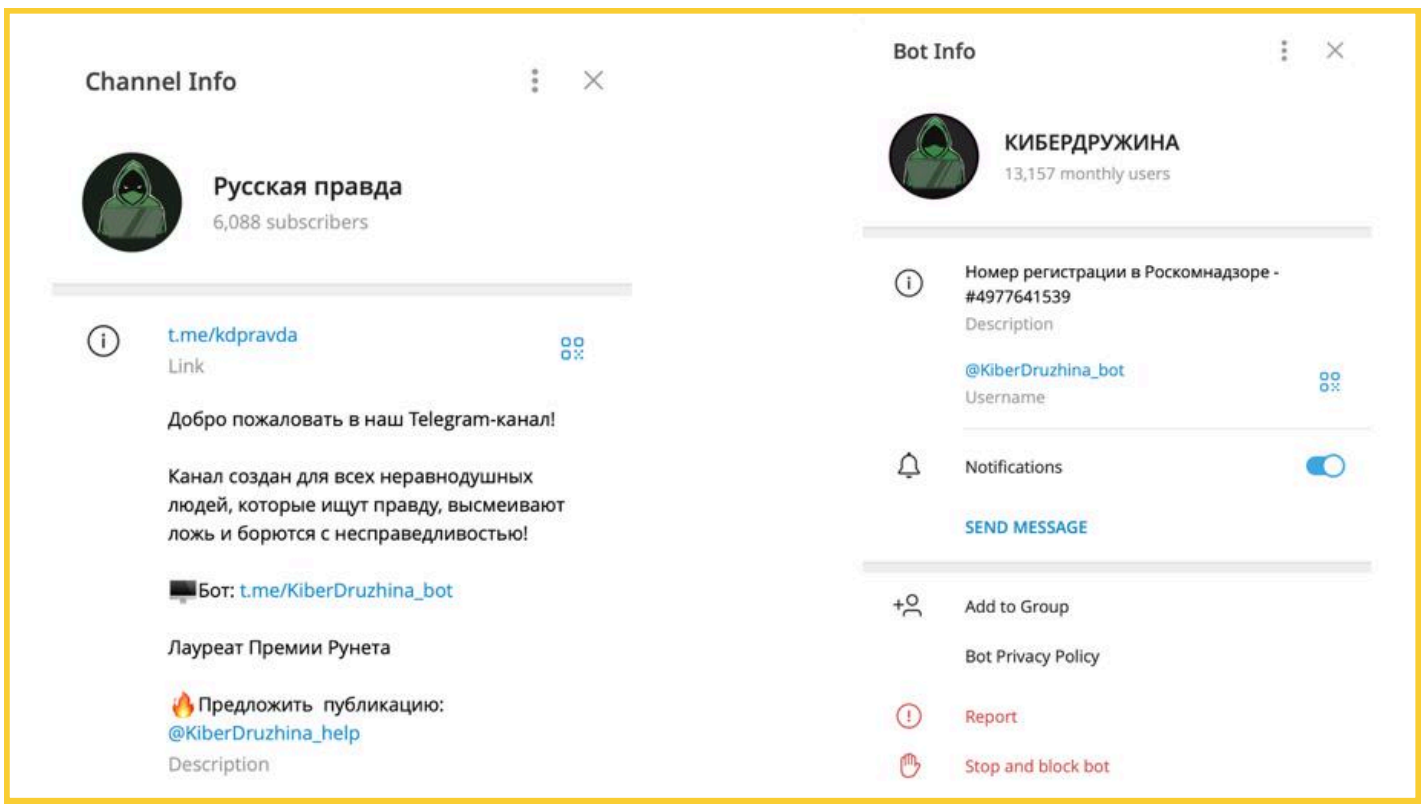


Figure 9: Two screenshots (left to right) displaying the CyberSquad Channel and Bot pages.
Source: CyberSquad Telegram Channel and Bot

CyberSquad bot operates as a bot-based system for onboarding, task distribution, and a points-based ranking hierarchy. For our analysis, we interacted with the bot to examine its activity and task structure. Upon joining, the bot welcomes new participants with a message. It immediately assigns them a military-style rank, a clear use of gamified hierarchy designed to instill a sense of belonging, discipline, and mission-oriented purpose.

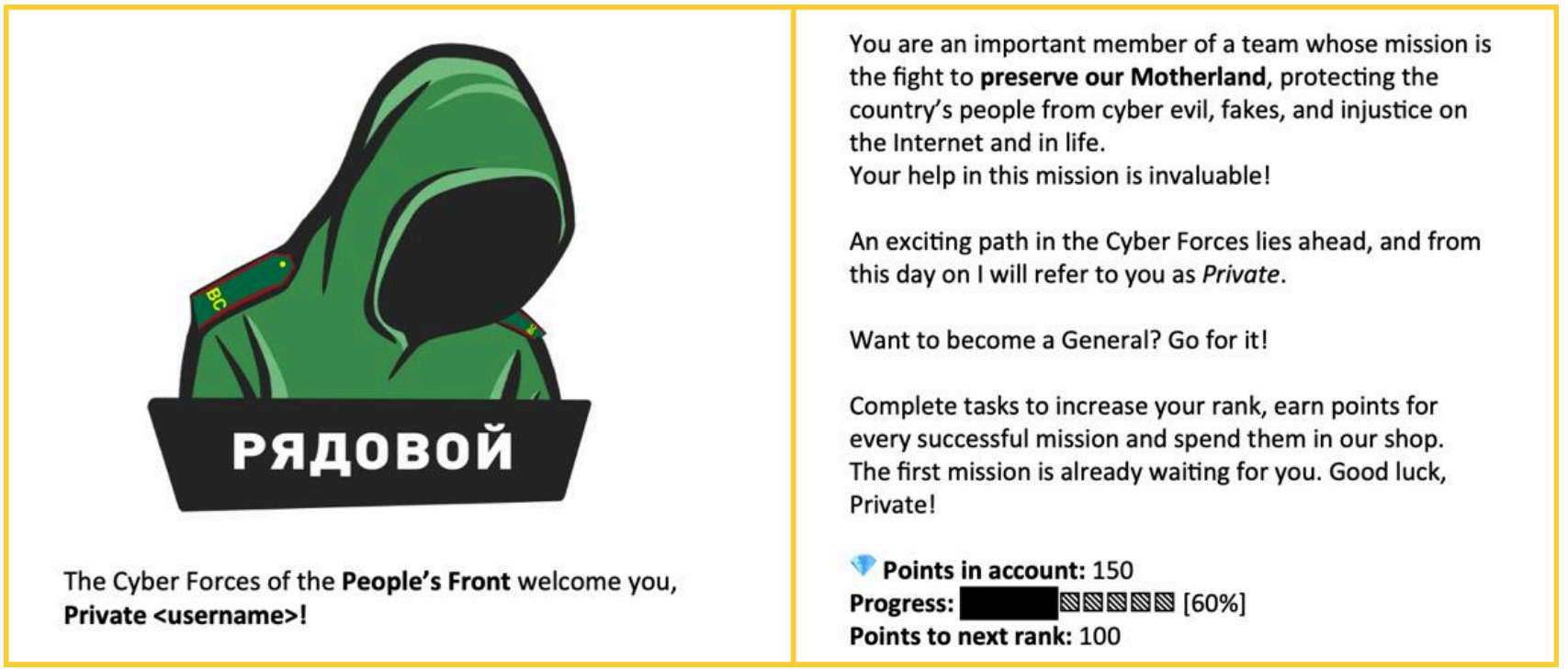


Figure 10: Welcoming message from the CyberSquad bot, automatically assigning the user a military-style rank of "Private" (Rus: **Рядовой**) upon initial interaction.
Source: CyberSquad Bot

Then we navigated to the "**Tasks**" section, which redirected us to the daily task list. One of the assignments involved submitting a complaint against content identified as "Russophobic", in this case, published by the **OSINT Bees** (Rus: OSINT **Бджоли**) Telegram channel. According to our analysis, OSINT Bees is a Ukrainian volunteer OSINT collective established in April 2022, describing itself as non-commercial and independent, focused on supporting Ukraine's defense against Russian aggression, identifying Russian war criminals and Ukrainian collaborators, and assisting accountability efforts.

Upon selecting an assignment from the task list, CyberSquad redirected us to the OSINT Bees post below. The post identifies a chief designer at the Malakhit Marine Engineering Bureau and calls for sanctions against him. The CyberSquad task frames this as "Russophobic" activity and instructs volunteers to mass-report the post for removal.

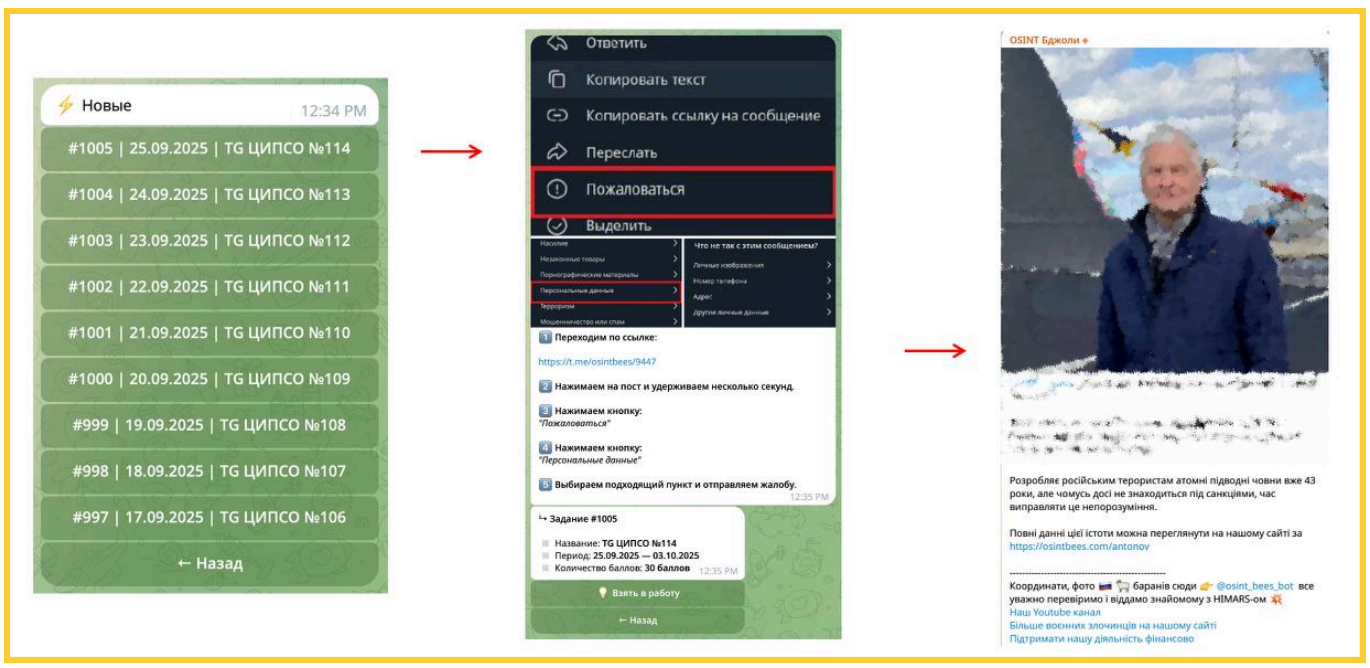


Figure 11: Images showing the CyberSquad bot interface: the first two screenshots display a list of tasks instructing users to submit complaints and report "Russophobic" content. In contrast, the final image (right) shows the targeted post slated for ban.
Source: CyberSquad Bot & OSINT Bees Channel

To motivate its members, the CyberSquad uses a rewards system that lets participants earn points, which increase their rank and build their "career" within the project. Each completed task grants users points, 30 points in the specific example described above. Participants can then spend these points in an in-app store on various rewards such as branded merchandise, Telegram Premium subscriptions, or access to additional missions. In addition, CyberSquad members receive public recognition during official ceremonies, further intensifying their engagement and promoting the initiative to a broader audience. This strategy reinforces a sense of pride and belonging, transforming digital participation into a publicly validated act of patriotism.

The Telegram channel **Russian Truth** plays an important role in the CyberSquad digital ecosystem. It functions as an amplifier channel that serves three main purposes:

- Direct calls to action: Bot links and submission handles in headers provide low-friction pathways for user participation. Digital monitoring is reinforced through the regular publication of CyberSquad metrics, such as the number of blocked pages or videos (for example: “22 pages blocked on Odnoklassniki, 14 YouTube videos”).
- Social rewards: Public recognition of volunteers and “awardees” reinforces loyalty through visible status. One example is the coverage of the official award ceremony for three CyberSquad participants, all citizens of occupied Donetsk. The three men were presented with “Everything for Victory” badges for their work guarding the internet and countering so-called Russophobic content.
- Narrative Keeping: The channel maintains a strongly militarized framing, featuring public praise for CyberSquad volunteers. Its content often includes mocking or hostile portrayals of opponents through ironic memes, quotes, and visual satire targeting Western actors and Ukrainian forces, which reinforce an “us vs. them” mindset. Most posts are short, image-heavy, and frequently forwarded, designed for quick consumption and viral sharing. The repeated use of slogans such as “Everything for Victory!” further ties everyday digital engagement to the broader wartime narrative of unity and loyalty.

Figure 12: Three CyberSquad participants are being awarded the “Everything for Victory” badges in recognition of their contributions to CyberSquad activities.
Source: https://dontimes.ru/

CyberSquad shows how ordinary citizens are softly integrated into militarized structures by becoming digital soldiers. Through state-promoted patriotism and appeals to civic duty, the program invites individuals to take part in defending the “information front.” Together, these mechanisms demonstrate how gamification and digital control have become central tools in Russia’s broader militarization strategy. Through ranking systems, reward points, and public recognition, the ONF’s CyberSquad transforms civic participation into a structured form of digital service. This dynamic blurs the line between civilian engagement and digital warfare, fusing entertainment and surveillance into a single, continuous system of mobilization.

The ONF’s activities receive top-level validation, reinforcing the perception that participation in CyberSquad is not merely volunteering but contributing to a sanctioned, patriotic mission aligned with the Kremlin’s goals. At the ONF forum “Everything for Victory!” on July 7, 2025, President Vladimir Putin personally praised CyberSquad, noting that it already included about 60,000 “**hardened, experienced fighters, programmers, and IT specialists who fight for the country, for the truth**”, on the digital front.

The setting itself was carefully choreographed: behind Putin, two large banners read “Everything for Victory” and “All-Russia People’s Front”, a visual synthesis of patriotism, mobilization, and organizational legitimacy. Putin’s direct endorsement serves as a signal of approval from the highest level of power, granting the initiative not only institutional credibility but also symbolic authority.

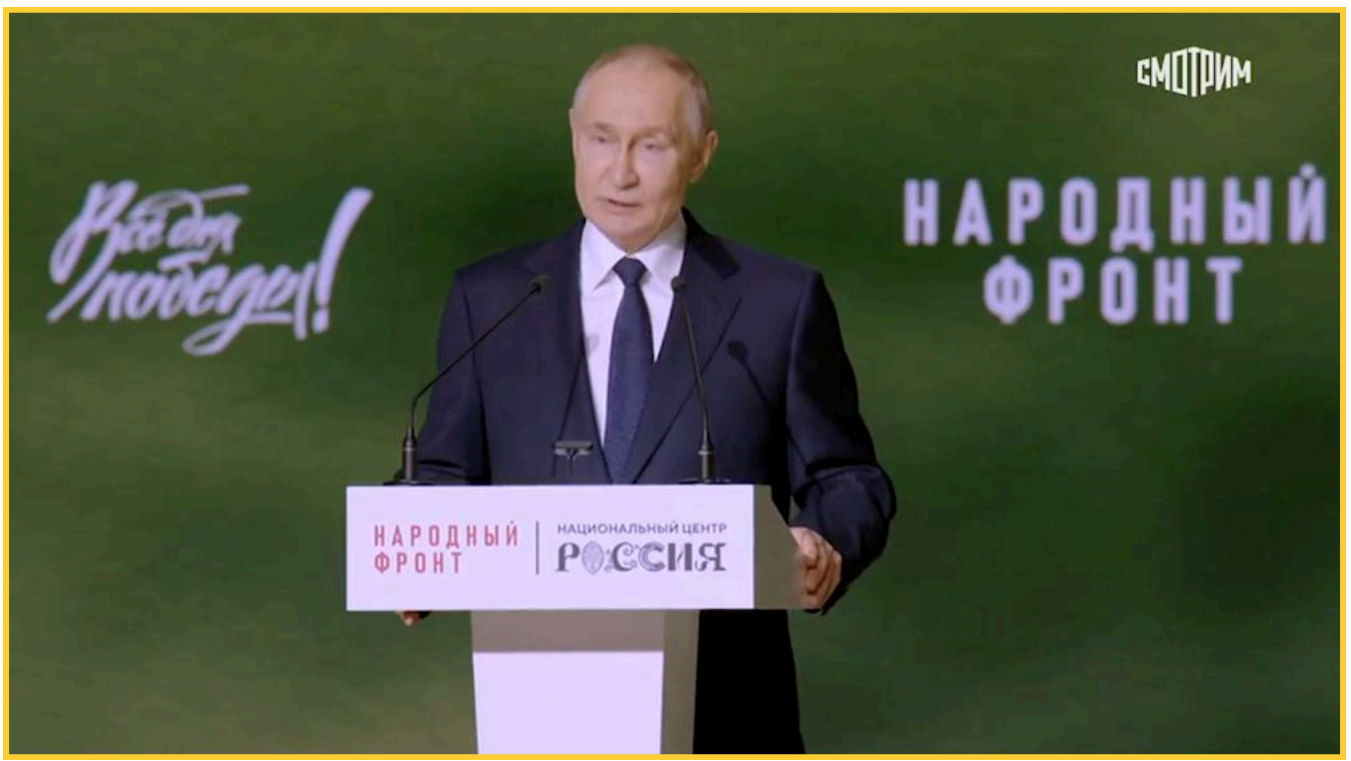


Figure 13: Vladimir Putin delivering a speech at the ONF “Everything for Victory!” forum, where he praised CyberSquad and its members for their role in defending Russia on the “digital front.”
Source: Dzen

Putin’s involvement once again lends legitimacy to the ONF project. It immediately signals that the behavior promoted by its activities, including those in the digital sphere, is approved and encouraged from the highest level of power. To further connect the leader with the public through symbols of loyalty and belonging, the ONF introduced another emblematic initiative: the “**Putin Team**” Award (Rus: **Премия «Команда Путина»**), launched in October 2022.

The award celebrates citizens who **“help the Motherland”**, explicitly including professionals and volunteers whose work supports regional development and, since 2022, the invasion of Ukraine. It reframes wartime contribution as civic virtue, publicly honoring those whose labor, teaching, or volunteering aligns with state priorities. Awards are presented at both national and regional ceremonies, often attended by local officials, governors, and cultural figures. Celebrity presenters, such as athletes and actors, add visibility and prestige, reinforcing the award’s aspirational tone.

Over time, the “Putin Team” evolved beyond an award into a slogan and lifestyle brand used to further unify participants and project loyalty to the masses. Badges, hoodies, caps, and T-shirts are distributed to volunteers and event participants, and also sold through online stores. Templates and design kits (shared via Yandex Disk links) are made available for regional adaptation, transforming political loyalty into wearable identity. These visual symbols, along with the St. George’s ribbon, function as portable signs of belonging. Wearing them signifies more than affiliation; it marks participation in a civic-military identity project that merges political loyalty, cultural symbolism, and emotional attachment into a single, state-defined expression of patriotism.

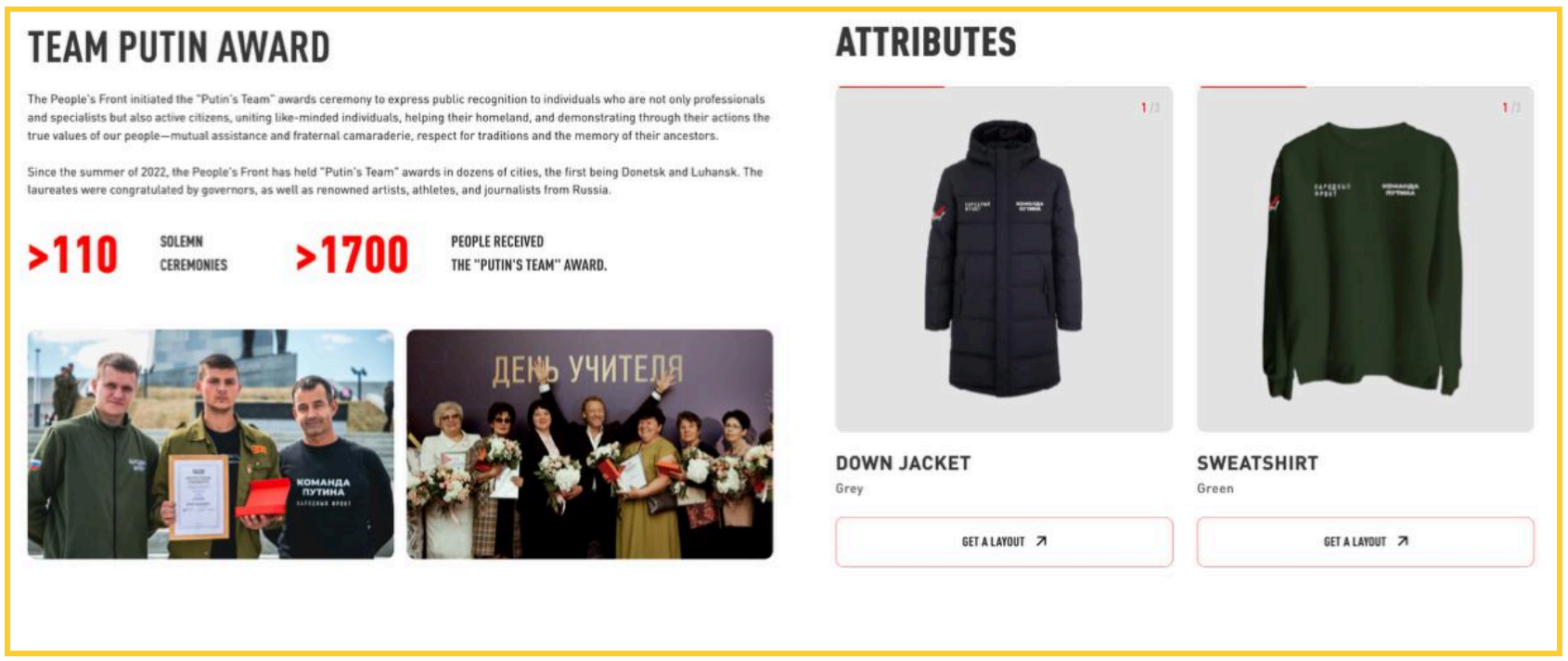


Figure 14: Screenshots showing the "Putin Team" award page and the merchandise page on the ONF website.
Source: ONF Website

Ever wonder who else gets all that "Putin Team" merch? Well, apparently, REvil, one of Russia's most notorious ransomware gangs, is on the fan list too. These are the same actors arrested after the Kaseya attack, the one that coincided with the Biden–Putin summit in Geneva in 2021 and later pushed through a series of high-profile court hearings. At one such hearing, one of the accused showed up wearing a "Putin's Team" sweatshirt. Because nothing says "we're misunderstood entrepreneurs" like state-endorsed leisurewear.

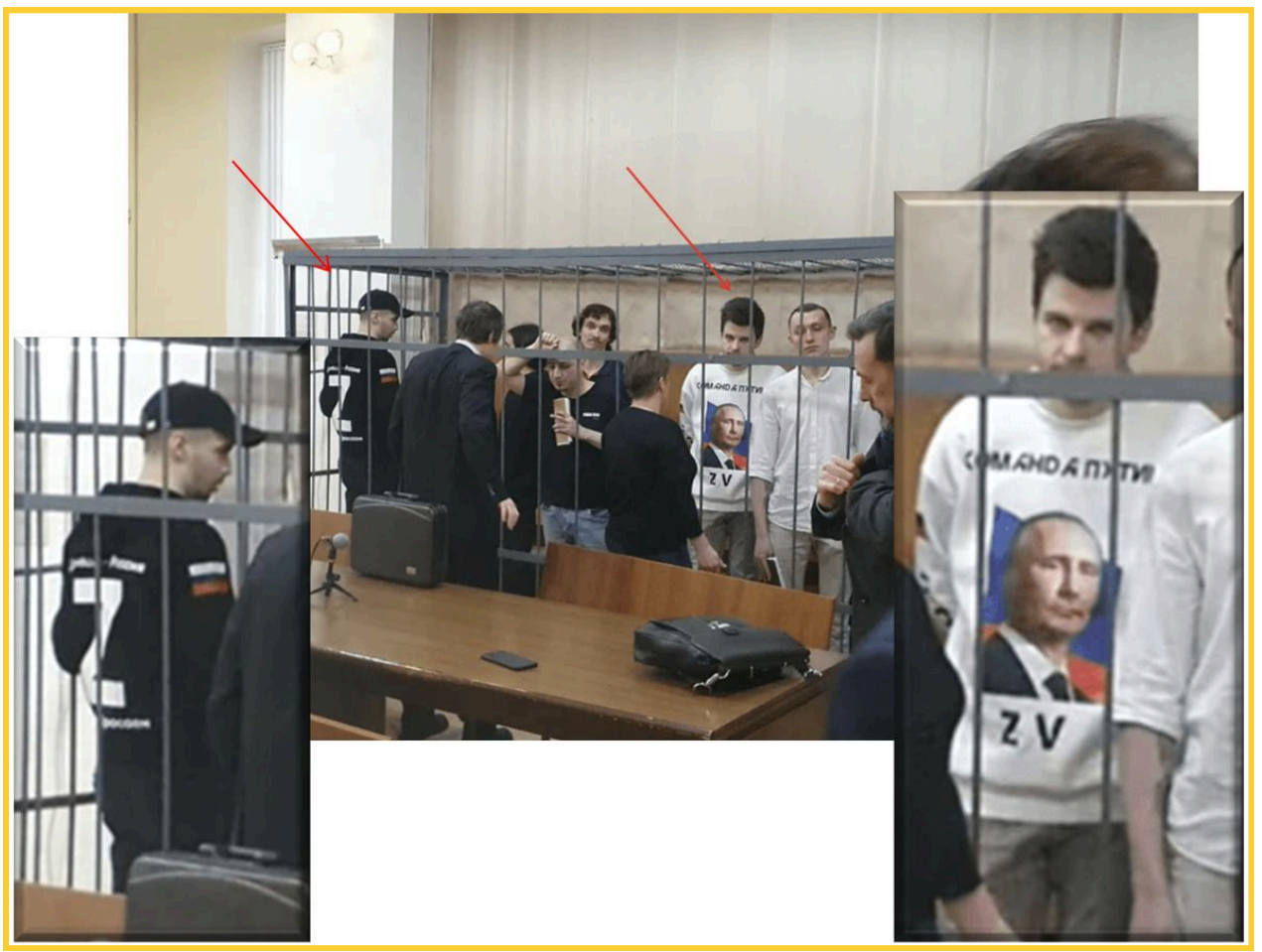


Figure 15: REvil defendants during a Russian court hearing, one wearing a "Putin's Team" sweatshirt and another dressed in a "Z" hoodie featuring the Russian flag merging official state ONF symbolism with cybercrime
Source: Kommersant

The scene is almost too good to be true: ransomware operators in patriotic merch, standing behind bars, unintentionally capturing the perfect fusion of propaganda, performance, and power. And the irony doesn't stop there. The Cyber Army of Russia, the so-called hacktivist group we'll examine next, is just as saturated with symbols, slogans, and theatrics. As we move forward, the question, long whispered in cybersecurity circles, comes back sharper than ever: Is the state involved in Russian cybercrime and in hacktivist groups' activities? To answer that and assess its influence, we turn to the language of signs, signals, and symbols, because sometimes the propaganda logos say more than the payloads ever could.

Nyet or Da on State Ties to Pro-Russian Hacktivists: Putting Red Strings on the Conspiracy Board

First, let's be clear: hacktivism, especially modern hacktivism, is cybercrime, regardless of its origins. It's destructive, often causes real-world harm, and shouldn't be sugar-coated as merely "digital protest." Suspicions that Russian cybercriminals and the state might be cooperating have circulated for years. But are they really marching together, and what evidence would point to that? That question sits at the core of this analysis. Historically, the answer leans toward yes. There have been multiple documented cases in which Russian government officials, particularly from the FSB and GRU, were charged or publicly implicated in cyberattacks and coordinated criminal operations. In addition, Moscow's reluctance to take action is a signal of approval as well as, in some cases, with visible support, as we will see further in this section.

Oops, We Did It Again: Past Cases of State Involvement

One prominent example is the Yahoo breach, which directly involved FSB officers. On March 15, 2017, the U.S. Department of Justice indicted Dmitry Dokuchaev and Igor Sushchin, both active FSB agents, along with two criminal co-conspirators, for hacking 500 million Yahoo accounts. The operation targeted not only users for profit but also Russian journalists, U.S. and Russian officials, telecom and finance employees, and even a Russian cybersecurity company, a target list consistent with state intelligence priorities.

The Yahoo case serves as a textbook example of how the Russian state and cybercrime ecosystems overlap, with the state effectively using criminals as assets. The two FSB officers were not bystanders; they were in command. Dokuchaev served inside Center 18, the FSB's cyber unit, ironically, the very bureau meant to liaise with the FBI on joint cybercrime investigations. As the DOJ put it, "The criminal conduct at issue, carried out and otherwise facilitated by officers from an FSB unit that serves as the FBI's point of contact in Moscow on cybercrime matters, is beyond the pale."

One of the conspirators, Alexsey Belan, was already a notorious cybercriminal, publicly indicted in 2012 and 2013, and named to the FBI's Cyber Most Wanted list in November 2013. An Interpol Red Notice for his arrest had been out there since July 26, 2013, including with Russia. Belan was detained in a European country in June 2013 on a U.S. extradition request, but escaped to Russia before extradition could take place.

Rather than arresting one of the FBI's Most Wanted hackers, the FSB turned Belan into an asset. Instead of handing him over, they used him to infiltrate Yahoo's internal systems, effectively outsourcing state operations to a career criminal. While the FSB pursued intelligence collection, Belan simultaneously monetized the stolen data, selling access and running spam operations for profit. The result was a hybrid operation: espionage at the top, cybercrime for profit below, functioning seamlessly under a single command structure.

Ransomware actors follow the same pattern. Russia dominates the ecosystem, and despite years of U.S. and EU indictments, Moscow provides little meaningful assistance in arrests or extradition. Since 2021, at least eight individuals linked to LockBit and other ransomware groups have been indicted. Of these, three were eventually prosecuted, while five are believed to remain in Russia, effectively untouchable.

What does that imply about state posture? Russia routinely rejects foreign legal cooperation on cybercrime, especially amid the ongoing war in Ukraine and the broader geopolitical confrontation with the West. This creates a safe-harbor effect: indicted actors who stay on Russian soil are shielded from prosecution and can continue operating with minimal consequence.

This situation fuels a persistent hypothesis in the research community that some ransomware operators serve as usable assets or implicit bargaining chips for the Russian state. The REvil saga, with its cycles of arrests, quiet releases, and sudden reappearances, suggests that when state interests are at stake, cybercriminal cases can be leveraged as policy tools rather than prosecuted as crimes.

While it is not direct evidence of a direct command-and-control, the consistent non-cooperation, coupled with documented cases of state officials working with criminals (as seen in the Yahoo/FSB case), reinforces the hypothesis. The outcome is a structural trust gap: when law enforcement agencies are implicated and offenders remain protected domestically, international partners default to distrust, undermining collaboration, takedown operations, and global deterrence.

If protecting cybercriminals wasn't already a message, Russia took it a step further by literally laying out the red carpet. On August 1, 2024, in a highly choreographed diplomatic exchange, Russia welcomed back convicted hackers Vladislav Klyushin and Roman Seleznev as part of a multinational prisoner swap. State TV showed them stepping off the plane to a warm reception from Vladimir Putin, who personally thanked them for their **"loyalty to the Motherland".**

This scene wasn't just a ceremony; it was a signal. By celebrating the return of convicted cybercriminals, the Kremlin effectively blurred the line between crime and service. The message to the cybercrime community is clear: as long as your actions target "the enemy" and serve Russia's interests, you'll be protected, perhaps even honored. It's not just a pardon; it's encouragement. In Russia's current wartime logic, cybercrime against adversaries is framed as patriotism. Putin's personal involvement adds the final seal: approval from the highest level of power.

Figure 16: Vladimir Putin personally welcomed individuals from the Russia–U.S. prisoner exchange, greeting them at the airport. Source: WSJ

In the case study that follows, the Cyber Army of Russia illustrates how state influence can shape and steer cyber operations. Claims of direct state control require the highest level of assessment evidence and must be approached carefully. However, state influence through ideology, incentives, and social conditioning can still be assessed probabilistically. To do this, we analyze messaging signals, explicit slogans, references to geopolitical events, patriotic calls to action, and the deliberate targeting of the state's declared enemies. These markers help us estimate the likelihood and degree of state influence, whether direct or indirect, revealing how political narratives migrate into the cyber domain and transform digital operations into instruments of national strategy.

Cyber Army of Russia Case Study

When Russia invaded Ukraine in February 2022, the physical battlefield quickly extended into the digital domain with the emergence of so-called hacktivist groups. Early operations focused on website defacements and denial-of-service attacks, flooding the information space. However, what initially looked like typical grassroots hacktivism soon revealed a different reality: the forces behind many of these operations differed from typical hacktivist collectives.

In our previous research, we identified core characteristics of these modern hacktivist groups that operate with the structure, discipline, and strategic alignment typical of state-linked operations. These groups exhibit a high degree of coordination, extensive membership networks, and activities that closely mirror or support state objectives. The likelihood of government influence, whether direct or indirect, is high, as their campaigns frequently advance the state's political or ideological goals.

Cyber Army of Russia (CARR) was part of this crowded pro-Russia hacktivist ecosystem and closely aligns with these characteristics. The group emerged in March 2022, with its first Telegram channel, CyberArmyOfRussia, registered on March 4, 2022, and later moved to a second channel, CyberArmyofRussiaReborn (now defunct), registered on April 1, 2022. In addition, CARR maintained accounts across other platforms, including Twitter, Instagram, YouTube, and Telegraph.

To analyze potential state influence, we focus on the group's Telegram activity, which served as its primary communication channel. We identify measurable signals, such as symbols and slogans, recurring communication patterns, and observed similarities with known official initiatives (e.g., the previously analyzed CyberSquad). To assess potential connections and the degree of state influence, our evaluation is structured around three main categories:

1. **Symbolism & Content Signals**
2. **Targeting Patterns & Language**
3. **Media Support Analysis**

Symbolism & Content Signals

Content signals and symbolism are essential tools in any propaganda effort. They create a sense of unity and order, allowing consistent messages to resonate across domains and effectively bind individuals to a shared ideological framework. When CARR launched, its very first messages already felt... familiar. Too familiar. The group's slogans, tone, and symbols echoed the Kremlin's talking points almost word-for-word, like a digital echo chamber rehearsing a script from Moscow. Published both on its Telegram channel and mirrored in a Telegraph article, the message read:

"Ukraine, under the leadership of the United States, has launched an information war against our citizens. We created this movement to respond together to any actions directed at our compatriots. All our operations aim to convey a simple message — we will not tolerate threats to our country's security."

Original in Russian with all emojis retained for contextual accuracy: “**Украина 🐷 под руководством Соединенных Штатов 🇺🇸 развернула информационную войну против наших граждан. Мы создали это движение, чтобы вместе реагировать на любые действия, направленные против наших соотечественников 🇷🇺. Все наши операции направлены на донесение простой мысли — мы 👊 не приемлем угрозу безопасности для нашей страны. ⚔️**”

It reads less like a hacker manifesto and more like a Ministry of Defense press release with emojis. The tone is too clean, too rehearsed, and too official. In short, ordinary people don’t usually speak this way. This opening statement mirrors the state’s information playbook almost perfectly. The West as aggressor, the defense of Russian citizens, and the moral justification of (digital) warfare are the same pillars that have anchored Russian state communication since 2014. By echoing this discourse, CARR positions itself not as a spontaneous hacktivist movement but as part of a broader information mobilization network in which patriotic defense, propaganda, and cyber activity converge under a single ideological banner.

Visuals and symbols actively used by CARR, as they do more than decorate a message; they synchronize meaning. Many of the symbols mirror those long adopted and promoted by the Russian state, many of which we’ve described throughout this research. In the three images below (from left to right), we see a clear example of the extension of state messaging, translating familiar wartime symbols into the language of the digital front.

In the first image, the “Z” is rendered in St. George’s ribbon colors. What began as a WWII commemorative symbol has been repurposed as a carrier of the present ideology. Since the full-scale invasion of Ukraine in February 2022, the “Z” itself became a civilian badge of loyalty, a shorthand for alignment with the state’s “special military operation.” It also appears inside slogans like “**За Свободу**” (Eng: For Freedom), mixing the Latin Z with Cyrillic to brand loyalty linguistically as well as visually.

The second image shows a visual pairing of a Russian soldier and a Ukrainian fighter associated with Azov, a formation of the National Guard of Ukraine that began as a volunteer militia in 2014. Framed by the slogan “Good conquers evil” (Rus: **Добро побеждает зло**), the moral coding is explicit: the Russian soldier embodies duty and righteousness; the Ukrainian is cast as evil.

On a third image, a screenshot of CARR’s Twitter account. The profile lists Mariupol (an occupied Ukrainian city) as its location, a move of digital territorial signaling, not random geography but a claim of ideological sovereignty that aligns online activity with physical occupation. The page also invokes Putin’s well-known line, “If a fight is inevitable, strike first” (Rus: **Если драка неизбежна, бить надо первым**). Once said by Putin during a press conference, the quote has since been widely circulated across the media, capitalizing on Putin’s image and functioning as a moral warrant for preemptive action. On a hacktivist channel, cyberattacks are reframed as acts of national defense, less a breach of law than a duty to protect.

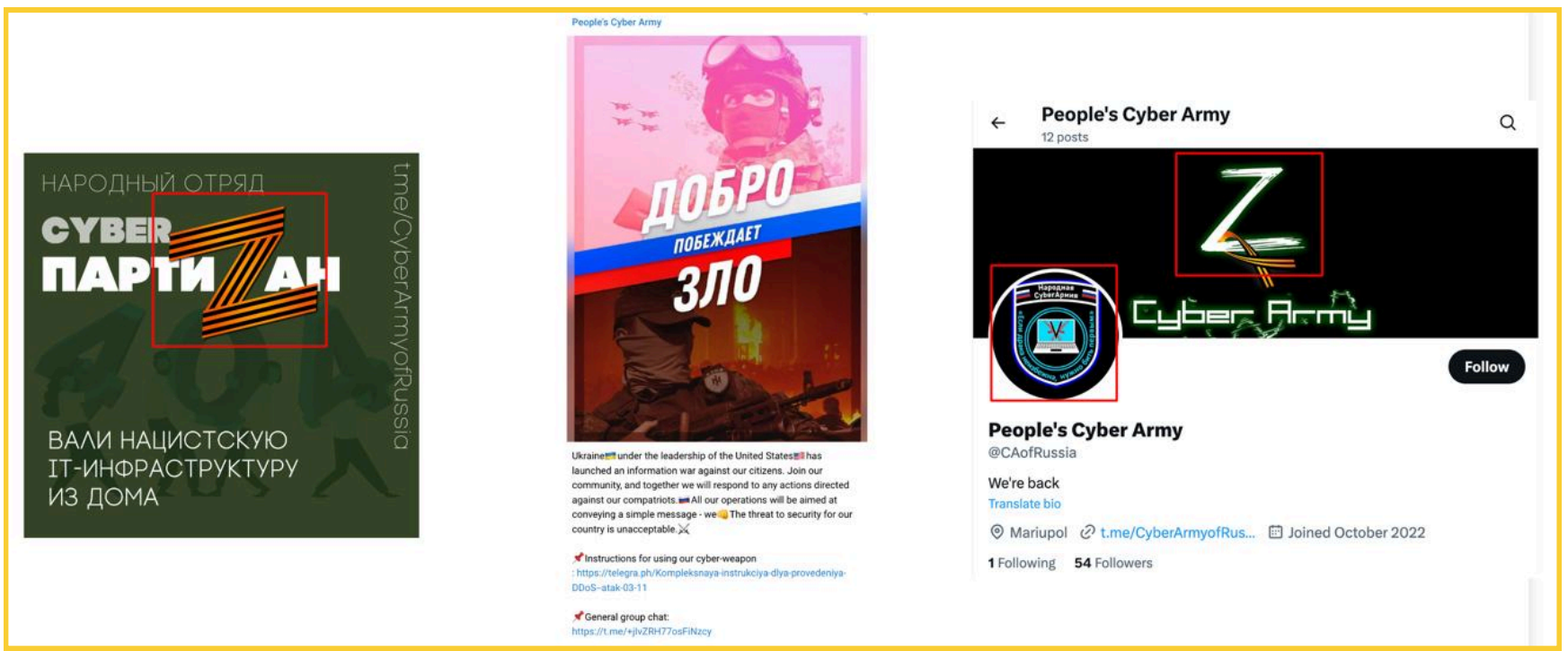


Figure 17: Screenshots from left to right show symbols and narratives used by CARR that mirror Russia’s state narratives and the visual language employed in official campaigns.
Source: CARR Telegram, Telegraph, and Twitter

Targeting Patterns & Language:

Targeting patterns are another key indicator of potential state influence or alignment, and the CARR Telegram channel is an excellent source for this analysis. Each attack claimed by the group was highly publicized by design, consistent with the performative and demonstrative nature typical of hacktivist-style operations. Their posts not only showcase technical actions but also embed narrative framing that mirrors official discourse, messages amplified through state-aligned media outlets and affiliate Telegram channels that act as force multipliers for visibility.

The intensity and complexity of CARR's operations have steadily grown, supported by coordinated information campaigns. Initially focused on DDoS attacks, their methods quickly expanded to include data breaches, system compromises, and incidents causing real-world physical damage. In January 2024, for example, CARR claimed responsibility for overflowing municipal water storage tanks in Abernathy and Muleshoe, Texas. The group posted videos on public forums showing the manipulation of human–machine interfaces, resulting in the loss of tens of thousands of gallons of water and other physical damage to infrastructure, one of the few clear cases where hacktivist activity crossed into the physical domain.

Their language and tone are equally revealing. On April 23, 2024, following the Texas water tank incident, the group shared a link to a YouTube video featuring a speaker discussing the attack. In their accompanying comment, they wrote: "This is another way to poke in the face of those who consider our team weak, while they themselves are selling gold and giving useless interviews."

This short statement demonstrates several important dynamics. First, it shows how CARR blends self-legitimization, using the language of strength, pride, and rivalry, terms deeply embedded in Russian wartime and patriotic rhetoric. This rhetoric turns cyberattacks into a moralized contest of power, positioning the group not as criminals but as digital warriors defending national honor. Second, the statement reveals an obsession with public image and credibility, a hallmark of state-influenced information operations. By portraying themselves as the disciplined, CARR reinforces its image as a technically advanced patriotic collective, pushing back against the "script-kiddie" label.

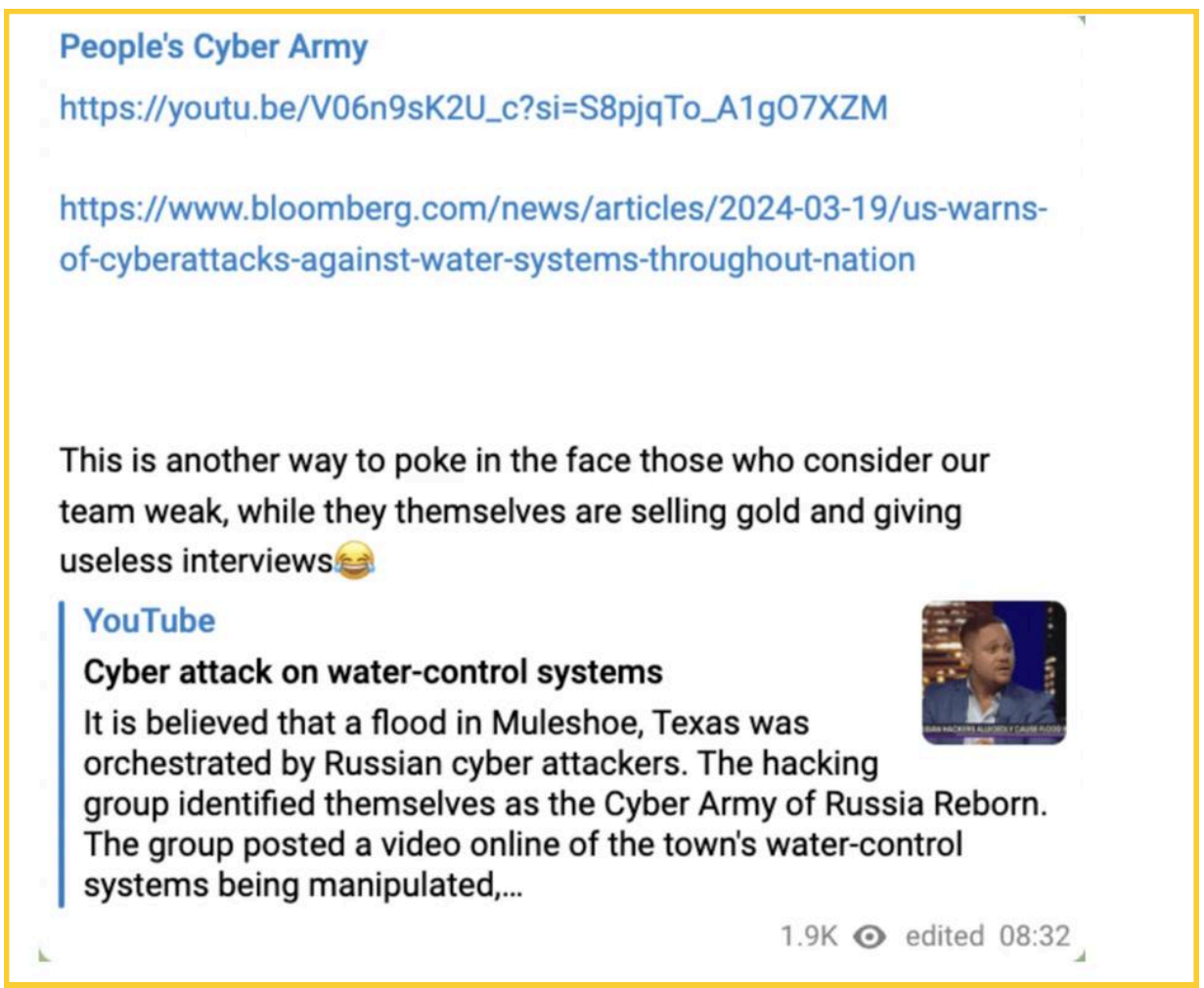


Figure 18: Post by CARR discussing its attack on municipal water storage tanks in Abernathy and Muleshoe, Texas, boasting about the operation while showcasing it as a display of strength.
Source: CARR Telegram Channel

A notable reaction came from the group regarding two individuals indicted for their roles in CARR operations, including the Muleshoe attack. On July 19, 2024, Yuliya Vladimirovna Pankratova was identified as the spokesperson overseeing command-and-control for the group, while Denis Olegovich Degtyarenko was named as the primary hacker behind multiple compromises, including the SCADA system of a U.S. energy company.

In response to sanctions against these members, the group did what it usually does: leaned into bravado, amplifying a post from a pro-Russian channel and wishing law enforcement "good luck" with the hunt. The shared "WANTED" banner read, "Especially Dangerous Patriots of the Russian Federation," and ironically misspelled "Russian" as "**Росийсской**" instead of "**Россиийской**." Perhaps, for a movement that wraps itself in patriotic credentials, a spellcheck could bring harsher punishment from the top than any U.S. indictment. No reporting of Russia taking action against the two members was observed. Yet again, the message to Russian cybercrime is clear: as long as your actions align with the state's agenda, you're welcome.

Figure 19: CARR's reaction to the indictment of its members, praising them as "patriots" while mockingly wishing the FBI good luck in trying to arrest them.
Source: CARR Telegram

These examples show that CARR's targeting is not random; it is contextually synchronized with state priorities. Whether hitting symbolic Western institutions, critical infrastructure, or moments of international visibility, each campaign is politically aligned and. U.S. actions are met with public mockery. The result is a pattern of cyber operations that blurs the line between independent activism and state-aligned digital warfare, extending Russia's broader agenda and militarization strategy into the cyber domain.

Media Support Analysis

Media coverage surrounding these hacktivist groups in Russia is also revealing. It demonstrates how the state and its affiliated media ecosystem have learned to capitalize on the global image of the "Russian hacker." What began as an external accusation, popularized after alleged Russian interference in the 2016 U.S. elections, has since been internalized and repurposed as a point of national pride and soft power.

While officials publicly deny involvement ("nyet, nyet"), state-aligned outlets increasingly promote stories that mythologize Russian hackers as skilled defenders of the homeland. Beginning in 2022, this narrative became more explicit: hackers were no longer just digital outlaws; they were portrayed as patriotic cyber warriors, standing on the digital front lines of Russia's confrontation with the West.

Hacktivist groups are often interviewed in Russian media and on television, where they tell their version of the story, and, heads up, it's usually framed as patriotism, not crime. In a November 26, 2024, interview with Anna News, a CARR representative described the group as a "people's project," born in March 2022 during what they called a **"wave of patriotic enthusiasm".** According to them, ordinary citizens **"wanted to defend the Motherland in the IT and information space",** turning the online battlefield into an extension of Russia's war effort.

They even explained the origins of their channel name: the current Telegram account was created in April 2022 after the previous one was "attacked by enemy bots." The suffix "Reborn", they added, wasn't symbolic; it literally marked the creation of a new channel, though they joked that some mistakenly call them the "Cyber Army of the Russia Reborn."

When asked about their activities, the spokesperson stated: "Our main work is disrupting the operation of websites through distributed denial-of-service (DDoS) attacks." But they didn't stop there, CARR also conducts server breaches, data theft, and industrial system compromises, proudly admitting to altering ("defacing") websites and running psychological operations under the supervision of "Doctor of Psychology V. Rozanov."

The tone of the interview is striking. Rather than a group of criminals hiding behind anonymity, CARR presents itself as a digital battalion, complete with ranks, strategy, and a sense of civic mission. Their words blur the line between hacktivism and official propaganda, reinforcing the state's larger narrative: that cyber operations are not crimes but acts of patriotism in defense of the homeland.

Does this narrative sound like the official CyberSquad of ONF? **Da.**

Does that mean the state is also involved in hacktivist operations? **Da Da... Nyet Nyet... or maybe just highly likely.**

But before we proceed with our conspiracy board, let's flip the camera and see how others talk about these hacktivists.

When analyzing Russian media coverage of hacktivist activity, four central narratives consistently emerge across state-aligned outlets. These narratives serve not only to justify the groups' actions but also to integrate them seamlessly into the broader ideological framework of state communication and digital mobilization.

They tend to repeat across multiple outlets and appearances, from one article to another and from television interviews to Telegram posts, often featuring the same hacktivist representatives or "experts" delivering nearly identical talking points. For the sake of demonstration, we focus here on a specific example: an interview with Valery Rozanov, the Coordinator of the Central Federal District for Cooperation between the Cossacks and the Media (**координатор ЦФО по взаимодействию Казачества со СМИ**) and, likely, the one CARR stated as their PsyOps advisor. All citations and quotations that follow are drawn directly from this source.

*Note: The Cossacks (**казаки**) are a historically militarized community in Russia, dating back to the Tsarist era, once serving as border guards and irregular cavalry. In post-Soviet Russia, they have been reintegrated into the state apparatus as both a cultural-patriotic movement and a paramilitary auxiliary force.

First, **patriotic framing and normalization**. Media outlets present hacktivism not as a crime but as a civic duty, the digital continuation of the battlefield. The rhetoric of "hybrid war," "Russophobia," and "defending the Motherland" dominates headlines and interviews. In this framing, hackers are not rogue actors but citizen-soldiers protecting Russia's informational borders from Western aggression. By dressing cyberattacks in patriotic language, the state narrative provides moral and emotional justification for operations that would otherwise be criminal.

Translation: “In early April, the Russian People’s Cyber Army destroyed almost all of Slovenia’s information infrastructure in response to the expulsion of our diplomat. Next up are the Czech Republic and Poland. Official representatives of Slovenia’s president even appealed to the Cyber Army for mercy.”

Rus: **В начале апреля Российская Народная Кибер Армия уничтожила почти всю информационную структуру Словении в ответ на высылку нашего дипломата. На подходе — Чехия и Польша. Официальные представители Президента Словении, даже обращались к Кибер Армии с просьбой о пощаде**.

Second, recruitment and training narratives run throughout these stories. Articles highlight that “anyone can join,” emphasizing low entry barriers and even offering training programs for aspiring “cyber-defenders.” This mirrors the offline mobilization seen in organizations like the ONF’s CyberSquad, transforming everyday users into participants in Russia’s “information front.” Hacktivism becomes a career path, a civic contribution, and a symbol of belonging.

Translation: “The Cyber Army trains people from scratch and without any age limits, creating every opportunity for professional growth in various areas, even in creative work (media content) for distribution across different platforms. If you don’t have a computer, a mobile phone is enough to perform many tasks. We provide all the necessary software, and we develop much of it ourselves.”

Rus: **Кибер Армия обучает с нуля и без ограничений в возрасте, каждому создаются все возможности профессионального роста в разных направлениях — даже в создание креатива (медиаконтент) для распространения на различных площадках. Если у вас нет компьютера, достаточно мобильного телефона, чтоб выполнять многие задачи, все необходимые программы мы предоставляем и многие создаем сами**.

Third, there is justification and glorification of indicted actors, signaling to both domestic and international audiences that participation carries no real consequence, at least within Russia. Figures like Juliya Pankratova, referred to as “**Юля-Ярославна**,” known organizers or public faces of hacktivist operations, are publicly celebrated. Media profiles describe them as “true patriots” or “guardians of digital sovereignty.” This praise sends a clear message to the cybercrime community: as long as your actions serve national interests, you’ll be rewarded, not punished.

Translation: “On one patriotic platform, I had a pleasure to meet one of the leaders of the Cyber Army, a woman with the call sign “Yulia-Yaroslavna,” who holds enormous authority in the hacker community of both Russia and abroad, as well as well-deserved hatred and respect from our adversaries.”

Rus: **На одном патриотическом ресурсе, мне посчастливилось познакомиться с одним из Руководителей Кибер Армии, девушкой с позывным Юля- Ярославна, которая имеет огромный авторитет в сообществе хакеров России и Зарубежья, а также заслуженную ненависть и уважение у наших противников**.

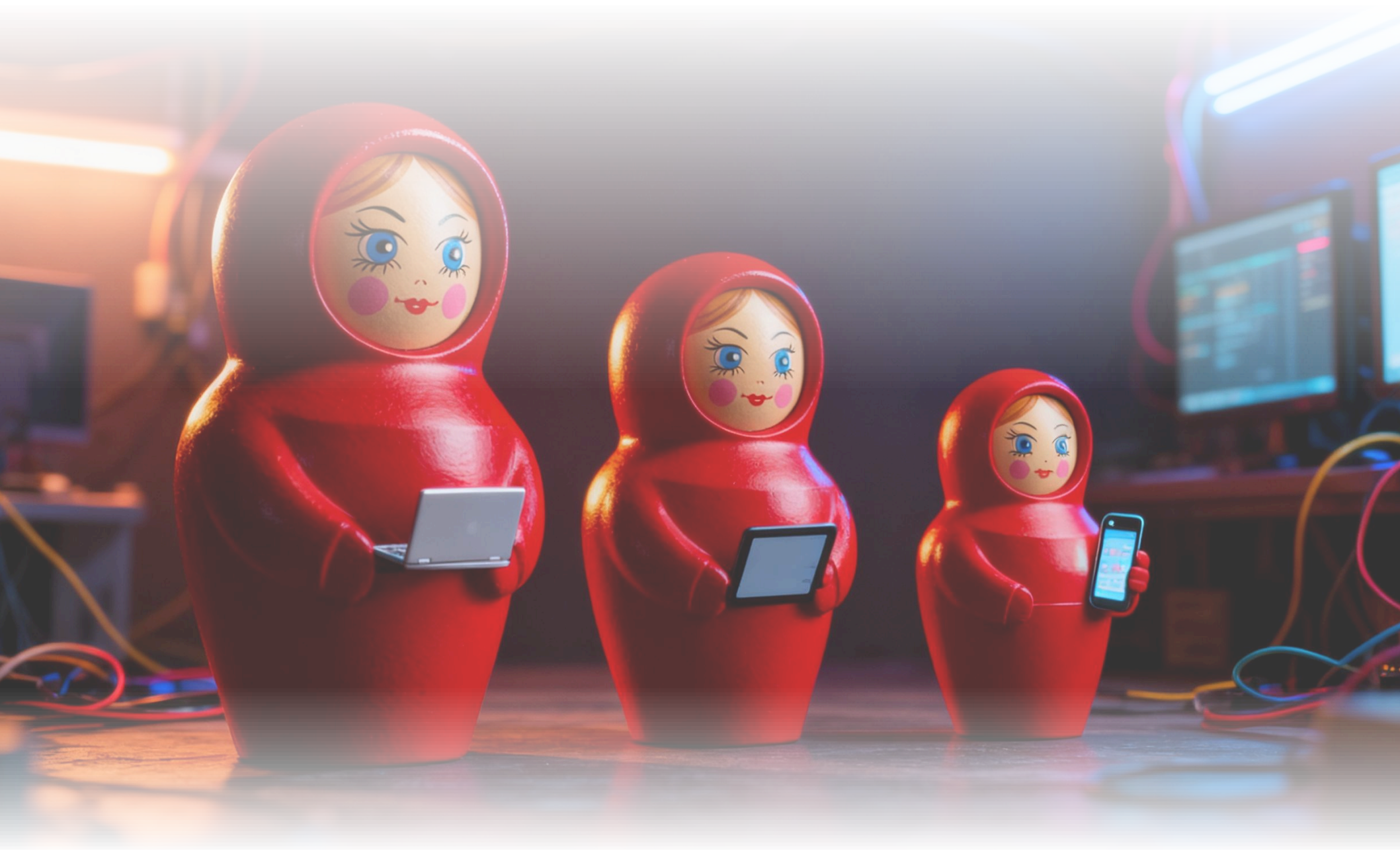
Finally, synchronization with state narratives ties it all together. Media coverage aligns its timing and tone with geopolitical flashpoints, sanctions, diplomatic expulsions, and military escalations, portraying hacktivist operations as responses to Western provocation. The sequencing is deliberate: cyber events are embedded into the same emotional and ideological script as conventional warfare, amplifying the sense of unity between state, media, and “grassroots” actors.

Translation: “There is currently a global confrontation between Russia and the West being waged by the hands of Ukrainian nationalists. The fighting is taking place not only along the line of contact, and not only deep in the rear, where missiles and drones strike from both sides. The most important battle is for the hearts and minds of people, those living in Russia and Ukraine, as well as beyond the warring countries. And the main weapon in this battle is information technology. That is why, in our time, the relevance of information security is increasing.”

Rus: Сейчас продолжается глобальное противостояние между Россией и Западом руками украинских националистов. При этом бои идут не только на линии боевых столкновений, и не только в глубоком тылу, куда с обеих сторон прилетают ракеты и беспилотники. Самая главная битва - за умы и сердца людей, как живущих в России и Украине, так и за пределами воюющих стран. И главным оружием в этой битве являются информационные технологии. Именно поэтому в нынешнее время возрастает актуальность информационной безопасности».

Through those four narratives, **patriotic framing, recruitment, justification, and synchronization**, state-aligned media doesn't just cheerlead; it normalizes hacktivism as a civic duty. Patriotism provides the moral cover ("defense of the Motherland"), recruitment offers the on-ramp (simple tasks, public praise), justification explains why ("they started it," "hybrid war"), and synchronization ties campaigns to the state's agenda of further militarization of its society.

So why do people join, and why will they keep doing it? Short answer: because the mix of propaganda, pressure through laws, and fear of prosecution, forming a new identity, and gamified rewards works. Longer answer coming up. If you're still with us, congrats, you've survived the red string section of the board. Now let's place the final pins on our conspiracy board and ask the only question that you **are here for: are the state and Russian cyber actors marching together?** On to the conclusion.



Conclusion (Bring Extra Tape)

First things first. Do we think the Russian state is involved in hacktivist activity? Yes**.** Based on the evidence we've laid out, our level of confidence is high. Let's start with the state's general stance toward everyday life: it has its hands in everything: domestic policy, legislation, social control, and the constant pressure on dissent. So, to imagine that the Kremlin would simply ignore one of the most strategic domains of power, cyberspace, would be, to put it simply, illogical.

Moving further, by analyzing official movements like **CyberSquad** alongside hacktivist collectives such as the **Cyber Army of Russia**, we observed repeating patterns: identical language, identical tone, even identical emojis. The same slogans, the same platforms, all wrapped in patriotism and the mantra of "defending the Motherland." The target patterns and the language around claimed attacks speak just as loudly, reinforcing the state's proclaimed narrative that the West is the main enemy. In our assessment, these overlaps are far from accidental. They reveal a structured system of influence, likely coordinated, at least in part, under state command and control, and amplified through civic and digital channels to recruit ordinary citizens.

Why do they involve ordinary citizens? Firstly, to take the blame away from the state and masquerade its offensive operations under the guise of traditional cybercrime. But on top of that, there is no less scary motive than the continuous militarization of its society. The digital front has become equally important, merging offensive and defensive capabilities into the state's modern arsenal. What started with legislation, school curricula, and patriotic concerts has now evolved into Patriotism-as-a-Service and extended online. In this ecosystem, hacktivism doesn't just echo the state's message; it serves it. We also assume that many of those participating likely have no idea they're pieces on a larger chessboard, puppets in a remarkably well-orchestrated performance.

Why do people join, and why will they keep doing it? Psychology gives us the answer. Economic hardship, sanctions, and constant exposure to mobilization rhetoric generate collective strain, anger, fear, and the search for meaning. The state turns those emotions into action through gamified engagement: ranks, points, badges, and public praise. Add fear of prosecution on top of that, plus one repressive law after another, and you've got a perfect recipe for mass conscription: both physical and digital.

The forecast? Not optimistic. The volume and sophistication of offensive cyber activity will only increase, and so will the risks. As Russia's hybrid warfare continues to merge propaganda, policy, and cyber operations, the tools of influence will reach further into society, normalizing a permanent state of digital mobilization. In this new paradigm, "defending the Motherland" is no longer a metaphor; it's a 24/7 online mission. Digital warfare isn't coming; it's already here. And in Russia's case, it is a country-sized army wearing a Putin Team hoodie with a St. George's ribbon, one click away from its next mission.


ANALYST1®