

Russian Hybrid Warfare

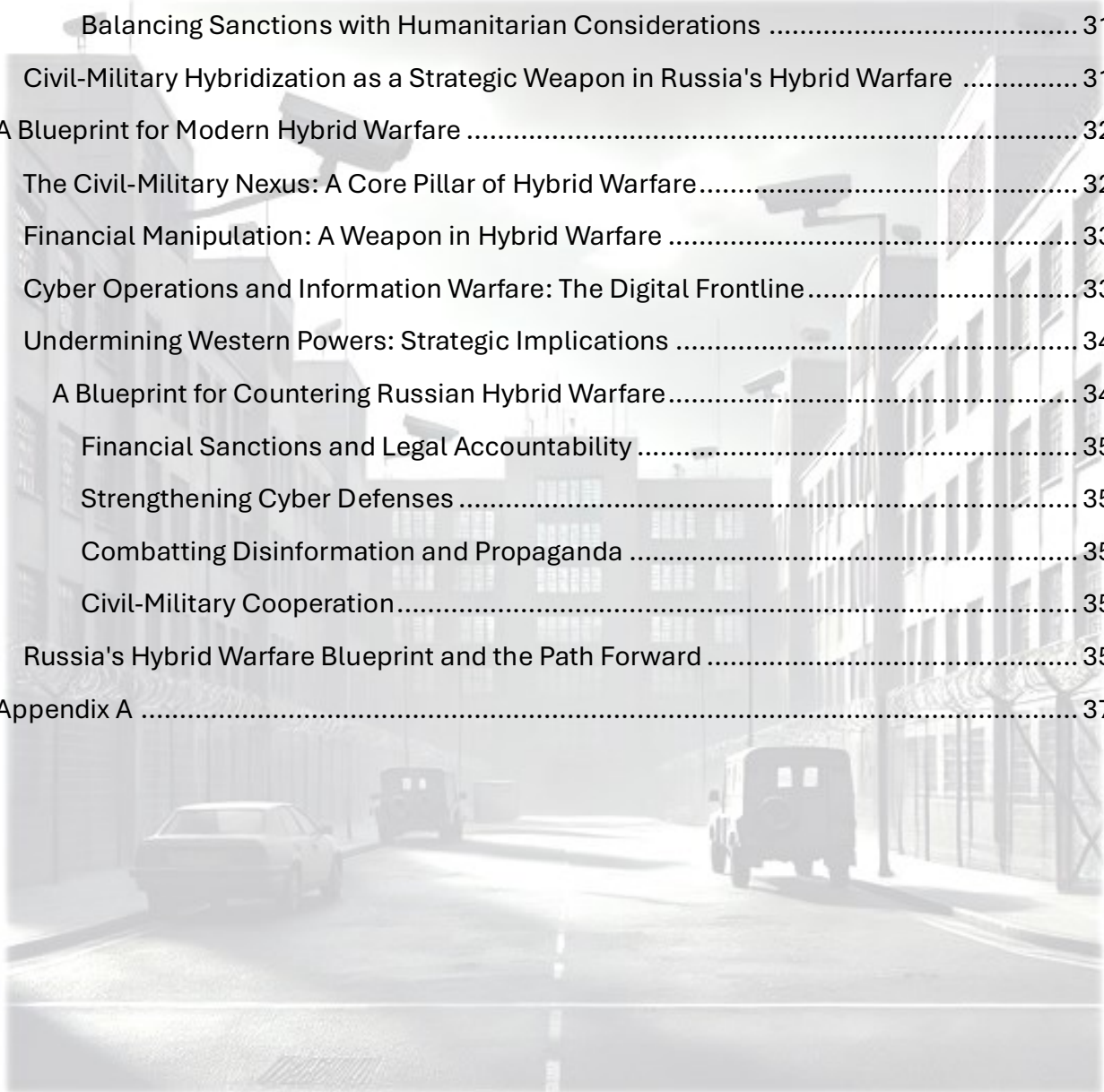
Covert Integration of Civilian and Military Power



Introduction.....	5
Russia's Use of the <i>Everything for Victory</i> Platform	6
Civilian Technological Contributions	7
Financial Obfuscation Through Legal Entities	7
Mobilization of Civilian Resources Through the "Everything for Victory" Platform: A Strategic Exploitation of Public Contribution	8
Civilian Mobilization as a Dual-Purpose Weapon: Strategic Exploitation	8
The People's Front Charity: A Legal Veneer for Military Support	8
Engaging Civilian Expertise: Extracting Technology and Innovation	9
Weaponizing Civilian Contributions: Intelligence Analysis of the Public Mobilization Strategy.....	11
Financial Flow Obfuscation: A Key Intelligence Insight	11
Information Warfare as a Reinforcing Mechanism	12
Expanding Capabilities Through Public Exploitation: Implications for U.S. and Allied Nations	12
Targeting of U.S. Allies	12
Counterintelligence Recommendations	13
Kulibin Club - Militarizing Innovation	13
Civilian Expertise as a Force Multiplier.....	14
Filling Gaps Left by Sanctions	15
Civilian Contributions as a Tool for Asymmetric Warfare	15
Rapid Adaptation to Battlefield Needs	15
UAVs and Cyber Tools as Pillars of Modern Warfare	16
Russia's Strategic Exploitation of Civilian Talent	16
Exploiting the Line Between Civilian and Military	16
Targeting of Civilian Innovators	17
Implications for the United States and Allied Nations	17
Strategic Risks for Western Nations	18

Recommendations for Counterintelligence	18
Information Warfare, Psychological Operations, and Financial Mobilization	18
Financial Mobilization and Psychological Operations: A Dual-Function Strategy	19
Supporting Morale Through Information and Financial Control	19
Financial Transparency as a Shield for Military Funding	20
Information Warfare and Propaganda Amplification: Shaping Perceptions	20
Media Figures and Propaganda Amplification	20
International Propaganda and Disinformation	21
The Feedback Loop of Financial and Information Warfare: A Hybrid Model	21
Using Public Sentiment for Long-Term Conflict	21
Western Vulnerabilities: Countering the Hybrid Model	22
Weaponizing Civilian Support Through Financial and Information Control	22
Russian Cyber and Information Warfare in the Context of Hybrid Warfare	23
Integration of Financial and Cyber Operations: A Strategic Nexus	23
Financial Resilience Under Sanctions	23
Cyber Operations as a Pillar of Hybrid Warfare	24
Symbolism and Financial Narratives in Propaganda: The Role of Imagery and Nationalism	24
Mobilizing Civilian Participation through Symbolism	25
Propaganda Amplification and External Influence	25
Strategic Implications for the United States and Western Allies	25
Financial and Cyber Vulnerabilities	26
Countering the Narrative and Disrupting the Feedback Loop	26
A Hybrid Warfare Model Fueled by Financial and Cyber Integration	27
Strategic Impact of Civil-Military Hybridization in Russia's Hybrid Warfare	27
Financial Infrastructure and Sanction Resilience: A Pillar of Russian Hybrid Warfare ..	28
Promsvyazbank: A Shield Against Sanctions	28
Civilian Platforms as a Cover for Military Financing	28
Legal and Financial Cover for Military Operations: The Grey Zone Strategy	29

People's Front Charity: Blurring the Civilian-Military Divide.....	29
State-Backed Financial Institutions as Legal Shields	29
Strategic Challenges for the International Community	30
Countering Russia's Financial and Legal Tactics	30
Balancing Sanctions with Humanitarian Considerations	31
Civil-Military Hybridization as a Strategic Weapon in Russia's Hybrid Warfare	31
A Blueprint for Modern Hybrid Warfare	32
The Civil-Military Nexus: A Core Pillar of Hybrid Warfare.....	32
Financial Manipulation: A Weapon in Hybrid Warfare	33
Cyber Operations and Information Warfare: The Digital Frontline.....	33
Undermining Western Powers: Strategic Implications	34
A Blueprint for Countering Russian Hybrid Warfare.....	34
Financial Sanctions and Legal Accountability	35
Strengthening Cyber Defenses	35
Combatting Disinformation and Propaganda	35
Civil-Military Cooperation.....	35
Russia's Hybrid Warfare Blueprint and the Path Forward	35
Appendix A	37



Introduction

Russia's hybrid warfare strategy integrates multiple sectors—military, cyber, financial, and civilian—into a cohesive framework designed to support its military objectives and counter external pressures, particularly from Western countries and sanctions. The combination of civil society mobilization, cyber operations, financial maneuvering, and information warfare is critical to Russia's ability to sustain and expand its influence globally. Platforms like Everything for Victory and the People's Front charity exemplify this strategy, acting as conduits for public participation, financial support, and information campaigns. These elements reinforce the military-industrial complex while circumventing international restrictions, mainly targeting the United States and its allies. This comprehensive analysis examines how these sectors interact and the implications of Russia's hybrid warfare efforts.

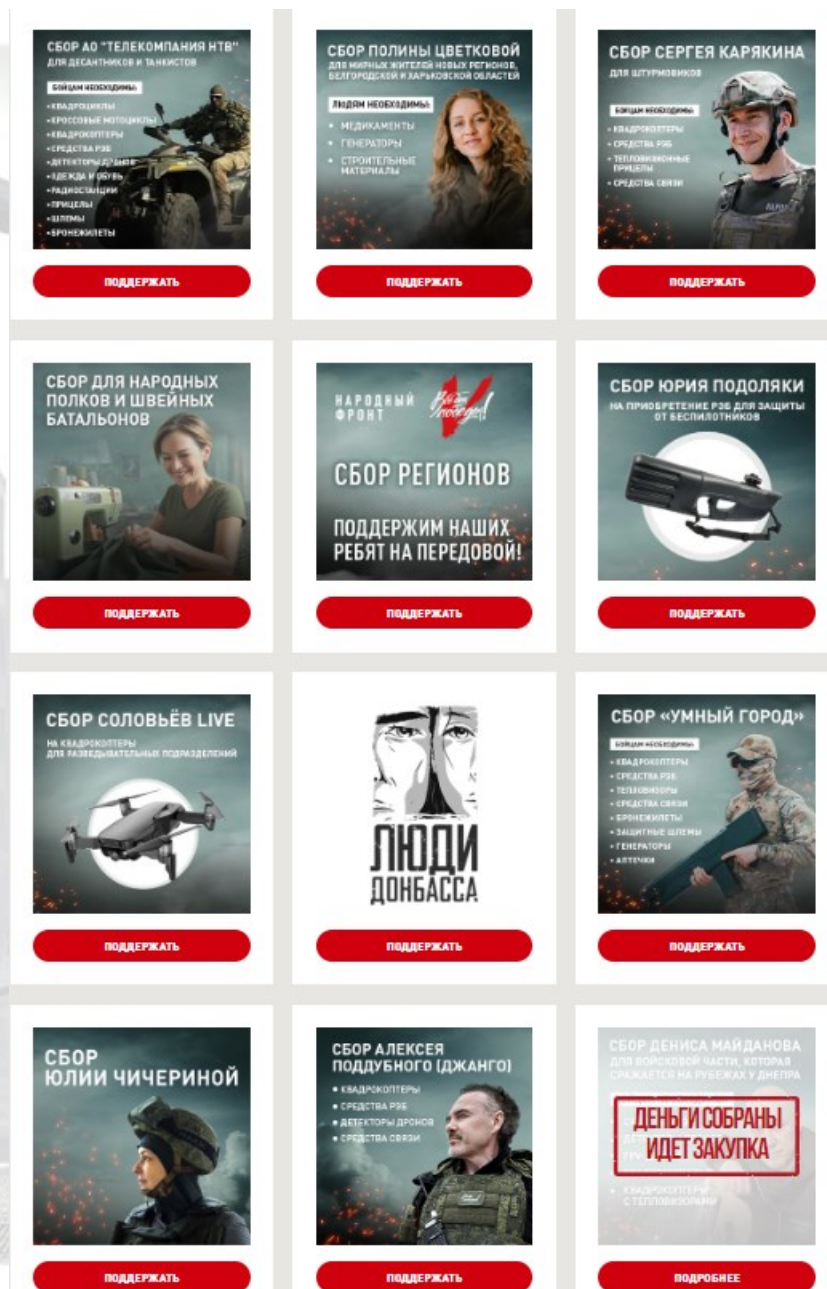


Figure 1 Everything for Victory

Russia integrates military, cyber, financial, and information operations through its hybrid warfare strategy. Civilian

mobilization, cyber warfare, and economic tactics are vital to evading international sanctions and promoting Russia's geopolitical interests.

Russia's hybrid warfare intends to expand influence globally by exploiting civilian resources, mainly through platforms like *Everything for Victory*, which masquerade as humanitarian efforts but are used to channel funds into military operations. This strategy also includes cyber operations and using domestic technological expertise to develop military capabilities.

The approach allows Russia to sustain its military operations and influence while bypassing international sanctions, complicating the U.S.'s and its allies' efforts to contain Russian aggression. Blending civilian and military assets under legal veneers challenges traditional defensive measures.

The increasing pressure from Western sanctions and geopolitical tensions, particularly with the West's support of Ukraine, has forced Russia to innovate in its hybrid warfare. The ongoing conflict in Ukraine and NATO's stance have intensified Russia's need for alternative methods to sustain its operations while evading sanctions.

Russia has effectively used civilian fundraising and technological expertise to enhance military capabilities, maintain cyber operations, and finance military activities under the guise of humanitarian work. The legal structures supporting these activities further shield Russia from international legal scrutiny.

Russia will likely continue expanding its hybrid tactics as sanctions tighten and military pressures increase. The ability to mask military operations as civilian-driven will further complicate international diplomatic and financial countermeasures, leading to more refined strategies aimed at exploiting legal loopholes and civilian goodwill.

Intelligence gaps include a complete understanding of Russia's civilian involvement in its military operations and the specific impact of these efforts on the broader international financial systems. Further clarity on the scope of domestic technological advancements being absorbed into military projects is also needed.

Russia's Use of the *Everything for Victory* Platform

The Everything for Victory platform is central to diverting civilian funds and expertise into military operations. Civilian contributions, under the guise of humanitarian aid, directly support Russian military actions in conflict zones. The platform's use demonstrates the

dual-use nature of civilian engagement in Russia's hybrid strategy. The *People's Front* charity, positioned as a humanitarian entity, channels funds to military operations. Civilian engineers contribute technological expertise, which Russia uses to develop military tools like drones. The use of civilian tactics allows Russia to circumvent sanctions while maintaining the appearance of legality, complicating international responses.

Civilian Technological Contributions

Russia taps into civilian innovation, using clubs like the *Kulibin Club* to develop military technology, including unmanned aerial vehicles and cyber tools. Civilian expertise, often unwittingly, is absorbed into military projects to bypass international technology restrictions. The *Kulibin Club* has been used to harness civilian-developed military technology. These innovations include critical advancements in cyber warfare and drone technology, which have been deployed in Ukraine, underscoring how Russia integrates civilian R&D to avoid reliance on foreign military technologies, enhancing its asymmetric warfare capabilities.

Financial Obfuscation Through Legal Entities

Russia obfuscates financial flows through charities like the *People's Front*, which masks the diversion of civilian donations into military expenditures. The legal structure provides Russia with a shield against international financial scrutiny. The *People's Front* charity provides a financial infrastructure that hides the true destination of donations. These donations are often used to purchase military equipment or fund cyber operations. The ability to hide military funding behind legal entities adds a layer of complexity to international efforts to target Russia's financial networks.

НАРОДНЫЙ ФРОНТ – ОБЩЕСТВЕННОЕ ДВИЖЕНИЕ, ЛИДЕРОМ КОТОРОГО ЯВЛЯЕТСЯ ПРЕЗИДЕНТ РОССИИ ВЛАДИМИР ПУТИН. МЫ ОБЪЕДИНЯЕМ АКТИВНЫХ ЛЮДЕЙ НАШЕЙ СТРАНЫ ДЛЯ РЕШЕНИЯ ВОПРОСОВ, ВАЖНЫХ ДЛЯ КАЖДОГО ГРАЖДАНИНА. С ФЕВРАЛЯ 2022 Г. НАРОДНЫЙ ФРОНТ СОБИРАЕТ И ДОСТАВЛЯЕТ ГУМАНИТАРНУЮ ПОМОЩЬ РЕБЯТАМ НА ПЕРЕДОВУЮ И НАСЕЛЕНИЮ НОВЫХ И ПРИГРАНИЧНЫХ РЕГИОНОВ.

Mobilization of Civilian Resources Through the "Everything for Victory" Platform: A Strategic Exploitation of Public Contribution

The Everything for Victory platform plays a pivotal role in Russia's hybrid warfare strategy, particularly in its effort to extract resources from the public to support military operations and information warfare. This dual-purpose platform, presented under humanitarian assistance, uses civilian donations, technological innovations, and logistical support to sustain military activities in contested regions like Donbas and Zaporizhzhia. Using tools such as the People's Front charity—a legally registered entity—the Kremlin can legitimize these financial activities while hiding their military applications under a humanitarian narrative. This strategic manipulation not only bypasses international sanctions but also exploits civilian goodwill under false pretenses, engaging citizens in a con-like manner to unwittingly support military objectives. By analyzing the intelligence methods behind this strategy, we can further understand how Russia's hybrid warfare intertwines civilian involvement with its broader geopolitical aims.

Civilian Mobilization as a Dual-Purpose Weapon: Strategic Exploitation

At the heart of the Everything for Victory platform is Russia's ability to harness public sentiment, turning nationalistic fervor into a tool for advancing its military-industrial complex. This tactic is especially effective because it relies on civilian contributors—individuals who believe they support humanitarian efforts—while covertly channeling these resources into military and paramilitary operations. This type of dual-use mobilization is central to Russia's hybrid warfare strategy, where civilian and military lines are intentionally blurred, allowing the Kremlin to scale its capabilities through civilian engagement.

The People's Front Charity: A Legal Veneer for Military Support

The People's Front charity, as outlined in the rekvisity.pdf document, provides the formal financial infrastructure necessary to facilitate donations, presenting itself as a legally compliant, humanitarian entity. However, intelligence analysis reveals that this charity operates as a financial arm of Russia's military operations, serving as a channel to divert civilian funds into military ventures. By positioning this entity as a charity, Russia can shield itself and its donors from international scrutiny, masking the true nature of the funds.

COUNTERPARTY CARD

Full name of the legal entity (in accordance with the constituent documents)	Charity Fund "People's Front. Everything for Victory"
Legal address (in accordance with the constituent documents)	119285, Moscow, Mosfilmovskaya st., 40
Postal address and zip code	119285, Moscow, Mosfilmovskaya st., 40
Telephone, code.	(495)981-56-99
INN	7729452720
KPP	772901001
OKPO code	33687207
OKATO code	45268584000
Primary state registration number (OGRN) and details of the state registration document	1147799011766 Federal Tax Service Office for Moscow date of issue: 25.07.2014
Payment details	
Current account Full	40703810700000003587
name of the bank Location of the bank	Bank PJSC "PROMSVYAZBANK"
Correspondent account BIC	Moscow
	30101810400000000555
	044525555
Purpose of payment	Charitable donation for statutory activities

Figure 2 Rekvisity

This process enables Russia to bypass international sanctions, a key intelligence finding that demonstrates the financial resilience of Russia's hybrid warfare tactics. Donations ostensibly intended for humanitarian causes are redirected to purchase military equipment, fund logistical operations, or support cyber warfare initiatives while maintaining the illusion of civilian goodwill. This con-like exploitation of civilian trust reinforces the Kremlin's hybrid warfare doctrine, where legal protections and humanitarian narratives serve as a cover for military buildup.

Engaging Civilian Expertise: Extracting Technology and Innovation

In addition to monetary contributions, the Everything for Victory platform encourages civilians to contribute their technological expertise, mainly through initiatives like the Kulibin Club. This civilian-driven club, named after Russian inventor Ivan Kulibin serves as a conduit for technological innovations to be weaponized. Civilian engineers and technologists are

invited to develop drones, robotic platforms, and cyber tools to support humanitarian or defensive objectives.

Всё для победы! **НАРОДНЫЙ ФРОНТ** О ПОРТАЛЕ ЧЕМ ПОМОЧЬ? КУПИМЫН-КЛУБ ПУНКТЫ СБОРА СВОДКИ ВОПРОСЫ СЛОВА ПОДДЕРЖКИ

УЗНАЙ, КАК ПОДДЕРЖАТЬ МИРНЫХ НАСЕЛЕНИЕ ДОКАЗА 8 (800) 200-34-11



ПОДДЕРЖАТЬ

О ПОРТАЛЕ

ПОД ДЕВИЗОМ «ВСЁ ДЛЯ ПОБЕДЫ!» НАРОДНЫЙ ФРОНТ ПРОСИТ ПОДДЕРЖАТЬ БОЙЦОВ НА ПЕРЕДОВОЙ СВО И МИРНЫХ ЖИТЕЛЕЙ НОВЫХ И ПРИГРАНИЧНЫХ РЕГИОНОВ. НА ПОРТАЛЕ МЫ РАССКАЗЫВАЕМ, КАК ПЕРЕЧИСЛИТЬ ДЕНЬГИ, ГДЕ ПРИНИМАЮТ ВЕЩИ, ЧТО ТРЕБУЕТСЯ ВОЕННЫМ И ЖИТЕЛЯМ ЛНР, ДНР, ХЕРСОНСКОЙ, ЗАПОРОЖСКОЙ, КУРСКОЙ И БЕЛГОРОДСКОЙ ОБЛАСТЕЙ. ЗДЕСЬ ЖЕ МОЖНО УЗНАТЬ, КАК ГРУЗЫ ДОСТАВЛЯЮТСЯ АДРЕСАТАМ.

ПОДДЕРЖАТЬ БОЙЦОВ НА ПЕРЕДОВОЙ

ПОДДЕРЖАТЬ

ПО БАНКОВСКИМ РЕКВИЗИТАМ
И СОГЛАСИИ С УСЛОВИЯМИ ОФЕРТЫ

СКАЧАТЬ

ПО QR КОДУ

Figure 3 Everything for Victory

These contributors may not realize that their innovations are quickly absorbed into military projects designed to enhance Russia's offensive capabilities. Through these initiatives, Russia can bypass international sanctions on military technology by relying on domestic civilian expertise to fill gaps created by foreign embargoes, reducing dependence on foreign technology but also accelerating the development of asymmetric warfare tools, such as

unmanned aerial vehicles (UAVs) and electronic warfare systems, which have been integral to Russia's hybrid warfare tactics in Ukraine and beyond.

By engaging civilian technologists under the guise of patriotism and national service, Russia turns its civilian population into an R&D arm of the state, extracting innovations that would otherwise be unavailable due to international restrictions. This strategic exploitation highlights how civilian capabilities are weaponized, transforming innocuous technological advancements into tools of war.

Weaponizing Civilian Contributions: Intelligence Analysis of the Public Mobilization Strategy

Russia's use of the Everything for Victory platform represents a highly sophisticated form of civilian exploitation, where public enthusiasm and national loyalty are funneled into the military apparatus. This dynamic functions on multiple levels, each designed to obscure the true purpose of civilian contributions. Intelligence methods, such as target analysis, motivational profiling, and network analysis, provide deeper insights into how Russia achieves these outcomes.

Financial Flow Obfuscation: A Key Intelligence Insight

One critical element of Russia's strategy is its ability to obfuscate financial flows, ensuring that the origin and destination of funds remain ambiguous. The rekvisity.pdf document demonstrates how charitable entities like the People's Front are instrumental in legalizing the flow of funds. This tactic allows Russia to maintain the appearance of legality, which is particularly important when donations are made by foreign sympathizers or international organizations that believe they are contributing to legitimate humanitarian causes.

Through intelligence-led financial tracking, we can see how these donations are laundered through legitimate channels, ultimately supporting military logistics and cyber operations. The use of state-backed banks like Promsvyazbank, which are directly involved in military financing, highlights the confluence of legal cover and military objectives. These banks serve as intermediaries, converting civilian donations into operational resources that sustain Russia's war efforts, particularly in regions where the military footprint is significant but publicly displayed.

Information Warfare as a Reinforcing Mechanism

In parallel to financial exploitation, Russia uses information warfare to reinforce the civilian mobilization effort. Public perception management is a crucial tactic wherein state-controlled media and bloggers promote the notion that civilian contributions—whether financial or technological—are part of a noble national defense effort. This propaganda reinforces the legitimacy of the Everything for Victory platform, ensuring that civilians continue to contribute without questioning the true nature of their involvement.

Psychological operations (PSYOPs) also play a critical role in shaping how the public perceives its role in the military campaign. By amplifying nationalistic themes, Russian media constructs a narrative where support for military activities is presented as patriotism, embedding these ideas into the public consciousness, creating a self-sustaining feedback loop where the mobilization of civilian resources continues unchecked, driven by national pride and a desire to defend Russian interests against perceived external threats.

ВОЕННЫЕ ДЕЙСТВИЯ ПОСТОЯННО ТРЕБУЮТ НОВЫХ РЕСУРСОВ. АВТОМОБИЛИ, ДРОНЫ, ВСЕ ВЕЩИ, КОТОРЫЕ МЫ СОБИРАЕМ ИЛИ ЗАКУПАЕМ ДЛЯ РЕБЯТ НА ПЕРЕДОВОЙ, – РАСХОДНЫЙ МАТЕРИАЛ, НЕОБХОДИМЫЙ ВОЕННЫМ ЕЖЕДНЕВНО. ЕСТЬ ОГРОМНЫЙ ЗАПРОС НА СРЕДСТВА ОБНАРУЖЕНИЯ И ПОДАВЛЕНИЯ БЕСПИЛОТНИКОВ. СВОЕВРЕМЕННАЯ ПОМОЩЬ ПОМОГАЕТ СБЕРЕЧЬ ЖИЗНИ И ЗДОРОВЬЕ РЕБЯТ. И САМОЕ ГЛАВНОЕ, ПОЛУЧАЯ ЭТУ ПОМОЩЬ, БОЙЦЫ В ОКОПАХ ЧУВСТВУЮТ ПОДДЕРЖКУ, ВИДЯТ, ЧТО ЗА ИХ СПИНАМИ – ВСЯ РОССИЯ.

Expanding Capabilities Through Public Exploitation: Implications for U.S. and Allied Nations

Russia's ability to expand its military and cyber capabilities by exploiting civilian skills presents a significant strategic challenge for the United States and its allies. The Everything for Victory platform offers a blueprint for how public mobilization can be weaponized to bypass sanctions and fill gaps in military capabilities. The challenge for Western intelligence agencies lies in countering this diffuse network of civilian contributors who may not fully understand the military implications of their support.

Targeting of U.S. Allies

This strategy directly impacts U.S. allies, particularly in regions where Russia seeks to undermine Western influence. Using disinformation campaigns, cyber operations, and public mobilization platforms, Russia can destabilize political systems and sow division in

Western countries. Furthermore, the ability to attract foreign donations under the guise of humanitarian aid allows Russia to indirectly extract resources from non-Russian civilians, particularly those sympathetic to pro-Russian narratives.

Counterintelligence Recommendations

To counter Russia's public mobilization strategies, counterintelligence operations should focus on:

- Tracking financial flows that move through charitable organizations like the People's Front and state-backed banks.
- Disrupting propaganda campaigns that promote the legitimacy of these organizations, using information warfare techniques to expose their dual-use nature.
- Engaging in public awareness campaigns aimed at Western civilians, highlighting the risks of contributing to Russian organizations that may indirectly support military operations.

Additionally, allied nations should invest in cyber intelligence operations that can identify and disrupt Russian efforts to engage civilian technologists in military innovation projects, mainly through platforms like the Kulibin Club.

Russia's use of the Everything for Victory platform exemplifies a highly sophisticated form of public exploitation, where civilian contributions are harnessed to expand military capabilities and reinforce information warfare. By positioning itself as a humanitarian effort, the People's Front charity operates as a financial arm of the state, effectively bypassing international sanctions and extracting resources from unsuspecting civilians. This dual-use exploitation, coupled with technological extraction, creates a self-sustaining model for military expansion under the guise of civic duty.

For the United States and its allies, understanding and countering this form of hybrid warfare is critical to undermining Russia's ability to weaponize its civilian population for military ends. By employing intelligence analysis methods and focusing on public awareness, Western nations can disrupt Russia's public mobilization efforts and prevent further civilian exploitation.

Kulibin Club - Militarizing Innovation

The Kulibin Club, an initiative closely tied to Russia's Everything for Victory platform, is an example of how the Kremlin uses civilian technological expertise to advance its military objectives. This initiative is part of Russia's broader strategy to mobilize civilian talent and

resources to fill the gaps caused by international sanctions and the loss of access to Western technology. By providing a structured channel for civilian innovators to contribute to developing drones, robotics, cyber tools, and electronic warfare systems, the Kulibin Club plays a critical role in Russia's hybrid warfare tactics. It exploits civilian innovation to address battlefield needs rapidly, bypassing traditional military supply chain restrictions while embedding patriotic duty into the public consciousness. Below, we delve deeper into the strategic exploitation at play, examining how this initiative transforms civilian technological advancements into weapons of war, often without full awareness of the contributors.

1. Militarizing Civilian Innovation: Strategic Exploitation

The Kulibin Club demonstrates a strategic shift in how Russia's military-industrial complex operates, particularly under the constraints of sanctions. By recruiting civilian technologists, the Kremlin can bypass the traditional military-industrial supply chain and instead focus on domestic innovation as a source of advanced military technologies. This tactic effectively turns civilian innovations into military assets, blurring the distinction between civilian and military sectors and allowing Russia to scale its technological capabilities with minimal reliance on imports.

Civilian Expertise as a Force Multiplier

At the core of the Kulibin Club's strategy is the extraction of civilian expertise for military use. Civilian engineers, software developers, and technologists—often working in fields that appear disconnected from military applications—are drawn into the war effort under the pretense of patriotism and national service. Many of these contributors believe they are developing defensive tools or humanitarian technologies, unaware of the full extent to which their work is weaponized, making the Kulibin Club con-like exploitation of civilian skills, where the lines between civilian and military applications are deliberately blurred.

For instance, initially pitched as surveillance tools, unmanned aerial vehicles (UAVs) are quickly repurposed for combat missions, targeted strikes, or electronic warfare. Cyber tools developed to defend critical infrastructure are reconfigured into offensive hacking systems, targeting Western allies' infrastructures, political institutions, and communication networks. Civilian contributions thus become force multipliers that allow the Russian military to maintain technological superiority without relying on imports.

Filling Gaps Left by Sanctions

One of the primary drivers behind the Kulibin Club is Russia's need to overcome the technological deficit created by Western sanctions. These sanctions, aimed at limiting Russia's access to high-tech military components, have disrupted its traditional military supply chains. As a response, the Kulibin Club acts as a bridge, connecting civilian innovation with military demands, thereby circumventing restrictions on military imports.

The intelligence behind this approach is straightforward: Russia can sustain its defense capabilities and operational readiness by mobilizing domestic technological talent without importing sanctioned components. The initiative recruits civilian technologists, particularly in robotics, cybersecurity, AI, and drones, to create dual-use technologies—civilian technologies that are quickly adaptable to military functions, mitigating the impact of sanctions and accelerating the development of cutting-edge military tools.

ЧТО МОЖНО ПРИНЕСТИ В ПУНКТ ПРИЕМА? В ПУНКТЫ ПРИЕМА, РАСПОЛОЖЕННЫЕ В РЕГИОНАЛЬНЫХ ОТДЕЛЕНИЯХ НАРОДНОГО ФРОНТА, ВЫ МОЖЕТЕ ПРИНЕСТИ: БРОНЕЖИЛЕТЫ. КАСКИ. РАЦИИ ЦИФРОВЫЕ С ДАЛЬНОСТЬЮ 5-10 КМ. КВАДРОКОПТЕРЫ С КАМЕРАМИ И ДАЛЬНОСТЬЮ ПОЛЕТА ОТ 3 КМ. КАРТЫ ПАМЯТИ ДЛЯ КВАДРОКОПТЕРОВ. ТАКТИЧЕСКИЕ АПТЕЧКИ. АККУМУЛЯТОРЫ ДЛЯ ЭЛЕКТРОННЫХ УСТРОЙСТВ И ЗАРЯДНЫЕ УСТРОЙСТВА К НИМ. ПЛАНШЕТЫ И НОУТБУКИ. ТЕПЛОВИЗОРЫ. БИНОКЛИ. ПРИЦЕЛЫ. ПРИБОРЫ НОЧНОГО ВИДЕНИЯ. БОЛЕЕ ПОДРОБНО ВАС ПРОКОНСУЛЬТИРУЮТ ПО ТЕЛЕФОНУ 8 (800) 200-34-11.

Civilian Contributions as a Tool for Asymmetric Warfare

A vital advantage of the Kulibin Club is its ability to use civilian-led innovations to develop technologies suited for asymmetric warfare. Unlike traditional, large-scale military operations, asymmetric warfare focuses on using technology and tactics that allow smaller, more mobile forces to exploit the vulnerabilities of larger adversaries. In this regard, Russia's civilian technologists are critical to building unmanned systems, cyber weapons, and AI-driven platforms that give Russia a strategic edge in non-traditional warfare.

Rapid Adaptation to Battlefield Needs

One of the most significant aspects of civilian-led innovation is its ability to rapidly adapt to changing battlefield conditions. Unlike traditional military R&D, which can be slow and cumbersome due to bureaucratic processes, civilian technologists often innovate quickly and deliver solutions to the front lines in record time. The decentralized nature of these civilian efforts allows Russia to rapidly prototype, test, and deploy technologies, particularly in areas like UAVs, cyber operations, and robotic platforms.

For instance, during the conflict in Ukraine, Russian forces have increasingly relied on drones for reconnaissance and targeting, many of which were developed or improved upon by civilian engineers through the Kulibin Club. Similarly, cyber tools designed to infiltrate enemy communication networks have been enhanced by civilian hackers, who are often motivated by patriotism and unaware of the broader military context.

UAVs and Cyber Tools as Pillars of Modern Warfare

The development of UAVs and cyber tools has become central to Russia's modern military doctrine, where the emphasis is placed on asymmetric tactics that use technological superiority. Civilian-led innovation, particularly in unmanned systems and cyber warfare, gives Russia a distinct operational advantage over its adversaries. UAVs developed by civilian technologists are used for surveillance and target acquisition, electronic warfare, and payload delivery—critical components of asymmetric warfare.

The cyber dimension is equally critical, as civilian hackers involved in the Kulibin Club contribute to developing offensive cyber tools to disrupt Western critical infrastructure, penetrate secure networks, and exfiltrate sensitive data. These contributions expand Russia's ability to conduct cyber espionage, disinformation campaigns, and covert operations while remaining within the legal framework of civilian innovation.

Russia's Strategic Exploitation of Civilian Talent

From an intelligence perspective, Russia's Kulibin Club initiative represents a deliberate effort to exploit civilian talent for military gain while maintaining deniability regarding the true nature of the projects being developed. Intelligence analysis methods, including motivational profiling, target analysis, and network mapping, reveal Russia's systemic approach to recruiting, incentivizing, and directing civilian innovators into military applications. This process relies on nationalistic appeals and the exploitation of patriotic duty narratives to mask the fundamental military objectives behind these innovations.

Exploiting the Line Between Civilian and Military

A core tactic Russia uses is to blur the distinction between civilian and military contributions, creating a grey area where dual-use technologies are developed without clear delineations. The Kulibin Club fosters a collaborative environment where civilian engineers are encouraged to work on technologies with peaceful applications that are easily adapted for military use, allowing Russia to build an indigenous defense capability that operates under the cover of civilian innovation.

The exploitation of civilian technologists is particularly concerning because many contributors may be unaware that their innovations are used in offensive military actions. This con-like exploitation mirrors Russia's broader hybrid warfare strategy, where civilian entities, public platforms, and legal frameworks are co-opted to serve military purposes without overt acknowledgment.

HOW TO SUPPORT CIVILIANS? IN THE SECTION "ASSISTANCE TO CIVILIANS" YOU CAN SUPPORT RESIDENTS OF SPECIFIC AREAS WITH FOOD KITS, BASIC ITEMS, MEDICINE, BUILDING MATERIALS, AND PROVIDE TARGETED ASSISTANCE TO THOSE IN NEED. WHAT SPECIFICALLY DOES THE PEOPLE'S FRONT DO? WAR CORRESPONDENTS, BLOGGERS, FAMOUS PEOPLE, AND MEDIA EDITORIALS TALK ABOUT THE POSSIBILITY OF MAKING THEIR CONTRIBUTION. WE SCALE THEIR ACTIVITIES, PURCHASE GOODS IN LARGE BATCHES, PROVIDE WAREHOUSE SPACE AND INFORMATION SUPPORT, ORGANIZE LOGISTICS CHAINS, ASSISTANCE IN THE SECURITY OF FINANCIAL TRANSACTIONS. WHERE DO THE APPLICATIONS COME FROM? APPLICATIONS COME FROM WAR CORRESPONDENTS, JOURNALISTS, FAMOUS PEOPLE WHO BECOME CURATORS OF THE CAMPS, AS WELL AS THE COMMAND OF MILITARY UNITS. HOW TO GET ACQUIRED WITH THE REPORTS? WHEN POSSIBLE, DUE TO SECURITY REQUIREMENTS, WE PREPARE A VIDEO OF THE DELIVERY AND POST IT ON THE SOCIAL NETWORKS OF THE PEOPLE'S FRONT. ALSO, CONTROL OVER THE DELIVERY IS CARRIED OUT BY MILITARY CORRESPONDENTS AND WELL-KNOWN PEOPLE WHO ARE THE CURATORS OF THE COLLECTIONS. AND ON THE PAGE OF EACH COLLECTION, INFORMATION IS POSTED ABOUT THE COMPOSITION OF THE PURCHASE, THE FUNDS COLLECTED AND SPENT.

Targeting of Civilian Innovators

Russia's ability to recruit highly skilled civilian innovators underscores its focus on talent exploitation. Target analysis reveals that many technologists contributing to the Kulibin Club are drawn from Russia's robust STEM sectors, including universities, research institutes, and private tech firms. These individuals are often targeted for recruitment through patriotic appeals, social pressures, and government incentives, making them unwitting participants in Russia's military apparatus.

In some cases, the Kulibin Club may even recruit foreign technologists, particularly those who sympathize with Russia's geopolitical stance or operate in regions with strong Russian influence, broadening the talent available to Russia and making the innovation pipeline more resilient to sanctions and international isolation.

Implications for the United States and Allied Nations

Russia's use of the Kulibin Club to militarize civilian innovations poses a direct challenge to the United States and its allies, particularly in the domains of cybersecurity, UAV development, and electronic warfare. The dual-use nature of many technologies emerging from the Kulibin Club means that civilian innovations can be quickly adapted for military

purposes, complicating efforts to regulate exports and control technologies that could be weaponized.

Strategic Risks for Western Nations

For Western nations, Russia's exploitation of civilian talent creates significant intelligence gaps in understanding how military innovations are developed and deployed. The reliance on domestic technologists makes it difficult for foreign intelligence agencies to track the development pipeline of critical military technologies, mainly when they are created outside traditional military research institutions.

Recommendations for Counterintelligence

To counter the Kulibin Club model, counterintelligence efforts should focus on:

- Tracking civilian-led innovations that will likely be adapted for military use in Russia, particularly in UAVs, cyber tools, and electronic warfare.
- Monitoring recruitment efforts targeting technologists in Russia and abroad, who may contribute to developing dual-use technologies.
- Engaging in public awareness campaigns that highlight the risks of contributing to military-related projects under the guise of civilian innovation.

The Kulibin Club represents a strategic effort by Russia to exploit civilian innovation for military purposes, using domestic technologists to develop advanced technologies critical to modern warfare. By masking these efforts as patriotic contributions to national defense, Russia can mobilize civilian expertise without the constraints of international sanctions. For the United States and its allies, understanding and countering this tactic is critical to undermining Russia's technological advancements and preventing the weaponization of civilian innovations.

Information Warfare, Psychological Operations, and Financial Mobilization

Russia's hybrid warfare model seamlessly integrates information warfare, psychological operations, and financial mobilization to sustain public support for military actions while undermining Western cohesion. The People's Front charity plays a crucial role in this synthesis, acting as a financial and information conduit, where civilian contributions are channeled into military operations under the guise of humanitarian assistance. This

strategic exploitation of public sentiment is reinforced by a well-orchestrated propaganda machine that uses media figures, bloggers, and war correspondents to manipulate perceptions at home and abroad. By combining financial control with information dominance, Russia ensures a steady stream of resources and public loyalty, even as economic sanctions take their toll. Below, we delve into the mechanics of these intertwined elements, demonstrating how Russia's hybrid warfare framework exploits civilian donations, media influence, and information control to sustain its military campaigns and project power globally.

Financial Mobilization and Psychological Operations: A Dual-Function Strategy

The People's Front charity represents a sophisticated model of financial mobilization that merges public contributions with information warfare to sustain military operations. The economic infrastructure outlined in the [rekvisity.pdf](#) document underscores how Russia uses civilian donations to provide a steady flow of resources to military and humanitarian efforts. The inclusion of Promsvyazbank, a state-backed financial institution with links to defense funding, ensures that the charity operates with legal and financial transparency, masking its dual-use function as a channel for military support. This exploitation of public resources through a charitable veneer highlights how psychological operations and financial control are weaponized to maintain public morale and operational sustainability.

Supporting Morale Through Information and Financial Control

The People's Front charity is a prime example of how Russia employs financial control for resource mobilization and psychological operations. By framing donations as a way for civilians to contribute to national defense, the charity transforms financial support into an expression of patriotism and national unity. The combination of legal compliance—through Promsvyazbank—and public transparency gives the charity an air of legitimacy, allowing it to evade scrutiny even when funds are redirected toward military engagements.

From an intelligence analysis perspective, this model allows Russia to bypass international sanctions while ensuring that the financial lifeblood of its military campaigns continues unabated. The psychological element comes into play as the charity taps into nationalistic fervor, presenting financial contributions as a moral obligation. In essence, Russia uses the People's Front charity as a psychological operations tool, reinforcing the narrative that the public's financial sacrifices are part of a collective war effort—a strategic manipulation of civilian sentiment.

Financial Transparency as a Shield for Military Funding

Including Promsvyazbank in the financial pipeline allows the charity to operate with legal transparency and provides cover for these donations' military purposes. As a state-backed institution historically linked to defense spending, Promsvyazbank ensures that the funds funneled through the charity can be easily rerouted to military logistics, equipment procurement, or cyber operations. The legal structure allows Russia to present its financial activities as humanitarian while serving to sustain military operations.

For Western intelligence agencies, tracking these financial flows becomes a significant challenge, as the charity's legal veneer effectively obscures the end-use of funds. This tactic highlights the sophistication of Russia's financial mobilization strategy, where psychological manipulation of public sentiment and legal transparency work together to create an unassailable front that continues to fund military expansion.

Information Warfare and Propaganda Amplification: Shaping Perceptions

In parallel with financial mobilization, information warfare is a key component of Russia's strategy to sustain public morale and control narratives domestically and internationally. Media figures, including bloggers, war correspondents, and journalists, are integral to amplifying pro-Russian narratives, framing the military effort as a defensive mission against Western aggression. This information ecosystem creates a feedback loop where donations and propaganda reinforce each other, ensuring that the Russian public sees their financial support as part of a broader civic duty.

Media Figures and Propaganda Amplification

The role of media figures in Russia's information warfare apparatus cannot be overstated. Influential bloggers, journalists, and war correspondents amplify state-sponsored propaganda, crafting narratives that align public sentiment with Kremlin objectives. These media personalities are central to normalizing the idea that civilian contributions—whether through donations, support for troops, or participation in technological innovation—are vital to Russia's survival in the face of Western hostility.

By presenting the conflict as a defensive war, media figures frame donations as a way for the public to protect Russian sovereignty. This framing is crucial in maintaining public support for military operations, even as economic hardships caused by sanctions deepen. The psychological impact is significant, as it creates a perpetual cycle of support, where the donation of resources and the consumption of state-aligned media continuously reinforce

one another. This feedback loop ensures that the Russian public remains engaged and loyal to the state's objectives, regardless of the economic consequences.

(800) 200-34-11 FIND OUT HOW TO SUPPORT THE CIVILIAN POPULATION OF DONBASS MOSCOW, MOSFILMOVSKAYA ST., 40 8 (495) 980-25-61 8 (800) 200-34-11 POBEDA@ONF.RU

International Propaganda and Disinformation

Beyond the domestic sphere, Russia's information warfare extends globally through platforms like RT and Sputnik, which are instrumental in spreading disinformation targeting Western audiences and U.S. allies. These outlets disseminate polarizing narratives, fueling division and distrust within Western institutions. Russian media channels have been particularly effective in exploiting societal divisions during events such as the 2016 U.S. elections and Brexit, amplifying voices that undermine Western unity.

From an intelligence standpoint, Russia's ability to weave disinformation into the global information landscape is a powerful force multiplier for its hybrid warfare strategy. By undermining confidence in Western institutions and creating internal discord, Russia diverts attention away from its activities while destabilizing its geopolitical rivals. The tactic reinforces domestic morale and erodes the cohesiveness of Western alliances, allowing Russia to pursue its objectives with fewer obstacles.

The Feedback Loop of Financial and Information Warfare: A Hybrid Model

The feedback loop created by the fusion of financial mobilization and information warfare is critical to Russia's ability to sustain public support for its military campaigns. Despite economic hardships, this hybrid model ensures that the Russian population continues to see its financial contributions as essential to the state's survival. At the same time, the state-controlled narrative amplifies this support, ensuring that monetary donations are perceived as a form of patriotic duty. This self-reinforcing cycle is key to Russia's hybrid warfare, allowing it to maintain military capabilities and information control.

Using Public Sentiment for Long-Term Conflict

Russia's hybrid approach allows the Kremlin to stretch resources over long-term conflicts, effectively using the Russian population as a resource pool to sustain military efforts. The charitable framework of the People's Front enables the state to collect financial support without overtly acknowledging the military applications of these funds. By continually shaping public perceptions through information warfare, the state ensures that the

population remains invested in the conflict emotionally and financially despite the economic strain caused by sanctions.

From a military intelligence perspective, this represents a significant force multiplier for Russia, ensuring the home front remains resilient and committed. The strategic exploitation of civilian donations combined with the perpetual flow of state-sponsored propaganda ensures that public dissent is minimized while financial and material resources continue to flow into military operations.

Western Vulnerabilities: Countering the Hybrid Model

The West faces significant challenges in countering this hybrid model, particularly when disrupting the financial flows and information channels that sustain Russia's military campaigns. While sanctions have targeted Russia's ability to import critical technologies and access global financial markets, the People's Front charity demonstrates how domestic mobilization can bypass these restrictions. Furthermore, the international reach of Russian disinformation—through platforms like RT and Sputnik—complicates efforts to disrupt the propaganda sustaining public support.

To effectively counter Russia's hybrid warfare model, intelligence agencies and Western policymakers must focus on dismantling the feedback loop created by financial mobilization and information control. The model includes:

- Disrupting financial flows that support Russian military operations, particularly those routed through state-linked charities and domestic banking institutions like Promsvyazbank.
- Combating disinformation at the domestic and international levels, focusing on neutralizing the narratives that sustain public support for Russian aggression.
- It exposes the true nature of organizations like the People's Front and reveals the military objectives behind what is presented as humanitarian aid.

Weaponizing Civilian Support Through Financial and Information Control

The fusion of financial mobilization and information warfare in Russia's hybrid strategy represents a sophisticated exploitation of public sentiment, resources, and media control. Through platforms like the People's Front charity, Russia ensures a steady flow of civilian contributions directly supporting military engagements while maintaining plausible deniability. Simultaneously, the information warfare apparatus, led by media figures and

state-controlled outlets, ensures that the public narrative remains aligned with the state's objectives.

For Western nations, understanding and countering this hybrid model is critical to undermining Russia's ability to sustain long-term conflicts. By focusing on disrupting financial channels, combating disinformation, and exposing the civilian-military nexus, the West can begin to dismantle the feedback loop that enables Russia's hybrid warfare machine to operate with impunity.

Russian Cyber and Information Warfare in the Context of Hybrid Warfare

Russia's hybrid warfare strategy is a sophisticated blend of financial, cyber, and information operations to advance its geopolitical objectives while destabilizing its adversaries, particularly the United States and Western allies. The rekvisity.pdf document and related content highlight how Russia effectively integrates financial networks, cyber capabilities, and propaganda narratives to sustain its military operations and offensive cyber efforts. Russia's hybrid warfare model creates a multidimensional battlefield that extends beyond conventional military operations by using state-sponsored and civilian cyber actors alongside carefully crafted symbolism and disinformation campaigns. Below is an in-depth analysis of these interrelated aspects, focusing on the integration of financial and cyber operations, the role of symbolism in propaganda, and the broader implications for U.S. and allied nations.

Integration of Financial and Cyber Operations: A Strategic Nexus

Russia's ability to seamlessly merge financial systems with cyber operations is critical to its hybrid warfare strategy. The rekvisity.pdf document underscores the role of Promsvyazbank, a state-backed financial institution, in handling defense-related transactions and ensuring that funds raised through civilian platforms like the People's Front are directed toward military production and cyber operations, demonstrating how Russia's financial networks, despite facing international sanctions, remain resilient and operational, supporting the Kremlin's offensive cyber capabilities.

Financial Resilience Under Sanctions

Promsvyazbank's involvement is crucial to Russia's ability to circumvent financial sanctions imposed by the U.S. and the EU. By repurposing this bank to manage defense-related financial flows, Russia creates a legal and financial firewall that allows it to continue funding

military ventures and cyber operations. Donations funneled through the People's Front are channeled into military production, including cyber warfare tools, highlighting how financial and cyber infrastructures are intertwined within Russia's broader hybrid warfare model.

For Russia, this creates a dual-use system where civilian donations—ostensibly meant for humanitarian or national defense purposes—are redirected to offensive capabilities, including developing and deploying ransomware, malware, and phishing attacks. The integration of civilian financial contributions into these cyber operations underscores Russia's ability to weaponize public resources while presenting them as acts of patriotism.

Cyber Operations as a Pillar of Hybrid Warfare

The integration of cyber operations into Russia's hybrid warfare model is most evident in its state-sponsored Advanced Persistent Threat (APT) groups, including Fancy Bear (APT28) and Cozy Bear (APT29). These groups, often working alongside civilian hackers and private contractors, conduct cyber attacks on U.S. critical infrastructure, elections, and military assets, causing widespread disruption and advancing Russian interests covertly.

Using cyber tools such as ransomware, malware, and phishing demonstrates the breadth of Russia's cyber warfare capabilities. These tools are used for intelligence gathering and to create chaos, weaken public confidence, and disrupt economic systems in targeted nations. By integrating financial manipulation and cyber warfare, Russia's hybrid model allows it to conduct sustained offensive operations while remaining below the threshold of conventional conflict, making detection and attribution more difficult for Western intelligence agencies.

Symbolism and Financial Narratives in Propaganda: The Role of Imagery and Nationalism

Russia's hybrid warfare strategy extends beyond tactical operations, integrating symbolism and narratives to shape public perceptions. The Братство: Сила Народа ("Brotherhood: Power of the People") imagery is a prime example of how financial mobilization, cyber efforts, and military campaigns are unified under a nationalistic banner. This symbolic narrative plays a crucial role in shaping the information environment, ensuring that public participation in the war effort is seen as a moral obligation and an expression of national pride.

Mobilizing Civilian Participation through Symbolism

The Братство: Сила Народа imagery reflects a carefully constructed narrative that emphasizes the unity between civilian efforts, military operations, and cyber activities. This symbolic representation mobilizes the Russian public, framing financial contributions, technological innovations, and cyber participation as essential elements of national defense. The imagery resonates deeply within Russian society, reinforcing the idea that civilians are part of the war effort, whether through donations or technological support.

This narrative is central to Russia's psychological operations, where public engagement is encouraged and moralized. The symbolism of brotherhood suggests that the Russian people, including hackers, engineers, and everyday citizens, have a shared responsibility to protect the nation from foreign threats. The shared responsibility enables a self-perpetuating cycle where financial support and national pride are intertwined, ensuring that public resources continue to flow into military and cyber operations.

Propaganda Amplification and External Influence

The financial narratives amplified through state-controlled media extend to Russia's disinformation campaigns aimed at foreign audiences. Propaganda outlets like RT and Sputnik are instrumental in spreading disinformation that undermines confidence in Western institutions and creates internal divisions within targeted nations. Their propaganda campaigns are particularly evident in Russia's campaigns around the 2016 U.S. election and Brexit, where disinformation efforts sought to amplify societal tensions and weaken Western unity.

The symbolism of financial support is not confined to domestic audiences. It is projected outward through disinformation narratives that frame Russia as a resilient nation under siege, encouraging sympathizers abroad to view Russian military efforts as legitimate defenses against Western aggression. This disinformation is designed to destabilize Western alliances and sow confusion about the true nature of Russian activities, all while promoting a myth of unity between Russian civilians and the state.

Strategic Implications for the United States and Western Allies

Russia's integration of financial networks, cyber warfare, and propaganda represents a complex challenge for the United States and its allies. The blurring of lines between civilian contributions and military operations makes it difficult for Western nations to disrupt these activities without infringing on legal civilian activities. The integration of financial and cyber

operations, coupled with the strategic use of propaganda, presents a comprehensive threat that requires a comprehensive counter-strategy.

Financial and Cyber Vulnerabilities

One of the critical vulnerabilities for Western nations is the inability to fully track and disrupt financial flows that fund Russian cyber operations. State-backed banks like Promsvyazbank allow Russia to create legal shields around its financial networks, complicating efforts to impose sanctions or freeze assets without affecting legitimate civilian activities. This financial camouflage enables Russia to continue funding offensive cyber activities, even as international efforts seek to isolate its economy.

The cyber dimension of Russia's hybrid warfare strategy also poses a significant challenge for critical infrastructure in the U.S. and Europe. Ransomware and malware attacks—facilitated by state-sponsored APT groups—have targeted vital sectors such as energy, communications, and government systems. These attacks not only serve to weaken confidence in the resilience of Western nations but also provide valuable intelligence that Russia can exploit in future conflicts.

Countering the Narrative and Disrupting the Feedback Loop

In addition to addressing financial and cyber vulnerabilities, Western nations must focus on countering the narratives that Russia uses to legitimize its actions. The symbolism promoted through campaigns like Братство: Сила Народа must be exposed as propaganda that exploits civilian sentiment for military gain. Public awareness campaigns that reveal the true nature of these organizations can help disrupt the feedback loop that sustains Russian military operations through civilian contributions.

Moreover, Western intelligence agencies should enhance their efforts to trace financial networks, particularly those linked to Russian military operations, and identify dual-use technologies that could be weaponized in cyber conflicts. Coordination between financial institutions and cyber defense agencies will be critical in detecting and disrupting these networks before they can be fully operationalized in hybrid warfare.

A Hybrid Warfare Model Fueled by Financial and Cyber Integration

As revealed through financial and cyber operations integration, Russia's hybrid warfare model represents a sophisticated form of asymmetric conflict that exploits financial networks, cyber capabilities, and information warfare to achieve its objectives. Using platforms like the People's Front and state-backed financial institutions like Promsvyazbank, Russia can bypass sanctions, fund military operations, and mobilize civilian resources for offensive cyber campaigns.

At the same time, propaganda and symbolism, such as the Братство: Сила Народа imagery, reinforce the idea that public participation in these efforts is a patriotic duty, further blurring the lines between civilian and military involvement. For the United States and its allies, countering this hybrid model requires a comprehensive approach addressing Russia's strategy's financial, cyber, and information warfare dimensions, disrupting financial networks, countering disinformation, and exposing the narratives that fuel Russia's domestic and international support.

Understanding and dismantling this multidimensional threat is crucial to undermining Russia's hybrid warfare capabilities and protecting Western interests from future aggression.

Strategic Impact of Civil-Military Hybridization in Russia's Hybrid Warfare

Russia's hybrid warfare model, which integrates civilian efforts with military operations, showcases a strategic fusion of financial infrastructure, legal protections, and military capabilities. Using state-backed financial institutions, civilian organizations, and charitable entities, Russia has developed a resilient system that circumvents international sanctions while continuing to fund military operations. This civil-military hybridization allows Russia to operate within legal frameworks that blur the lines between humanitarian aid and army financing, making it difficult for the international community to disrupt these financial networks. Below is an expanded and enhanced analysis of how Russia's economic resilience and legal cover through civilian organizations enable the state to sustain its military-industrial complex and cyber operations, even under the weight of Western sanctions.

Financial Infrastructure and Sanction Resilience: A Pillar of Russian Hybrid Warfare

Russia's ability to adapt to international sanctions is a feature of its hybrid warfare strategy, particularly in using financial infrastructure to protect military funding. The rekvisity.pdf document provides insight into how Russia channels funds through state-backed financial institutions, such as Promsvyazbank, to bypass sanctions and ensure that military production and cyber operations remain well-financed. The resilience of this monetary system, despite multiple rounds of sanctions from the U.S. and the EU, is a testament to Russia's capacity to operate within legal grey zones and use civilian-facing platforms as a cover for its military agenda.

Promsvyazbank: A Shield Against Sanctions

Promsvyazbank is critical in Russia's sanction resilience, serving as a financial shield for the military-industrial complex. Repurposed by the Kremlin to handle defense-related financial transactions, Promsvyazbank operates under legal protections that make it difficult for foreign entities to target its activities directly without impacting broader Russian economic operations, creating a buffer against sanctions, ensuring that military funds continue to flow despite Western efforts to cripple Russia's defense sector.

For Russia, this structure allows military financing to remain operational under the guise of legal and civilian activities. Funds raised through civilian organizations, such as the People's Front charity, are processed through Promsvyazbank, providing an aura of legitimacy to donations that ultimately support military production. This dual-use financial system complicates international efforts to track financial flows and ensures that sanctions do not ultimately stifle Russia's ability to mobilize resources for defense purposes.

Civilian Platforms as a Cover for Military Financing

Russia's ability to use civilian organizations and charitable entities as a front for military financing represents a significant challenge for the international community. For example, the People's Front charity presents itself as a humanitarian organization but plays a crucial role in channeling civilian donations to fund military efforts. By routing these funds through state-backed financial institutions, Russia can launder money into its military-industrial complex while maintaining legal cover to shield these activities from foreign scrutiny.

This tactic allows Russia to operate within a legal framework that obscures the true purpose of these donations. The ability to blend civilian and military operations through financial channels ensures Russia can continue its military expansion without facing the full brunt of

sanctions. For the international community, this presents a dilemma: targeting these financial flows without disrupting legitimate civilian and humanitarian efforts.

Legal and Financial Cover for Military Operations: The Grey Zone Strategy

A core element of Russia's hybrid warfare approach is its ability to operate in legal grey zones, where the lines between civilian and military operations are intentionally blurred. The People's Front charity, despite its public-facing role as a humanitarian entity, serves as a legal cover for military financing. This tactic is central to Russia's ability to maintain legal protections while continuing to fund military engagements, including its cyber operations. Using state-backed financial institutions and civilian-facing platforms, Russia ensures its military operations are protected from direct sanctions, making it difficult for foreign entities to disrupt these activities without infringing on civilian rights.

People's Front Charity: Blurring the Civilian-Military Divide

The People's Front charity is a prime example of how Russia uses civilian organizations to create legal cover for military activities. The charity operates as a humanitarian entity, raising funds to support civilians and military personnel in contested regions such as Donbas and Zaporizhzhia. However, the charity's deep ties to state-backed financial institutions, such as Promsvyazbank, reveal a more insidious purpose: providing a legitimate front for military financing.

By framing donations as humanitarian aid, the People's Front can evade scrutiny and maintain legal protections, making it difficult for foreign entities to target the individuals and organizations involved. The blurring of lines between civilian and military functions is a hallmark of Russia's hybrid warfare strategy, allowing the state to operate in a grey zone where it can fund military operations while maintaining legal deniability.

The grey zone operations present a significant challenge for foreign intelligence agencies and sanction enforcement bodies. The dual-use nature of these funds—where they can be directed toward humanitarian efforts and military operations—makes it difficult to isolate and target the financial flows that sustain Russia's military-industrial complex. This legal ambiguity allows Russia to operate with impunity, further complicating efforts to hold it accountable for its actions in the international arena.

State-Backed Financial Institutions as Legal Shields

The use of state-backed financial institutions, such as Promsvyazbank, provides an additional layer of legal protection for Russia's military operations. By handling donations

and processing civilian contributions, these institutions create a legal firewall that protects Russia's military-industrial complex from the full impact of international sanctions. By embedding military transactions within civilian financial flows, Russia ensures that any attempt to disrupt these transactions could inadvertently harm legitimate civilian operations—a risk that Western governments are often unwilling to take.

This legal cover is particularly adequate in hybrid warfare, where the distinction between civilian support and military funding is intentionally blurred. By using charitable organizations as intermediaries, Russia can launder funds into its military-industrial complex while maintaining the pretense of legality, making it difficult for foreign governments to sanction or target those involved, as the risk of collateral damage—including harm to legitimate humanitarian efforts—is too high.

Strategic Challenges for the International Community

Russia's use of civilian organizations as a front for military financing presents a complex challenge for the international community, particularly in the context of sanction enforcement and financial tracking. The ability to blend military and civilian functions within legal frameworks makes it difficult for foreign governments to effectively target the financial flows that sustain Russia's military operations. The dual-use nature of these financial networks—where donations can be used for humanitarian aid and army production—creates a legal grey zone that Russia exploits to its advantage.

Countering Russia's Financial and Legal Tactics

To counter Russia's hybrid warfare model, the international community must develop strategies that address the legal grey zones in which Russia operates. The strategies include:

- Enhancing financial intelligence capabilities to track and disrupt dual-use funds routed through charitable organizations and state-backed financial institutions.
- Improving coordination between intelligence agencies, sanction enforcement bodies, and financial institutions to detect better and isolate military-related financial flows.
- Targeting legal loopholes that allow Russia to launder military funds through humanitarian fronts, ensuring that sanctions are more effective in disrupting military financing.

Balancing Sanctions with Humanitarian Considerations

A key challenge in addressing Russia's financial tactics is balancing the need to disrupt military financing with the risk of harming legitimate humanitarian efforts. Russia's use of civilian organizations as intermediaries complicates the task of sanction enforcement, as any action taken against these organizations could result in collateral damage to humanitarian operations. To mitigate this risk, the international community must develop targeted sanctions that focus on the military dimensions of these organizations while ensuring that humanitarian aid remains unaffected.

Targeted sanctions require a nuanced approach to sanction enforcement, where legal and financial expertise is used to differentiate between legitimate humanitarian activities and military funding operations. By focusing on state-backed financial institutions and military-linked transactions, the international community can disrupt the financial flows that support Russia's military operations without causing undue harm to civilian efforts.

Civil-Military Hybridization as a Strategic Weapon in Russia's Hybrid Warfare

Russia's ability to integrate civilian organizations and state-backed financial institutions into its military financing operations represents a key component of its hybrid warfare strategy. By using charitable entities like the People's Front as a legal cover and routing funds through Promsvyazbank, Russia ensures a steady flow of resources into its military-industrial complex while maintaining legal protections that complicate efforts to disrupt these activities.

The dual-use nature of these financial flows—where donations can be used for humanitarian aid and military purposes—creates a legal grey zone that Russia exploits to its advantage, presenting a significant challenge for the international community as efforts to sanction or disrupt these financial networks must be carefully balanced against the risk of harming legitimate civilian efforts.

By understanding the legal and financial dimensions of Russia's hybrid warfare, the international community can develop more effective strategies to counter these tactics, ensuring that military financing is disrupted without causing unnecessary harm to humanitarian operations, which is critical in undermining Russia's ability to sustain its military engagements and cyber operations and in ensuring that international sanctions are more effective in achieving their objectives.

A Blueprint for Modern Hybrid Warfare

Russia's integration of civilian platforms, financial operations, and cyber capabilities into its hybrid warfare strategy represents a highly sophisticated approach to modern conflict, combining state and non-state resources to advance military and geopolitical goals. The use of platforms like Everything for Victory and the People's Front charity as conduits for mobilizing civilian participation and laundering financial resources into military ventures underscores the effectiveness of this strategy. At the same time, cyber operations, disinformation campaigns, and financial manipulation serve to undermine Western powers and destabilize global institutions, creating a comprehensive battlefield where Russia's asymmetric tactics can flourish.

The Civil-Military Nexus: A Core Pillar of Hybrid Warfare

One of the defining characteristics of Russia's hybrid warfare model is its ability to use civilian participation to support its military-industrial complex directly. Platforms like Everything for Victory exemplify this by encouraging monetary donations, technological innovations, and public engagement under the guise of nationalistic duty. Including initiatives such as the Kulibin Club—which harnesses civilian expertise to develop advanced technologies like drones, robotic systems, and cyber tools—further strengthens the connection between civil society and military efforts.

Всё для победы!

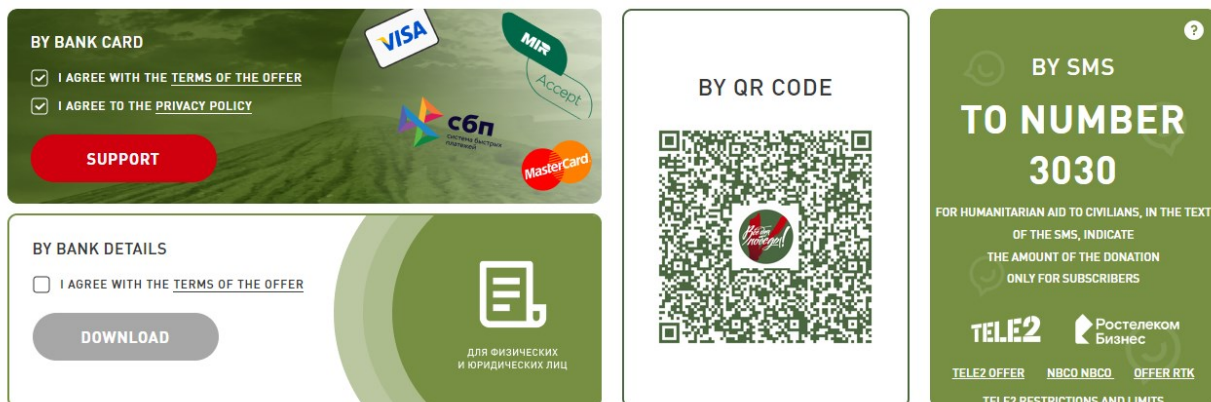
This civil-military nexus is key to Russia's resilience under international sanctions, as it allows the state to tap into civilian resources and innovation to fill the gaps created by Western restrictions on military imports. By blurring the line between civilian and military sectors, Russia transforms its population into an active participant in its defense strategy, all while framing this engagement as a patriotic duty. This approach sustains Russia's military-industrial base and reinforces national unity, ensuring a steady support flow for its military operations.

Financial Manipulation: A Weapon in Hybrid Warfare

Using financial systems to channel resources into military operations is another cornerstone of Russia's hybrid strategy. The rekvisity.pdf document reveals how state-backed financial institutions, such as Promsvyazbank, are repurposed to handle defense-related transactions, allowing Russia to bypass international sanctions. The integration of civilian platforms, like the People's Front charity, into this financial ecosystem demonstrates Russia's ability to use legally protected civilian organizations as financial conduits for military purposes.

Using these financial loopholes, Russia ensures that donations raised through humanitarian efforts can be repurposed for military production, including developing cyber capabilities. This tactic of blurring financial flows between humanitarian aid and army ventures creates a legal firewall that complicates efforts by the international community to track and disrupt these funds. The ability to operate within this grey zone shields Russia's military operations from sanction enforcement and enables the sustained flow of resources into its military-industrial complex.

Cyber Operations and Information Warfare: The Digital Frontline



The image shows a donation interface for 'People's Front' with four main sections:

- BY BANK CARD:** Includes checkboxes for 'I AGREE WITH THE TERMS OF THE OFFER' and 'I AGREE TO THE PRIVACY POLICY', a red 'SUPPORT' button, and logos for VISA, MIR, and MasterCard.
- BY QR CODE:** Features a large QR code with the 'People's Front' logo in the center.
- BY SMS:** Prompts the user to 'TO NUMBER 3030' for humanitarian aid. It includes instructions to indicate the donation amount in the SMS text and mentions 'TELE2 OFFER', 'NBCD NBCO', and 'OFFER RTK'.
- BY BANK DETAILS:** Includes a checkbox for 'I AGREE WITH THE TERMS OF THE OFFER' and a 'DOWNLOAD' button. It also mentions 'для физических и юридических лиц' (for physical and legal entities).

At the heart of Russia's hybrid warfare strategy is its ability to integrate cyber operations with information warfare to create a digital frontline that complements its financial manipulation and military activities. State-sponsored cyber units, such as APT28 (Fancy Bear) and APT29 (Cozy Bear), play a critical role in conducting cyber espionage, ransomware attacks, and malware campaigns aimed at U.S. infrastructure, Western elections, and military assets.

These cyber tools allow Russia to weaken its adversaries while maintaining plausible deniability and avoiding direct military confrontation.

The integration of disinformation campaigns into these cyber operations further amplifies their impact. By using domestic media outlets, like RT and Sputnik, alongside international disinformation campaigns, Russia spreads false narratives that undermine confidence in Western institutions and sow divisions among the U.S. and its allies. This information warfare is not limited to cyber tools alone. However, it is amplified through the use of symbolism, as seen in campaigns like Братство: Сила Народа ("Brotherhood: Power of the People"), which frame financial contributions and civilian participation as essential to national defense. This narrative reinforces the public's sense of duty, ensuring economic and moral support for Russia's military operations remains strong.

Undermining Western Powers: Strategic Implications

The ultimate goal of Russia's hybrid warfare is to undermine Western powers and their global influence by exploiting their vulnerabilities through cyber attacks, financial manipulation, and disinformation campaigns. Russia's ability to sustain its military capabilities despite sanctions speaks to the resilience of its hybrid warfare model, where civilian engagement, cyber tools, and financial systems work in tandem to counteract Western pressure. These operations create instability within Western institutions, such as election systems, financial markets, and critical infrastructure, weakening the overall cohesion of U.S. alliances and exposing vulnerabilities that Russia can exploit.

Russia's hybrid warfare tactics, particularly cyber operations, allow it to exert influence without engaging in conventional warfare, making it difficult for the U.S. and its allies to counter these threats effectively. Russia complicates efforts to attribute attacks, impose sanctions, or disrupt financial flows by maintaining plausible deniability and operating in legal grey zones. This asymmetric advantage gives Russia strategic flexibility, allowing it to disrupt adversaries while expanding its influence in vital geopolitical regions.

A Blueprint for Countering Russian Hybrid Warfare

Understanding Russia's hybrid warfare model is crucial for developing effective countermeasures that address the full spectrum of threats posed by its financial channels, cyber tools, and information warfare tactics. The key to disrupting Russia's hybrid strategy lies in targeting the interconnected systems that sustain it, from the financial networks that

fund military operations to the cyber infrastructures that enable covert attacks and disinformation campaigns.

Financial Sanctions and Legal Accountability

- Tightening financial sanctions against state-backed institutions like Promsvyazbank and tracking dual-use financial flows through charitable platforms can help disrupt the monetary resources that Russia uses to sustain its military operations.
- Legal accountability measures should be expanded to target civilian organizations that serve as fronts for military financing, ensuring that donors and financial institutions involved in laundering military funds are held accountable under international law.

Strengthening Cyber Defenses

- Cybersecurity infrastructure in Western nations must be strengthened to protect against state-sponsored attacks, particularly in critical sectors such as energy, communications, and financial markets. Enhanced intelligence-sharing among U.S. allies will be essential in detecting and neutralizing cyber threats before they can cause significant damage.

Combatting Disinformation and Propaganda

- Countering Russian disinformation requires a comprehensive approach that includes public education campaigns, media literacy efforts, and technological solutions to identify and neutralize false narratives. By exposing the true nature of Russia's hybrid warfare tactics, Western nations can erode public support for these efforts domestically and abroad.

Civil-Military Cooperation

- A focus on increasing civilian-military cooperation is essential for effectively countering Russia's hybrid warfare tactics, developing legal frameworks that clarify the boundaries between civilian and military sectors, and ensuring that humanitarian efforts are protected while military financing is isolated.

Russia's Hybrid Warfare Blueprint and the Path Forward

Russia's hybrid warfare strategy—a blueprint for modern conflict—relies on its ability to blend civilian resources, financial networks, and cyber tools to sustain its military-industrial complex and project influence on the global stage. Using platforms like Everything for Victory



and People's Front charity, Russia creates a system where public engagement and nationalism are mobilized to support military operations. Simultaneously, cyber operations and disinformation campaigns serve to undermine Western powers, creating instability and weakening alliances.

Understanding and countering these interconnected strategies is essential for the United States and its allies to dismantle the hybrid warfare model, a comprehensive approach that addresses the financial channels, cyberinfrastructure, and information warfare systems Russia uses to achieve its objectives. By disrupting financial flows, strengthening cyber defenses, and countering disinformation, the international community can undermine Russia's hybrid warfare capabilities and protect Western interests from future aggression.



Appendix A



SUPPORT THE SOLDIERS AND CIVILIANS
WHO HAVE BEEN AFFECTED BY UKRAINE'S
MILITARY ACTIONS!

SUPPORT

ABOUT THE PORTAL

UNDER THE MOTTO "EVERYTHING FOR VICTORY!" THE PEOPLE'S
FRONT ASKS TO SUPPORT THE FIGHTERS ON THE FRONTLINE AND

КУЛИБИН-КЛУБ

THE PEOPLE'S FRONT SELECTS, TESTS, AND SUPPORTS SERIAL PRODUCTION OF THE
BEST DEVELOPMENTS OF DOMESTIC ENGINEERS.

THANKS TO THIS INITIATIVE, IT WAS POSSIBLE TO DELIVER THOUSANDS OF INNOVATIVE
ELECTRONIC WARFARE SYSTEMS TO THE FRONT LINES TO COUNTER ENEMY DRONES,
QUADCOPTERS, SELF-PROPELLED ROBOT CARTS, AND MUCH, MUCH MORE.

IF YOU INVENT NEW TECHNOLOGIES, ASSEMBLE EQUIPMENT FOR FIGHTERS, KNOW
HOW TO IMPROVE THE CHARACTERISTICS OF EXISTING MODELS, WRITE TO US, LET'S

CONTRIBUTE TOGETHER TO VICTORY AND SAVING THE LIVES OF FIGHTERS ON THE FRONT LINES.

DOWNLOAD THE KULIBIN CLUB PARTICIPANT APPLICATION FORM AND SEND IT TO KULIBINCLUB@ONF.RU .

PARTICIPANT FORM

ALSO, RUSSIAN INVENTORS AND PRODUCTION ORGANIZERS

CAN TAKE PART IN THE IMPLEMENTATION OF THE NATIONAL PROJECT



Developer questionnaire for support

from the People's Military-Industrial Complex

Company representative's full name:

Enter your full name

Contact e-mail:

Enter your contact e-mail address

Contact phone number:

Enter your contact phone number in the format +7-912-345-67-89

Company name:

Enter your company name

Actual location of the company:

Indicate your actual location in the format: subject, city, street, house, office/premises

Type/category of the proposed solution:

Tactical electronic warfare and reconnaissance equipment / UAVs, their systems and components / Robotic platforms / Equipment and gear / Tactical medicine / Communications equipment / Other: specify

Leave only the necessary categories from the list, delete the rest

Brief description of the solution:

Leave a brief description of the proposed solution, its advantages, description of operation and competitive advantages

What combat missions are solved with the help of your development?

Write what combat tasks it accelerates, automates and/or optimizes, how this problem was identified

Where was the solution tested?

Indicate all installation information with exact dates of tests, names of institutes/companies that conducted the examination, installation data of the units on the LBS that used the product/solution

Link to technical documentation, tests, presentations and drawings for the product on the Yandex.Disk platform:

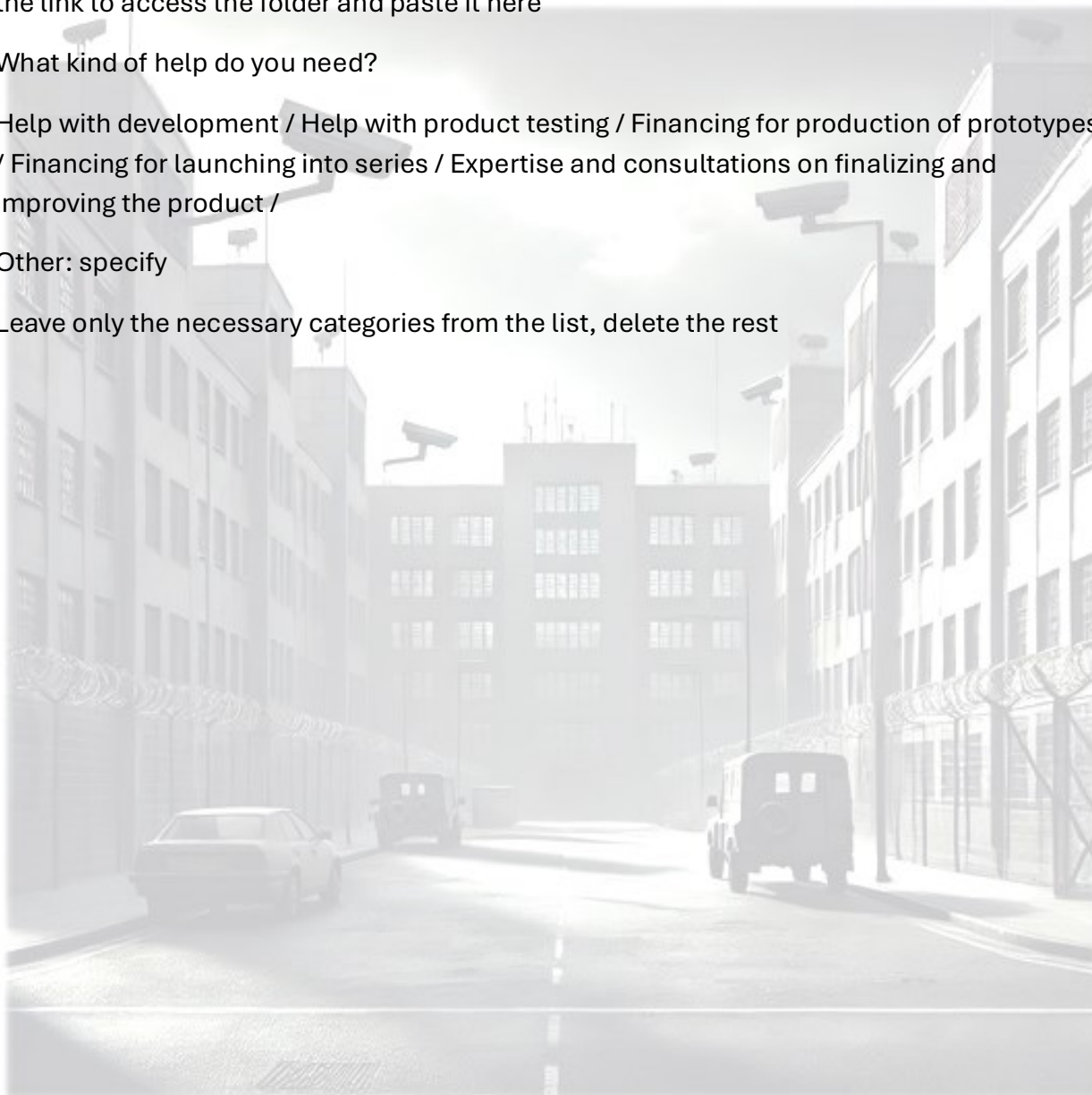
Create a folder on the Yandex.Disk platform with access via link, upload detailed text descriptions in .txt format, drawings and photo materials (if necessary) in .pdf format, copy the link to access the folder and paste it here

What kind of help do you need?

Help with development / Help with product testing / Financing for production of prototypes / Financing for launching into series / Expertise and consultations on finalizing and improving the product /

Other: specify

Leave only the necessary categories from the list, delete the rest



Help the front: <https://pobeda.onf.ru/>

ABOUT THE PORTAL

HOW CAN I HELP?

KULIBIN CLUB

COLLECTION POINTS

SUMMARIES

QUESTIONS

WORDS OF ENCOURAGEMENT

FIND OUT HOW TO SUPPORT

THE CIVILIAN POPULATION OF DONBASS

8 (800) 200-34-11

SUPPORT THE SOLDIERS AND CIVILIANS WHO HAVE BEEN AFFECTED BY UKRAINE'S
MILITARY ACTIONS!

SUPPORT

ABOUT THE PORTAL

UNDER THE MOTTO "EVERYTHING FOR VICTORY!" THE PEOPLE'S FRONT ASKS TO
SUPPORT THE FIGHTERS ON THE FRONTLINE AND THE CIVILIANS OF THE NEW AND
BORDER REGIONS. ON THE PORTAL WE TELL YOU HOW TO TRANSFER MONEY, WHERE
THEY ACCEPT THE THINGS THAT ARE REQUIRED BY THE MILITARY AND RESIDENTS OF THE
LPR, DPR, KHERSON, ZAPOROZHYE, KURSK AND BELGOROD REGIONS. HERE YOU CAN
ALSO FIND OUT HOW THE CARGO IS DELIVERED TO THE ADDRESSEE.

SUPPORT THE FIGHTERS ON THE FRONT LINES

BY BANK CARD

I AGREE WITH THE TERMS OF THE OFFER

I AGREE WITH THE PRIVACY POLICY

SUPPORT

BY BANK DETAILS

I AGREE WITH THE TERMS OF THE OFFER

DOWNLOAD

BY SMS

TO NUMBER 3030

FOR HUMANITARIAN AID TO CIVILIANS,

PLEASE INDICATE THE DONATION AMOUNT IN THE SMS TEXT MESSAGE

FOR SUBSCRIBERS ONLY

TELE2 OFFER

RNKO OFFER

RTK OFFER

TELE2 RESTRICTIONS AND LIMITS

HOW CAN I HELP?

COLLECTION IS UNDERWAY

COLLECTION COMPLETED

COLLECTION OF ALEXANDER KOTS FROM 23.09
SUPPORT

REGIONAL GATHERING FOR FIGHTERS, DEFENSI...
SUPPORT

MEETING "RUSSIAN MOTORCYCLISTS - TO STORMTROOPERS...
SUPPORT

NIKOLAY DOLGACHEV'S COLLECTION FOR UNITS...
SUPPORT

COLLECTION "DEFENDERS OF BELGOROD" FROM 26.03
SUPPORT

SPECIAL COLLECTION "FOR MILITARY DOCTORS" FROM 09...
SUPPORT

COLLECTION BY DENIS MAIDANOV FROM 03.06
SUPPORT

COLLECTION OF JSC "NTV TELEVISION COMPANY" FOR PARATROOPERS...
SUPPORT

POLINA TSVETKOVA'S COLLECTION FOR CIVILIANS...
SUPPORT

SERGEY KARYAKIN'S COLLECTION FOR STORMTROOPERS FROM ...
SUPPORT

COLLECTION FOR PEOPLE'S REGIMENTS AND SEWING BATTALIONS...
SUPPORT

THE PEOPLE'S FRONT OPENED FUNDING IN EVERY REGION...

SUPPORT

COLLECTION BY YURI PODOLYAKI FOR RADIO-ELECTRONIC MEANS...
SUPPORT

COLLECTING NIGHTINGALES LIVE ON QUADROCOPTERS FOR ...
SUPPORT

YULIA BARANOVSKAYA'S COLLECTION FOR THE PEOPLE OF DONBASS...
SUPPORT

"SMART CITY" COLLECTION FROM 26.04
SUPPORT

YULIA CHICHERINA'S COLLECTION FOR THE ARMED FORCES UNITS...
SUPPORT

COLLECTION OF ALEXEY PODDUBNY (DJANGO) "TO ...
SUPPORT

ALEXEY IVANOV'S CAMP FOR MOTORIS...
THE MONEY HAS BEEN COLLECTED AND THE PURCHASE IS UNDERWAY.
[READ MORE](#)

COLLECTION OF GUSEYN GUSEINOV FROM 30.07 FOR G...
THE MONEY HAS BEEN COLLECTED AND THE PURCHASE IS UNDERWAY.
[READ MORE](#)

[VIEW ALL REQUESTS](#)

[DOWNLOAD POSTERS OF THE FOUNDATION](#)

"EVERYTHING FOR VICTORY"

PLACING POSTERS OF THE PEOPLE'S FRONT FUND "EVERYTHING FOR VICTORY!" IS
ANOTHER WAY TO SUPPORT OUR DEFENDERS ON THE FRONT LINE.

ALL FUNDS RAISED THANKS TO YOU GO EXCLUSIVELY TO THE NEEDS OF THE DEFENDERS.
USUALLY PEOPLE LEARN ABOUT US THROUGH INFORMATION PARTNERS AND SOCIAL
ADVERTISING. BUT THIS IS NOT ENOUGH TO FULFILL ALL THE REQUESTS OF THE GUYS.

YOU CAN HELP US BY PLACING A POSTER OF THE "EVERYTHING FOR VICTORY!" FUND AT
YOUR ENTRANCE, STORE, ESTABLISHMENT OR ENTERPRISE. THIS WAY EVEN MORE PEOPLE
WILL LEARN ABOUT US, AND THE GUYS ON THE FRONT LINE WILL RECEIVE EVERYTHING
THEY NEED TO LIBERATE NEW REGIONS.

PRINT AND HANG THE POSTER
IN THE ENTRANCE OF YOUR BUILDING!

DOWNLOAD KULIBIN CLUB

THE PEOPLE'S FRONT IS ENGAGED IN THE SELECTION, TESTING, AND SUPPORT OF SERIAL PRODUCTION OF THE BEST DEVELOPMENTS OF DOMESTIC ENGINEERS.

THANKS TO THIS INITIATIVE, IT WAS POSSIBLE TO PUT THOUSANDS OF INNOVATIVE ELECTRONIC WARFARE SYSTEMS TO THE FRONT LINES TO COUNTER ENEMY DRONES, QUADCOPTERS, SELF-PROPELLED ROBOT CARTS AND MUCH, MUCH MORE.

IF YOU INVENT NEW TECHNOLOGIES, ASSEMBLE EQUIPMENT FOR FIGHTERS, KNOW HOW TO IMPROVE THE CHARACTERISTICS OF EXISTING MODELS, WRITE TO US, LET'S CONTRIBUTE TOGETHER TO THE VICTORY AND SAVING THE LIVES OF FIGHTERS ON THE FRONT LINES.

DOWNLOAD THE KULIBIN CLUB PARTICIPANT FORM AND SEND IT
TO KULIBINCLUB@ONF.RU .

PARTICIPANT FORM

ALSO, RUSSIAN INVENTORS AND PRODUCTION ORGANIZERS
CAN TAKE PART IN THE IMPLEMENTATION OF THE NATIONAL PROJECT
"UNMANNED AERIAL SYSTEMS", DETAILS ON THE WEBSITE OF
THE MINISTRY OF INDUSTRY AND TRADE .

COLLECTION POINTS

IN EVERY SUBJECT OF THE RUSSIAN FEDERATION THERE ARE REGIONAL OFFICES OF THE PEOPLE'S FRONT. HERE YOU CAN BRING THE THINGS THE GUYS ON THE FRONT LINES NEED. THE CURRENT LIST CAN BE VIEWED IN THE QUESTIONS AND ANSWERS SECTION . TO SEE WHERE THE PEOPLE'S FRONT OFFICE IS IN YOUR REGION, POINT THE CURSOR OVER THE MAP.

WORDS OF ENCOURAGEMENT TO THE FIGHTERS

HERE YOU CAN LEAVE A TEXT MESSAGE FOR THE DEFENDERS, AND WE WILL DEFINITELY PASS IT ON!



SUPPORT OUR FIGHTERS WITH A KIND WORD!

YOUR NAME

E-MAIL

SEND

TOGETHER WITH US

Previous

EDGARD ZAPASHNY
GENERAL DIRECTOR
OF THE GREAT MOSCOW CIRCUS,
PEOPLE'S ARTIST
OF THE RUSSIAN FEDERATION

ДЕНИС ЛЕБЕДЕВ
ЧЕМПИОН МИРА ПО БОКСУ

ЮРИЙ ПОДОЛЯКА
ПОПУЛЯРНЫЙ БЛОГЕР

ЮЛИЯ ЧИЧЕРИНА
РОССИЙСКАЯ РОК-ПЕВИЦА,
МУЗЫКАНТ, АКТРИСА

ДМИТРИЙ ПЕВЦОВ
НАРОДНЫЙ АРТИСТ РОССИИ,
АКТЁР

ДЕНИС МАЙДАНОВ
ЗАСЛУЖЕННЫЙ АРТИСТ
РОССИЙСКОЙ ФЕДЕРАЦИИ

АНДРЕЙ СОКОЛОВ
НАРОДНЫЙ АРТИСТ
РОССИЙСКОЙ ФЕДЕРАЦИИ

АНТОН ШАГИН

АКТЁР ТЕАТРА И КИНО

ВЛАДИМИР СОЛОВЬЕВ
ЖУРНАЛИСТ

ПЕТР ТОЛСТОЙ
ЖУРНАЛИСТ,
ВЕДУЩИЙ ПЕРВОГО КАНАЛА

АЛЕКСАНДР СКЛЯР
МУЗЫКАНТ,
ЛИДЕР ГРУППЫ ВА-БАНК,
ЗАСЛУЖЕННЫЙ АРТИСТ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ИВАН ОХЛОБЫСТИН
АКТЁР, КИНОРЕЖИССЁР,
СЦЕНАРИСТ, ДРАМАТУРГ, ПИСАТЕЛЬ

РУСЛАН ОСТАШКО
ЖУРНАЛИСТ,
ВЕДУЩИЙ ПЕРВОГО КАНАЛА,
МУЗЫКАНТ

ТАРАС ХТЕЙ
СПОРТСМЕН, АМБАССАДОР
ВСЕРОССИЙСКОЙ ФЕДЕРАЦИИ
ВОЛЕЙБОЛА

ИРИНА АПЕКСИМОВА
ЗАСЛУЖЕННАЯ АРТИСТКА
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОЛИНА ЦВЕТКОВА
ВЕДУЩАЯ ПЕРВОГО КАНАЛА

ЭДГАРД ЗАПАШНЫЙ
ГЕНЕРАЛЬНЫЙ ДИРЕКТОР
БОЛЬШОГО МОСКОВСКОГО ЦИРКА,
НАРОДНЫЙ АРТИСТ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ДЕНИС ЛЕБЕДЕВ
ЧЕМПИОН МИРА ПО БОКСУ

ЮРИЙ ПОДОЛЯКА
ПОПУЛЯРНЫЙ БЛОГЕР

ЮЛИЯ ЧИЧЕРИНА
РОССИЙСКАЯ РОК-ПЕВИЦА,
МУЗЫКАНТ, АКТРИСА

ДМИТРИЙ ПЕВЦОВ
НАРОДНЫЙ АРТИСТ РОССИИ,
АКТЁР

ДЕНИС МАЙДАНОВ
ЗАСЛУЖЕННЫЙ АРТИСТ
РОССИЙСКОЙ ФЕДЕРАЦИИ

АНДРЕЙ СОКОЛОВ
НАРОДНЫЙ АРТИСТ
РОССИЙСКОЙ ФЕДЕРАЦИИ

АНТОН ШАГИН
АКТЁР ТЕАТРА И КИНО

ВЛАДИМИР СОЛОВЬЕВ
ЖУРНАЛИСТ

ПЕТР ТОЛСТОЙ
ЖУРНАЛИСТ,
ВЕДУЩИЙ ПЕРВОГО КАНАЛА

АЛЕКСАНДР СКЛЯР
МУЗЫКАНТ,
ЛИДЕР ГРУППЫ ВА-БАНК,
ЗАСЛУЖЕННЫЙ АРТИСТ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ИВАН ОХЛОБЫСТИН
АКТЁР, КИНОРЕЖИССЁР,

СЦЕНАРИСТ, ДРАМАТУРГ, ПИСАТЕЛЬ

РУСЛАН ОСТАШКО
ЖУРНАЛИСТ,
ВЕДУЩИЙ ПЕРВОГО КАНАЛА,
МУЗЫКАНТ

ТАРАС ХТЕЙ
СПОРТСМЕН, АМБАССАДОР
ВСЕРОССИЙСКОЙ ФЕДЕРАЦИИ
ВОЛЕЙБОЛА

ИРИНА АПЕКСИМОВА
ЗАСЛУЖЕННАЯ АРТИСТКА
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОЛИНА ЦВЕТКОВА
ВЕДУЩАЯ ПЕРВОГО КАНАЛА

ЭДГАРД ЗАПАШНЫЙ
ГЕНЕРАЛЬНЫЙ ДИРЕКТОР
БОЛЬШОГО МОСКОВСКОГО ЦИРКА,
НАРОДНЫЙ АРТИСТ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Next

ПОСЛЕДНИЕ СОБЫТИЯ

READ THE LATEST NEWS ABOUT HELPING FIGHTERS ON THE FRONTLINES AND CIVILIANS
IN OUR SOCIAL NETWORKS: VKONTAKTE AND TELEGRAM

WAR CORRESPONDENT ALEXANDER KOTS OPENED HIS SEVENTH TRAINING CAMP
23.09.2024 / 12:00

RUSSIAN SINGER DJANGO OPENED A NEW TRAINING CAMP FOR ASSAULT AND
MOTORIZED RIFLE UNITS ON THE FRONT LINES OF THE SVO

17.09.2024 / 15:00

CHANNEL ONE CORRESPONDENT ALEXEY IVANOV OPENED A RECRUITMENT FOR THE
"ATLANT" BATTALION

05.09.2024 / 09:00

FIGHTERS ON THE KURSK BORDER RECEIVED EQUIPMENT PURCHASED THANKS TO THE
COLLECTION

15.08.2024 / 16:00

CHANNEL ONE MILITARY CORRESPONDENT GUSEYN GUSEINOV OPENS A TRAINING CAMP FOR MARINES

30.07.2024 / 15:00

THE PEOPLE'S FRONT HAS OPENED AN URGENT TRAINING CAMP FOR AIRBORNE TROOPS

29.07.2024 / 16:00

WAR CORRESPONDENT NIKOLAI DOLGACHEV OPENED A NEW TRAINING CAMP FOR SVO FIGHTERS

22.07.2024 / 13:00

ALL NEWS

QUESTIONS AND ANSWERS

WHO ARE WE?

THE PEOPLE'S FRONT IS A PUBLIC MOVEMENT LED BY RUSSIAN PRESIDENT VLADIMIR PUTIN. WE UNITE ACTIVE PEOPLE OF OUR COUNTRY TO SOLVE ISSUES IMPORTANT TO EVERY CITIZEN. SINCE FEBRUARY 2022, THE PEOPLE'S FRONT HAS BEEN COLLECTING AND DELIVERY OF HUMANITARIAN AID TO GUYS ON THE FRONTLINES AND TO THE PEOPLE OF NEW AND BORDER REGIONS.

WHY DID WE CREATE A FUNDRAISING WEBSITE?

MILITARY OPERATIONS CONSTANTLY REQUIRE NEW RESOURCES. CARS, DRONES, ALL THE THINGS WE COLLECT OR PURCHASE FOR THE GUYS ON THE FRONT LINES ARE CONSUMABLES THAT THE MILITARY NEED ON A DAILY BASIS. THERE IS A HUGE DEMAND FOR DETECTION AND SUPPRESSION EQUIPMENT FOR DRONES. TIMELY ASSISTANCE HELPS SAVE THE LIVES AND HEALTH OF THE GUYS. AND MOST IMPORTANTLY, RECEIVING THIS ASSISTANCE, THE SOLDIERS IN THE TRENCHES FEEL SUPPORT, SEE THAT ALL OF RUSSIA IS BEHIND THEM.

HOW TO HELP?

YOU CAN MAKE A FINANCIAL DONATION , OR IF YOU HAVE SOMETHING FROM THE LIST OF NECESSARY THINGS , BRING THEM TO THE BRANCHES OF THE PEOPLE'S FRONT, OPERATING IN 85 REGIONS OF RUSSIA.

WHAT CAN I BRING TO THE COLLECTION POINT?

YOU CAN BRING THE FOLLOWING TO THE COLLECTION POINTS LOCATED IN THE REGIONAL BRANCHES OF THE PEOPLE'S FRONT:

BULLETPROOF VESTS.

HELMETS.

DIGITAL RADIOS WITH A RANGE OF 5-10 KM.

QUADCOPTERS WITH CAMERAS AND A FLIGHT RANGE OF 3 KM.

MEMORY CARDS FOR QUADCOPTERS.

TACTICAL FIRST AID KITS.

BATTERIES FOR ELECTRONIC DEVICES AND CHARGERS FOR THEM.

TABLETS AND LAPTOPS.

THERMAL IMAGERS.

BINOCULARS.

SIGHTS.

NIGHT VISION DEVICES.

FOR MORE DETAILED INFORMATION, PLEASE CALL 8 (800) 200-34-11 .

HOW TO SUPPORT CIVILIANS?

IN THE SECTION "ASSISTANCE TO THE CIVILIAN POPULATION" YOU CAN SUPPORT RESIDENTS OF SPECIFIC TERRITORIES WITH FOOD PACKAGES, ESSENTIAL ITEMS, MEDICINES, BUILDING MATERIALS, AND PROVIDE TARGETED ASSISTANCE TO THOSE IN NEED.

WHAT EXACTLY DOES THE PEOPLE'S FRONT DO?

MILITARY CORRESPONDENTS, BLOGGERS, FAMOUS PEOPLE, AND MEDIA EDITORIALS TALK ABOUT THE POSSIBILITY OF MAKING THEIR CONTRIBUTION. WE SCALE THEIR ACTIVITIES, PURCHASE GOODS IN LARGE BATCHES, PROVIDE WAREHOUSE SPACE AND INFORMATION SUPPORT, ORGANIZE LOGISTICS CHAINS, AND ASSIST IN THE SECURITY OF FINANCIAL TRANSACTIONS.

WHERE DO APPLICATIONS COME FROM?

APPLICATIONS COME FROM WAR CORRESPONDENTS, JOURNALISTS, FAMOUS PEOPLE WHO BECOME CURATORS OF THE TRAINING CAMP, AS WELL AS THE COMMAND OF MILITARY UNITS.

HOW CAN I GET ACQUAINTED WITH THE REPORTS?

WHEN POSSIBLE, DUE TO SECURITY REQUIREMENTS, WE PREPARE A VIDEO OF THE DELIVERY AND POST IT ON THE SOCIAL NETWORKS OF THE PEOPLE'S FRONT. ALSO, CONTROL OVER THE DELIVERY IS CARRIED OUT BY MILITARY CORRESPONDENTS AND WELL-KNOWN PEOPLE WHO ARE THE CURATORS OF THE COLLECTIONS. AND ON THE PAGE OF EACH COLLECTION, INFORMATION IS POSTED ABOUT THE COMPOSITION OF THE PURCHASE, THE FUNDS COLLECTED AND SPENT.

Источник: https://pobeda.onf.ru/#qa_anch

