

# The Cloud of War: How Russian Military Mobile Applications Exploit Western Tech in the War Against Ukraine

**Volodymyr Styran**

State Cyber Protection Center

State Service of Special Communications and Information Protection

Kyiv, Ukraine

**Abstract:** This study conducts an analysis of Russian mobile applications deployed in the ongoing war of aggression against Ukraine, focusing specifically on their dependency on Western cloud and IT infrastructure. The investigation involved acquiring APK files of various apps used in military and intelligence operations, revealing a staggering prevalence of Western technology in their architecture. Key findings indicate that these applications extensively utilize Western cloud services for data storage, media streaming, and access management, alongside the global DNS services, anti-DDoS, and cybersecurity solutions to secure communication channels and protect against cyberattacks.

The study also uncovered significant reliance on global cloud service providers, which play a critical role in supporting the backend infrastructure of these apps. Furthermore, virtual private server (VPS) providers were identified as integral components in maintaining server operations and data processing for these war-related tools.

This widespread adoption of Western technological resources in applications directly tied to the military efforts of a state engaged in an aggressive invasion raises profound ethical and strategic concerns. It highlights a paradox in which companies from democratic nations—often nations imposing sanctions against Russia—inadvertently support the technical backbone of Russia’s military operations. The study calls for a reevaluation of the policies governing the use of these platforms in conflict zones, emphasizing the need for stricter regulations and greater accountability from tech giants.

**Keywords:** *Russian mobile apps, war in Ukraine, cloud service providers, military technology, cyber warfare, digital geopolitics, technological dependencies, ethical implications, Western IT infrastructure*

## 1. INTRODUCTION

The war in Ukraine has highlighted the transformative power of technology in modern conflict. As Russian aggression continues, international technology companies have played a critical role in bolstering Ukraine's defenses, reshaping the battlefield in unprecedented ways.<sup>1</sup> Notable examples include SpaceX's Starlink, which has ensured uninterrupted connectivity amidst widespread infrastructure damage,<sup>2</sup> and Microsoft, whose cybersecurity efforts have shielded Ukraine's critical systems from persistent cyberattacks.<sup>3</sup> Additionally, companies like Palantir Technologies have provided advanced data analytics platforms, enabling Ukrainian forces to process vast amounts of information for strategic and tactical decision-making.<sup>4</sup>

These contributions underscore how technology, once a tool of convenience, has become a lifeline in wartime scenarios. However, this technological support has not been one-sided. Paradoxically, the very platforms that aid Ukraine also serve the adversary, creating a complex web of dependency and ethical dilemmas. Western cloud infrastructure and cybersecurity solutions, integral to Ukraine's defense, are simultaneously exploited by the Russian military.

Discussions under international humanitarian law (IHL) have raised concerns about technology companies supporting Ukraine's defense being considered military targets, given their role in aiding military operations.<sup>5</sup> However, there has been little to no discourse on the implications of these same companies inadvertently aiding the adversary. This oversight ignores critical questions about whether such involuntary support makes these companies complicit in potential violations of IHL and whether it imposes a duty to mitigate such risks.

<sup>1</sup> Diya Li, "On the Digital Front Lines: How Tech Companies Are Supporting Ukraine," U.S. Chamber of Commerce, March 29, 2022, <https://www.uschamber.com/technology/on-the-digital-front-lines-how-tech-companies-are-supporting-ukraine>.

<sup>2</sup> Dearbail Jordan, "Ukraine War: Elon Musk's Starlink System Helps Ukrainian Army Strike Russian Targets," BBC News, September 8, 2023, <https://www.bbc.com/news/world-europe-66752264>.

<sup>3</sup> Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War," Microsoft, June 22, 2022, <https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/>.

<sup>4</sup> Vera Bergengruen, "AI in Ukraine War: How Palantir's Technology Helps in the Fight Against Russia," Time, February 8, 2024, <https://time.com/6691662/ai-ukraine-war-palantir/>.

<sup>5</sup> Jonathan Horowitz, "When Might Digital Tech Companies Become Targetable in War?" Tech Policy Press, October 13, 2023, <https://www.techpolicy.press/when-might-digital-tech-companies-become-targetable-in-war/>.

The lack of clear guidance on the ethical and legal responsibilities of global technology providers in conflict zones reveals a critical gap that demands urgent attention. This study seeks to bring this issue to the forefront of discourse, urging tech firms to recognize and address the abuse of their technologies. By highlighting the dual-use nature of these technologies, the study underscores the urgent need for a robust response to prevent their further exploitation in the prosecution of an illegal war.

## 2. METHODOLOGY

The research methodology employed in this study consisted of the following key steps:

### 1. Application Download and Dynamic Analysis

The first step involved searching, cataloguing, and downloading a set of military mobile applications and reviewing their features in an isolated, controlled environment. This dynamic analysis sought to confirm the military purpose of each app by observing functionality and data. This approach ensured that only apps with a confirmed military purpose were included in subsequent analyses.

### 2. Static Analysis for Network Data Extraction

Once the military purpose was confirmed, static analysis was performed on the applications. This involved decompiling the APK files to examine their code, configurations, and embedded resources. The goal was to extract networking data, including domain names, IP addresses, API endpoints, and other identifiers pointing to external resources and services. These data points revealed the infrastructure supporting the operational functionality of the apps.

### 3. Network Data Analysis

In the next stage, the extracted networking data was analyzed to identify the ownership and geographical distribution of the supporting resources. This included determining the cloud service providers, hosting platforms, and applications supplying the apps with essential data and services.

This approach provided an understanding of the technological dependencies of the apps, focusing on their military relevance and operational context. While minor inaccuracies may arise from obsolete or unused resources embedded in the apps, these are negligible and do not affect the validity of conclusions drawn from the significant volume of findings.

### 3. SAMPLE SELECTION

To examine the exploitation of Western technology in Russian military operations, a collection of 243 mobile applications was analyzed. These apps were identified as being used by Russian military forces on the battlefield. In the initial phase, civil, dual-use, and repurposed Ukrainian applications were excluded to narrow the focus to strictly military tools. This exclusion resulted in a final sample of 62 applications classified as strictly military. See Table I for the list of selected military apps.

The selected sample of strictly military mobile applications was categorized based on their primary functions. The largest categories, “Artillery Management” and “AUV Management,” included, respectively, 25 and 14 apps designed to assist with reconnaissance, targeting, and fire control. “Ballistic Calculators” and “Explosives Calculators” accounted for two apps each, providing precise computational tools for projectile trajectories and explosives parameters. “Field Logistics & Support” included four apps dedicated to managing supplies and operational logistics. “Mapping & Navigation” featured six apps, emphasizing geospatial awareness and navigation in tactical scenarios. Additionally, the sample contained tools for “Medical & Training,” “Meteorological Tools,” and “Tactical Communication,” showcasing a diverse array of functions critical to battlefield operations. See Table II for the list of identified military app categories.

**TABLE I:** RUSSIAN MILITARY APPS UNDER ANALYSIS

Category	App Name	Description
Artillery Management	120-note	Artillery app for managing 120mm systems.
Artillery Management	122-note	Artillery app for managing 122mm systems.
Artillery Management	152-note	Artillery app for managing 152mm systems.
Artillery Management	2A80-note	Artillery app for managing 2A80 systems.
Artillery Management	2B11-note	Artillery app for managing 2B11 mortar.
Artillery Management	2B16-note	Artillery app for managing 2B16 Nona-K.
Artillery Management	2C4-notepad	Artillery app for managing 2C4 system.
Artillery Management	2S7 note	Artillery app for managing 2S7 Pion system.
Artillery Management	30-82-100	Artillery app for managing 30-82-100 mortar.
Artillery Management	Art-note	Versatile artillery fire control tool.

Artillery Management	BM21-note	Artillery app for managing BM-21 Grad.
Artillery Management	PUO-10E	A tool for artillery fire management.
Artillery Management	HM16 note	A tactical app for managing mortar artillery tasks.
Artillery Management	Hyacinth	Artillery app for Hyacinth system.
Artillery Management	M-46 note	Artillery app for M-46 field gun operations.
Artillery Management	Msta-note	Artillery app for Msta howitzer operations.
Artillery Management	Nona-note	Artillery app for 2C9 Nona operations.
Artillery Management	Spotter	Defining positions, calculating trajectories, and adjusting magnetic declination for accurate targeting.
Artillery Management	ZeVs—PZK	Assists in maintaining artillery performance by monitoring and calculating barrel wear over time.
Artillery Management	ZeVs—Artillery Grid	Supports artillery operations by enabling precise targeting and adaptability to environmental conditions.
Artillery Management	ArtGruppa	Part of the "Veterok-ArtGruppa" tactical software suite for reconnaissance and artillery units.
Artillery Management	ArtSkill	Fire adjustment training and test app.
Artillery Management	Armor	Tactical fire control application designed to assist in indirect fire operations.
Artillery Management	Armor-notepad	Tactical application for managing artillery operations and reconnaissance.
Artillery Management	D1-note	Artillery app for D-1 howitzer operations.
Ballistic Calculator	Strelok Pro	Advanced ballistic calculator.
Ballistic Calculator	Strelok+	Ballistic calculator.
Explosives Calculator	Calculator PR	Calculates explosive charges for various objects and materials.
Explosives Calculator	Engineer's Directory	Explosives, grenades, and detonators calculator.
Field Logistics & Support	Leon	Tactical-technical characteristics of rifles, grenades, and special armaments.
Field Logistics & Support	ZMops SOFT	Military software inventory.
Field Logistics & Support	Control BK—Molot	Tracks ammunition inventory and usage for artillery systems.

Field Logistics & Support	Skrezhet	Reduces operator radio visibility, maximizes channel range, and ensures mobility and year-round weather resistance.
Mapping & Navigation	Dots	Software for encoding electronic maps (objects, routes, areas).
Mapping & Navigation	Z Map Viewer	Offline navigation app.
Mapping & Navigation	ZMops Maps	Navigation maps with integrations to various battle apps.
Mapping & Navigation	ZOV Maps	Mapping application designed for operational use.
Mapping & Navigation	ZOV Maps Demo	ZOV Maps Demo is a demonstration version of the ZOV Maps application.
Mapping & Navigation	Topogeodeziya SK-42	Field topography calculations using full or reduced coordinates within one zone or adjacent zones.
Medical & Training	VMedA Tactical Medicine	Guidance on first aid, managing injuries, and critical medical skills.
Meteorological Tools	Meteo	Meteorological data analysis for artillery, UAVs, and tactical planning.
Meteorological Tools	ZeVs—METEO	Provides meteorological data critical for artillery operations.
Meteorological Tools	ZeVs—METEO ALPHA	Provides meteorological data critical for artillery operations.
Tactical Communication	ZOV Chat	Communication app designed for devices running licensed versions of "ZOV Maps," providing connectivity and chat functionality.
Tactical Communication	Groza	Tactical communication platform that integrates with drones, radios, and meteorological systems for data exchange, coordination, and fire adjustment.
Tactical Communication	Calculator STC	Quick calculations in radiocommunications, including visibility, signal attenuation, antenna gain, and coordinate conversions.
Tactical Communication	Loktar	Provides secure, low-visibility tactical communication, data transfer, mapping, and drone detection capabilities.
Tactical Communication	Malina	A Raspberry Pi-based system for integrating radios with networks, enabling secure tactical communication and device coordination.
UAV Management	Drone Detector	Identifies and tracks drones using frequency analysis.
UAV Management	DroneAlert	Monitors and alerts on detected radio signals, including those from drones.
UAV Management	Eye Lite	Tactical drone software system designed for reconnaissance, target identification, telemetry integration, and artillery fire adjustment.

UAV Management	FlyStat	UAV flight statistics.
UAV Management	Karlson3	Assists in drone operations, focusing on artillery fire correction, and providing tools like distance grids, offline maps, and directional calculations.
UAV Management	UavData	Organizes operational documentation and intelligence reporting during UAV missions.
UAV Management	ZeVs—BPLA	Supports drone operators in precise targeting and reconnaissance tasks.
UAV Management	Veterok	Part of the “Veterok-ArtGruppa” tactical software suite for reconnaissance and artillery units.
UAV Management	Veterok-T	Part of the “Veterok-ArtGruppa” tactical software suite for reconnaissance and artillery units.
UAV Management	Glaz 3	Tactical drone software system.
UAV Management	Glaz 4T	Tactical drone software system.
UAV Management	Glaz 2	Tactical drone software system.
UAV Management	Flight Log Avacha—Operator	Flight log app.
UAV Management	Trepet ID	Drone software designed for target identification, artillery fire adjustment, and ammunition drop assistance.

**TABLE II: NETWORKED MILITARY APP CATEGORIES**

Category	Number of Apps
Artillery Management	25
UAV Management	14
Mapping and Navigation	6
Tactical Communication	5
Field Logistics & Support	4
Meteorological Tools	3
Ballistic Calculator	2
Explosives Calculator	2
Medical & Training	1

The diverse array of app functionalities reflects a systematic effort to digitize and streamline military operations. It also underscores the strategic importance of technology in enabling effective battlefield management, situational awareness, and resource optimization, all critical components of contemporary military strategy.

## 4. EXAMPLES OF MILITARY APPS

To provide deeper insights into the functionality and technological dependencies of Russian military mobile applications, this section highlights notable examples from different categories identified during the study. These examples illustrate the diverse roles these apps play on the battlefield, from artillery management to reconnaissance and meteorological support.

Each app selected represents a critical component of military operations. We have highlighted each app's primary purpose, networked functionality, and reliance on external infrastructure. By analyzing these apps, we can better understand how they leverage global technological resources and what the implications of their usage are in the context of modern warfare.

The examples presented here serve to emphasize the operational sophistication and interconnectedness of these tools, shedding light on the broader ecosystem enabling their use in conflict scenarios.

### *ZeVs—METEO ALPHA*

App name: ZeVs—METEO ALPHA

Package name: zevs.team.arta

Analyzed version: 2.1 (ZeVs—METEO 2.10 ALPHA.apk,

MD5: ab1ef838e792d4aeb4c6cd1551c39dab)

Category: Meteorological Tools

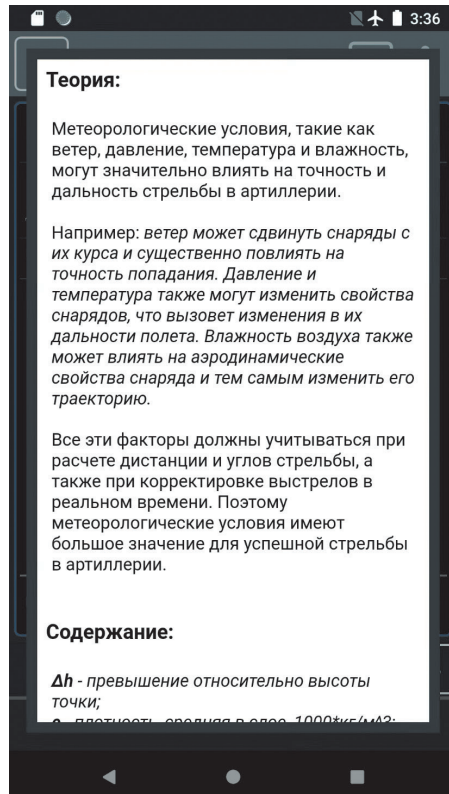
### **Description**

ZeVs—METEO provides essential meteorological data to enhance artillery precision. It calculates deviations caused by atmospheric factors such as wind, air pressure, temperature, and humidity. The app generates detailed meteorological bulletins and facilitates real-time adjustments to firing angles and ranges based on environmental conditions. Additionally, ZeVs—METEO integrates seamlessly with other apps by the same developer group, as well as a broader ecosystem of military apps, enabling a cohesive operational environment for Russian forces.

## Screen Translation

The functionality of ZeVs—METEO, as described in the mobile app’s help section, is presented on Figure 1, translation follows.

FIGURE 1: HELP SCREEN OF ZeVs—METEO ALPHA ALONG WITH TRANSLATION



### Theory:

“Meteorological conditions, such as wind, pressure, temperature, and humidity, can significantly impact the accuracy and range of artillery fire.

“For example, wind can shift projectiles off course, greatly affecting targeting accuracy. Pressure and temperature can also alter projectile properties, resulting in changes to their flight range. Additionally, air humidity can affect the aerodynamic properties of the projectile, thereby altering its trajectory.

“All these factors must be taken into account when calculating shooting distances and angles, as well as when adjusting fire in real time. Therefore, meteorological conditions play a critical role in the success of artillery operations.”

### **Domains Used**

The app communicates with a range of hosts, including mapping, topography, and cloud service providers:

- android.com (1 occurrence)
- autonavi.com (4 occurrences)
- chartbundle.com (1 occurrence)
- cloudmade.com (4 occurrences)
- google.cn (4 occurrences)
- google.com (6 occurrences)
- nationalmap.gov (1 occurrence)
- openptmap.org (1 occurrence)
- openseamap.org (1 occurrence)
- openstreetmap.nl (1 occurrence)
- openstreetmap.org (3 occurrences)
- opentopomap.org (3 occurrences)
- t.me (1 occurrence)
- tianditu.com (6 occurrences)
- wikimedia.org (1 occurrence)
- wmflabs.org (1 occurrence)
- zevstech.ru (1 occurrence)

### **Geographic Distribution**

The app’s hosts are distributed across several countries, reflecting a reliance on international infrastructure:

- United States (US): 18 occurrences
- China (CN): 8 occurrences
- Germany (DE): 5 occurrences
- Netherlands (NL): 1 occurrence
- Russia (RU): 1 occurrence
- Antigua and Barbuda (AG): 1 occurrence

### **IP Ownership**

The app relies on infrastructure from multiple global technology providers:

- Google: 9 occurrences
- Huawei: 10 occurrences
- Alibaba: 5 occurrences
- Amazon: 4 occurrences
- Deutsches Forschungsnetz: 4 occurrences
- Fastly: 3 occurrences
- Telegram: 1 occurrence
- TimeWeb: 1 occurrence

### **Analysis**

The ZeVs—METEO ALPHA app not only demonstrates the reliance on a globally distributed network of services but also highlights its integration with other tools within the broader military app ecosystem. This interconnectedness amplifies the app’s operational utility, allowing real-time data sharing and streamlined workflows in military contexts.

### **Symbolism in Naming**

The letters Z and V, initially tactical markings on Russian military vehicles, have evolved into pro-war propaganda symbols. Z likely stands for “Zapad” (West) or “Za pobedu” (For Victory), while V may signify “Vostok” (East) or “Victory.” Widely adopted in Russian propaganda,<sup>6</sup> these symbols represent support for the invasion of Ukraine and are used to foster nationalism. Their inclusion in military apps like ZeVs—METEO ALPHA ties the tools to Russia’s military identity and ideological objectives.

### *Karlson3*

App name: Karlson3

Package name: ru.karlson

Version analyzed: 0.2.1 (Karlson3—0.2.1.apk,

MD5: 26e948f80909fdbdc0bee574efd3c7a4)

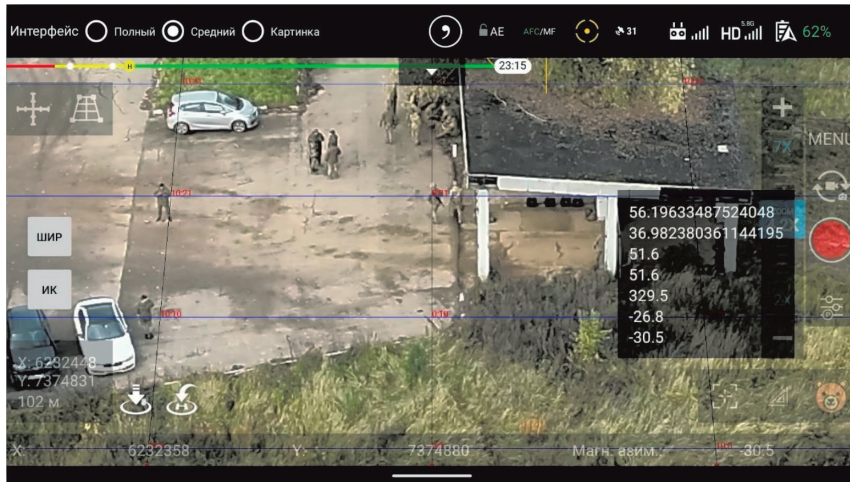
Category: UAV Management

### **Description**

The Karlson (in Russian, Карлсон) app facilitates drone operations with a focus on artillery fire correction. It provides tools such as distance grids, offline maps, and directional calculations to support precision targeting. The app is compatible with various drone models from the Chinese tech company DJI, enhancing accuracy and operational efficiency in combat scenarios. The user interface of the Karlson mobile app is presented on Figure 2.

<sup>6</sup> Orysia Hrudka, “Why Have Z and V Become Russia’s Pro-war Symbols?” Euromaidan Press, March 24, 2022. <https://euromaidanpress.com/2022/03/24/why-do-z-and-v-become-russians-pro-war-symbols/>.

FIGURE 2: KARLSON3 USER INTERFACE



### Domains Used

The app communicates with a wide range of domains, spanning drone management, mapping, cloud services, and general infrastructure:

- a9.com (1 occurrence)
- amap.com (11 occurrences)
- amazon.com (1 occurrence)
- amazonaws-china.com (1 occurrence)
- amazonaws.com (1 occurrence)
- apache.org (1 occurrence)
- autonavi.com (1 occurrence)
- biying.com (1 occurrence)
- chartbundle.com (1 occurrence)
- cloudmade.com (4 occurrences)
- creativecommons.org (1 occurrence)
- dji-flighthub.com (1 occurrence)
- dji.com (4 occurrences)
- dji.net (1 occurrence)
- djistatic.com (1 occurrence)
- georss.org (1 occurrence)
- github.com (1 occurrence)
- githubusercontent.com (1 occurrence)
- godaddy.com (3 occurrences)

- google.com (3 occurrences)
- gov.cn (1 occurrence)
- ionicons.com (1 occurrence)
- mapbox.com (4 occurrences)
- maptiler.com (1 occurrence)
- nationalmap.gov (1 occurrence)
- openptmap.org (1 occurrence)
- openseamap.org (1 occurrence)
- openstreetmap.org (1 occurrence)
- opentopomap.org (3 occurrences)
- thunderforest.com (3 occurrences)
- virtualearth.net (1 occurrence)
- wikimedia.org (1 occurrence)
- wmflabs.org (1 occurrence)
- xmlpull.org (1 occurrence)
- zetetic.net (1 occurrence)

### **Geographic Distribution**

The app's infrastructure spans multiple countries, reflecting its reliance on global technology resources:

- United States (US): 44 occurrences
- China (CN): 19 occurrences
- Germany (DE): 9 occurrences
- Netherlands (NL): 1 occurrence
- United Kingdom (GB): 1 occurrence

### **IP Ownership**

The app leverages services from major technology providers and networks:

- Alibaba: 12 occurrences
- Amazon: 11 occurrences
- Cloudflare: 7 occurrences
- Hetzner: 6 occurrences
- Deutsches Forschungsnetz: 6 occurrences
- Microsoft Corporation: 3 occurrences
- GitHub: 1 occurrence
- Google: 2 occurrences

## **Analysis**

Karlson3 underscores the integration of drone-specific functionalities with tools for precision artillery targeting. Its reliance on a mix of Western and Chinese infrastructure highlights the global interconnectedness of the military-app ecosystem. Key dependencies include DJI's ecosystem for drone operations and mapping platforms like Mapbox and CloudMade for geospatial intelligence. The app's use of multiple mapping and cloud services mirrors its focus on operational accuracy and redundancy.

## **Symbolism in Naming**

The name Karlson in the app Karlson3 references the character Karlsson-on-the-Roof (in Russian, Карлсон, который живет на крыше), a children's book character created by Swedish author Astrid Lindgren. Karlsson is a mischievous man with a propeller on his back, allowing him to fly—arguably a symbolic nod to the app's focus on drone operations.

## *Veterok*

App name: Veterok

Package name: ru.niissu.veterok

Version analyzed: 1.16.2 (Ветерок—1.16.2.apk,

MD5: 369939097892f0d57f8e9ae24ba398a0)

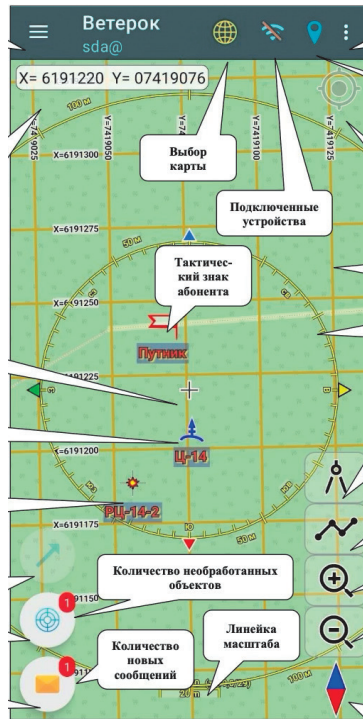
Category: Artillery Management

## **Description**

Veterok is part of the Veterok-ArtGruppa (in Russian, Ветерок-АртГруппа,) complex, a tactical software suite designed for reconnaissance and artillery units. The app supports object detection, data transmission, artillery fire adjustment, and geographical calculations. Its focus on reconnaissance-strike automation<sup>7</sup> makes it a critical tool in integrating intelligence and artillery fire operations. The tactical screen of the Veterok-ArtGruppa mobile app is presented on Figure 3.

<sup>7</sup> The term “reconnaissance-strike complex” refers to an integrated military system that combines real-time intelligence gathering with precision-strike capabilities to engage high-value targets efficiently. This concept, developed by the Soviet Union and later revived by Russia, utilizes advanced surveillance, automated command and control, and long-range precision weapons to detect and destroy targets swiftly.

FIGURE 3: VETEROK MAIN SCREEN AS ILLUSTRATED IN A USER MANUAL



### Domains Used

The app connects to various domains for mapping, data integration, and cloud services:

- 2gis.com (1 occurrence)
- arcgisonline.com (1 occurrence)
- chartbundle.com (1 occurrence)
- cloudmade.com (4 occurrences)
- google.com (2 occurrences)
- hereapi.com (1 occurrence)
- nakarte.me (1 occurrence)
- nationalmap.gov (1 occurrence)
- opengis.net (1 occurrence)
- openptmap.org (1 occurrence)
- openseamap.org (1 occurrence)
- openstreetmap.nl (1 occurrence)
- openstreetmap.org (4 occurrences)

- opentopomap.org (4 occurrences)
- telegram.me (1 occurrence)
- 12andex12ia.org (1 occurrence)
- wmflabs.org (1 occurrence)
- xmlpull.org (1 occurrence)
- 12andex.net (3 occurrences)

### **Geographic Distribution**

The infrastructure supporting the app spans multiple countries, emphasizing global dependencies:

- United States (US): 18 occurrences
- Germany (DE): 7 occurrences
- Russia (RU): 3 occurrences
- Netherlands (NL): 1 occurrence
- Antigua and Barbuda (AG): 1 occurrence

### **IP Ownership**

The app relies on a range of technology providers for its functionality:

- Amazon: 6 occurrences
- Cloudflare: 1 occurrence
- Google: 2 occurrences
- Deutsches Forschungsnetz: 4 occurrences
- Fastly: 4 occurrences
- Hetzner: 1 occurrence
- NetCup: 2 occurrences
- Telegram: 1 occurrence
- Wikimedia: 1 occurrence
- Yandex: 3 occurrences

### **Analysis**

Veterok exemplifies the integration of reconnaissance and artillery-fire automation through its comprehensive tactical features. The app's reliance on mapping and geospatial services (e.g., OpenStreetMap, ArcGIS, HERE) underscores its focus on precision and situational awareness. With a mix of global and Russian infrastructure, Veterok demonstrates the dual dependency on Western technology and localized Russian resources, reflecting the complexity of modern military software ecosystems. Its integration with communication platforms like Telegram further enhances its utility in real-time battlefield scenarios.

### **Symbolism in Naming**

The names Veterok (“light breeze”) and ArtGruppa (“artillery group”) reflect their military roles. Veterok symbolizes agility and real-time reconnaissance, aligning with its use in dynamic operations, while ArtGruppa directly references artillery coordination, emphasizing its tactical purpose in team-based fire adjustments. Both names are practical and resonate with their operational contexts.

## **5. ANALYSIS RESULTS**

The analysis of the selected military mobile applications revealed extensive use of online services to support their operational functions. Across the functionality, configuration, and resources of these apps, a total of 1,594 network addresses (DNS hostnames and IP addresses) were identified. To ensure accurate representation and avoid duplication, each service and IP address was accounted for only once. This resulted in a refined dataset of 323 distinct hostnames and 387 corresponding distinct IP addresses that was subjected to further analysis.

Each of these distinct data elements was examined to determine its geographical location and network ownership. The GeoIP analysis provided insights into the global distribution of resources utilized by the apps, while the ownership information revealed the entities responsible for hosting these services. The findings highlight a significant reliance on infrastructure provided by international cloud service providers, VPS platforms, and cybersecurity services.

The detailed breakdown of these results, including ownership distribution and geographical spread, is provided in the following sections.

### *Identified Domains*

The examination of 323 hostnames embedded in the source code of Russian military apps revealed a distribution across 204 distinct level-2 domains. Below is a detailed analysis of the top 20 domains:

#### **1. cloudmade.com (132 occurrences)**

CloudMade.com was a mapping and navigation platform that leveraged OpenStreetMap data and later transitioned to AI-driven services for the automotive industry.

#### **2. openstreetmap.org (110 occurrences)**

OpenStreetMap.org is a collaborative, open-source mapping platform providing free, editable geospatial data used for various applications worldwide.

### **3. opentopomap.org (105 occurrences)**

OpenTopoMap.org is an open-source mapping platform offering topographic maps generated from OpenStreetMap data, tailored for outdoor and geographical use.

### **4. mapbox.com (103 occurrences)**

Mapbox.com is a platform providing customizable mapping and geospatial tools, including APIs and SDKs, for developers to integrate location-based features into applications.

### **5. google.com (79 occurrences)**

Google's popularity here reflects a reliance on its ecosystem for APIs, backend data handling, and other infrastructure services.

### **6. wmflabs.org (72 occurrences)**

Wmflabs.org is a hosting platform for Wikimedia Foundation projects, supporting development, testing, and tools related to Wikimedia's open knowledge initiatives.

### **7. amap.com (36 occurrences)**

Amap.com is a Chinese mapping and navigation service, also known as AutoNavi, providing real-time traffic, location-based services, and geospatial data.

### **8. openptmap.org (34 occurrences)**

OpenPtMap.org visualizes public transport networks using OpenStreetMap data, offering a clear overview of transit routes and infrastructure.

### **9. nationalmap.gov (34 occurrences)**

NationalMap.gov is a US government platform providing geospatial data, including topographic maps and environmental datasets, for public and professional use.

### **10. chartbundle.com (34 occurrences)**

Chartbundle.com was a hobbyist website offering digital aviation charts for flight planning (now discontinued), with its source code available on GitHub.

### **11. openstreetmap.nl (33 occurrences)**

OpenStreetMap.nl is the Dutch OpenStreetMap community hub, providing resources and tools for collaborative map editing in the Netherlands.

### **12. openseamap.org (33 occurrences)**

OpenSeaMap is a free, worldwide nautical chart project that enhances OpenStreetMap with maritime information, including sea marks, harbors, and water depths, to support navigation and marine activities.

**13. github.com (32 occurrences)**

GitHub.com is a platform for version control and collaborative software development, enabling users to host, share, and manage code repositories.

**14. android.com (30 occurrences)**

Android.com is the official website for Google's Android operating system, offering resources for users, developers, and device manufacturers.

**15. thunderforest.com (27 occurrences)**

Thunderforest.com provides customizable map styles and APIs for outdoor activities, built on OpenStreetMap data, catering to developers and enthusiasts.

**16. xmlpull.org (25 occurrences)**

Xmlpull.org is a resource for the XML Pull Parser API, offering lightweight, efficient tools for XML parsing in Java-based applications.

**17. tilestream.net (19 occurrences)**

Tilestream.net is a platform for hosting and serving custom map tiles, enabling developers to create and manage personalized map visualizations.

**18. firebaseio.com (19 occurrences)**

Firebaseio.com is a domain used by Google Firebase to provide backend services like real-time databases, authentication, and cloud functions for applications.

**19. googlesyndication.com (16 occurrences)**

Googlesyndication.com is a domain used by Google for delivering ads, dynamic content, and resources through its advertising and content platforms.

**20. wikimedia.org (15 occurrences)**

Wikimedia.org is the official domain of the Wikimedia Foundation, hosting projects like Wikipedia and providing free, open-access knowledge and resources.

The data reveals a heavy reliance of Russian military apps on open-source, commercial, and global cloud platforms for critical functionalities like mapping, navigation, and backend operations. Open-source tools such as [openstreetmap.org](https://openstreetmap.org) and commercial platforms like [mapbox.com](https://mapbox.com) provide customizable geospatial data, while global cloud providers, such as Google ([google.com](https://google.com), [firebaseio.com](https://firebaseio.com)), enable real-time data handling and app distribution. Public resources like [nationalmap.gov](https://nationalmap.gov) and niche platforms like [openseamap.org](https://openseamap.org) demonstrate how freely available data and specialized tools are repurposed for military objectives.

This domain-level analysis illustrates how military apps leverage a mix of global, open-source, and commercial resources to achieve military operational efficiency. The widespread use of publicly available platforms raises critical questions about their unintended use in conflict scenarios, further emphasizing the ethical and legal complexities of technology in modern warfare. See the list of identified domain names in Table III.

**TABLE III: TOP 20 DOMAIN NAME OCCURRENCES IN MILITARY APPS**

Domain name	Number of occurrences
cloudmade.com	132
openstreetmap.org	110
opentopomap.org	105
mapbox.com	103
google.com	79
wmflabs.org	72
amap.com	36
openptmap.org	34
nationalmap.gov	34
chartbundle.com	34
openstreetmap.nl	33
openseamap.org	33
github.com	32
android.com	30
thunderforest.com	27
xmlpull.org	25
tilestream.net	19
firebaseio.com	19
googlesyndication.com	16
wikimedia.org	15

### *Geographic Distribution*

The geographical distribution of the 387 distinct IP addresses supporting the networked military apps underscores a heavy reliance on infrastructure located in the United States, with 283 IPs (73%) linked to US-based services. This dominance reflects the widespread use of global cloud service providers headquartered in the US.

Other significant contributors include China (30 IPs, 8%) and Germany (24 IPs, 6%), suggesting secondary hubs for hosting and infrastructure. Notably, Russia (17 IPs, 5%) ranks fourth, representing locally managed or proximate services supporting the military apps.

European nations such as France (6 IPs), Switzerland (4 IPs), the Netherlands (3 IPs), Finland (3 IPs), Ireland (2 IPs), the United Kingdom (2 IPs), Bulgaria (1 IP), Romania (1 IP), and Italy (1 IP) collectively account for 12% of the distribution. This reflects the involvement of various hosting and infrastructure providers across Europe.

A smaller number of IPs were distributed across other regions, including Singapore (3 IPs), New Zealand (1 IP), Japan (1 IP), Australia (1 IP), and Antigua and Barbuda (2 IPs). The presence of Ukraine (1 IP) is notable but minimal.

This distribution highlights the global reach and dependence of these military apps on foreign infrastructure, with US and European services playing a particularly critical role. The geographical distribution of identified IP addresses is presented in Table IV and on Figure 4.

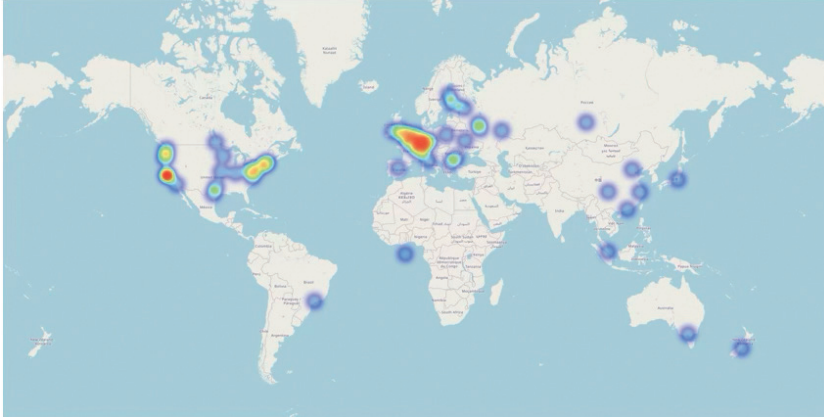
**TABLE IV: IDENTIFIED IP ADDRESSES' AUTONOMOUS SYSTEMS COUNTRY CODES**

ASN Country Code	Number of hosts
US	283
CN	30
DE	24
RU	17
FR	6
CH	4
SG	3
NL	3
FI	3
IE	2
GB	2
AG	2
UA	1
RO	1
NZ	1
JP	1
IT	1
BG	1
AU	1

### *IP Address Ownership*

The analysis of the 387 distinct IP addresses revealed a clear pattern of ownership concentrated among major technology and infrastructure providers. This distribution highlights the heavy reliance of Russian military mobile applications on well-established international platforms.

**FIGURE 4: HEAT MAP OF IP ADDRESSES' GEOGRAPHIC DISTRIBUTION**



### 1. Dominant Cloud Service Providers

- Amazon Web Services (127 IPs, 33%): AWS accounts for over a third of the IPs analyzed, reflecting its dominant position in global cloud hosting and backend support services.
- Google Cloud Platform (53 IPs, 14%): GCP is the second-largest provider, underscoring its widespread use for storage, APIs, and data processing.
- Microsoft (5 IPs) and DigitalOcean (4 IPs) also play notable roles, albeit on a smaller scale.

### 2. Content Delivery and Network Security

- Cloudflare (30 IPs, 8%): Cloudflare is known for its Distributed Denial of Service (DDoS) protection and Content Delivery Network (CDN) services. Its infrastructure is a critical enabler of secure communication for respective apps.
- Fastly (14 IPs) and Akamai (4 IPs) contribute additional content delivery capabilities.
- Sucuri (4 IPs) provides security and monitoring solutions.

### 3. Chinese Technology Giants

- Alibaba Cloud (26 IPs, 6%) and Huawei (10 IPs, 3%) reflect the significant involvement of Chinese infrastructure providers, with Alibaba serving both hosting and database needs.

#### 4. European Hosting Providers

- Hetzner (18 IPs, 5%) and OVH (3 IPs) represent key European hosting platforms, often favored for their affordability and reliability.

#### 5. Russian-Owned Services

- Yandex (8 IPs) and SprintHost (3 IPs) are Russian-owned, reflecting local services utilized in some cases to ensure proximity and compliance with Russian regulations.

The reliance on US-based platforms such as Amazon, Google, and Cloudflare underscores the paradox of Western infrastructure supporting adversarial military apps. Chinese providers like Alibaba and Huawei play a smaller but significant role, highlighting a secondary dependency on non-Western platforms. European providers such as Hetzner and OVH are also part of the ecosystem, further diversifying the technological dependencies of these apps.

#### *Developer Organization and Structure*

Russian military app development is largely driven by civilian developers, not official military programmers. While a few applications have reached the final stages of official adoption, requiring companies to restructure as joint stock companies with state ownership, most remain relatively independent grassroots projects.

Developers come from various backgrounds, including:

- Volunteers ideologically motivated to contribute to military tech.
- Private sector employees developing tools as part of a company's bid to secure government contracts.
- Academic or scientific institutions providing research and development capacity.
- Crowdfunded or unofficially compensated groups of individuals.

Most developers label their projects as “инициативные разработки” (initiative-based development) or “перспективные разработки” (promising developments), indicating that these apps are not yet officially adopted but are intended for eventual military integration.

Nonetheless, these military apps are already widely used in operations. The most successful ones have thousands to tens of thousands of active users, depending on their complexity and purpose. Their development teams and sponsoring organizations

conduct regular training sessions for military personnel, including in active operational zones, and oversee testing exercises at military facilities. Some apps have even been formally documented in official military textbooks, detailing their functionality and usage in combat scenarios, and integrated into military institutes' coursework.

The military mobile apps ecosystem represents a hybrid private-public partnership, where software development is loosely coordinated but strictly aligns with official military requirements.

### *Rationale Behind Cloud Selection*

It is reasonable to conclude that Russian military apps use Western cloud services and APIs not out of deliberate preference, but because they are more accessible, cost-effective, and reliable than domestic alternatives—if such alternatives even exist. These choices are shaped by infrastructure convenience, data availability, and the advantages of mature developer ecosystems, rather than strategic selection. Notably, four leading Russian cloud providers—Rostelecom, Cloud.ru, Selectel, and MTS—are conspicuously absent from this ecosystem. A fifth, Yandex Cloud,<sup>8</sup> is minimally represented, hosting only eight IP addresses identified in this study.

As this study demonstrates, cloud service providers play a critical role in military app development by hosting or securing essential services, such as meteorological forecasts and geospatial intelligence. This explains why Western clouds predominate at the infrastructure (e.g., IP address) level in the observed results.

Russia lacks high-quality meteorological and geospatial data, making Western sources indispensable.<sup>9</sup> Accurate weather forecasting requires supercomputing resources, which Russia struggles to maintain.<sup>10</sup> And while Russia has domestic mapping services, they do not provide the high-precision datasets needed for targeting and artillery support.<sup>11</sup> Particularly, Russia's reliance on OpenStreetMap and commercial geospatial APIs suggests that domestic mapping lacks the necessary resolution and detail.

Google Cloud and Firebase are widely used because they are practically free via the Free Tier GCP offering and the no-cost Firebase Spark plan, require no official developer accounts, have extensive documentation, and are broadly popularized by online training programs and video tutorials.

<sup>8</sup> “Бизнес сгущает облака”, Коммерсант, August 8, 2024, <https://www.kommersant.ru/doc/6879530>.

<sup>9</sup> Reade Levinson, “Russia Receives Western Weather Data That Some Fear Could Aid Attack Planning,” Reuters, March 22, 2022, <https://www.reuters.com/article/world/russia-receives-western-weather-data-that-some-fear-could-aid-attack-planning-idUSKCN2LJ0U5/>.

<sup>10</sup> “Суперкомпьютеры, в том числе задействованные в прогнозировании погоды в России могут продолжить работу в течении трех лет,” Метеожурнал, April 28, 2022, <https://meteojournal.ru/superkompyutery-v-tom-chisle-zadejstvovannyye-v-prognozirovani-pogody-v-rossii-mogut-prodolzhit-rabotu-v-techenii-treh-let/>.

<sup>11</sup> Michael Peck, “Why Russian Space Satellites Are Failing in the Ukraine War”, Popular Mechanics, March 29, 2023, <https://www.popularmechanics.com/military/a43444628/why-russian-satellites-are-failing-in-ukraine/>.

Unlike Apple’s App Store,<sup>12</sup> Google’s Play Market, with its less restrictive policies, enables easy sideloading and unofficial distribution channels,<sup>13</sup> making Android the preferred platform for Russian military apps.

### *Policy Prescriptions*

To mitigate the exploitation of Western technology, targeted restrictions must be implemented at multiple levels. The key concern here is the high-threat areas, where the development or use of military apps takes place. Establishing criteria or identifying high-threat areas falls beyond this study’s scope and involves international law and IHL considerations. For this study, we set the scope of high-threat areas to states that sponsor or conduct illegal wars of aggression and the territories they occupy or annex.

#### **Cloud Service Providers (AWS, Cloudflare, etc.)**

- Enhance verification processes for user origins to limit access from sanctioned and high-threat areas.
- Implement geofencing for high-threat areas using user IP addresses and more sophisticated geolocation technologies.
- Proactively identify military usage in high-threat areas in the way current measures against universally illegal activities, such as child exploitation content, are implemented.

#### **SDK and Developer Ecosystem Providers (Google)**

- Limit access to development tools (SDKs, APIs, supporting cloud services, distribution channels, etc.) for users from high-threat areas like Apple did for enterprise developers from Russia in February 2025.<sup>14</sup>
- Restrict access to sensitive APIs, including meteorological and geospatial services, exclusively to applications distributed through official app stores, thereby preventing the unauthorized sideloading of critical software.

#### **Critical Applications and Services (Meteorology, Cartography, etc.)**

- Extend abuse policies to include military applications developed and used in high-risk areas.
- Establish reporting mechanisms to identify and eliminate access to services that are used for military purposes in the high-threat areas.

<sup>12</sup> Apple, “Building a Trusted Ecosystem for Millions of Apps: A Threat Analysis of Sideloading”, October, 2021, [https://www.apple.com/privacy/docs/Building\\_a\\_Trusted\\_Ecosystem\\_for\\_Millions\\_of\\_Apps\\_A\\_Threat\\_Analysis\\_of\\_Sideloading.pdf](https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps_A_Threat_Analysis_of_Sideloading.pdf).

<sup>13</sup> “Alternative Distribution Options”, Google Android Developers, last updated April 16, 2020, <https://developer.android.com/distribute/marketing-tools/alternative-distribution>.

<sup>14</sup> “Apple закрыла россиянам доступ к платформе разработки бизнес-приложений,” РБК, February 24, 2025, [https://www.rbc.ru/technology\\_and\\_media/24/02/2025/67b9be389a79470a2de2be8a](https://www.rbc.ru/technology_and_media/24/02/2025/67b9be389a79470a2de2be8a).

## Regulatory Actions

- Establish legal accountability for cloud providers that offer services to unverified or malicious users in high-risk areas.
- Create official reporting channels for national CERT teams to flag military applications from high-risk areas for review and possible removal.
- Prohibit military software developers originating from high-risk areas from employment in Western companies or obtaining residency in Western countries.
- Launch national bug bounty programs to crowdsource intelligence on apps used in military aggression.

## 6. CONCLUSION

The study reveals the rise of a grassroots “people’s military-industrial complex” in Russia, leveraging open-source and Western technological resources to create military Android applications. These apps reflect strong cultural cohesion and operational innovation, becoming highly effective tools in wartime. Their success is facilitated by the openness of the Google Android ecosystem and the unrestricted access to global cloud services, which collectively enable their rapid development, scale, and distribution.

The exploitation of these platforms raises serious ethical and strategic concerns. Major cloud providers and open ecosystems inadvertently support this ecosystem by failing to implement controls that could restrict access by the states prosecuting illegal war or prevent the weaponization of their resources. This reliance on global infrastructure highlights a critical gap in accountability and governance in the technology sector during conflict.

To counter this exploitation, access restrictions and regulatory controls are crucial. Cloud service providers must implement regional access controls, monitor resource usage, and restrict applications exploited for unlawful military operations. Developer ecosystems must deny access to programming toolkits and critical services for software developers engaged in wars of aggression. Providers of essential services, such as geospatial intelligence and meteorological data, must ensure their platforms are used solely for legitimate purposes. Regulators should enforce compliance by incentivizing adherence to these measures while penalizing violators.

Limiting access to global infrastructure would compel Russian developers to depend on less capable and reliable domestic resources and attempt to circumvent network

access controls by additional means such as VPN, undermining their operational effectiveness. These measures are vital for curtailing the misuse of global technology in illegal warfare while preserving the ethical integrity of open and commercial platforms.