Weaponized DJI Firmware "1001" Analytic Report

Treadstone 71 · Cyber & Strategic Intelligence

Weaponized DJI Firmware "1001" — External Edition

Russian Hackers - Фронту and the РОКОТ-ЦЕНТР / РОКОТ-ГОРИЗОНТ Network: Specifications, Capabilities, Attribution, Training, and Geographic Footprint

Report date 29 July 2026

Analytic basis Adversary manuals (Mavic 3 / 3T-3E-M30 / Matrice 4), live primary Telegram + VK + Russian state-media pulls, secondary corroboration

Methods structured environmental scan, a proprietary threat-priority index, Analysis of Competing Hypotheses, Cultural Nexus (Hofstede), pre-attack kill-chain mapping, expanded Admiralty (STANAG 2511), ASA Evidence Standard tri-score

Anonymous volunteer coders ("Русские Хакеры - Фронту") wrote a modified DJI firmware, "1001," that strips manufacturer safety and identification controls off consumer and enterprise drones and turns them into hardened frontline reconnaissance and strike platforms. A named Vladimir-Oblast volunteer war-support organization, РОКОТ-ЦЕНТР / РОКОТ-ГОРИЗОНТ, integrates the firmware and distributes it free through a federal grid of 400-plus workshop "terminals" across Russia and occupied Ukraine. Operator training runs through the same centers. The network claims 500,000 drones flashed as of the report date and continues to widen model coverage. Two gains decide the fight for Russian forces: Remote-ID silence and immunity to GPS spoofing. RF jamming remains the residual counter, because the firmware does not alter DJI operating frequencies.

Bottom line. "1001" is a mature, industrial-scale drone-weaponization program, assessed **Almost certain (95-99)** to materially raise the battlefield survivability of Russian DJI drones on the line of contact. The two decisive gains, Remote-ID silence and spoofing immunity, rate **Highly likely (85 to <95)** to blunt Ukrainian and allied passive-RF detection and to sap electronic-warfare effects against Russian DJI fleets.

Attribution. The developer cell stays pseudonymous. Downstream, the distribution and integration layer stands doxxed by its own advertising: the РОКОТ-ЦЕНТР | 33 hub in Vladimir, with state-TV coverage, a visiting LDPR federal leader, and a United Russia regional footprint. A state or FSB sponsor (the "Positive Technologies" rumor) rates **Unlikely (15 to <45)** on present evidence, single-source and uncorroborated.

So what. The single most attackable point is the closed server-and-terminal supply layer, struck twice already (July 2025, February 2026). Counter-effort against Russian DJI fleets

should shift weight to RF jamming and non-Remote-ID detection, and against the network to its update-server, terminal, and VPN backend.

What this product answers (for a first-time reader). It establishes what "1001" is and what it does to a DJI drone, per model and per command; who builds and distributes it (a pseudonymous developer cell plus the state-adjacent РОКОТ-ЦЕНТР 33 in Vladimir, sole contact a single named coordination contact); how it spreads and at what claimed scale (free, through a federal network, 500,000 airframes self-reported); where the install network sits (the group's published roster and two maps at the regional level); how the two networks link through shared operators across front and rear; and how to prioritize counter-effort (threat-priority index ranking, the pre-chain kill chain, the vendor and detection-fallback picture, and collection tasking).

What it does not answer. It does not confirm that any listed node is active now: the roster is the adversary's own advertisement, so presence is a claim, not verification. Geolocation is town-centroid and analytic, not facility-level or aim-point grade, and medium and low-confidence nodes need resolution before any operational use. It carries no battle-damage assessment and no measure of any counter-effort's effect. Scale figures (500,000 flashed, the daily rate) are self-reported and unaudited. The developers' real-world identities stay unresolved; attribution runs to the distribution layer, not to named persons. The firmware binary was not reverse-engineered, so capability rests on the operator manuals, the group's own video and demonstrations, and secondary reporting, not a code audit. Vendor posture is drawn from open reporting, not DJI-internal data. This edition is sanitized for external distribution.

Bottom line for the reader. This answers what, who, where, and how big, well enough to prioritize. It does not answer which nodes are live right now, or what a strike would achieve. Those need confirmation collection on top of it.

Handling. TLP:GREEN. Sanitized for external distribution: this edition omits sources, collection methods, proprietary indices, the installer roster, geolocation, and named identities. Figures are the group's self-reported claims unless attributed otherwise.

Executive summary

What. "1001" is Russian-modified firmware for DJI Mavic 3 and Matrice 3 and 4 drones. It removes manufacturer safety and identification controls, defeats Remote ID and AeroScope tracking, grants immunity to GPS spoofing, forces high-power transmit, and changes lost-link behavior to autonomous return. It converts a commercial camera drone into a military reconnaissance and strike platform.

Who. A pseudonymous developer group writes the firmware. A state-adjacent volunteer war-support organization in Vladimir, Russia integrates and distributes it free, with regional-government and state-media ties.

How big. 500,000 airframes self-reported flashed as of late July 2026, growing on the order of 500 per day, distributed at no cost through a federal network of workshop points.

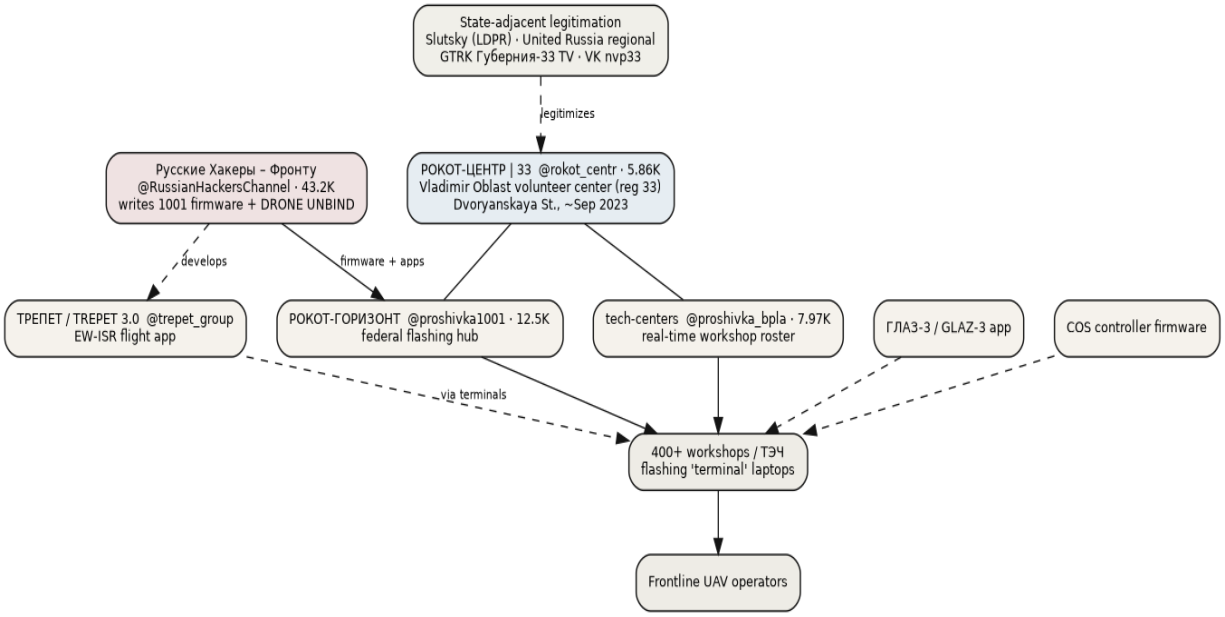
Where. Installer points span occupied Ukraine (Donetsk, Luhansk, Zaporizhzhia, Kherson, and Kharkiv axes) and mainland Russia, heaviest in the border oblasts of Kursk and Belgorod and the Moscow region, with points from Kaliningrad to Vladivostok.

So what. The program strips two of the defender's cheapest counter-drone tools, passive Remote-ID tracking and GPS spoofing, at industrial scale and for free, faster than attrition degrades the fleet. Highest-value counter-effort targets the closed supply and update pipeline and multi-sensor non-cooperative detection, not the individual drone.

Bottom line. This answers what, who, where, and how big, well enough to prioritize. It does not answer which nodes are live right now, or what a strike would achieve. Those need confirmation collection. Scale figures are self-reported.

2. WHO: Attribution

The program runs on two layers. A pseudonymous software team writes the exploit. Above the coders sits a named, regional, quasi-official volunteer organization that flashes airframes and runs the workshop "terminals" pushing the code to pilots.



2.1 The developer layer

"Русские Хакеры - Фронту" launched a Telegram channel in early July 2023 and shipped the first "1001" build for the DJI Mavic 3 within weeks. The persona set stays first-name and handle only. The published rosters name a single named coordination contact as the sole installation and support contact for the mainland and Novorossiya networks alike, a confirmed coordination node. No open source establishes a real name for the coders. The developer channel enforces a join-wall, so its posts reach analysts through verbatim forwards on the distribution channels.

2.2 The integration and distribution layer (doxxed)

РОКОТ-ЦЕНТР | 33 self-identifies as a Vladimir-Oblast volunteer center ("Владимирская Русь," region code 33), opened around September 2023 on Dvoryanskaya Street in Vladimir. Its own channel lists named contacts for firmware installs, 3D-printed parts, and regional volunteer points. The РОКОТ-ГОРИЗОНТ hub calls itself a "federal network of centers for preparing UAVs for the front." Regional state TV (GTRK Губерния-33) profiled the center in September 2023. LDPR federal leader Leonid Slutsky visited it in July 2023 (Izvestia). United Russia hosted it regionally (vladimir.er.ru). An official VK community operates at vk.com/nvp33 as a registered "public movement."

2.3 Origin sequence (hardware first, software second)

Regional state TV records the sequence that Western secondary reporting missed. Vladimir volunteer engineers first built an "аппаратный сдвиг" (hardware shift), a soldered board plus programming that made a DJI drone broadcast false coordinates. The hacker community then reproduced the same GPS deception in firmware, which became "1001." The manuals confirm the lineage: the GPS-off mode reads as a software analogue of the board installed in un-flashed drones. Spread reached "from Sakhalin to Kaliningrad" inside two months. The same Vladimir center also produces a 9-inch kamikaze drone, "Сокол-1 / Sokol-1," carrying a 1.9 kg warhead to about 12 km.

2.4 Network structure

The network presents through named volunteer personas and regional coordinators, with a single coordination contact for installation and support across both rosters. Individual identifiers are withheld from this edition.

2.5 Institutional ties and confidence

The credible institutional ties attach to the distribution and integration layer (РОКОТ-ЦЕНТР 33), not to the pseudonymous developer cell, and they run to ruling-party, parliamentary, and state-media structures rather than to a security company or an intelligence service. The strongest defensible reading is a state-adjacent volunteer center operating under quasi-official cover inside the wider state-backed volunteer drone-workshop ecosystem, not a proven state or intelligence program. Ties are graded on the expanded Admiralty scale (source reliability A to F and information credibility 1 to 6), scored separately and never averaged.

Institutional ties, graded. Reliability and credibility scored separately.

Tie	Nature of the link	Admiralty (R / C)	Assessment
РОКОТ-ЦЕНТР 33 / РОКОТ-ГОРИЗОНТ (Vladimir)	Integration and free-distribution hub; self-identified	B / 2	Anchor tie. Corroborated by state media and party coverage.

Tie	Nature of the link	Admiralty (R / C)	Assessment
State regional TV (GTRK Губерния-33)	Favorable profiling of the volunteer drone effort	A / 2	Documented; confers quasi-official cover.
LDPR (parliamentary party)	Federal-leader visit (Izvestia); that leader is sanctioned	B / 2	Political proximity, not control.
United Russia (ruling party)	Regional association (vladimir.er.ru)	B / 2	Party footprint around the hub.
Vladimir Oblast government; VK community	БПЛА-training publicity; registered "public movement"	B / 3	Regional-government and civil-registry footprint.
State-party volunteer drone-workshop ecosystem (ЦБСТ; United Russia and the "Наша Правда" fund; People's Front; Presidential defense-industrial administration; Navy command)	Surrounding "people's VPK" milieu; no confirmed direct link to 1001 or РОКОТ	B / 3 (as ecosystem)	Align as milieu, not as a wiring diagram.
Positive Technologies (security company, FSB-tied, US-sanctioned) as creator or backer	Claim originates on pro-Russian UAV channels; no primary corroboration; the firm denies it	E / 4	Unlikely (15 to <45). Do not align as fact. See note below.
Developer cell "Русские Хакеры – Фронту"	Pseudonymous; no organizational identity established	- / -	No institutional tie.

Positive Technologies claim (low confidence). The link between the 1001 developers and Positive Technologies is asserted only on the group's own side, circulated by pro-Russian UAV channels and repeated by a single open-source aggregator, with no primary corroboration; the firm denies any such role. Positive Technologies is itself a genuinely state-tied entity, sanctioned by the US Treasury in 2021 as a company that supports FSB clients and whose flagship event was described as an FSB and GRU recruiting venue. That weight is the reason to withhold the claim, not to accept it: aligning an unverified Positive Technologies attribution would convert a self-serving rumor into an intelligence-service attribution. Held at Admiralty E/4, Unlikely (15 to <45), pending primary evidence.

3. WHAT: Specifications, Functions, Capabilities

"1001" overwrites factory DJI firmware and blocks re-flashing back to a stock civilian build. Command entry runs through the drone-name / device-name field inside DJI Fly or DJI Pilot, or through alternate apps (TREPET, GLAZ-3). A visual tell on power-up: the satellite icon counts down 99-88-77-66-55-44-33-22-11, and the GPS-off mode shows a white zero.

3.1 Model coverage and version lineage

Supported airframes and firmware state. "777" is a native Chinese interim build, not a 1001 build.

Platform	Class	1001 state (Jul 2026)	Notes
Mavic 3 / 3 Classic / 3 Pro	Consumer	Mature (to v53)	Baseline family
Mavic 3T / 3E / 3 Multispectral	Enterprise	Mature (to v53)	Thermal recon workhorse
Mavic 3T Advanced (3TA)	Enterprise	Interim v36 only	Reduced command set
Matrice 30 / 30T	Enterprise	Supported	Ported Apr 2025
Matrice 300	Enterprise	Supported	Ported Apr 2025
Matrice 4T / 4E	Enterprise (new)	Full v54 (Apr 2026)	Preceded by "777" interim
Mavic 4 Pro	Consumer (new)	In test	Work started 2026
DJI Neo / Neo 2	Micro	In test	Indoor/inspection use case
DJI Avata 2	FPV	Porting begun	Target late 2026

3.2 Core function set (Mavic 3 family, primary manuals)

Command reference from the operator manuals. Each command terminates with a comma in the name field.

Function	Enable	Disable	Effect
Remote ID / DroneID / OpenDroneID off	default	-	Airframe stops broadcasting its position, home point, and operator position. Defeats AeroScope-class passive detection.
No-Fly-Zone off	default	-	Drone ignores NFZ enforcement; app warning is cosmetic.
GPS-off "white zero" (anti-spoof)	`gps_off,`	`gps_on,`	Ignores GNSS; coordinates forced to a static value; flight by camera only; immune to position spoofing.
FCC high-power radio	`fcc_on,`	`fcc_off,`	Adds 5.8 GHz and raises transmit power; extends control range.
Full disable of 1001 radio changes	`fcc_default,`	-	Hands radio back to stock behavior (for booster-equipped drones).
Altitude ceiling	`up9999,` (10 km)	`up1000,` (1 km)	Removes factory altitude limits.
Sport mode under GPS-off	`cine_sport,`	`cine_normal,`	Higher speed and tilt, obstacle ignore.
Lower-sonar override	`tof_on,`	`tof_off,`	Allows descent when the sonar is blocked by a payload; on Matrice 4 also kills the laser-rangefinder illuminator.
Nav lights	`leds_on,`	`leds_off,`	Beam LEDs on or off (signature control).
Battery-check bypass	`bad_battery,`	-	Runs motors on any battery or a ground wire; zeroes battery errors; shows supply voltage. Warning: does not repair a weak cell.

Function	Enable	Disable	Effect
Wind-loss guard	`wind_atti,`	`wind_normal,`	Forces ATTI for 8 seconds at critical wind to arrest altitude loss.
Low-battery auto-land off	`bat_land_off,`	`bat_land_on,`	Stops forced landing on the last charge percent.
Lost-link climb	`lost_2000,` to `lost_100,`	`lost_off,`	On link loss, climbs 100 to 2000 m to escape jamming. `lost_500,` is default.
Lost-link compass return	`lost_compass,`	`lost_off,`	Turns toward the recorded inbound bearing and flies back toward the operator; Matrice 4 runs it in ATTI and adds visual return to the takeoff point.
Hidden lower light double-tap	`c_lights_on,`	`c_lights_off,`	Reassigns a controller button to a covert lower-light / invisibility mode.
AeroScope spoofing (Matrice 4)	`aeroscope_random,` / `_z,` / `_heart,`	`aeroscope_off,`	Broadcasts decoy DroneID: random ghost drones or Z / heart shapes on the AeroScope display, without revealing the real operator.
Airsense (ADS-B) off	default	-	Removes manned-aircraft proximity warning and control lockout.
Flight-log removal	default	-	No track or home point extractable if captured (except 3 Pro).

3.3 Matrice 4 v54 capability deltas (higher-end platform)

Delta	Operational meaning
FCC tri-band 2.4 / 5.2 / 5.8 GHz auto-switch	Longer link, frequency agility against single-band jamming.
UNBIND built into firmware	Any controller flies the drone, no 50-flight cap; simplifies field re-pairing and captured-airframe reuse.
`lost_compass,` in ATTI + visual return-to-takeoff	Autonomous egress from jamming even without GNSS.
`tof_off,` kills laser-rangefinder illuminator	Lower night-vision signature.
`bad_battery,` shows supply voltage	Enables non-DJI and tethered power packs for endurance builds.
Reserve build 77.77.7778 (interim "sevens")	Fallback if 1001 drops. The "sevens" do NOT disable DroneID, so operators must jam GNSS on the drone and the controller when flying it near the line of contact.

Interim "777" caution (adversary self-admission). The 77.77.7777 build for Matrice 4T is native Chinese firmware "from unreliable sources," un-audited, with no backdoor guarantee. It does **not** disable DroneID. The group instructs operators to jam GNSS on the drone and the controller when flying it near the line of contact, or risk rapid counter-battery. Read as a capability gap the adversary itself flags.

Capability video. A group-distributed capability video (254 seconds, DJI Matrice 4 focus, DJI Neo referenced) shows offline device binding with the internet disconnected, a firmware-set 10 km maximum altitude, Sport-mode speed of 21 m/s (75.6 km/h) against 15 m/s (54 km/h) in Normal mode, and a lost-link sequence that navigates by azimuth to a point without GNSS. It corroborates Matrice 4 support, altitude-limit removal, offline binding, the speed unlock, and lost-link autonomy.

4. Maliciousness

Malicious character sits in intent and effect, not in exotic code. "1001" removes safety and accountability controls that manufacturers embed for airspace and civil protection, then adds combat behaviors. The result converts a commercial camera drone into a military reconnaissance and strike asset for use against Ukraine.

Removed control	Civil purpose defeated	Military effect
Remote ID / DroneID	Accountable identification of the aircraft and operator	Operator survivability; blinds passive detection
No-Fly-Zones	Airport, border, and sensitive-site protection	Unrestricted operation over contested airspace
Airsense (ADS-B)	Manned-aircraft collision avoidance	Silent operation near crewed aviation
Altitude and distance limits	Line-of-sight and safety envelope	Deep standoff reconnaissance
Battery safety checks	Cell-fault protection	Endurance and payload builds, at crash risk
Flight-log retention	Incident forensics	No exploitable data if captured

AeroScope-decoy commands (`aeroscope_random / z / heart`) cross from evasion into active deception: the airframe pollutes a defender AeroScope display with ghost tracks and shapes, an information-operations effect against the counter-UAS picture. Pairing with the in-house Sokol-1 FPV munition and TREPET attack-point planning places the program inside a kill chain, not merely a nuisance-evasion role.

5. Stealth

Stealth in "1001" works across several sensor bands.

Layer	Mechanism	Sensor defeated
RF identity	Remote ID / DroneID off	AeroScope and passive Remote-ID receivers
RF deception	AeroScope decoy broadcast (random / Z / heart)	Counter-UAS operator picture

Layer	Mechanism	Sensor defeated
Navigation	GPS-off white zero, barometric-locked altitude	GNSS spoofing and position hijack
Optical / IR	`leds_off,`; `tof_off,` kills sonar IR and laser-rangefinder illuminator; invisibility LED mode	Night-vision and IR spotting
Data	Flight-log removal; no home-point extraction	Post-capture forensics

Residual signature: the drone still radiates on DJI control and video frequencies. RF direction-finding and jamming stay effective, and jammed DJI airframes over friendly ground often soft-land for recovery. GPS-off flight also degrades the drone: above roughly 200 m the airframe drifts and drops into ATTI, so stealth trades against stability. Assessment: detection-defeat is **Highly likely (85 to <95)** to reduce passive-RF and spoofing-based counters; RF jamming remains the counter of choice, **Likely (55 to <85)** to retain effect against un-modified frequency behavior.

5.1 Vendor posture and the detection fallback

The manufacturer has been walking away from the very controls "1001" strips. DJI discontinued its AeroScope drone-detection system in 2023, and independent research confirmed that DJI DroneID is broadcast unencrypted, readable by any passive receiver. That is why deleting it matters: the firmware removes the defender's cheapest cooperative-identification layer. DJI then ended its own geofencing software in January 2025 and moved no-fly enforcement to the operator, so the firmware NFZ removal now overlaps a change the vendor made itself.

Western controls on the airframe supply tighten in parallel. DJI sits on the US Department of Defense "Chinese military company" list and the Commerce Entity List, and US Customs began holding DJI shipments under the Uyghur Forced Labor Prevention Act in early 2025. In December 2025 the FCC, on a national-security determination tied to Section 1709 of the FY2025 NDAA, added DJI and Autel and, in a first-of-its-kind step, all foreign-produced UAS and critical components to its Covered List, blocking new US equipment authorizations. Existing fleets are not grounded, and 500,000 units are already flashed, so the near-term effect on the Russian program is supply friction, not denial.

Detection fallback. With Remote ID and DroneID off, cooperative passive-RF identification fails and the defender drops to non-cooperative sensing: control-link and video-downlink RF detection and direction finding, radar, acoustic arrays, and electro-optical or infrared tracking, backed by jamming and kinetic intercept. The control and video links still radiate and stay jammable and detectable with DroneID disabled, so "1001" raises the cost and latency of detection rather than making the drone invisible. Counter-effort should move spend from Remote-ID readers toward multi-sensor non-cooperative detection.

6. Where They Teach, Groups Involved, and Locations

6.1 Training and knowledge transfer

Channel	Content	Audience
Manuals on @RussianHackersChannel	Per-model, per-version operator instructions and command memos	Operators
Terminal-based install	Flash + service functions (gimbal calibration, sensor re-write), alt-app load	Workshop technicians
Master-classes at РОКОТ-ЦЕНТР	Dozens of sessions; FPV piloting, tactical medicine, small-arms drill	Volunteers, operators, departing soldiers
TREPET Operator / Simulator modes	Spectrum, frequency-hopping, GNSS-free routing, attack-point planning	Advanced operators
Enrolment and recruiting	Telegram sign-up (a volunteer-onboarding contact), volunteer onboarding	New volunteers

6.2 Group structure

Group	Function
Русские Хакеры - Фронту	Firmware and app development (1001, DRONE UNBIND)
РОКОТ-ЦЕНТР | 33 (Vladimir)	Parent volunteer center; training; FPV munition build (Sokol-1)
РОКОТ-ГОРИЗОНТ (proshivka1001 / _bpla)	Federal flashing hub and workshop coordination
ТРЕПЕТ / TREPET group	EW-ISR flight application
Workshops / ТЭЧ (400+)	Local flashing, un-bind, app install

6.3 Geographic footprint

The РОКОТ-ЦЕНТР 33 network publishes its installer roster openly, as two maps and two contact lists: occupied Ukraine ("Новороссия") and mainland Russia ("материк"). Both lists are reproduced below in full from the group's own posting. Each entry is a Telegram contact that flashes "1001" on a walk-in basis. The one coordination contact for the whole program, mainland and occupied alike, is a single named coordination contact.

Figure 3. РОКОТ-ЦЕНТР 33 published map of "1001" installation centers in occupied Ukraine ("Новороссия"). Green markers = active points; the black comma is the group's "1001" glyph.

Figure 4. РОКОТ-ЦЕНТР 33 published map of "1001" installation centers across the Russian Federation ("материк").

Occupied Ukraine ("Новороссия") installer footprint, by sector (locality counts; individual points withheld).

Sector / region	# localities
DNR / Donetsk axis	30
LNR / Luhansk axis	24

Sector / region	# localities
Zaporizhzhia axis	13
Tavria / Kherson axis	10
Kharkiv axis (Vovchansk-Kupiansk)	8

Mainland Russia ("материк") installer footprint, by region (locality counts; individual points withheld).

Sector / region	# localities
Moscow region	5
Kursk Oblast (+ districts)	11
Belgorod Oblast	5
Central Russia	7
Northwest	4
South	4
Volga	6
North Caucasus	2
Urals	2
Siberia	3
Far East	1

Footprint read. The published footprint spans occupied Ukraine (Donetsk, Luhansk, Zaporizhzhia, Kherson, and Kharkiv axes) and mainland Russia, heaviest in the border oblasts of Kursk and Belgorod and the Moscow region, with points from Kaliningrad to Vladivostok. The mainland map (Figure 4) plots more nodes than any list, so the footprint is broad and still widening. The roster is the group's own advertisement, so presence is a claim of an active point, not independent confirmation.

6.4 Network linkage

Contact reuse across the two rosters shows some operators servicing both occupied-territory and mainland points, which indicates coordination across the front and the rear rather than two separate networks. A single named contact coordinates installation and support for the whole network.

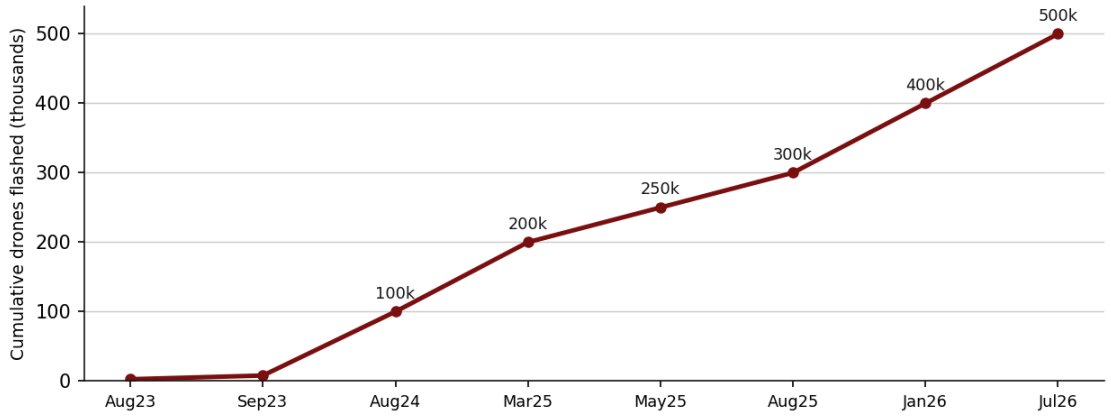
7. SO WHAT / WHY NOW

So what. "1001" turns a cheap, abundant commercial drone into a survivable military ISR and strike node at industrial scale, for free, faster than a defender degrades the fleet. Detection-defeat and spoofing immunity strip two of the counter-UAS defender's cheapest tools (passive Remote-ID tracking and GNSS spoofing).

Why now. Four developments converge in 2026. The network passed 500,000 flashed drones on the report date. Full 1001 support reached the higher-end Matrice 4 in April 2026. TREPET 3.0 added spectrum sensing, frequency-hopping, GNSS-free routing, and attack-point planning, an electronic-warfare and targeting uplift beyond the firmware alone. Model expansion into Mavic 4 Pro, Neo micro-drones, and Avata 2 FPV widens the mission set into indoor inspection and FPV strike.

8. Impacts So Far

Figure 1. Self-reported cumulative drones flashed to "1001" (Aug 2023 - Jul 2026)



Figures are self-reported by the network. Treat the curve as directional, not audited. Implied throughput near report date: 500 to 560 drones per day across the grid.

Impact area	Observed effect	Confidence
Detection	Russian DJI fleets go dark to AeroScope-class passive tracking	Highly likely (85 to <95)
Electronic warfare	GNSS spoofing loses effect against GPS-off airframes	Highly likely (85 to <95)
Scale and cost	Free flashing at 400+ nodes sustains fleet renewal faster than attrition	Likely (55 to <85)
Targeting uplift	TREPET turns recon quads into EW-ISR and attack-planning nodes	Likely (55 to <85)
Resilience	Two cyberattacks paused but did not end the pipeline	Confirmed (primary)

9. Structured Analysis

9.1 Structured environmental scan

Drivers of change bearing on the "1001" program.

Dimension	Indicator	Relevance
Social	Mass volunteer "народный ВПК" movement	Sustains free labor, donations, and recruitment

Dimension	Indicator	Relevance
Technical	DJI dominance; open Remote-ID; jailbreak lineage	Large, cheap, hackable airframe base
Economic	Free-of-charge model; grey-market DJI import	Cost asymmetry favors the attacker
Military	Drone-saturated line of contact	Firmware feeds a live operational demand signal
Political	LDPR and United Russia proximity; state-TV coverage	Quasi-official cover and protection
Legal	DJI market exit; export controls (Entity List, 1260H)	Grey supply persists despite controls
Education	Master-classes, simulator app, Telegram manuals	Repeatable operator pipeline
Security	Closed terminal model; internal enforcement rhetoric	Proliferation control and OPSEC posture
Plus: Religion	Orthodox-patriotic framing on channels	Cohesion and legitimacy signaling
Plus: Demographics	Regional volunteers, veterans, families	Broad manpower base
Plus: Psychology	Victory framing; enforcement threats to leakers	Morale and internal discipline lever
Plus: Culture	Hofstede: high collectivism, high power distance	Centralized coordination, strong in-group mobilization

9.2 Threat-priority ranking

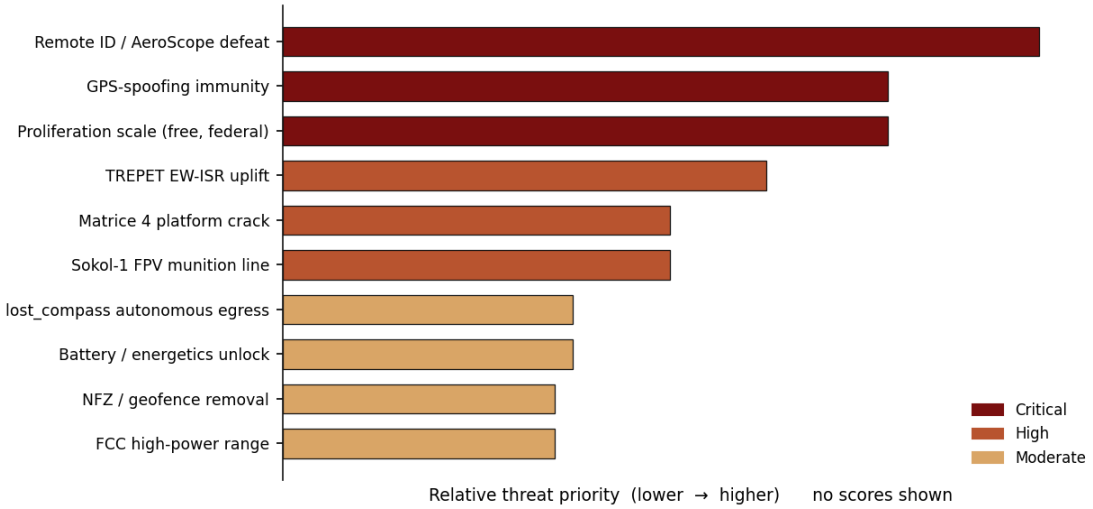
Threats are ranked with the Treadstone 71 threat-priority index (proprietary). Exact scores and the calculation are withheld from this edition; the ranking, the priority tier, and the relative weight below carry the assessment.

Threat-priority ranking. Tier and relative weight only; underlying scores are proprietary and withheld.

Rank	Threat factor	Priority tier	Relative weight
1	Remote ID / AeroScope defeat (detection blinding)	Critical	■■■■■
2	GPS-spoofing immunity (EW defeat)	Critical	■■■■▒
2	Proliferation scale (free, federal, 500k)	Critical	■■■■▒
4	TREPET EW-ISR and attack-planning uplift	High	■■■▒▒
5	Matrice 4 higher-end platform crack	High	■■■▒▒
5	Sokol-1 FPV munition line at the same hub	High	■■■▒▒
7	`lost_compass`, autonomous EW egress	Moderate	■■▒▒▒
7	Battery / energetics unlock (endurance builds)	Moderate	■■▒▒▒

Rank	Threat factor	Priority tier	Relative weight
9	NFZ / geofence removal	Moderate	■■▒▒
9	FCC high-power range extension	Moderate	■■▒▒

Figure 2. Threat-priority ranking (relative)



Ranking reflects likelihood, severity, and strategic impact judged by the analyst and compared factor against factor. New reporting this cycle raised the Matrice 4 platform assessment and lowered the geofence-removal factor (the vendor ended its own geofencing), and added a micro-drone factor.

9.3 Analysis of Competing Hypotheses: who wrote the code

C = consistent, I = inconsistent, N = neutral against the evidence.

Evidence	H1 Grassroots volunteers, ROKOT-integrated	H2 State / FSB (Positive Technologies)	H3 Commercial jailbreak lineage repurposed
Free-of-charge, no monetization	C	N	I
Pseudonymous developer cell	C	C	C
Named regional volunteer integrator (Vladimir)	C	I	N
State-TV coverage, party proximity	C	C	I
No primary evidence of a state entity	C	I	C
Positive Technologies claim is single-source rumor	C	I	C
Tooling echoes CopterSafe / Drone-Hacks lineage	N	N	C
Closed terminal model, OPSEC discipline	C	C	N
Assessment	**Most consistent Likely (55 to <85)**	Least consistent Unlikely (15 to <45)	Partial contributor Roughly even (45 to <55) on lineage

H1 carries the fewest inconsistencies. H3 explains only the technical genealogy, not the volunteer, free, regionally-integrated model. H2 rests on one self-published OSINT site citing unnamed channels, with no primary corroboration; treat as deception-aware low confidence.

10. Outlook: Strategic Foresight

General Morphological Analysis of the drivers yields three internally coherent 6-to-18-month scenarios.

Scenario	Drivers	Trajectory	Probability
S1 Continued scaling (baseline)	Model expansion completes; terminal grid recovers fast after attacks	Neo, Avata 2, Mavic 4 Pro enter service; count passes 700k; TREPET matures	Likely (55 to <85)
S2 Disrupted pipeline	Repeated cyber and physical strikes on servers, terminals, VPN backend	Multi-week outages; local shortfalls; slower renewal; morale effect	Roughly even (45 to <55)
S3 Countermeasure erosion	DJI hardens later models; Ukraine fields Remote-ID-independent detection at scale	Higher-end platforms resist cracking (see "777" FCC gap); defender picture recovers	Unlikely (15 to <45) near term

Indicators of change to watch (pre-attack indicator set)

Indicator	Points to
Version release beyond v54; full FCC on Matrice 4T	Higher-end platform maturity (S1)
Confirmed Neo / Avata 2 field use	Mission-set widening into indoor and FPV strike (S1)
Third cyberattack or physical strike on servers/terminals	Pipeline disruption (S2)
Roster contraction on `proshivka_bpla/3` and `/4`	Node attrition (S2)
DJI firmware or Remote-ID re-encryption update	Countermeasure erosion (S3)

11. Gaps and Flow Issues

11.1 Collection gaps

- Real identities of the developer cell and TREPET authors remain unresolved.
- VK admin roster (`vk.com/nvp33`) and wall threads sit behind login on the present pass.
- Workshop activation status at the `/3` and `/4` rosters not captured at single-post granularity.
- Server, update-domain, and VPN backend infrastructure behind DRONE UNBIND not yet mapped.
- The "777" Chinese-firmware supply channel (grey-market vendor) is unnamed.

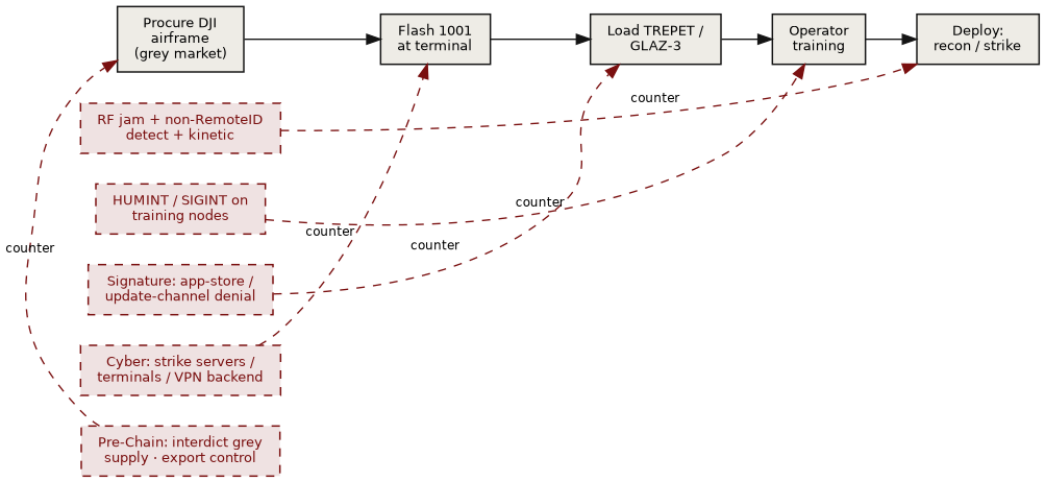
11.2 Adversary pipeline flow issues (attack surface)

Choke point	Weakness	Prior strike
Central update servers	Single logical dependency for all terminals	July 2025 breach
Terminal laptops	Require server-side re-flash to function; recoverable if seized	July 2025 disable order
Support Telegram bot	Account-takeover exposure	February 2026 hijack
DRONE UNBIND VPN backend	Internet-dependent; credential re-issue after breach	Indirect, July 2025
"777" interim on Matrice 4T	DroneID stays on; un-audited source	Self-flagged gap

11.3 Analytic flow issues

- Scale figures are self-reported with a propaganda incentive; hold as directional.
- Capability claims derive partly from adversary manuals; several features are not independently bench-tested in the West.
- Telegram is the primary layer; deception and morale-management framing run through it.

12. Opportunities



Opportunity	Effect	Priority (threat-priority index-linked)
Cyber interdiction of the server/terminal/VPN layer	Pauses the whole grid; proven twice	Top
Counter-UAS weight on RF jamming and non-Remote-ID detection	Defeats the residual signature 1001 cannot hide	Top
Roster geolocation for interdiction and targeting support	Maps the physical node network	High
Export-control and grey-market pressure on DJI/Autel supply	Raises airframe cost at the pre-attack	High

Opportunity	Effect	Priority (threat-priority index-linked)
Detection tuning for the 99-88-77 boot tell and white-zero indicator	Field identification of flashed airframes on capture	Medium

13. Recommendations

1. Re-weight counter-UAS doctrine against Russian DJI fleets toward RF jamming, acoustic and EO/IR detection, and kinetic intercept. Assume no Remote-ID broadcast.
2. Prioritize cyber and physical effects on the central update servers, the flashing terminals, and the DRONE UNBIND VPN backend, the pipeline choke points struck in July 2025 and February 2026.
3. Stand up authenticated collection against `vk.com/nvp33` and the live rosters at `proshivka_bpla/3` and `/4`; geolocate active nodes at city granularity.
4. Open a discrete product file on the Sokol-1 FPV munition line and the TREPET application as an EW-ISR capability in its own right.
5. Task attribution collection on the network coordinators, "Daniil," and `@trepet_group` developer metadata; treat the Positive Technologies claim as unproven.
6. Feed the threat-priority index ranking into counter-effort prioritization and re-run on each version release or confirmed model expansion.

14. Source Grading (STANAG 2511, expanded)

Axes scored separately, never averaged. ASA Evidence Standard tri-score applied to the central attribution claim: Testimonial strength high, Documentary strength high, Forensic strength moderate.

Reliability of source (A to F)

Grade	Definition	Applies to
A	Completely reliable	GTRK Губерния-33, Izvestia (registered media of record)
B	Usually reliable	Group Telegram channels (interested party, self-consistent, cross-forwarded); United Russia regional; VK community
C	Fairly reliable	tgstat.ru third-party metrics
D	Not usually reliable	-
E	Unreliable	Single-source rumor sites (Positive Technologies claim)
F	Reliability cannot be judged	-

Credibility of information (1 to 6)

Grade	Definition	Applies to
1	Confirmed by other independent sources	Attribution to РОКОТ-ЦЕНТР 33 / Vladimir (state TV + press + party + VK)
2	Probably true (logical, consistent, not yet confirmed)	Version changelogs, tooling detail, cyberattack accounts, capability deltas
3	Possibly true (reasonably logical)	Self-reported flashed-drone totals; VK-gated content
4	Doubtful	State-sponsor claim

Grade	Definition	Applies to
5	Improbable	-
6	Credibility cannot be judged	-

Per-source scores

Source	Reliability	Credibility
Group Telegram (proshivka1001 / _bpla / rokot_centr / RH forwards)	B	2
Operator manuals (Mavic 3 / 3T / Matrice 4)	B	2
GTRK Губерния-33 (trc33.ru)	A	2
Izvestia (iz.ru)	A	2
United Russia regional (vladimir.er.ru)	B	2
VK community (vk.com/nvp33)	B	3
tgstat.ru analytics	C	3
Positive Technologies sponsor claim	E	4

16. Wrap-up

"1001" has moved past novelty into infrastructure. A pseudonymous cell writes the exploit, a state-adjacent volunteer center in Vladimir turns it into a free federal service, and 500,000 self-reported installs later the program strips detection and spoofing off cheap DJI airframes faster than a defender degrades the fleet. The install network is mapped, the coordination contact is named, and the counter-effort priorities are ranked.

The bottom line for a first-time reader: this answers what, who, where, and how big, well enough to prioritize. It does not answer which nodes are live right now, or what a strike would achieve. Those need confirmation collection on top of it.

The decision it drives is to shift counter-effort off the drone and onto the pipeline, the closed server, terminal, and VPN supply layer, and onto multi-sensor non-cooperative detection, while tasking confirmation on the highest-value nodes: the operators who appear on both the front and the rear, and the border-oblast hubs in Kursk and Belgorod.

It leaves open questions worth the next collection cycle: which advertised nodes are active today, who the developers actually are, whether the Matrice 4 crack has reached full FCC parity, how the December 2025 FCC controls bite the airframe supply the program depends on, and what the two claimed cyberattacks on the network achieved. Each is a discrete, taskable lead.

1001 Firmware — Installer Location and Handle Register

Treadstone 71 · Appendix A to the "1001" firmware threat report · Compiled 29 July 2026

What this is. The complete installer roster as published by the distribution network itself, consolidated into one register: every advertised install location with the Telegram handle(s) listed for it, plus the OpenStreetMap locality-centroid coordinate where resolved. Two networks: occupied Ukraine ("Новороссия") and mainland Russia ("материк").

Sourcing. Primary source is РОКОТ-ЦЕНТР / РОКОТ-ГОРИЗОНТ (region code 33), the Vladimir volunteer war-support center that integrates and distributes "1001," through its Telegram channel @proshivka_bpla (the two pinned installer rosters) and the group's two published installer maps. Related channels: @rokot_centr, @proshivka1001; developer channel @RussianHackersChannel (join-walled). t.me/s/ previews render for the distribution channels; developer content obtained via forwards.

Reliability caveat. This is the group's own advertisement. A listing is a *claimed* active install point, not independently confirmed. Coordinates are town-level analytic centroids, not facility locations; per-node confidence flags and the KML are in the companion target deck. Some toponyms are ambiguous (for example Lyman appears in two oblasts; a few localities are listed twice under different sectors).

Network 1 — Occupied Ukraine ("Новороссия")

85 advertised install points across 81 localities, 125 distinct handles, in five front-adjacent sectors.

Source. РОКОТ-ЦЕНТР 33 occupied-territory installer roster, Telegram @proshivka_bpla (Новороссия list) + the group's Новороссия installer map. Sector labels are a Treadstone 71 analyst overlay on the source's unlabeled tiered blocks.

DNR / Donetsk axis

Location	Coordinates (OSM)	Installer handle(s), as published
Donetsk	48.0159, 37.8013	@nicksite114, @zombi_drones, @kozlyatnya, @kent228v2, @mrL0st, @PrizrakTech, @mr_dezzz_90, @Altay_centr, @Mirage_privat, @zlooooooo1, @petlya23, @poohtech57, @mdsmers, @tomkruser, @Herald150, @dimasPisec2025, @Vitos6v, @Irtyshlugansk, @TakovPut11rus
Airport	48.0714, 37.7408	@Kooooorben, @compas1993

Location	Coordinates (OSM)	Installer handle(s), as published
Gorlovka	48.3059, 38.0028	@ZOV_KpoBu, @Leshei1111, @babai2257, @villifog
Volnovakha	47.6015, 37.4934	@Laboratory_V
Grafovka	47.6763, 37.4116	@Dargo161
Avdeevka	48.1339, 37.7467	@Foxeeeeeer, @LCP88
Marinovka	48.1795, 37.3483	@BERKUT455
Enakievo	48.2305, 38.1850	@karlson_ru, @Technik89, @BeReStA12
Dokuchaevsk	47.7499, 37.6716	@NeboChistogo
Dmitrovka	46.5706, 34.2864	@Motorv8
Kurakhovo	47.9835, 37.2826	@dr_tech_161
Mironovskoye	48.4621, 38.2755	@SKV2006
Krasnaya Polyana	47.5601, 37.0723	@objektum
Spartak	48.0805, 37.7688	@Panteleich69

Location	Coordinates (OSM)	Installer handle(s), as published
Yalta (Mariupol)	—	@dron_dji_svo
Artemovsk	48.4388, 38.7215	@minba2t, @sahalin1442, @armyFTT
Paraskoviivka	47.8692, 37.4425	@Ijarenm56
Metallist	48.6224, 39.2841	@TOMEN_Y0293
Marinovka	48.1795, 37.3483	@Burke45
Mironovsky	48.4621, 38.2755	@invictus141
Selidovo	48.1281, 37.2986	@Konor_tech, @stay_device
Yasinovataya	48.1271, 37.8590	@senya190588, @TechPyx, @Liber444, @VarPanda
Avdotino	47.9175, 37.8494	@RCBS_ADMIN
Svetlodarsk	48.4380, 38.2235	@ev_sandrov
Debaltsevo	48.3397, 38.3999	@PrizrakTech4
Kuteinikovo	47.8098, 38.2865	@portnoyz

Location	Coordinates (OSM)	Installer handle(s), as published
Vladimirivka	49.8401, 37.3208	@Dargo161, @PrinceAiri
Krasny Pakhary	48.4930, 38.2907	@vlasov_artem17
New York	48.3320, 37.8366	@Bobbobing
Ukrainsk	48.0947, 37.3587	@SkySeven0

LNR / Luhansk axis

Location	Coordinates (OSM)	Installer handle(s), as published
Luhansk	48.5717, 39.2973	@kent22856, @rombo_fly
Kremennaya	49.0463, 38.2179	@bullrv, @Nemec_7351
Novokrasnyanka	49.1394, 38.2671	@YaVZoR
Staraya Krasnyanka	49.0377, 38.2886	@mike_kolhoz
Kolomychikha	49.4471, 37.9718	@Mitagor
Beloutsk	49.2068, 39.5912	@hantsvo
Verkhnyaya Duvanka	49.6941, 38.0682	@clandestineZZ
Zaydarovka	—	@FalconsVVP
Konstantinovka	49.7420, 38.9740	@skRipaG
Kuzmovka	49.5240, 37.9849	@AlexKama03

Location	Coordinates (OSM)	Installer handle(s), as published
Chernopopovka	—	@zlodey_Dji
Belovodsk	49.2068, 39.5912	@XFailesX
Severodonetsk	48.9479, 38.4936	@Mason_68
Lysychansk	48.9173, 38.4286	@RD_DED
Berestovoye	50.4380, 30.5550	@ilichtyk
Novopskov	49.5384, 39.1022	@matvei_san
Starobelsk	49.2822, 38.8974	@dj_crimea
Yamy	49.7615, 38.3705	@vladivostok_komi
Novozvanovka	48.5846, 38.3622	@Djiser
Pervomaysk	48.6252, 38.5373	@goose_firmware
Varvarovka	49.0727, 38.4052	@REMARTI189
Zaliman	49.2575, 38.1669	@raghardalex
Irmino	48.6014, 38.6019	@muhomor90
Artemovsk	48.4388, 38.7215	@armyFTT

Zaporizhzhia axis

Location	Coordinates (OSM)	Installer handle(s), as published
Melitopol	46.8467, 35.3827	@Arion_dji, @vic10tory01, @leva229, @HotHeats104, @Aist137

Location	Coordinates (OSM)	Installer handle(s), as published
Berdyansk	46.7557, 36.7888	@Chya_Chye
Marinopol	47.6219, 36.3611	@laimier
Tokmak	47.2550, 35.7092	@RussianAngryBirds
Prishib	47.2495, 35.3283	@Dzimmineitron
Zelenopol	48.3295, 37.5774	@SmileFlyRc
Mikhailovka	48.4968, 38.9021	@ProshivkaSueta, @ful_pipez
Vasilyevka	47.4432, 35.2803	@SmagaWaR, @mr126rus
Rabotino	47.4431, 35.8261	@grozator
Chernigovka	47.1949, 36.2075	@Sova_3434
Priazovskoye	46.7300, 35.6390	@Chita_65
Osipenko	46.9164, 36.8200	@Sokollipets
Veseloye	47.0179, 34.9211	@lex_grand

Tavria / Kherson axis

Location	Coordinates (OSM)	Installer handle(s), as published
Tavria	46.6723, 32.6340	@VLG1611
Tarasovka	46.1422, 33.1179	@Lab28_70
Darovka	46.1965, 33.1893	@xyu1234uyx
Dmitrovka	46.5706, 34.2864	@Black99991
Stroganovka	46.2504, 33.8729	@BplGROMM
Novotroitskoye	46.3558, 34.3364	@HotHeads104
Novoaleksandrovka	46.9707, 34.4167	@Sanodelkin, @Akela184, @Giry_12
Vinogradovo	46.3719, 32.9394	@MasterFobos17, @MironSVO
Blagodatnoye	46.7902, 32.3405	@Strannik0154
Tavriysk	46.7550, 33.4248	@ViRUS_MASON

Kharkiv axis (Vovchansk-Kupiansk)

Location	Coordinates (OSM)	Installer handle(s), as published
Vladimirivka	49.8401, 37.3208	@LUXOPADKA58198
Veliky Vyselok	49.8358, 37.8840	@KutuzKutuzov
Lyman	49.5886, 36.5256	@sto_dji_25
Vtoroy Lyman	49.9530, 37.8703	@RUSaViator
Tavolzhanka	49.8388, 37.7758	@RPKRF
Olshany	50.0514, 35.8839	@stone_stone_55

Location	Coordinates (OSM)	Installer handle(s), as published
Orlyanka	49.6882, 37.9253	@zoomarikjan
Bogdanovskoye	48.9561, 36.5807	@RPKRF

Network 2 — Mainland Russia ("материк")

50 advertised install points across 50 localities/districts, 65 distinct handles, from Kaliningrad to Vladivostok.

Source. РОКОТ-ЦЕНТР 33 mainland installer roster, Telegram @proshivka_bpla (материк list) + the group's mainland installer map.

Moscow region

Location	Coordinates (OSM)	Installer handle(s), as published
Moscow	55.5987, 38.1199	@evgenich_z, @ZOV_army_911
Moscow + Zelenograd	55.9920, 37.2142	@khukhrynchanin
Serpukhov, Kolomna	54.9155, 37.4196	@SkyCopter
Podolsk	55.4309, 37.5453	@EDI_299
Pushkino	56.0104, 37.8462	@yunga190

Kursk Oblast (+ districts)

Location	Coordinates (OSM)	Installer handle(s), as published
Kursk	51.7270, 36.1922	@TinWoodman46, @igolka56D, @Suba913, @nolik_tut
Rylsky district	51.5714, 34.6240	@dron_drug76

Location	Coordinates (OSM)	Installer handle(s), as published
Maryino	51.5869, 34.9405	@servic_777
Lgovsky district	51.6198, 35.1329	@Aist137, @dronesreboot, @komsadron
Kurchatovsky district	51.6822, 35.5408	@Hakerrrr
Konyshevsky district	51.8409, 35.2901	@Zhora_51
Sudzhansky district	51.2464, 35.2216	@Is08827
Oboyansky district	51.2346, 36.0784	@nomad_23
Zheleznogorsky district	52.2326, 35.4575	@Timon7777, @Sokollipets
Mazepovka	51.6138, 34.8363	@igolka56D
Korenevsky district	51.3694, 34.9815	@Karl810

Belgorod Oblast

Location	Coordinates (OSM)	Installer handle(s), as published
Belgorod	50.5956, 36.5873	@dry_eye1, @meteorit50, @drone_technik
Dubovoye	50.5376, 36.5846	@Zzzolzzz
Shebekinsky district	50.4575, 37.0956	@AdPaters, @Tech_dji_15, @DimMedBLA

Location	Coordinates (OSM)	Installer handle(s), as published
Valuyevsky district	50.2113, 38.1002	@Kabina186
Rovensky district	49.9147, 38.8920	@skRipaG

Central Russia

Location	Coordinates (OSM)	Installer handle(s), as published
Bryansk	53.2789, 34.3659	@ra3yja
Voronezh	51.6606, 39.2006	@SkyRokot36
Yaroslavl	57.6264, 39.8934	@yar_teh
Vladimir	56.1289, 40.4075	@it_rokot
Lipetsk	52.6935, 39.1123	@Fly_Lipetsk
Ryazan	54.6703, 39.6884	@voffka62, @rzn1001
Obninsk	55.0999, 36.6093	@scout_ob

Northwest

Location	Coordinates (OSM)	Installer handle(s), as published
St. Petersburg	59.9607, 30.1587	@III_Torpeda_III, @SHAMAN_9_5_45, @remkopter, @HackSpb78
Kaliningrad	54.7046, 20.4566	@mechanic735
Syktyvkar	61.6685, 50.8352	@MobilMAX777

Location	Coordinates (OSM)	Installer handle(s), as published
Murmansk	68.9707, 33.0750	@Sever_IPA

South

Location	Coordinates (OSM)	Installer handle(s), as published
Sevastopol	44.6054, 33.5221	@Shitovaya1001
Rostov-on-Don	47.2610, 39.7249	@Araddgan, @DJIROSTOVSERVICE
Novocherkassk	47.4107, 40.1020	@MMA_67
Volgograd	48.7082, 44.5153	@Atomangl

Volga

Location	Coordinates (OSM)	Installer handle(s), as published
Nizhny Novgorod	56.3265, 44.0051	@BPLA_52
Kazan	55.7946, 49.1115	@OrnitologZilant
Saratov	51.5300, 46.0347	@kobakirill
Samara	53.1956, 50.1015	@art_ladya
Penza	53.1953, 45.0190	@ptica_58
Izhevsk	56.8605, 53.1977	@ncbs_bot

North Caucasus

Location	Coordinates (OSM)	Installer handle(s), as published
Stavropol	45.0345, 41.9739	@uZ_247_26
Grozny	43.3086, 45.7066	@Iskra_nohcho

Urals

Location	Coordinates (OSM)	Installer handle(s), as published
Yekaterinburg	56.8382, 60.6008	@URALDRONE_BOT
Tyumen	57.1535, 65.5423	@khasanovas

Siberia

Location	Coordinates (OSM)	Installer handle(s), as published
Novosibirsk	55.0288, 82.9227	@Ermak0019
Tomsk	58.6124, 82.0475	@Beck_Ris
Irkutsk	52.2891, 104.2798	@ldaxbx

Far East

Location	Coordinates (OSM)	Installer handle(s), as published
Vladivostok	43.1151, 131.8856	@Dron_vvo

Cross-network operators (appear in both rosters)

The following handles are listed on both the occupied-territory and the mainland rosters, indicating operators or coordinators servicing points across the front and the rear: @Aist137, @skRipaG, @Sokollipets. These are the strongest single leads for mapping coordination between the two networks. A single named contact coordinates installation and support across the whole network (held in the main report).