Russian Government Protection of Ransomware & Cybercrime Actors

An Exploitation Framework for LE and IC Analysts

FBI · DOJ · USSS · DIA · CIA · FinCEN · Treasury

March 2026 | Version 3.0

Developed by Reno

Executive Summary

Russia's ransomware ecosystem is not just tolerated by the state, it is actively structured, protected, and in many cases directed by it. This document examines seven Russian government entities through a single lens: how each one protects cybercriminals, what breaks that protection, what we can do about it, and what will blow back on us if we push the wrong way. Updated May 2026: Mintsifry Order No. 1174 (registered 22 May 2026) expanded SORM collection requirements to mandate real-time linkage of passport data, home addresses, tax IDs, bank account details, and geolocation to every IP address on Russian infrastructure. Concurrently, Russia crashed its own banking system in April 2026 — briefly eliminating electronic payments nationwide — while enforcing VPN restrictions, demonstrating willingness to accept macroeconomic self-harm to extend internet control. Neither development changes the analytical framework in this document. Both strengthen its core premise: FSB has comprehensive technical visibility into domestic criminal infrastructure and maintains a deliberate policy of non-enforcement. The "Russia didn't know" counter-argument is now categorically untenable.

This is not a document about Russian law enforcement. It is a document about Russian institutional behavior, and how to exploit the gaps, contradictions, and internal pressures within that behavior to degrade the ecosystem from the inside out.

Entities covered:

- FSB, architect of the protection ecosystem; recruits, tasks, and shields elite actors
- MVD / Department K, primary domestic enforcer; constrained by FSB but the highest-confidence mid-tier lever available
- Rosfinmonitoring, financial intelligence mapping node; feeds CBR and MVD; Egmont-suspended but domestically motivated
- CBR, non-attributable financial friction via 115-FZ banking controls; no court order needed
- FNS, tax authority; exposes lifestyle and income gaps without triggering FSB protection reflexes
- GRU, military intelligence; uses cybercrime as a strategic tool; sets the scope boundary for this framework
- SVR, foreign intelligence; lower ransomware footprint but relevant infrastructure and personnel overlap

The single most important principle in this framework:

Direct pressure on FSB-shielded actors, public attribution, extradition requests, media naming campaigns, reliably activates protection rather than degrading it. The highest-ROI approach routes pressure through domestic financial and legal frameworks that register as bureaucratic friction rather than foreign interference. This is not a soft option. It is how you avoid handing FSB a reason to shield an actor it might otherwise discard.

Entity	Protection Role	Actionability	Primary Blowback Risk
FSB	Recruits, shields, and tasks elite actors. Architect of the krysha model.	**Low (direct)**	Public attribution activates protection
MVD / Dept K	Primary domestic cyber enforcer. Mid-tier arrests. FSB can override.	**High (mid-tier)**	Including FSB names in referral packages

Rosfinmonitoring	Maps crypto-fiat flows. Flags to CBR and MVD. Egmont-suspended.	**High (mapping)**	Burning the Belarus FIU back-channel
CBR	115-FZ banking controls. Non-attributable friction without court orders.	**High (stealth)**	Naming without activating the pipeline
FNS	Tax exposure. Lifestyle vs. income gaps. No arrest power.	**High (low risk)**	Framing as counterintelligence product
GRU	Deploys cybercrime as a military tool. State employees, not co-opted freelancers.	**Low (direct)**	Using any domestic Russian lever against GRU-nexus actors
SVR	Infrastructure and IAB market overlap. Lower direct ransomware footprint.	**Low-Med**	Exposing SVR overlap indicators without IC compartmentation review

Engagement Triggers and Blowback Risk

This section covers the actions that consistently cause Russian agencies to protect, absorb, or redirect cybercriminals rather than suppress them. These are not theoretical risks, they are documented patterns drawn from post-2022 enforcement history. Every entity section in this document references these triggers. Read this first.

The core problem with getting this wrong isn't that the action fails. It's that the action makes the target harder to reach, sometimes permanently. FSB absorption of an actor is not reversible through additional pressure, it requires dismantling the protection relationship before re-engaging the criminal.

Protection Activation Triggers

These are the actions that flip an actor from criminal liability to protected asset in FSB's calculus:

Trigger / Action	What Happens	Operational Implication
Public attribution by a foreign government	Actor converts from criminal liability to national security asset. Once named by the U.S. or a partner government, FSB/GRU may treat the actor as a soft-state asset regardless of prior behavior.	Attribution hardens protection. Delay public naming until the actor is already isolated from protection, not before.
Formal extradition or arrest request to Russia	Triggers defensive nationalism. Russian doctrine opposes surrender of nationals. The request signals foreign ownership of the case, which activates institutional resistance across all agencies.	Extradition-first strategies produce the opposite of suppression. Use third-country arrest pre-positioning instead.
Media naming and shaming without domestic framing in place	Agencies treat it as hostile information warfare. Labeling actors 'Russian cybercriminals' without a domestic criminal charge equivalent reads as sovereignty violation, not law enforcement.	Domestic criminal framing (tax fraud, organized crime, Russian victim harm) must be established before any public naming campaign.
Indication of actor cooperation with foreign LE	Actor becomes a counterintelligence interest. Suspected cooperators are arrested, disappeared, or neutralized, FSB views cooperation as a double-agent risk.	Cooperator handling requires extreme operational security. Exposure of cooperation triggers reverse enforcement, not suppression of the actor, suppression of the cooperator.
Actor has technical value or recruitment potential	Delays or cancels enforcement. Actors with malware development or infrastructure capabilities are considered recruitable state assets. FSB will absorb rather than allow arrest.	Prioritize disruption of capability before it triggers recruitment. Once recruited, the actor is effectively off the board for domestic enforcement.

Target selection aligned with Russian strategic interests	Actor becomes functionally aligned with state objectives. Operations against Western banks, NATO infrastructure, or sanctions enforcement targets are viewed as symbiotic by Russian agencies.	Document target patterns to predict and preempt state absorption. If an actor's victim set serves Russian strategic interests, FSB absorption is likely regardless of operational history.
Krysha relationship in place (internal elite sponsorship)	Actor is immune from arrest regardless of cybercrime visibility. The protection relationship is more important than the criminal act.	Pressure must first weaken or circumvent the sponsor relationship. FNS and Rosfinmonitoring exposure of the protecting officer is a prerequisite, not an afterthought.
Multilateral Western pressure without domestic Russian framing	Resistance across all Russian agencies. Pressure through Western consortiums without domestic Russian criminal charge equivalents reads as sovereignty violation, not law enforcement cooperation.	Align multilateral pressure with simultaneous domestic framing. The two tracks must run together.

The Public Outing Track, Using Domestic Exposure Against Protected Actors

One of the most effective tools against FSB-protected actors is public exposure of their non-cyber domestic crimes, not their ransomware activity. This is the Conti/Black Basta/Nefedov model: surface financial misconduct, fraud, drug use, corruption, or other domestic law violations through investigative journalism channels (OCCRP, Bellingcat, iStories, Meduza) rather than through official attribution.

Why this works: when an actor's domestic misconduct becomes publicly visible, FSB faces a calculus shift. Shielding a known criminal whose crimes are embarrassing to the regime costs more than it returns. The protection value of that actor declines. In some cases FSB will distance itself, or competing FSB factions will surface the liability to weaken the protecting officer.

What's required for this to work:

- The domestic crime must be genuine and documentable, fabrication risks are high if the exposure is later challenged
- The framing must be domestic Russian harm, not Western victim harm, 'he defrauded Russian citizens' lands differently than 'he hacked American hospitals'
- The exposure channel must not carry a visible foreign government fingerprint, investigative journalism outlets create domestic scandal framing without official attribution
- Timing matters: expose after financial and tax pressure is in place, not before, the combination is more destabilizing than either alone

Blowback conditions for this track:

- If the actor's domestic crime exposure is traced back to Western intelligence sourcing, it activates the foreign interference protection reflex, the opposite of the intended effect
- If the actor's domestic misconduct also implicates FSB officers directly, FSB may act to silence the exposure rather than distance from the actor

- Do not use this track on actors with confirmed GRU operational nexus, the mechanism doesn't apply to state employees

Sequencing for Minimum Blowback

Actions should be sequenced from lowest to highest blowback risk. Low-risk actions first establish the domestic framing that makes higher-risk actions viable without activating protection reflexes.

Sequence	Actions	Blowback Risk
First	Financial exposure (FNS lifestyle flags, Rosfinmonitoring mapping, OTC broker identification). Underground trust node disruption. Infrastructure provider pressure.	Low, no public fingerprint, no FSB trigger, no foreign attribution signal
Second	Domestic agency referrals through non-intelligence channels (FNS → MVD, Rosfinmonitoring → CBR). Investigative journalism pipeline with domestic crime framing.	Medium, domestic framing must be established first; avoid Western sourcing fingerprint
Third	OFAC/OFSI designations. Infrastructure takedowns. Public attribution. Officer exposure operations. Only when actor is already isolated from protection.	High, only viable after protection relationship is weakened or dismantled. Do not lead with these.

FSB, Federal Security Service

The FSB is the architect of Russia's cybercrime protection ecosystem. It doesn't merely tolerate ransomware actors, it recruits, tasks, shields, and when necessary, sacrifices them. Understanding FSB's behavior requires understanding that FSB is not a unified institution. It is a collection of competing factions, officers with divergent financial interests, and units in active competition for political favor. This internal fragmentation is as important as FSB's aggregate power, because it is exploitable.

Technical visibility note (updated May 2026): Every analytical argument in this section that rests on FSB's awareness of domestically resident criminal actors is materially strengthened by Mintsifry Order No. 1174, registered 22 May 2026. Under SORM's existing architecture, FSB has had real-time access to domestic internet traffic since SORM-2 (1998). Order No. 1174 extends this: all operators of technological communications networks with internet identifiers (ASNs) must now link passport data, home addresses, tax IDs, bank account details, and real-time geolocation coordinates to assigned IP addresses, with additional collection of domains accessed and user logins. FSB has statutory access to this dataset without a court order. Any assertion that FSB lacked the technical means to identify a domestically resident criminal actor operating on Russian internet infrastructure is no longer supportable. The protection model described throughout this document reflects a deliberate choice against a backdrop of comprehensive technical visibility — not a consequence of surveillance limitations.

How FSB Protects Cybercriminals

The krysha ("roof") model is the primary protection mechanism. An FSB officer or unit provides protection to a criminal actor in exchange for financial payment, intelligence collection capacity, or strategic operational capability. The relationship is transactional, not ideological.

Protection Tier	Examples	FSB Behavior	Protection Mechanism
Elite / Recruited	Evil Corp, Conti (Ukraine tasking)	Full krysha, active shielding from MVD and foreign pressure	Financial payments, family ties, intelligence contracts
Useful / Tasked	Ransomware groups targeting Western firms	Protected while producing value; outsourced operations	Implicit immunity; deflection of MVD inquiries
Theatrical / Inconvenient	REvil (post-Colonial Pipeline)	Choreographed arrest; used as diplomatic chip; releases follow	Controlled impunity; charges dropped on regime signal
Irrelevant / Expendable	Forum carders, low-tier actors	Handed off to MVD; no FSB interest	None, legitimate enforcement targets

FSB Internal Factions, The Exploitable Contradiction

FSB is not a single decision-maker. Competing units, the 13th Service (SIGINT), 16th Center (foreign intel), 18th Center (domestic cyber), have divergent interests, and individual officers compete for political favor, resources, and criminal financial relationships. This matters operationally because:

- An officer whose protected criminal actor becomes an attribution risk is a liability to competing FSB units, not an asset

- Surfacing one officer's criminal financial exposure to competing FSB units is a more achievable objective than seeking unified FSB cooperation
- When a protected actor repeatedly gets disrupted despite protection, the protecting officer looks operationally incompetent, which activates internal FSB factional pressure
- Officers with Western asset exposure face counterintelligence scrutiny from within FSB, which can be triggered deliberately

The goal is not to get FSB to cooperate as an institution. The goal is to create conditions where specific FSB factions or leadership figures find it in their interest to act against a specific officer's protection relationship. These are different and more achievable objectives.

FSB Officer Liability Track

FSB officers maintaining krysha relationships with high-volume ransomware actors accumulate financial exposure that doesn't match their declared government salary. Building this profile is an open-source and financial registry analytic task, it requires no HUMINT to initiate.

Officer Liability Build Steps	Exposure Channels
Build anomalous outflow profile from criminal actor finances, payments that don't fit operational cost profiles (hosting, tooling, affiliate splits) are protection payment candidates	FNS referral on lifestyle inconsistency, officer property holdings, vehicle registrations, children's school enrollment vs. declared government salary
Map officer family financial exposure: real estate in Russian registries (egrn.ru), corporate structures (egrul.nalog.ru), Western-held assets in EU property registries	Rosfinmonitoring flag on protection payment flows, feeds CBR 115-FZ freeze pipeline on officer-linked accounts
Surface officer-criminal financial relationship to competing FSB units via non-attributable channels, exploiting factional competition, not seeking unified FSB cooperation	Investigative journalism pipeline (OCCRP, Bellingcat, iStories, Meduza), domestic scandal framing without foreign government fingerprint
Simultaneous OFAC designation of officer and criminal network, eliminates reconstitution window; Western asset freeze plus correspondent banking pressure	Third-country legal pre-positioning, sealed indictments in viable European jurisdictions for officers with documented travel patterns

What Triggers FSB to Withdraw or Weaken Protection

FSB protection is not unconditional. These are the conditions under which it degrades:

- The protected actor's OPSEC failures create a documented link between a specific FSB unit and a high-profile operation, particularly U.S. critical infrastructure or healthcare, giving competing units leverage against that officer's unit
- The officer's financial exposure becomes visible in domestic Russian media or through FNS/Rosfinmonitoring processes, creates pressure on FSB leadership to demonstrate institutional integrity
- The actor repeatedly gets disrupted despite protection, makes the officer look ineffective and the protection relationship a waste of institutional resources

- The actor creates domestic harm that is visible enough to attract MVD attention, puts the protecting officer in the position of blocking domestic enforcement on behalf of a visibly harmful actor
- Kremlin signals the actor is a liability, typically follows regime-level embarrassment or diplomatic cost that exceeds the actor's strategic value

Do / Caution / Never

Do	Caution	Never
Route pressure through FNS and CBR, these are the vectors FSB cannot easily shield without political cost	Operations timed during active US-Russia diplomatic engagement windows carry elevated blowback risk	Never publicly attribute an actor known to hold FSB krysha before the protection relationship is weakened, attribution activates protection
Exploit the FSB/MVD rivalry: MVD has arrest incentives FSB doesn't always override for mid-tier actors	Investigative journalism exposure of officers carries medium blowback risk if the foreign government fingerprint is visible, minimize sourcing exposure	Never send formal extradition requests for FSB-shielded individuals as a primary lever, it signals foreign ownership of the case
Target mid-tier affiliates outside FSB protection to degrade RaaS recruitment pipelines	Simultaneous OFAC designation of officer and criminal network is medium-high risk, only viable after domestic framing is established	Never include FSB-adjacent names in MVD referral packages, FSB override is automatic
Build FSB officer financial profiles before engaging the criminal actor, protection layer first		Never sanction-name an actor without a downstream 115-FZ financial pipeline activation, public naming without financial friction is a warning signal that lets actors adapt
Use domestic harm framing in all referral products, tax fraud, organized crime, Russian citizen harm		Never frame referral products as counterintelligence or cybercrime, this triggers FSB review and potential protection activation
Surface officer liability to competing FSB factions, not to FSB leadership as an abstraction		

MVD / Department K, Ministry of Internal Affairs

MVD Department K is the highest-confidence actionable lever in this framework for mid-tier actor disruption. It's the primary domestic cyber enforcement body, but it operates under FSB override authority on anything deemed national security. That constraint is real, but it also has clear boundaries. For actors without confirmed FSB affiliation, MVD is responsive, quota-driven, and reachable through structured intelligence packages.

Post-2022, MVD enforcement has become more performative, arrests spike after major Western operations, but outcomes tend toward lenient sentences and early releases. The metric that matters is not conviction rate. It's forum fragmentation, affiliate panic, reconstitution delay, and operational tempo decline.

How MVD Operates Within the Protection Ecosystem

MVD sits below FSB in the ecosystem hierarchy. FSB can override MVD enforcement on any case it deems a national security matter, which in practice means any actor with RIS affiliation, current krysha, or strategic utility. Outside that protected tier, MVD operates with genuine arrest and prosecution authority.

- MVD enforces based on arrest and seizure metrics, quota pressure is a real institutional driver
- MVD is reputationally sensitive to domestic media scrutiny on cases involving Russian victims
- MVD has interagency rivalry with FSB, it will enforce where FSB has no stake, partly as a competitive dynamic
- FNS and Rosfinmonitoring referrals feed MVD without triggering FSB review, the domestic financial framing is the key
- MVD enforcement windows open after major Western operations, the 30-90 day window following a Western takedown or sanctions action is when MVD is most responsive to structured packages

MVD and BPH / IAB / Money Launderer Targeting

Bulletproof hosting providers, initial access brokers, and OTC money launderers sit in MVD's enforcement lane without FSB protection in most cases. These actors are the connective tissue of the ransomware ecosystem, and they are more accessible than the ransomware operators themselves.

Actor Type	MVD Enforcement Path	Why This Works
Bulletproof Hosting (BPH)	Art. 272 (illegal access) and Art. 273 (malware hosting), BPH operators are direct participants in the criminal infrastructure, not passive hosts	BPH operators rarely hold FSB krysha. They are commercial service providers to the criminal ecosystem. MVD can act without FSB override triggering.
Initial Access Brokers (IAB)	Art. 272 (unauthorized access) and Art. 159.6 (cyber fraud), IABs sell access to victim networks; criminal act is distinct from ransomware deployment	IABs are often mid-tier actors without protection. Disrupting the IAB market degrades RaaS affiliate capability without touching the protected ransomware core.
OTC Money Launderers	Art. 174.1 (money laundering) and Art. 198 (tax evasion), OTC brokers	OTC brokers are the most financially exposed actors in the ecosystem. They

	converting ransomware BTC to rubles are primary financial criminal targets	touch both the criminal and legitimate banking systems, creating maximum enforcement leverage.
Mule Networks	Art. 158/160 (theft/embezzlement) and Art. 210 (organized crime) when network structure is documented	Mule recruiters and operators are domestic Russian targets with clear domestic victim harm framing, exactly what MVD responds to.

Enforcement Pattern, Post-2022

Case	Date	MVD Action	Outcome / Insight
REvil	Jan 2022, Jun 2025	14 arrests, 25 sites raided, $5.6M seized	Time served / releases, US-responsive but performative. FSB hand visible in releases.
Ferum / Sky-Fraud	Feb 2022	Domains seized, 6 arrested	Mid-tier disruption. Forum ecosystem fragmented for 30-60 days.
Cryptex / PM2BTC (Op. Endgame)	2024	100+ arrests, $16M seized, Ivanov detained	Post-Western optics. MVD enforcement window exploited correctly.
Evil Corp (legacy)	2019+	Mid-tier arrests only	Yakubets untouchable, FSB family protection. MVD ceiling is clear here.

Do / Caution / Never

Do	Caution	Never
Deliver structured intelligence packages via FBI/NCA liaisons framed as laundering and tax evasion, not cybercrime	Avoid joint public announcements with MVD on ongoing operations, operational security degrades rapidly	Never include FSB-shielded actor names in MVD referral packages, FSB override is automatic and burns the package
Time referrals to coincide with post-Western-enforcement windows (30-90 days after major Western action)	Avoid over-relying on conviction rates as the measure of success, measure forum fragmentation and reconstitution delay instead	Never expect MVD to enforce against Kremlin-signaled assets regardless of evidence quality
Target BPH, IAB, and OTC broker networks explicitly, these sit in MVD's lane without FSB override in most cases	MVD enforcement windows are time-limited; packages delivered outside those windows get less traction	Never use MVD channels for actors with confirmed GRU or SVR nexus
Use Art. 159 (fraud) and Art. 174.1 (laundering) framing, maximizes MVD jurisdiction, minimizes FSB interest		Never treat an MVD arrest as an endpoint, without sustained follow-on pressure, reconstitution happens within 30-90 days
Frame all products around Russian victim harm and domestic revenue loss		

Identify actors explicitly without FSB affiliation in shared products, removes FSB override justification		

Rosfinmonitoring, Federal Financial Monitoring Service

Rosfinmonitoring is Russia's Financial Intelligence Unit and the primary domestic node for mapping crypto-to-fiat laundering flows. It doesn't make arrests. What it does is feed the CBR and MVD pipelines that create financial friction and enforcement referrals. Its Egmont membership was suspended in December 2022, which cut off direct Western FIU intelligence exchange, but its domestic institutional incentives remain strong independent drivers.

The core analytical value here is the pipeline it sits in: blockchain intelligence → Rosfinmonitoring flag → CBR 115-FZ freeze → MVD referral. Rosfinmonitoring is the node that connects crypto-chain analytics to domestic Russian enforcement. Treat it as a mapping and routing node, not an enforcement body.

How Rosfinmonitoring Intersects the Ransomware Protection Structure

- Mandatory reporting from VASPs and banks on transactions over 600K RUB feeds the FIU database, post-2024 VASP regulations expanded this significantly
- Ransomware proceeds converting BTC to rubles through OTC brokers generate transaction patterns that meet 115-FZ suspicious transaction thresholds
- Rosfinmonitoring flags feed CBR for banking-level freezes and MVD for criminal referrals, neither requires a court order at the flagging stage
- The Egmont suspension limits direct Western FIU-to-FIU exchange, but the Belarus FIU remains the only credible back-channel to Rosfinmonitoring post-2022
- Rosfinmonitoring has genuine domestic institutional motivation: ransom proceeds draining the ruble economy, sanctions evasion overlap, and regime stability concerns all align with its mandate

> **Structural Constraint Note (cross-reference EDP Module 14):** The pipeline described above reflects Rosfinmonitoring's theoretical function and domestic incentive structure. EDP Module 14 assesses this pathway as structurally constrained in practice for ransomware-connected flows for two reasons: first, Rosfinmonitoring operates within the same state protection framework (Dark Covenant) that provides implicit tolerance for high-value ransomware operators; second, Russian financial intelligence cooperation has historically been selectively responsive, actionable for cases the Kremlin wants pursued, not for protected actors. Treat Rosfinmonitoring as a routing node and formal channel to maintain, not as a reliable primary disruption mechanism for ransomware-connected flows. [ANALYST INFERENCE]

OTC Broker and Money Launderer Coverage

OTC brokers are Rosfinmonitoring's most actionable targets in the ransomware ecosystem. They sit at the intersection of the crypto and ruble economies, and their transaction patterns are exactly what 115-FZ is designed to surface.

Exploitation Approach	Mechanism / Note
Map BTC → mixer → OTC → ruble account chains using blockchain analytics (Chainalysis, TRM, Elliptic). The OTC broker node is the highest-value	OFAC designation of OTC brokers triggers correspondent banking pressure on the same

designation target, it serves multiple ransomware actor flows simultaneously.	accounts that Rosfinmonitoring flags domestically, the two pipelines reinforce each other
VASP KYC pressure forces exchange-level reporting into Rosfinmonitoring's database, even exchanges outside Russian jurisdiction that touch Russian-linked wallets create reporting obligations for Russian-regulated counterparties	Frame all intelligence products as domestic Russian financial harm, 'ransom proceeds draining domestic capital' lands better institutionally than any foreign victim framing
Use the Belarus FIU as the primary back-channel to Rosfinmonitoring. Belarus remains an Egmont member and operationally connected to Russian financial intelligence despite Union State status on enforcement.	Kazakhstan FIU is a secondary Egmont-adjacent channel, Kazakhstan has demonstrated actual enforcement cooperation on specific CIS cybercrime cases

Do / Caution / Never

Do	Caution	Never
Map BTC → OTC → ruble flows via blockchain analytics; deliver clusters to FinCEN and OFAC for VASP action that forces domestic Rosfinmonitoring visibility	Rosfinmonitoring is a mapping and exposure node, don't expect arrest referrals from it alone; it needs MVD or CBR to produce enforcement outcomes	Never attempt direct Egmont-channel requests to Rosfinmonitoring post-December 2022 suspension, requests will be ignored and will degrade back-channel credibility
Use Belarus FIU as the primary back-channel to Rosfinmonitoring post-Egmont suspension	The Belarus FIU back-channel is fragile, one clumsy referral that exposes Western sourcing kills it	Never attribute Rosfinmonitoring-sourced intelligence in shared LE products, eliminates the domestic incentive for continued operation of the channel
Frame all financial intelligence as domestic Russian harm, revenue loss framing outperforms counterintelligence framing		Never approach Rosfinmonitoring on FSB/GRU-shielded actors, referrals will be blocked at the political level
Pair Rosfinmonitoring exposure with CBR 115-FZ pipeline, Rosfin flags enable CBR freezes without prosecution		
Target OTC broker networks with OFAC designations that reinforce domestic 115-FZ scrutiny on the same accounts		

CBR, Central Bank of Russia

The Central Bank of Russia is not a ransomware enforcer. It's a financial control mechanism that can be used to create friction against ransomware cashout operations without naming individuals, without court orders, and without triggering FSB protection reflexes. That makes it the stealthiest disruption vector in the framework. Structural update (February 2026): FSB demanded that major Russian banks install SORM equipment on their mobile applications, classifying bank apps as "organisers of the distribution of information" under Russian communications law. Banks that refused were removed from the whitelist of services permitted to function during FSB-directed mobile internet shutdowns. This creates a new dependency: Russian banks now operate within the same SORM compliance architecture as telecoms, which means FSB has intercept access to bank application traffic in addition to the 115-FZ financial friction mechanisms already covered here. The pipeline from Rosfinmonitoring flag to CBR 115-FZ freeze is unchanged, but the SORM layer adds a parallel FSB visibility channel into domestic financial institution communications that did not exist before 2026.

The mechanism: ransomware actors must convert BTC proceeds to rubles to access the Russian domestic economy. That conversion, typically through OTC brokers and CIS-linked exchanges, is the point of maximum vulnerability. A Rosfinmonitoring flag on the destination ruble account triggers a CBR 115-FZ instruction to the receiving bank. The bank freezes the account. No arrest, no prosecution, no public naming, no FSB trigger.

115-FZ as a Disruption Tool

- Banks report transactions over 600K RUB flagged as suspicious; CBR can order blocking without court process
- Extended to VASP transactions post-2022, directly intersects ransomware ruble inflows
- War sanctions evasion context has heightened CBR AML scrutiny across the board, ransomware actors using the same crypto-fiat infrastructure as sanctions evaders face collateral friction
- No attribution required, the friction registers as a compliance action, not a law enforcement action
- CBR's institutional motivation is genuine: correspondent banking relationships with Western banks are the CBR's primary vulnerability to external pressure, and it actively seeks to protect them

The Pipeline

CBR doesn't generate its own intelligence. It acts on Rosfinmonitoring flags and correspondent banking pressure. The pipeline looks like this:

BTC Payment	Rosfin Flag	CBR 115-FZ	Bank Freeze
Ransom → mixer → OTC broker conversion to rubles	Transaction cluster identified as suspicious under 115-FZ thresholds	CBR instructs receiving bank to freeze without court order	Actor cannot access proceeds. No public naming. No FSB trigger.

Correspondent Banking Pressure

CBR's external vulnerability is correspondent banking relationships with Western financial institutions. This is the external pressure lever that reinforces the domestic 115-FZ pipeline:

- OFAC designation of OTC brokers and CIS-linked exchanges triggers de-risking by Western correspondent banks, CBR-supervised Russian banks that rely on those relationships have strong institutional incentive to comply with 115-FZ more aggressively
- FATF grey-listing pressure on Russia creates compliance burden that increases CBR AML scrutiny across all suspicious transaction categories, ransomware cashout flows benefit from this collateral friction
- This track does not require Russian cooperation, it operates through Western financial system control points

Do / Caution / Never

Do	Caution	Never
Build the blockchain → Rosfinmonitoring → CBR pipeline: cluster identification feeds VASP sanctions which feed domestic 115-FZ flags	CBR will not enforce against FSB/GRU-protected actors at the political level, the mechanism works for mid-tier and infrastructure actors, not for krysha-protected core groups	Never attempt direct engagement with CBR via diplomatic channels for ransomware purposes, wrong lever, counterproductive
Use OFAC designations on OTC brokers as the trigger for CBR correspondent banking scrutiny, no direct CBR engagement needed	Correspondent banking pressure takes time to produce friction, build the pipeline early, not as a last step	Never sanction-name actors without activating the downstream 115-FZ plan simultaneously, public naming without financial pipeline activation is a warning signal that lets actors move assets before the freeze lands
Exploit the sanctions evasion / ransomware infrastructure overlap, CBR's post-2022 AML posture creates broader friction		
Measure effectiveness via ruble inflow disruption, OTC broker network reconstitution timelines, and VASP compliance reports		

FNS, Federal Tax Service

FNS is the highest-confidence, lowest-blowback domestic lever in the framework. Tax exposure doesn't trigger FSB protection reflexes the way cybercrime attribution does. It exploits a structural gap between what an actor earns from ransomware and what they can declare to the Russian tax authority, and that gap is enormous for most mid-to-high-tier actors living in Russia.

FNS has no arrest power. Its value is as an exposure and referral node that feeds MVD without geopolitical sensitivity, and as a domestic harm framing tool that makes actors liabilities to the Russian state rather than assets of it.

How FNS Creates Pressure on Protected Actors

Ransomware actors living in Russia must spend their proceeds domestically. Real estate, vehicles, business ownership, and consumer spending all create a financial footprint that FNS digital audits can surface. The gap between declared income, often zero or minimal, and visible assets constitutes the basis for an Art. 198 referral without requiring any attribution of the underlying ransomware activity.

- Post-2022 war economy pressures have heightened FNS institutional motivation, domestic revenue protection is a genuine driver, not just a framing convenience
- FNS digital audit platform (nalog.ru) has expanded significantly, cross-referencing property registries, corporate ownership, and banking records is now largely automated
- Shell company and front business exposure through Art. 199 (organizational tax evasion) is a separate but parallel track, corporate registry analysis (egrul.nalog.ru) surfaces nominee-held entities
- FNS referrals to MVD for laundering charges (Art. 174.1) do not require FNS to identify the predicate cybercrime, laundering of unspecified proceeds is sufficient to open an MVD file

FNS and the Public Outing Track

FNS lifestyle data, property holdings, vehicle registrations, corporate interests, is also the raw material for investigative journalism exposure of cybercriminal actors and their FSB handlers. The Conti/Nefedov model demonstrated how domestic financial misconduct exposure through journalism channels creates domestic embarrassment that FSB cannot easily suppress without acknowledging the underlying relationship.

- Build the lifestyle intelligence package from open Russian registries before approaching any referral channel
- FNS referral and investigative journalism exposure are complementary, the referral creates a domestic paper trail; the journalism creates public pressure that makes ignoring the paper trail politically costly
- The FSB officer liability track (see FSB section) uses the same FNS methodology applied to the protecting officer rather than the criminal actor, lifestyle inconsistency on a government salary is the entry point

Do / Caution / Never

Do	Caution	Never
Use FNS as the primary domestic prosecution pathway that bypasses FSB protection, tax referrals don't carry counterintelligence sensitivity	FNS enforcement alone won't produce incapacitation, it is a friction and exposure node that feeds MVD; plan for the full chain	Never frame FNS referral products as counterintelligence or cybercrime products, this triggers FSB review and potential protection activation
Build lifestyle intelligence packages from open Russian registries: property records, vehicle registrations, corporate interests, travel patterns	FNS referrals require political greenlight at senior levels for actors with any regime-adjacent relationships, don't expect automatic action	Never deliver FNS-destined intelligence through channels that expose Western sourcing, domestic framing only
Route through Rosfinmonitoring → MVD chain using laundering statutes (Art. 174.1) when prosecution is the goal, FNS feeds the referral		Never approach FNS on FSB-integrated actors with regime-level political cover, the referral will be blocked
Apply the same FNS methodology to FSB officer targets, lifestyle inconsistency on a government salary is the entry point for the officer liability track		
Use corporate registry analysis (egrul.nalog.ru) to surface front companies and shell structures under Art. 199		

GRU, Main Directorate of the General Staff

The GRU section serves as a scope boundary for this framework as much as it serves as an analytical target. GRU-nexus actors are not accessible through the domestic Russian institutional levers that make up the rest of this document. Understanding who falls into GRU overlap, and recognizing it early, is operationally critical precisely because the approach for those actors is fundamentally different.

GRU's relationship with ransomware differs from FSB's krysha model. GRU does not recruit and protect criminal freelancers the same way. It deploys cybercrime capabilities as strategic military tools, particularly destructive operations (NotPetya, wiper campaigns) using ransomware-style deployment as cover. The actors are state employees, not co-opted civilians.

GRU Ecosystem Intersection Points

Intersection Type	Description	Implication
Shared Infrastructure	BPH providers, VPN layers, and OTC exchanges used by criminal ransomware groups are shared with GRU operational toolchains. The same infrastructure nodes serve both.	Infrastructure takedowns affect both. This is a feature, not a complication, target the node, not the user.
Ransomware as Cover-for-Action	GRU units (Sandworm / Unit 74455) deploy ransomware-style tools for destructive operations framed as criminal ransomware. NotPetya is the canonical case.	Technical attribution of 'ransomware' ops as GRU destructive ops shifts legal framing from criminal to state-sponsored, enabling different escalation paths.
IAB Market Overlap	GRU operators purchase or exchange network access from criminal initial access brokers, the same brokers supplying ransomware affiliates.	IAB networks are legitimate criminal enforcement targets regardless of who the downstream buyer is.
Wartime Absorption	Criminal actors whose targeting patterns align with active Russian military objectives may have been operationally absorbed into GRU wartime operations.	These actors fall outside this framework. Flag separately for state-sponsored track. Indicators: NATO/Ukrainian infrastructure targeting, targeting aligned with active military objectives.

Do / Caution / Never

Do	Caution	Never
Target shared infrastructure nodes, disrupts GRU and criminal operations simultaneously without direct confrontation	Don't conflate GRU destructive operations with profit-motivated ransomware in analytical products, the distinction matters for legal framing and escalation authority	Never attempt to use Russian domestic channels (MVD, FNS, CBR) against GRU-nexus actors, no domestic lever applies to state employees

Use GRU attribution to shift criminal cases to state-sponsored legal framing, unlocking different escalation paths and legal tools	Infrastructure nodes shared between GRU and criminal actors may encounter harder resistance to takedown, factor this into operational planning	Never expose GRU-linked HUMINT sources via shared LE referral products without strict IC compartmentation
Target IAB networks as criminal enforcement targets, the downstream GRU buyer doesn't change the criminal act of the IAB		Never assume GRU protection operates like FSB krysha, the mechanism is different, the intervention logic must follow
Document actor targeting patterns to identify wartime absorption indicators early, flag these cases before engaging domestic Russian levers		

SVR, Foreign Intelligence Service

SVR has a lower direct footprint in ransomware operations than FSB or GRU, but it intersects the ecosystem through infrastructure overlap and the initial access broker market. SVR's primary cyber operations target government, defense, and diplomatic networks (APT29 / Cozy Bear / SolarWinds). Like the GRU section, this primarily serves as a scope boundary, but the IAB market overlap makes it relevant for analysts building infrastructure and access broker targeting packages.

SVR Ecosystem Intersection Points

Intersection Type	Description	Implication
IAB Market Overlap	SVR operators purchase network access from criminal IABs, the same brokers supplying ransomware affiliates. The criminal act of the IAB is the same regardless of buyer.	IAB networks remain legitimate criminal enforcement targets.
Infrastructure Overlap	BPH providers, anonymization layers, and VPN infrastructure are shared between SVR operational toolchains and criminal ransomware actors.	Infrastructure takedowns affect both. Document SVR indicators to inform IC compartmentation before sharing with LE partners.
Personnel Proximity	Cybercriminals with SVR connections have been identified. SVR does not actively protect them the way FSB does krysha, but it does not expose them either.	Limited sourcing. Treat with caution in analytical products.

Do / Caution / Never

Do	Caution	Never
Use SVR supply chain operations as legal basis for broader infrastructure takedowns affecting shared criminal/SVR nodes	Don't attribute SVR and ransomware actors in the same public product unless the technical basis is solid, conflation weakens both cases	Never use Russian domestic channels against SVR-linked actors, same scope boundary as GRU
Target IAB networks as criminal enforcement, SVR buyer overlap doesn't change the criminal act	Don't approach SVR-adjacent infrastructure takedowns without IC compartmentation review	Never expose SVR overlap indicators in shared LE products without IC compartmentation review
Track infrastructure overlaps via technical indicators; share through IC channels, not LE channels		

Integrated Disruption Strategy

The entity sections above are most valuable when applied as a coordinated framework, not as isolated actions. This section describes the compounding feedback loop, the three referral tracks, and the measurement framework that ties everything together.

The Compounding Feedback Loop

Each pressure cycle strengthens the next. This is the mechanism that turns individual actions into ecosystem degradation:

Criminal-side financial pressure
→ Anomalous outflow identification (protection payment candidates surface)
→ FSB officer financial profile built from open registries
→ FNS referral + investigative journalism exposure of officer
→ Domestic liability created for officer within FSB factions
→ Protection relationship weakens or collapses
→ Criminal actor becomes accessible to MVD enforcement
→ MVD enforcement generates more intelligence on financial flows
→ **Stronger anomalous outflow identification on successor actors**
Repeat. Each cycle strengthens the next.

The Three Referral Tracks

Three parallel tracks, operated simultaneously, produce compounding pressure without triggering FSB protection reflexes:

Track	Mechanism	Key Note
Track 1 115-FZ Fraud Framing	RF Criminal Code Arts. 159-159.6 (fraud) → FNS → MVD. Ransomware actors reframed as domestic fraudsters, avoids political protection triggers.	Fraud framing is the key. It does not carry the geopolitical sensitivity of 'cybercrime against Western victims' and is harder for FSB to shield institutionally.
Track 2 Egmont FIU Back-Channel	Belarus FIU (only credible backdoor to Rosfinmonitoring post-2022 Egmont suspension) → Rosfinmonitoring → CBR/MVD pipeline.	Belarus is the sole remaining Egmont-adjacent channel to Rosfinmonitoring. Kazakhstan FIU is secondary. Direct Egmont requests to Rosfinmonitoring are suspended and unproductive.
Track 3 FATF / Correspondent Banking	OFAC VASP designations → FATF grey-listing pressure → correspondent banking de-risking → CBR 115-FZ scrutiny on flagged ruble accounts.	Doesn't require Russian cooperation. Operates through Western financial system control points. Creates collateral friction against ransomware and sanctions evasion infrastructure simultaneously.

Measurement Framework

Don't measure effectiveness by Russian prosecution or conviction rates. Measure by ecosystem health indicators:

Indicator	What It Measures	Collection Method
Forum fragmentation and affiliate panic posts	MVD enforcement effectiveness on mid-tier	Dark web monitoring
RaaS affiliate reconstitution delay (target: 30-90 days)	Depth of disruption vs. cosmetic action	HUMINT, forum analysis
Ransom payment volume (quarterly)	Financial pressure effectiveness	Chainalysis, TRM quarterly
OTC broker network disruption and migration patterns	CBR 115-FZ pipeline effectiveness	VASP intelligence, on-chain analytics
Victim breach reports post-operation	Operational tempo of targeted groups	CISA, IC3, industry partners
Ruble account freeze rate on flagged wallets	Rosfinmonitoring → CBR pipeline output	FinCEN, VASP cooperation reports
Protection relationship reconstitution (who fills the vacated FSB handler role and how fast)	Whether protection layer disruption is producing lasting degradation or just transitions	HUMINT, dark web monitoring, financial pattern analysis

Quick Reference

Entity	Protection Role	Best Lever	Never Do	Actionability
FSB	Recruits, shields, tasks elite actors via krysha	FNS/CBR routing; FSB/MVD rivalry exploitation; officer liability track	Publicly attribute FSB-shielded actors before protection is weakened	Low (direct) High (indirect)
MVD / Dept K	Domestic enforcer; FSB-constrained on protected actors	Intel packages + tax/fraud framing; BPH/IAB/OTC targeting; post-Western-op enforcement windows	Include FSB-shielded names in referral packages	**High (mid-tier + infrastructure)**
Rosfinmonitoring	FIU maps crypto-fiat flows; feeds CBR and MVD	Blockchain clusters → VASP sanctions → 115-FZ flags; Belarus FIU back-channel	Direct Egmont requests post-suspension; exposing sourcing	**High (mapping and pipeline)**
CBR	115-FZ banking controls; non-attributable friction without court orders	OFAC OTC designations → correspondent banking → 115-FZ freeze pipeline	Naming actors without simultaneously activating the pipeline	**High (stealth)**
FNS	Tax exposure; lifestyle vs. income gap; feeds MVD without FSB trigger	Lifestyle intel packages + domestic harm framing → MVD referral via Art. 198/199; officer liability track	Frame FNS products as counterintelligence or cybercrime	**High (lowest blowback)**
GRU	Deploys cybercrime as military tool; wartime absorption of criminal actors	Target shared infrastructure; use GRU attribution for state-sponsored legal framing; IAB network targeting	Use domestic Russian channels against GRU-nexus actors	Low (direct) Med (shared infra)
SVR	Infrastructure and IAB market overlap; indirect ransomware footprint	IAB network targeting; infrastructure takedowns via supply chain legal basis	Expose SVR overlap indicators without IC compartmentation review	Low-Med