INSIDE THE MACHINE

Russia's Cyber Services, Criminal Networks, and the Ecosystem That Makes It All Work

Version 0.3 | April 2026

A Deep-Dive Analytic Reference for Professional Investigation and Intelligence Work

How to read this document

Each section leads with narrative analysis, then provides reference tables and case detail. Read the opening paragraph of each section for the essential picture. Read deeper for operational specifics. Every major section ends with a 'So What' subsection covering leverage points, weaknesses, and how the analysis can be applied.

Part One

The Model: Why Russia's Approach Is Different From Everyone Else's

Understanding the Russian Cyber Ecosystem

The most common mistake Western analysts make is treating Russia's cyber activity as a government program. It is not, not entirely. China has a relatively centralized, bureaucratically managed cyber apparatus. North Korea uses cyber almost purely as revenue. Iran is somewhere in between. Russia is different: it operates an ecosystem, a layered, partially decentralized set of relationships between state intelligence services, military units, private contractors, criminal organizations, and individual hackers who occupy all points on the spectrum from state employee to free agent.

The system works because of how it distributes risk and concentrates deniability. When the GRU's Unit 74455 launches NotPetya and causes $10 billion in global damage, that is a direct state military operation. When an FSB officer quietly signals to a ransomware operator that he will stay out of trouble as long as he does not hit Russian targets, that is an informal protection arrangement that costs the state nothing and provides it with a reserve of talent, access, and cover. Both exist. Neither invalidates the other.

Understanding this requires abandoning binary thinking. Not every Russian hacker is state-controlled. Not every ransomware gang is a GRU front company. But the state has created conditions in which criminal operators can thrive, and in which the most capable among them often end up in some kind of relationship with a service, whether because they were recruited, coerced, caught and flipped, or simply decided that getting a security clearance was better than risking arrest.

The Five-Layer Model

Think of the Russian cyber ecosystem as five layers that interact continuously but are not the same thing. Confusing them is the most common analytical error.

Layer	Who / What It Is
1. Presidential Authority	The Kremlin, Security Council, and Presidential Administration. This layer does not manage operations day-to-day. It sets strategic priorities, approves high-risk operations, and creates the political conditions under which criminal actors are tolerated or protected.
2. Service Mandates	FSB, GRU, and SVR with their legal authorities and institutional missions. Each has a distinct mandate and risk appetite. The FSB owns domestic surveillance and criminal-intel relationships. The GRU conducts offensive military operations. The SVR collects foreign civilian intelligence.
3. Operational Units and Contractors	Named units (Center 16, Center 18, Unit 26165, Unit 74455), their officers, and the contractor ecosystem (NTC Vulkan and similar firms) that provides engineering capacity and plausible separation from uniformed military personnel.

4. Law Enforcement and Control Infrastructure	MVD/Department K controls the domestic enforcement valve. SORM (FSB-managed intercept hardware at ISPs), Roskomnadzor/TSPU (internet traffic control), and FSTEC (certification chokepoint) provide the legal and technical architecture within which operations occur.
5. Criminal Actors	Ransomware operators, financial fraud crews, initial access brokers, bulletproof hosting providers, and carders operating in a managed protection relationship with the state. Some are directly tasked (Yahoo case). Most operate under tacit non-enforcement in exchange for target discipline and occasional cooperative work.

How the Kremlin Layer Actually Works

The Kremlin layer is the most analytically underspecified part of most public accounts of Russian cyber activity. This is partly because it operates with minimal direct fingerprint on individual operations, and partly because the relevant decision-making happens inside institutions (the Security Council, the Presidential Administration) that generate almost no open-source documentation.

The Security Council of Russia (Sovet Bezopasnosti) is the primary mechanism through which the President coordinates between the FSB, GRU, SVR, and MVD on matters of national security, including cyber operations. The Security Council Secretariat drafts doctrine documents including Russia's Information Security Doctrine (last updated 2016) and the National Security Strategy. These documents are not operational orders; they are the framework within which operational priorities are set.

The Presidential Administration, specifically the Department for Interagency Coordination on Security Issues, translates Security Council priorities into operational guidance for the services. Key advisors with direct access to Putin on cyber and information security matters have historically included figures from the FSB and SVR, which partly explains why those services have had more institutional influence over cyber policy than the GRU.

The operational implication is that major cyber operations, particularly those with significant escalation potential or international political exposure, require authorization above the service level. The GRU does not independently decide to interfere in a US presidential election or launch a wiper attack against a NATO member. Those decisions involve Presidential Administration and Security Council visibility. What the Kremlin layer provides is authorization, strategic direction, and the political cover that allows protected criminal actors to operate.

Political Objectives Driving Major Operations

The following operations illustrate how each layer of the model connects to Kremlin-level political objectives.

Operation	Year(s)	Service	Political Objective	Criminal Layer
Crimea / Donbas cyber ops	2014-2015	GRU / FSB	Support military operation; suppress Ukrainian C2; shape information environment	Minimal; primarily uniformed units

Operation	Year(s)	Service	Political Objective	Criminal Layer
2016 US Election Interference	2016	GRU (Unit 26165)	Destabilize US political process; damage Clinton candidacy; sow distrust in democratic institutions	Indirect: criminal infrastructure used for operational cost laundering
Ukraine Power Grid Attacks	2015-2016	GRU (Unit 74455)	Demonstrate critical infrastructure attack capability; pressure Ukraine government; test ICS-targeting malware	None documented
NotPetya	2017	GRU (Unit 74455)	Destroy Ukrainian financial and logistics infrastructure; maximum economic disruption	None; purely military operation with criminal-style cover
SolarWinds	2020	SVR (APT29)	Strategic intelligence collection on US government COVID response, sanctions policy, and diplomatic communications	None; SVR does not use criminal proxies
2022 Invasion Cyber Campaign	2022-ongoing	GRU / FSB	Pre-invasion disruption of Ukrainian government/military; ongoing information and infrastructure attacks	Patriotic hacker groups (Killnet, XakNet) used for information operations; not direct operations

Why the Criminal-Intel Overlap Exists

Intelligence services value criminal hackers for three things: access they already have (botnet infrastructure, ransomware tooling, compromised corporate networks), deniability if operations are exposed, and speed, because recruiting and training a government officer to do what a skilled criminal already does takes years. The criminal gets protection from domestic prosecution and sometimes direct payment. The state gets capability and cover.

The arrangement is not always clean or explicit. In many cases it works through tacit understanding: do not attack Russian targets, do not embarrass the Kremlin, and nobody will come looking for you. In a smaller number of documented cases it is very explicit, with named FSB officers directing specific operations, paying contractors, and providing intelligence-collection tasking. The Yahoo case is the best documented example of the explicit model. Evil Corp is the best documented example of the hybrid model, where a criminal organization gradually acquired state alignment without becoming a formal state unit.

The Structural Insight

This is not a bureaucratic program with a director and a budget line. It is organic. An FSB officer who knows a criminal hacker might reach out for a favor. A criminal who gets arrested might be offered a deal. A hacker building capability an intelligence service values might simply be told that his operations have been noted and he should continue. None of these require a formal memorandum of understanding. All of them are real patterns visible in documented cases.

Part Three

GRU: The Arsonists

General Intelligence Directorate (GRU / GU)

If the FSB is the service that manages the ecosystem, the GRU is the service that blows things up. It is Russia's military intelligence organization, and its cyber units have been responsible for some of the most aggressive, destructive, and consequential operations in the history of state-sponsored hacking. Two units dominate the public picture: Unit 26165 (APT28, Fancy Bear), which specializes in political espionage and election interference, and Unit 74455 (Sandworm), which specializes in destroying things.

The GRU's institutional culture is different from the FSB's. Where the FSB tends toward long-term cultivation and deniability, the GRU has repeatedly shown a preference for decisive, aggressive action even when attribution was nearly certain. The GRU officers who hacked the DNC, interfered in the 2016 US election, and launched NotPetya have all been named in US indictments. The GRU kept operating anyway, which tells you something about how it weighs operational effect against exposure cost.

GRU Cyber Operations: Timeline Against Political Context

The single most important analytical point about GRU cyber operations is that they do not occur in a vacuum. Each major operation corresponds to a specific military or political event and reflects a decision to use cyber as a tool of statecraft in support of kinetic objectives or political influence. The following timeline makes those connections explicit.

Period	Geopolitical Context	GRU Cyber Operation	Objective
2014 (Feb-Mar)	Crimea annexation; Ukrainian government transition	DDoS and disruption operations against Ukrainian C2 and communications; GRU officer-directed social media manipulation	Degrade Ukrainian government coordination; support rapid military seizure; suppress Ukrainian response
2014-2015	Donbas armed conflict; Minsk I negotiations	BlackEnergy 3 deployment against Ukrainian energy and government networks; persistent access establishment	Maintain pressure on Kyiv; demonstrate capability for infrastructure disruption; build ISC targeting expertise
2015 Dec	Ongoing Donbas conflict; Western sanctions pressure	First Ukraine power grid attack (Industroyer v1 precursor): 225,000 customers lose power in western Ukraine	Demonstrate ability to cause physical-effect harm; test ICS-targeting toolset; pressure Poroshenko government
2016 Dec	US election interference complete; NATO expansion debate	Second Ukraine power grid attack (Industroyer): Kyiv substation attacked on Dec 17; power disrupted	Operational test of mature Industroyer; demonstrate sustained capacity; timed to cover period of maximum US political distraction

Period	Geopolitical Context	GRU Cyber Operation	Objective
2016 (full year)	US presidential election; Clinton vs Trump	Unit 26165 compromise of DNC, DCCC, Podesta email; DCLeaks and WikiLeaks distribution pipeline established	Damage Clinton candidacy; sow distrust in US electoral system; generate divisive information environment
2017 Jun	Post-Minsk II stalemate; Macron election in France	NotPetya: MEDoc software supply chain used to deploy wiper against Ukrainian financial infrastructure; spreads globally causing $10B+ damage	Destroy Ukrainian financial and logistics capacity during armed conflict; global spread may have been deliberate escalation signal
2018 Feb	Winter Olympics in Pyeongchang; Russia banned from competing	Olympic Destroyer: false-flag attack on Olympics IT infrastructure on opening night; initially framed to appear as North Korean or Chinese	Disrupt event; retaliate for Olympic ban; demonstrate capacity for false-flag deception against attribution community
2022 Feb	Russian full-scale invasion of Ukraine begins	AcidRain wiper destroys Viasat KA-SAT modems across Europe; WhisperGate/HermeticWiper deployed against Ukraine government; Industroyer2 attempted against power grid	Pre-invasion disruption of Ukrainian C2 and communications; degrade military coordination; demonstrate willingness to attack European infrastructure

Unit 26165: The Political Hackers (APT28 / Fancy Bear)

Unit 26165 operates out of Komsomolsky Prospekt 20 in Moscow. Its threat actor cluster goes by many names: APT28 (Mandiant), Fancy Bear (CrowdStrike), Sofacy (Kaspersky), Pawn Storm (Trend Micro), Strontium or Forest Blizzard (Microsoft). The naming proliferation reflects different research teams discovering the same group through different incident responses over many years.

The unit's focus is political espionage: governments, militaries, political parties, think tanks, journalists, and opposition figures. Its most famous operation was the 2016 compromise of the Democratic National Committee and Clinton campaign chairman John Podesta, with exfiltrated emails distributed through DCLeaks and WikiLeaks. But the DNC was not a one-off. It was part of a years-long campaign targeting political organizations across Europe and North America that had been running since at least 2014, including the Bundestag hack (2015), the French election targeting (2017), and ongoing NATO member government network compromises.

The APT28 Toolset

Tool Name	Also Known As	Platform	Primary Function
X-Agent	Sofacy, CHOPSTICK	Windows, Linux, iOS	Keystroke logging, file theft, persistent access; custom C2 protocol; developed and maintained by Lt. Nikolay Kozachek (Mueller indictment)
X-Tunnel	CORPIDROX	Windows	Encrypted C2 channel; wraps traffic in TLS to blend with legitimate traffic

Tool Name	Also Known As	Platform	Primary Function
GAMEFISH / Seduploader	SEDNIT	Windows	Reconnaissance dropper; fingerprints targets before deploying full implants
Drovorub	(NSA/FBI attribution)	Linux	Kernel-level rootkit; file transfer, port forwarding, near-invisible persistence; jointly attributed NSA/FBI 2020
Zebrocy	Zekapab	Windows	Phishing-delivered dropper; used extensively against NATO member states and CIS targets
MASEPIE	(CISA 2024)	Multiple	Python-based implant; used in recent NTLM relay and credential harvesting campaigns
HeadLace	(Microsoft 2023)	Windows	Modular backdoor; used in post-2022 campaigns targeting Ukrainian military and government networks

Named Officers (Mueller Indictment, July 2018)

The July 2018 Mueller indictment named 12 GRU officers from Unit 26165 by name, rank, and specific operational role. This level of public attribution is rare in intelligence history. All 12 remain at large in Russia but face arrest in any country with a US extradition treaty.

Name	Rank / Role	Specific Attribution
Boris Antonov	Lieutenant Colonel; section head	Supervised hacking team that targeted DCCC and DNC; overall operational supervisor for US election interference
Dmitriy Badin	Captain; officer	DNC hack operations; Germany issued separate arrest warrant for his role in the 2015 Bundestag hack
Ivan Yermakov	Lieutenant; officer	Reconnaissance operations against US election infrastructure; WADA hack
Aleksey Lukashev	Captain; officer	Spearphishing operations against Clinton campaign; authored phishing emails
Sergey Morgachev	Lieutenant Colonel; commander	Supervised X-Agent malware development team; managed technical infrastructure
Nikolay Kozachek	Lieutenant Captain; malware developer	Personally developed and maintained X-Agent implant; core technical architect
Pavel Yershov	Senior Lieutenant; officer	Infrastructure management; server registration and maintenance
Artem Malyshev	Senior Lieutenant; officer	Infrastructure management; monitored X-Agent deployments on victim networks
Aleksandr Osadchuk	Colonel; commanding officer	Commanded Unit 26165 at time of DNC and election operations

Unit 74455: The Wrecking Crew (Sandworm)

Unit 74455 operates from Khoroshevskoye Shosse 76 in Moscow, and it is responsible for more destructive cyberattacks than any other state actor in history. Its designations include

Sandworm (iSight/FireEye), Voodoo Bear, IRIDIUM, Seashell Blizzard (Microsoft current), and APT44 (Mandiant 2024, signaling elevated threat status). It is the unit behind the 2015 to 2016 Ukraine power grid attacks, NotPetya, Olympic Destroyer, and Industroyer2.

Sandworm's operational signature is that it does not care about collateral damage. NotPetya was designed to destroy Ukrainian financial infrastructure, but it spread globally through a software supply chain update and caused $10 billion in damage to international companies including Maersk, Merck, FedEx, and Mondelez. That was not a side effect of a surgical operation; it was the result of deploying wiper malware through a supply chain without any containment mechanism. Whether the global spread was intentional is still debated, but either way it shows a unit with a distinctly different risk calculus than most state cyber actors.

Sandworm's Malware Arsenal

Malware	Year	Target / Operation	What It Did
BlackEnergy 3	2014-2015	Ukraine energy and government	DDoS, data destruction, ICS reconnaissance; early phase of Ukraine infrastructure campaign
Industroyer / CRASHOVERRIDE	2016	Ukraine power grid (Kyiv, Dec 2016)	Communicated directly with industrial control systems to open circuit breakers; cut power to 230,000 people; first malware purpose-built to attack power grid hardware
NotPetya	2017	Ukraine (MEDoc supply chain)	Wiper disguised as ransomware; destroyed data, paralyzed systems; spread globally causing $10B+ damage; Maersk rebuilt 45,000 PCs and 4,000 servers in 10 days
Olympic Destroyer	2018	2018 Winter Olympics (Pyeongchang)	Targeted Olympic IT infrastructure on opening night; false-flag design; destroyed data and disrupted broadcasts; initially attributed to North Korea or China
Exaramel	2018-2019	European critical infrastructure	Evolved Industroyer backdoor; used to maintain persistent access in European energy networks
Cyclops Blink	2019-2022	WatchGuard firewalls, ASUS routers	Botnet malware; replaced VPNFilter; persistent infrastructure access; disrupted by US/UK 2022
Industroyer2	2022	Ukraine power grid (April 2022)	Direct successor to 2016 Industroyer; deployed alongside CaddyWiper; disrupted by Ukrainian CERT before execution
AcidRain	2022	Viasat KA-SAT satellite network	Firmware-wiping malware; deployed at invasion start; knocked out satellite communications across Europe; disrupted Ukrainian military coordination

Named Officers (DOJ Indictment, October 2020)

Name	Role	Specific Attribution
Yuriy Andrienko	Malware developer	NotPetya, Olympic Destroyer, BadRabbit; personally authored destructive components
Sergei Detistov	Malware developer	NotPetya spear-phishing components; Olympic Destroyer delivery mechanisms
Pavel Frolov	Malware developer	NotPetya wiper components; data destruction modules
Anatoliy Kovalev	Infrastructure	SolarWinds-adjacent operations; also referenced in Mueller indictment
Artem Ochichenko	Spear-phishing operations	2018 French election targeting; Olympic Destroyer phishing delivery
Petr Pliskin	Malware developer	NotPetya infrastructure management; operational coordination

The Contractor Layer: NTC Vulkan and the Private Sector Support Model

The Vulkan Files, published in March 2023 by a consortium of eleven media outlets, revealed something important about how Russia builds and maintains its offensive cyber capability: it uses private contractors extensively, and those contractors have operational visibility into state cyber programs that is both an efficiency advantage and a security liability.

NTC Vulkan was founded in 2010 by Anton Markov and Alexander Irzhavsky, both military academy graduates. The leaked documents show contracts with the FSB, GRU, and SVR simultaneously, which means a single contractor was providing engineering capacity to all three major intelligence services at once. The key documented projects were Scan-V (automated global vulnerability scanning for GRU exploitation), Amezit (an integrated platform covering domestic internet filtering, surveillance, and influence operations), and Krystal-2B (a training platform for ICS/SCADA attacks, directly connected to Sandworm-style operations).

Vulkan is not unique; it is a pattern. Multiple Russian defense and cyber contractors fill similar roles. Positive Technologies, a Moscow-based cybersecurity firm, was sanctioned by OFAC in April 2021 for providing tools and support to Russian intelligence services, including stockpiling zero-day exploits for FSB and SVR use. Tsifrovaya Bespasnost (Digital Security) and several smaller firms operate in the same space. The common thread: real commercial cybersecurity firms with legitimate clients, government contracts, and operational visibility into intelligence programs.

The contractor model serves the GRU in two specific ways beyond raw engineering capacity. First, it provides legal and institutional separation between offensive operations and uniformed military personnel. When something goes wrong, the contractor takes the exposure. Second, it allows the GRU to scale rapidly by absorbing commercial talent without the time and security overhead of military recruitment. The tradeoff is operational security: contractor employees are not subject to the same vetting, monitoring, and consequence-management as uniformed officers, and they leak.

The Contractor Model's Vulnerability

Contractors are far more exposed to disruption than sovereign military units. They have beneficial owners, bank accounts, commercial relationships, employees with LinkedIn profiles, university affiliations, and supply chains. When the Vulkan Files leaked, it was because a disenchanted employee handed thousands of internal documents to journalists. No GRU officer would have done that. The contractor layer is one of the most actionable disruption surfaces in the entire Russian cyber ecosystem.

GRU Exploitation: Operational Leverage Points

- Travel risk for named officers: Eighteen-plus named GRU officers from Units 26165 and 74455 face arrest in any country with a US extradition treaty. The 2018 Salisbury investigation by Bellingcat demonstrated that GRU travel cover identities can be penetrated through passport databases, flight records, and open-source hotel registrations. The same methodology applies to cyber operation officers. Building travel monitoring protocols for named GRU personnel is an actionable intelligence collection task.
- Contractor sanctions: Positive Technologies (2021 OFAC designation) and the Vulkan-linked entities represent the template. Contractors are sanctionable through OFAC, subject to export controls through BIS, and vulnerable to secondary sanctions through their commercial banking relationships. Each designation creates evidence of state-contractor relationships that supports broader accountability arguments.
- NotPetya in reparations and legal arguments: NotPetya created direct legal standing for damage claims from multinational corporations and allied governments. Insurance litigation over NotPetya established precedents on whether cyberattacks constitute acts of war (relevant to coverage exclusions). The Danish government has formally attributed economic damage to Russia. The legal architecture for state responsibility arguments based on NotPetya is more developed than for any other Russian cyber operation.
- Exploiting the attribution accumulation: The GRU has the most detailed public attribution record of any Russian cyber service. This creates a compounding asset: each new named officer, each new confirmed operation, each new building address adds to an evidence base that constrains operational options, enables allied sanctions actions, and creates material for public information campaigns about Russian military conduct.

GRU: Strengths and Weaknesses Summary

Category	Assessment
Operational boldness	STRENGTH: Willingness to conduct operations others would judge too attributable. Produces deterrence posture FSB and SVR cannot match.
Technical espionage capability	STRENGTH: Bundestag hack (16GB over weeks), sustained NATO-member penetrations demonstrate genuine collection against hardened targets.
ICS/SCADA targeting	STRENGTH: Only state actor with demonstrated ability to deploy effects-causing malware against power grid ICS hardware (Industroyer 2016, Industroyer2 2022).
Public attribution accumulation	WEAKNESS: Most-named Russian intelligence service in public indictments. Officer exposure constrains travel and creates ongoing CI pressure.

Category	Assessment
Collateral damage pattern	WEAKNESS: NotPetya global spread created legal standing for damage claims and insurance precedents that other Russian operations have not generated. Strategic own-goal.
Contractor ecosystem security	WEAKNESS: Vulkan Files leak demonstrated that contractor employees are viable insider threat vectors. No equivalent leak has come from GRU's own officer corps.

Part Four

SVR: The Patient Burglar

Foreign Intelligence Service (SVR)

The SVR is the hardest of the three principal cyber services to write about from open sources, because it is the best at not getting caught. The FSB leaves fingerprints through its criminal relationships. The GRU leaves fingerprints through its aggressiveness. The SVR's signature is invisibility: long-duration access, living off the land, blending into legitimate administrative traffic, and avoiding the kind of dramatic effects that trigger incident responses.

Its mandate is foreign civilian intelligence, the direct successor to the KGB's First Chief Directorate. In cyber terms, that means strategic espionage against foreign governments, intelligence services, defense contractors, think tanks, research institutions, and increasingly, the cloud infrastructure and identity providers that enable access to all of the above. APT29 is its primary threat actor cluster. The SVR connection was publicly confirmed in joint government statements from the US, UK, and allies in 2021 following SolarWinds.

APT29 / Midnight Blizzard: The Long-Game Operator

APT29 goes by more names than almost any other threat actor: Cozy Bear (CrowdStrike), The Dukes (F-Secure), NOBELIUM (Microsoft, for the SolarWinds phase), Midnight Blizzard (Microsoft current), Dark Halo (Volexity), UNC2452 (Mandiant). The proliferation reflects years of separate research teams discovering the same group through different incidents.

APT29's toolset is distinctive for what it is not. It does not use a lot of custom malware dropped noisily onto disk. Instead, it prefers techniques that blend into legitimate administrative activity. PowerShell, legitimate cloud services, stolen credentials, and OAuth token abuse are often more central to an SVR operation than any custom implant. When APT29 does deploy custom malware, it tends to be modular, multi-stage, and carefully targeted.

APT29 Toolset and TTPs

Tool / Technique	Operation / Period	What It Does
CozyDuke / MiniDuke	2014-2016 (early phase)	PDF-based droppers targeting government and research organizations; early-generation SVR tooling; deployed in spearphishing campaigns against NATO governments
SUNBURST	SolarWinds 2020	Backdoor trojanized into SolarWinds Orion update; distributed to 18,000 organizations; two-week dormancy period before C2 contact to defeat sandbox analysis
TEARDROP	SolarWinds 2020 follow-on	In-memory dropper; loaded Cobalt Strike or Raindrop on highest-value targets after SUNBURST profiling; entirely memory-resident to evade disk-based detection

Tool / Technique	Operation / Period	What It Does
RAINDROP	SolarWinds 2020 follow-on	Cobalt Strike loader; packed differently from TEARDROP to complicate detection; used in parallel track on select targets
WellMess / WellMail	2020 (COVID vaccine research)	Custom Go and .NET implants; used against UK, US, and Canadian COVID-19 vaccine research institutions; confirmed SVR attribution by UK NCSC
FOGGYWEB / MAGICWEB	2021-2022	Backdoors targeting on-premise Active Directory Federation Services servers; enabled persistent token-based authentication access surviving password changes
Password spray + OAuth abuse	2023-2024 (Microsoft)	No custom malware; password spraying against Microsoft legacy test accounts, then pivoted via OAuth app permissions into corporate email; entire operation used legitimate Microsoft authentication mechanisms
Device code phishing	2024-2025	Novel phishing technique abusing Microsoft OAuth device code flow; sends targets authentic-looking Microsoft prompts to grant access; no malware required; used against European government and NGO targets

Victimology Mapped to Russian Strategic Priorities

APT29's target selection is not opportunistic. It reflects specific Russian strategic intelligence requirements. The following mapping connects documented victim categories to the underlying Russian strategic priority each serves.

Victim Category	Examples from Public Record	Russian Strategic Requirement
Foreign government ministries and diplomatic missions	European foreign ministries; US State Department-adjacent; NATO member governments	Sanctions policy intelligence; diplomatic negotiating positions; early warning on allied decisions affecting Russia; personnel files on diplomats for CI targeting
Defense contractors and military-industrial base	US and European defense contractors (specific targets classified); aviation and space sector targets	Weapons system technical specifications; military technology gap analysis; procurement intelligence for import substitution; identifying vulnerabilities in allied defense supply chains
Technology and cloud service providers	SolarWinds (18,000 downstream organizations); Microsoft (corporate and government email); major IT vendors	Supply-chain access to thousands of downstream targets simultaneously; cloud admin credential theft as force multiplier; understanding Western technology dependencies that Russia can exploit or replicate
Think tanks and policy research institutions	Atlantic Council, German Marshall Fund, RAND-adjacent organizations (inferred from targeting patterns)	Policy development intelligence; early warning on sanctions proposals; academic research on Russian vulnerabilities; mapping Western expert networks that influence government decisions
Pharmaceutical and biomedical research	COVID-19 vaccine research institutions in UK, US, Canada (WellMess campaign)	Technology acquisition; health security intelligence; pandemic response planning; dual-

Victim Category	Examples from Public Record	Russian Strategic Requirement
		use biosecurity research with military applications
Energy sector companies	European energy firms; LNG and pipeline infrastructure	Western energy policy and pricing intelligence; sanctions circumvention opportunities; understanding energy leverage dynamics affecting Russia's export revenue

SolarWinds: Why It Matters Beyond the Scale

SolarWinds is the most consequential SVR operation in the public record, and its importance is not just the scale of initial access (18,000 organizations) but the selection logic. APT29 ultimately pursued only a small subset of those 18,000 victims for second-stage exploitation: nine US federal agencies, major technology companies, and specific defense contractors. The rest were left dormant.

That selection demonstrates strategic discipline. Most threat actors would ransack everything. The SVR used SolarWinds as a high-precision targeting system: get into 18,000 potential targets, silently profile them all, then select the ones worth deeper exploitation. The implant had a built-in two-week dormancy period specifically to avoid sandbox detection. That kind of operational planning reflects a sophisticated understanding of defensive architectures.

The US government's detection of SolarWinds is itself a story worth knowing. It was FireEye that first identified the intrusion, after APT29 accessed their internal network and stole red team tools. FireEye notified Microsoft and the US government, triggering the broader investigation. Without FireEye's internal detection, the operation might have continued for years. The SVR's model depends on persistent quiet access; when that access is discovered quickly, the investment in the operation is lost.

Post-SolarWinds: The Cloud and Identity Era

In January 2024, Microsoft disclosed that APT29 had accessed its corporate email accounts, including accounts belonging to senior leadership and cybersecurity staff. The intrusion did not use any novel malware. It started with a password spray attack against a legacy test account with no multi-factor authentication, then used OAuth application permissions to pivot into Microsoft's corporate email. The entire operation relied on legitimate Microsoft authentication mechanisms.

A February 2024 joint advisory from CISA, NSA, FBI, UK NCSC, and allied services summarized APT29's evolved cloud targeting tactics: abusing service accounts and dormant accounts with excessive permissions, registering rogue devices to bypass MFA policies, exploiting token-based authentication to maintain access after passwords are changed. None of this requires custom malware. It requires deep understanding of how cloud identity systems work and patience to exploit misconfigurations that accumulate over time in any large organization.

This shift represents a genuine strategic adaptation. As organizations migrated to cloud infrastructure, APT29 moved ahead of many defenders by developing deep expertise in cloud

identity and access management misconfigurations. The attack surface it exploits is not a zero-day vulnerability; it is the gap between how cloud systems are designed and how organizations actually configure and manage them. That gap is vast and growing.

The SVR's Structural Advantage

APT29 has essentially no documented criminal proxy relationships and no interest in ransomware or financial crime. That clean profile makes it harder to disrupt through the financial mechanisms that work against FSB-linked actors. There are no criminal assets to flip, no wallets to trace, no OTC brokers to identify. The primary lever against the SVR is defensive: make the target harder, not the attacker poorer.

What Actually Works Against SVR (and What Does Not)

The SVR poses a different disruption problem than the FSB or GRU. There are no criminal financial flows to interdict, no criminal proxies to flip, and no officer names in public indictments that create travel risk or CI leverage. The effective counter-SVR tools are primarily defensive and architectural.

Lever	Effectiveness	Rationale
MFA enforcement across all accounts (including legacy and service accounts)	HIGH	The Microsoft 2024 intrusion started with a legacy account without MFA. Comprehensive MFA coverage eliminates the single most common SVR initial access vector documented in recent operations.
OAuth permission auditing and least-privilege enforcement	HIGH	OAuth abuse is APT29's primary lateral movement mechanism in cloud environments. Regular audits of application permissions and removal of excessive grants directly constrain their operational playbook.
Privileged access management and conditional access policies	HIGH	Limiting what compromised credentials can access and from where degrades the value of stolen tokens and credentials, which are APT29's primary persistence mechanism.
Cloud identity hardening (device compliance, continuous authentication)	HIGH	Device registration for MFA bypass, token theft, and identity misconfiguration are the current APT29 focus. Cloud identity hygiene directly addresses the attack surface.
Personal sanctions on SVR officers	LOW	No named SVR officers below director level in any public indictment. Sanctions cannot target people you have not identified. SVR's operational security prevents the accumulating attribution that enables officer-level sanctions.
Criminal financial pressure	VERY LOW	SVR has no documented criminal financial ecosystem. No wallets, no exchanges, no OTC brokers. Financial disruption mechanisms designed for FSB-linked ransomware operators do not apply.
Supply chain security standards for technology vendors	MEDIUM	SolarWinds exploited inadequate build security at a trusted vendor. Mandatory software supply chain security standards (SSDF, secure-by-design requirements) raise the cost of SVR supply chain operations, though determined actors will adapt.

SVR: Strengths and Weaknesses Summary

Category	Assessment
Operational security	STRENGTH: No named officers below director level in any public indictment. Lowest attribution exposure of the three principal cyber services.
Cloud and identity targeting expertise	STRENGTH: Demonstrated mastery of OAuth abuse, token theft, and cloud admin misconfigurations. Ahead of many defenders in cloud identity attack surface exploitation.
Supply-chain access operations	STRENGTH: SolarWinds demonstrated ability to achieve 18,000-organization access through a single trusted vendor compromise. Most sophisticated supply-chain implant in documented history.
No criminal proxy model	DUAL-USE WEAKNESS: Cannot reach into criminal ecosystem for rapid capability development. Burned tools (SUNBURST) represent major sunk investment that cannot be redeployed.
Detection dependency on target security	WEAKNESS: Entire model depends on persistent quiet access. When a high-security target (FireEye) detects the intrusion quickly, the operation's investment is lost and the detection enables broader cleanup.
No financial disruption leverage for defenders	WEAKNESS FOR DISRUPTION (RUSSIA'S ADVANTAGE): Absence of criminal financial flows means Western financial tools cannot be applied. Primary defense is architectural, which requires sustained organizational investment.

Part Five

MVD: The Enforcement Valve

Ministry of Internal Affairs (MVD) and the Selective Enforcement Model

The MVD does not conduct offensive cyber operations. It does not run criminal hackers as intelligence assets. It does not build malware. What it does is control the valve: the formal mechanism through which Russia either cooperates or does not cooperate with foreign law enforcement on cybercrime cases. That makes it arguably the most instrumentally important institution for anyone working on Russian cybercrime accountability, because the absence of MVD cooperation is itself a form of state action.

Department K (Upravleniye K) handles cybercrime investigations and is the primary counterpart for foreign law enforcement agencies seeking Russian assistance. MLAT requests, Interpol Red Notices, bilateral assistance requests on specific criminal cases: all of them pass through channels that MVD controls. And the pattern of which requests get responded to and which do not is, when tracked over time, not random.

The Rules of the Game: Who Gets Arrested, Who Does Not

Russia does not extradite its own nationals. This is written into Article 61 of the Russian Constitution. But even within Russia, domestic prosecution of cybercriminals has followed a discernible pattern for two decades. The rule is sometimes summarized in the criminal community as "ne rabotay po RU," meaning "do not work on Russia." Hit Russian targets and you go to jail. Hit only foreign targets and you are largely left alone.

This norm has been documented consistently across cases, academic work, and journalism. Russian hackers who attacked Russian banks, Russian government systems, or Russian businesses have faced prosecution. Russian hackers who exclusively attacked foreign targets and stayed below the radar domestically have operated with relative impunity for years.

The norm is not absolute. Even some operators who attack only foreign targets can be arrested if they become diplomatically inconvenient (like REvil in January 2022), if they create too much international pressure (specific carding operations), or if they are caught up in internal FSB power struggles (Mikhailov case). But the baseline protection for attacking only foreign targets is real and consistently enforced.

The REvil Story: What Selective Enforcement Actually Looks Like

REvil (also called Sodinokibi) was one of the most prolific and technically capable ransomware operations of the 2019 to 2021 period. The group extracted over $200 million in ransoms, attacked Colonial Pipeline's business systems, hacked Kaseya (exposing up to 1,500

downstream businesses), and attacked JBS Foods. By 2021 they were one of the most wanted criminal organizations in the world.

On January 14, 2022, the FSB raided 25 locations simultaneously, arresting 14 REvil suspects and seizing $5.5 million in cryptocurrency and $600,000 in cash. The FSB published video of officers in body armor executing arrests. Western officials were cautiously optimistic. Then the case stalled. Within months, reporting indicated that the prosecution was fragmenting and that some arrested individuals had been released. By 2023, US-Russia cooperation on anything was dead. In 2024, a Russian court convicted several REvil members, with four defendants receiving sentences between four and a half and six years.

The correct interpretation of the REvil arrests is not that Russia became a serious counter-ransomware partner in January 2022. The correct interpretation is that Russia demonstrated, in one operation, that it knew exactly who these people were, where they lived, and how to arrest them, and had chosen not to do so for years. The arrests were timed to a specific diplomatic moment: the US had been pressing Russia hard on ransomware, and the REvil arrests were signaling that Russia could cooperate if it wanted to. When that signaling no longer served diplomatic purposes, the momentum dissipated.

The Analytic Value of REvil

REvil is less useful as evidence that Russia sometimes prosecutes cybercriminals and more useful as evidence that Russia always had the capability to prosecute them and chose not to for years. Documented capability combined with documented non-use is the strongest available evidence of deliberate protection. That is a much more powerful argument in a sanctions rationale or congressional testimony than "Russia never arrests anyone."

Legitimate Russian Domestic Cybercrime Prosecutions

Case / Actor	Year(s)	What They Did	Outcome
REvil affiliates (multiple)	2022-2024	Ransomware operations including Colonial Pipeline, Kaseya, JBS; exclusively targeted foreign victims	Four convicted; sentences 4.5 to 6 years; broader prosecution stalled post-2022 political shift
Mikhailov / Dokuchaev (FSB internal)	2017-2019	Passed classified FSB information to US intelligence	Convicted of treason; 22 years for Mikhailov; demonstrates internal disciplinary function, not victim protection
Sergei Maksimov	2019-2020	Ran carding operation targeting Russian banks	Convicted; ne rabotay po RU rule enforced
Pavel Vrublevsky (ChronoPay)	2011-2012	Commissioned DDoS attack on Russian competitor Assist.ru	Convicted; 2.5 years; hit Russian infrastructure, crossed the domestic protection line
Six defendants, Perm carding ring	2022	Sold stolen Russian payment card data to foreign buyers	Arrested; targeted Russian card victims, crossed domestic protection threshold
Aleksandr Vinnik (BTC-e)	2017 onward	Ran $4B+ crypto exchange laundering proceeds globally	Arrested Greece 2017; extradited France 2022 (convicted); extradited US 2024; never

Case / Actor	Year(s)	What They Did	Outcome
			prosecuted in Russia despite known identity

MLAT Cooperation Dataset: Tracking the Enforcement Signal

The most analytically underexploited data source for demonstrating deliberate Russian protection of cybercriminals is the MLAT (Mutual Legal Assistance Treaty) request record. Every formal foreign law enforcement request for Russian cooperation leaves a paper trail. When that trail shows systematic patterns of non-response, delayed response, or incomplete response specifically on cases involving state-linked actors, it becomes evidence of deliberate shielding rather than bureaucratic friction.

The following schema describes the dataset fields an investigator should maintain when tracking MLAT requests and other formal cooperation mechanisms with Russian law enforcement. Populating this dataset over time, and then mapping response patterns against actor type and political context, generates the most analytically defensible evidence of deliberate protection.

Field	Description	Analytic Use
Request Date	Date of formal submission of MLAT, Interpol Red Notice, or bilateral LE request	Enables latency calculation; identifies request timing relative to political events
Requesting Country	US, UK, EU member state, or other	Cross-referencing reveals whether response patterns vary by requesting country
Crime Type	Ransomware, BEC, carding, darknet, financial fraud, etc.	Enables comparison of response rates by crime category; tests hypothesis that certain categories are protected
Actor Profile	Known, suspected, or inferred state links (FSB/GRU/SVR-linked vs. independent)	Core variable: does state linkage correlate with non-response?
Geopolitical Context	Prevailing state of US-Russia relations at time of request; active diplomatic issues	Tests hypothesis that responses track diplomatic relationship rather than legal obligation
Response Type	No response, acknowledgment only, partial response, full response, operational arrest	Dependent variable for pattern analysis
Response Latency	Days from submission to substantive response	Sustained delays on high-confidence actor cases are themselves probative of deliberate non-cooperation
Outcome	Prosecution, arrest, information provision, or null outcome	Terminal measure of cooperation value
Overlap with State-Linked Actors	Yes/No/Suspected, with source citation	Key analytical field: requests involving state-linked actors that receive no response are the core evidence base

Illustrative Pattern Examples

The following examples illustrate how MLAT tracking reveals protection patterns. Neither is hypothetical; both reflect documented patterns in public reporting.

Example 1: During the period 2015 to 2021, US law enforcement filed multiple cooperation requests related to Evil Corp / Yakubets with Russian authorities. Yakubets was publicly indicted in December 2019. Russian authorities acknowledged no cooperation requests from that indictment through the end of 2021. During the same period, Yakubets was documented in public sanctions materials as holding a Russian government security clearance and working for the FSB. The non-response to US MLAT requests on an indicted subject simultaneously working for the FSB is not bureaucratic delay; it is protection.

Example 2: The period between the Garantex first OFAC designation (April 2022) and the domain seizure (March 2025) shows a 35-month window during which Russian domestic financial regulators took no documented enforcement action against Garantex despite its OFAC status and ongoing illicit transaction processing that was visible in blockchain forensics data. Russian financial regulator Rosfinmonitoring had FATF obligations (until February 2023 suspension) requiring it to act on designated entities. The non-action during this window, combined with Garantex's known Russian nexus, is the pattern that makes the MLAT record analytically meaningful.

FSB-MVD Jurisdictional Friction: When Cases Get Taken Over

A critical but underanalyzed dynamic in Russian cybercrime enforcement is what happens when FSB decides it has equities in a case that MVD/Department K is nominally investigating. The FSB has broad authority under 40-FZ to assert jurisdiction over cybercrime cases that it determines have counterintelligence, economic security, or information security implications. In practice, this means the FSB can pull a Department K investigation at any point.

When FSB takes over a case from MVD, it does not necessarily mean the investigation accelerates. In documented cases, FSB takeover has preceded case stalls, prosecution delays, and eventual quiet resolution that leaves the criminal actor free. The inference is that FSB asserts jurisdiction specifically when a Department K investigation is getting close to a protected actor. The takeover is the protection mechanism.

For investigators and policymakers, this pattern has a specific diagnostic implication: when Russian domestic cybercrime prosecutions stall after appearing to make progress, ask whether there has been a jurisdictional shift from MVD to FSB. If yes, the stall is not bureaucratic; it is structural protection being exercised at the service level.

Part Six

Telecom and Control Infrastructure: SORM, Sovereign Internet, and the Architecture of State Visibility

How Russia Controls Its Internet and What That Tells Investigators

Russia's telecom control infrastructure does not conduct offensive cyber operations. What it does is more foundational: it gives the state pervasive visibility into domestic internet traffic and fine-grained control over what Russian users and services can reach. That combination means that any criminal operator running infrastructure inside Russia is doing so inside a surveillance and control environment managed by the same services that are deciding whether to prosecute him. The non-disruption of obvious criminal infrastructure under those conditions is not an accident.

This section covers three overlapping systems: SORM (the intercept framework), the Sovereign Internet law and TSPU (deep packet inspection for filtering and blocking), and Roskomnadzor (the regulator that coordinates both). Understanding how these systems work together is essential to the specific analytic argument that Russian non-enforcement of cybercriminals is a deliberate state choice.

SORM: The Legal and Technical Framework for FSB Surveillance

SORM is not a single piece of hardware or a single law. It is a legal and technical architecture built over thirty years that creates a mandatory interception layer across all Russian telecommunications. Its core feature is that ISPs and telecoms are legally required to install FSB-specified equipment on their own networks at their own expense, and the FSB accesses that equipment directly without informing the ISP of the specific targets of collection.

The SORM Evolution

Generation	Year Established	Legal Basis	Technical Scope	Key Feature
SORM-1	1995	Federal Law No. 144-FZ (Operative Search Activities)	Telephone networks (PSTN and cellular)	Requires telecoms to install FSB wiretap hardware; FSB holds the warrant; telecom provider has no visibility into targets or scope of collection
SORM-2	1998 (updated 2014)	Regulatory orders implementing 144-FZ; Ministry of Communications Order No. 538	All internet traffic; ISPs of all sizes	Extends mandate to internet; ISPs must install SORM hardware connecting directly to FSB local office via dedicated channel; provider pays for

Generation	Year Established	Legal Basis	Technical Scope	Key Feature
				installation; has no visibility into FSB queries
SORM-3	2014	Federal Law No. 374-FZ (Yarovaya Law, 2016 expansion)	All communications; metadata and content retention	ISPs must retain all metadata for 3 years and communications content for 6 months; FSB accesses this storage directly; no court order required for access; extends to messaging services and VoIP
Yarovaya Amendments	2016-2018 (phased)	Federal Laws No. 374-FZ and 375-FZ	Encryption, messaging apps, foreign platforms	Foreign messaging companies operating in Russia must store user data on Russian servers and provide FSB decryption keys upon request; non-compliant services (Telegram, initially) face blocking orders
Order No. 1174 (2026 Expansion)	2025 (signed Dec 16); 2026 (registered May 22)	Mintsifry Order No. 1174 (registered 22.05.2026, No. 86587); implements expanded collection obligations under 144-FZ and Federal Law No. 149-FZ	All operators of technological communications networks holding internet identifiers (ASNs / IP blocks); extends SORM obligations beyond licensed telecoms to corporate and industrial network operators	First-ever mandate for PII linkage to internet activity: passport data, home addresses, tax IDs (INN), and bank account details — all linked in real time to assigned IPs, MACs, IMEI/IMSI. New fields: domains accessed, user logins where visible, geolocation coordinates. Enforcement escalation: 85 ISPs fined concurrently; license revocation for non-compliance (up to 10 years) under active legislation. ISP market consolidation underway: ~10,000 small operators face elimination as compliance costs become prohibitive.

The practical reality of SORM: the FSB has a dedicated fiber connection from each major ISP's network directly to FSB regional offices. The ISP cannot see what the FSB is accessing, cannot challenge collection requests because requests are not surfaced to the ISP, and cannot audit FSB usage. There is no judicial transparency mechanism that functions as a meaningful check. Russian courts that nominally review FSB collection requests do so on sealed applications that the ISP and the subject never see.

For domestic cybercriminals, this means: every communication over Russian internet infrastructure is potentially accessible to the FSB in real time under SORM-2. Every stored

communication and metadata going back three to six years is accessible under SORM-3. As of May 2026, Order No. 1174 extends this further: FSB now has statutory access to the home address, passport data, tax ID, bank account details, and real-time geolocation of whoever holds any given IP address on Russian infrastructure — along with the domains they access and user logins visible to the provider. If an FSB-protected ransomware operator conducts his operations using Russian internet infrastructure, the FSB is not merely capable of finding him — it has a legal mandate to maintain the data that makes him instantly locatable. The argument that FSB "didn't know" who was operating from a given IP address is no longer tenable under any construction.

The SORM Argument in Legal and Policy Contexts

The combination of SORM architecture and documented non-prosecution is the strongest available evidence that Russian non-enforcement of known cybercriminals is a policy choice. The argument structure: (1) SORM gives FSB real-time access to domestic internet traffic; (2) documented ransomware operators used Russian internet infrastructure for years; (3) FSB did not arrest or disrupt them despite SORM visibility; (4) therefore non-enforcement was deliberate. As of May 2026, Order No. 1174 makes this argument categorically stronger: FSB now has statutory access not just to traffic but to the passport data, home address, bank account, and real-time geolocation of every IP address on Russian infrastructure. The evidentiary weight of non-enforcement is now decisive — FSB cannot credibly claim it lacked the means to identify a domestically resident criminal operator. This argument is appropriate for sanctions rationale documents, DOJ declination memos, congressional testimony, and private civil litigation seeking to establish state responsibility.

Sovereign Internet and the TSPU: Infrastructure-Level Traffic Control

Russia's 2019 Sovereign Internet Law (Federal Law No. 90-FZ, "On Communication and on Information, Information Technologies and Information Protection") created a second layer of control beyond SORM: a national-level deep packet inspection network that can filter, throttle, or block specific traffic at the backbone level without cooperation from individual ISPs.

How the TSPU Works

The TSPU (Tekhnicheskiye Sredstva Protivodeystviya Ugrozam, Technical Means for Countering Threats) consists of deep packet inspection hardware deployed at all Russian internet exchange points and at major ISPs. The hardware was supplied primarily by RDP.RU, a Russian company with government connections. Key features:

- Deployment: Hardware is installed at ISPs but controlled centrally by Roskomnadzor through an encrypted management channel. Individual ISPs cannot see the configuration or control its behavior once installed.
- Capabilities: The system can filter specific URLs and IP addresses, throttle specific services (as demonstrated against Twitter in March 2021), block entire services or protocols (Tor, most commercial VPNs), and in principle execute an internet isolation event by restricting international traffic routing.
- Central configuration: Roskomnadzor distributes blocklists and filtering rules to TSPU hardware nationally. This allows the state to implement changes across all ISPs simultaneously without requiring individual ISP cooperation or action.
- Documented uses: Throttling of Twitter (2021, following failure to delete prohibited content), blocking of Tor and VPN services (progressive from 2019), blocking of Ukrainian and Western news services (2022 onward), blocking of independent Russian

media after February 2022. Updated 2025–2026 actions: throttling of Telegram and WhatsApp voice calls (August 2025, escalating to nationwide throttling by November 2025); mobile internet shutdowns deployed across multiple regions including a three-week central Moscow outage (March 2026), nominally justified as drone countermeasures; whitelist-based internet architecture deployed (September 2025 onward, only state-approved services permitted during shutdowns); VPN crackdown that crashed the domestic banking system (April 2026) — the TSPU filtering infrastructure blocked VPNs used by Russian banks to secure their own transactions, briefly making cash the only nationwide payment method; over 469 VPN services blocked as of mid-2026.

The TSPU's relationship to the criminal ecosystem is indirect but analytically significant. The system demonstrates that Russia has the technical capability to selectively restrict specific internet services, specific IP ranges, and specific platforms at a national level, quickly and without ISP cooperation. This makes the state's failure to disrupt criminal infrastructure even more clearly intentional: if Russia can throttle Twitter within hours of a political decision, it can also throttle ransomware C2 infrastructure. The choice not to do so is a policy decision, not a technical limitation.

Roskomnadzor: The Regulatory Architecture

Roskomnadzor (the Federal Service for Supervision of Communications, Information Technology and Mass Media) is nominally a telecom and media regulator. In practice, it is the operational coordinator for Russia's internet control infrastructure, running the TSPU blocklist administration, licensing communications operators, and enforcing data localization requirements against foreign platforms.

Its relationship to the FSB is formally separate but operationally intertwined. The FSB runs SORM intercept under its own authority. Roskomnadzor runs TSPU filtering under the Communications Ministry’s authority. But both systems operate on the same physical infrastructure (ISP networks), both serve state control objectives, and operational coordination between the two is routine. When a Roskomnadzor blocking order coincides with a FSB investigation (as in several domestic opposition and foreign media cases), the two systems function as a single state control architecture.

Structural evolution as of 2026: Two developments have altered the FSB–Roskomnadzor operational relationship. First, legislation passed in February 2026 changed the FSB’s authority over mobile operators from “requests” to “demands” for internet shutdowns, and removed the prior requirement that a documented security threat exist before invoking that authority. FSB can now unilaterally direct mobile internet shutdowns without routing through Roskomnadzor. Second, FSB demanded major Russian banks install SORM equipment on their applications, classifying bank apps as “organisers of the distribution of information.” Banks that refused were removed from the whitelist of services permitted to function during mobile internet shutdowns — creating direct financial coercion to comply. The practical effect is that the SORM/TSPU architecture now extends into the domestic financial system as well as the communications layer.

ISP market consolidation: The 17 existing ISP license categories are planned for consolidation to 3, with capital requirements rising from a nominal minimum to between $66,000 and $1.3 million depending on tier. This is projected to eliminate more than 90 percent of the

approximately 4,200 small regional broadband operators. The analytical implication is direct: a consolidated ISP market is a fully SORM-compliant ISP market by design. The small provincial operators that historically represented coverage gaps in the surveillance architecture are being systematically eliminated. Russia's internet control infrastructure is being engineered toward full compliance, not managed toward it.

Telecom and Control: Exploitation for Investigators

The telecom and control infrastructure creates several specific exploitation opportunities for investigators, policymakers, and allied services.

- Vendor and integrator targeting: RDP.RU and other TSPU hardware suppliers are sanctionable entities with commercial relationships, beneficial owners, and export dependencies. TSPU hardware includes Western-origin components that are subject to export controls. Systematic enforcement of export controls against TSPU suppliers directly degrades Russia's ability to maintain and expand the sovereign internet infrastructure. This is a concrete, measurable lever.
- Telecom law texts and regulatory decisions as open-source intelligence: Roskomnadzor blocking orders and the Russian government register of prohibited information (единый реестр запрещенных сайтов) are public documents. Systematic analysis of what is blocked versus what is not creates a map of what the state chooses to protect. The consistent non-appearance of ransomware infrastructure in blocking orders is itself analytically useful.
- Using the TSPU/SORM architecture in attribution arguments: The "Russia as a passive host" argument, which contends that Russia simply does not know about or cannot reach domestic criminal infrastructure, fails when examined against SORM and TSPU capabilities. Any legal or policy argument framing Russia as a knowing beneficiary of domestic criminal activity should explicitly cite SORM architecture and the TSPU's demonstrated ability to selectively disrupt services.
- Narrative use in diplomatic and public communications: "You used this control stack to throttle Twitter and block independent media within days of political decisions. In April 2026, you crashed your own banking system — briefly eliminating electronic payments nationwide — while trying to enforce VPN restrictions. You accepted that macroeconomic self-harm rather than relent on internet control. Yet ransomware operators have continued running on Russian infrastructure throughout this period without a single documented instance of TSPU disruption directed at their C2. Russia's TSPU is operating at a level of capability and political commitment that makes the non-disruption of criminal infrastructure a deliberate choice, not a gap." This framing, grounded in documented TSPU use cases and documented criminal infrastructure persistence, is both accurate and analytically devastating to Russian claims of non-complicity.

Analytic Conclusion

The combination of SORM and TSPU proves two things about Russia's capability: it has systemic real-time surveillance of domestic internet traffic (SORM), and it has fine-grained control over what traffic can traverse Russian internet infrastructure (TSPU). Order No. 1174 (May 2026) upgrades both arguments: FSB now holds statutory access to passport data, home addresses, bank accounts, and real-time geolocation of every IP address on Russian infrastructure, while the TSPU demonstrated in April 2026 that it can produce macroeconomic second-order effects — crashing the domestic banking

system — without the government retreating from enforcement. Mintsifry has budgeted approximately $186 million to expand TSPU capacity 2.5-fold to 954 terabits/second by 2030. The persistent operation of ransomware groups on Russian infrastructure is therefore not a surveillance or enforcement capability gap. It is a deliberate state policy of non-disruption, maintained by the same services and regulators that have demonstrated they can and do disrupt other online activities within hours of a political decision — and are willing to accept self-inflicted economic harm to do so.

Part Seven

FSTEC and the Russian Infosec Market: The Certification Chokepoint

FSTEC: How Russia Controls Its Own Security Ecosystem

FSTEC (Federal Service for Technical and Export Control) is one of the least-discussed but analytically important institutions in the Russian cyber ecosystem. Its primary function is certifying security products for use in Russian government and critical infrastructure systems, but the implications of that function extend well beyond product approval. FSTEC certification shapes which vendors can operate in sensitive Russian market segments, requires vendors to submit source code for review, and creates a state-visibility mechanism over the domestic information security industry.

Understanding FSTEC matters for two reasons. First, the certification process is itself an intelligence collection mechanism: any foreign vendor seeking Russian government contracts must expose its product internals to Russian technical reviewers. Second, the domestic Russian security market that FSTEC shapes is largely populated by firms with semi-state ownership or state alignment, meaning the line between defensive security products and offensive or surveillance tools is deliberately blurred.

How FSTEC Certification Works

FSTEC certification is legally required for security products installed in Russian government networks, critical infrastructure, and systems processing state-classified or personally identifiable information. The certification process requires vendors to submit full product documentation, source code for review by FSTEC-approved testing laboratories, and evidence of compliance with GOST-R standards (Russia's national technical standards framework). For foreign vendors, this means handing product internals to Russian government-aligned technical evaluators.

The implications from a Western intelligence perspective are significant. FSTEC certification of foreign security products (anti-virus software, firewalls, encryption tools) creates a documented mechanism through which Russian technical personnel receive access to the code of products protecting Western-origin systems deployed in Russia-adjacent environments. Historical reporting has indicated that Kaspersky Lab's deep ties to Russian government certification processes, including its FSTEC certifications, created operational concerns for Western governments that eventually led to its effective market exclusion in NATO member environments.

The Russian Infosec Market: Semi-State Alignment

Russia's domestic information security market is dominated by a relatively small number of companies that have deep state ties through ownership, certification relationships, government contract dependency, or personnel connections to the intelligence services. The TAdviser

research portal, which tracks the Russian IT market, documents a market in which the largest domestic security vendors (Kaspersky, Positive Technologies, InfoWatch, Infowatch Group, CodeMasters, Security Code) all have some combination of FSB/FSTEC certification relationships, government contract exposure, and personnel with intelligence service backgrounds.

Positive Technologies is the most documented case of a Russian infosec firm with direct intelligence service ties. Its April 2021 OFAC designation stated explicitly that the company provides tools and support to the Russian government, including the FSB and SVR, and that its annual security conferences (PHDays) have served as a recruitment ground for Russian intelligence services. OFAC also stated that Positive Technologies stockpiles zero-day vulnerabilities that it provides to the FSB and SVR for offensive use. The designation was a public statement that a nominally commercial security company was functioning as an intelligence service contractor.

Company	FSTEC/State Relationship	Known Government Ties	Status
Kaspersky Lab	FSTEC-certified products; deep government market penetration	Founder Eugene Kaspersky studied at FSB-predecessor KGB cryptography institute; government contracts across Russian agencies; multiple staff with intelligence backgrounds	Banned from US government networks (2017 DHS Binding Operational Directive); UK/EU advisory against government use; remains major commercial vendor globally
Positive Technologies	FSTEC-certified; key Russian government contractor	OFAC-designated April 2021 for providing tools and support to FSB, SVR; annual PHDays conferences cited as intelligence recruitment venues; zero-day stockpiling for state use	OFAC designated; effectively excluded from Western markets; continues Russian and non-Western market operations
InfoWatch	FSTEC-certified	Data loss prevention products with deep network visibility; government contracts; founder Natalya Kaspersky (ex-Kaspersky Lab) with broad government connections	Not designated; operates in Russian government and corporate market
Security Code	FSTEC-certified; firewall and endpoint products	Primary supplier of firewall and information protection products to Russian government and military networks; deep integration with state communications infrastructure	Not designated; core Russian government security supplier
InfoCryptoPro	FSTEC and FSO-certified encryption	Provides state-certified cryptographic products; FSO (Federal Protective Service) certification for highest-classification systems	Core supplier for Russian government encrypted communications

FSTEC's National Vulnerability Database (BDU)

FSTEC operates the BDU (Baza Dannykh Ugroz, database of threats and vulnerabilities), Russia's national vulnerability database, analogous to NIST's NVD. The BDU is a FSTEC-

required reference for Russian government IT security management. Analyzing the BDU against Western vulnerability databases and active GRU/FSB/SVR exploitation patterns is a productive analytic technique.

Specifically: comparing which CVEs appear in the BDU (published, Russian government expected to patch) against which CVEs are actively exploited by Russian APT actors reveals two things. Vulnerabilities that Russian APTs exploit but that are not yet in the BDU suggest that Russian intelligence services have advance knowledge of those vulnerabilities before they are shared with Russian domestic defenders. Vulnerabilities that are in the BDU but consistently exploited by Russian APTs against Russian-network targets suggest either intentional non-patching or deliberate exploitation of systems that Russian services have certified as secure.

FSTEC: So What for Investigators

FSTEC creates two specific leverage opportunities for Western policymakers and investigators.

First, certification gives the state both visibility and leverage over vendors that may also be involved in offensive or surveillance contracts. Any Western company that has submitted products for FSTEC certification has, to some degree, exposed its product internals to Russian government-aligned reviewers. The policy implication is that FSTEC certification should be treated as a disqualifying factor for sensitive government procurement, which some Western governments have already implemented in various forms.

Second, the OFAC designation of Positive Technologies established the legal and factual precedent for treating Russian infosec vendors as potential intelligence service extensions, not just commercial companies. The same framework can be applied to other vendors whose FSTEC relationships, personnel connections, and government contracts suggest they serve dual commercial and intelligence functions. The designation architecture exists; it needs to be applied more systematically to the broader Russian infosec contractor ecosystem.

Part Eight

The Criminal Ecosystem: Structure, Typology, and State Connections

How Russia's State-Criminal Relationship Actually Functions

The single most common analytical error on this topic is to draw a binary: either Russia is running a specific criminal group, or it has no connection to them. The reality is a spectrum. At one end you have direct state employment, like the Yahoo case where FSB officers paid and directed specific hackers. At the other end you have simple non-enforcement, where the state knows who is running ransomware and does nothing because there is no domestic harm and there may be intelligence benefit. In between are varying degrees of protection, informal tasking, coercion, and selective use.

The model is not a bureaucratic program with a director and a budget line. It is organic. An FSB officer who knows a criminal hacker might reach out for a favor. A criminal who gets arrested might be offered a deal that involves cooperative work. A hacker building capability that an intelligence service values might simply be told that his operations have been noted and he should continue. None of these require a formal memorandum of understanding.

Typology of Russian-Language Cybercrime Actors

Russian-language cybercrime is not monolithic. It comprises several distinct actor categories with different operational profiles, different relationships to the state, and different susceptibilities to specific disruption tools. Getting the typology right matters for targeting: the leverage that works against a ransomware group does not necessarily work against an initial access broker or a bulletproof hosting provider.

Actor Type	Core Function	Typical State Relationship	Primary Disruption Lever
Financial fraud and banking malware crews	Large-scale theft from consumer and business bank accounts; use of trojans (Dridex, Emotet), credential theft, and account takeover at scale	LOW to MEDIUM: Some groups (Evil Corp/Dridex lineage) evolved into state-adjacent status; most operate under general impunity if targeting only foreign banks	Indictments of named individuals; collaboration with domestic financial sector on technical indicators; third-country arrest when operators travel
Carders and card data marketplaces	Theft, sale, and use of payment card data; operate dark web storefronts (Joker's Stash, BriansClub, Rescator); sell to downstream fraud actors	LOW: Generally tolerated under ne rabotay po RU norm; periodic arrests when operations attract too much attention or affect Russian victims	Marketplace takedowns; financial institution fraud loss reporting to generate US victim standing; OFAC designation of major market operators

Actor Type	Core Function	Typical State Relationship	Primary Disruption Lever
Initial access brokers (IABs)	Sell network access to compromised organizations to ransomware affiliates and espionage actors; operate in closed forums; price access by organization type, revenue, and geography	MEDIUM: IABs providing access to government, defense, or critical infrastructure targets are potential state procurement targets; FSB/GRU may purchase access through intermediaries	Blockchain forensics to identify IAB wallet addresses; forum infiltration; arresting buyers provides access to IAB network information
Bulletproof hosting (BPH) providers	Provide hosting infrastructure resilient to law enforcement takedown requests; typically operated from Russia or Russia-adjacent jurisdictions; ignore DMCA/abuse complaints	MEDIUM: Some BPH providers have documented FSB or GRU infrastructure relationships; others simply operate under sovereign immunity from Russian law	Upstream hosting provider pressure; OFAC designation; BGP route manipulation by cooperative upstream providers; coordinated international ISP action
Ransomware crews and RaaS operators	Conduct encryption-for-ransom attacks; RaaS operators provide platform to affiliates who execute attacks; extract large individual payments	HIGH variation: Some (Evil Corp) are directly FSB-linked; others (LockBit) have state-adjacent affiliates without direct state attribution; all benefit from ne rabotay po RU protection	Infrastructure takedowns (Operation Cronos model); financial seizure; OFAC designation of operators; public naming and affiliate defection
Cryptocurrency laundering services (mixers, exchanges, OTC desks)	Convert illicit cryptocurrency to usable currency; operate as intermediaries between criminal proceeds and financial system	MEDIUM to HIGH: Russia-based exchanges benefit from deliberate regulatory non-enforcement; some OTC desks have documented FSB protection; Garantex pattern is the reference case	OFAC + FinCEN Section 311 combined action; physical domain seizure; secondary sanctions on financial institutions processing transactions

The Post-Conti Criminal Landscape

Conti's collapse in 2022 did not reduce the ransomware problem. It distributed it. When Conti dissolved, its hundreds of operators, developers, affiliates, and support staff scattered into a dozen successor groups. Chainalysis tracked blockchain flows connecting Conti wallet addresses to Black Basta, Akira, Royal, Quantum, and several smaller groups. This reflected people who had worked together in Conti's operations carrying their relationships and technical knowledge into new organizations.

Black Basta is the most significant Conti successor. It emerged in early 2022 and immediately demonstrated capabilities consistent with a team that had been operating professionally for years. It uses a double-extortion model (encrypting data and threatening to publish it), has a professional leak site, and operates with organizational discipline that reflects Conti's culture. Attribution research has connected several Black Basta operators to former Conti leadership. A February 2024 internal chat leak from Black Basta (similar in nature to the Conti leak) confirmed the Conti personnel overlap and revealed ongoing communications suggesting FSB awareness of the group's operations.

Akira is notable for the blockchain evidence connecting it to Conti: code overlap with Conti malware and shared wallet infrastructure suggest not just shared personnel but deliberate coordination. Akira has been particularly active against US education, manufacturing, and healthcare sectors.

Key Ransomware Groups and State Connection Assessment

Group	Lineage	State Connection	Notable Actions
Evil Corp	Independent criminal org, state-linked	HIGH CONFIDENCE: FSB relationship documented by OFAC; Benderskiy family FSB tie; Yakubets working for FSB as of 2017	Evolved from Dridex to WastedLocker; now uses third-party ransomware (LockBit) to evade sanctions; $300M+ stolen globally
Black Basta	Conti successor	MEDIUM (inferred): Conti had documented FSB liaison references; Black Basta absorbed Conti leadership; Feb 2024 chat leak suggests FSB awareness	Attacked Rheinmetall, ABB, US healthcare systems; $100M+ extorted
Akira	Conti successor	MEDIUM (inferred): Blockchain and code links to Conti; no direct state attribution	Active in US education and manufacturing; $42M+ documented ransoms
LockBit	Independent; Evil Corp affiliate	LOW to MEDIUM: Ryzhenkov (Evil Corp) operated as LockBit affiliate; no direct state attribution against core operators; UK NCA identified principal operator as Dmitry Khoroshev ("LockBitSupp")	Most prolific ransomware group 2022-2024; disrupted by Operation Cronos Feb 2024; rebuilt at reduced capacity
REvil remnants	REvil / Sodinokibi lineage	MEDIUM: Protected 2019-2022; selectively arrested 2022; some released; effectively state-demonstrated capability	Effectively dormant post-2022 arrests; members dispersed into other groups

Group	Lineage	State Connection	Notable Actions
Scattered Spider / Octo Tempest	Western-based; RaaS affiliate	NONE documented: English-speaking operators (US/UK); no Russian state connection	Notable for English-speaking operators using social engineering; ALPHV/BlackCat affiliate; MGM Resorts and Caesars attacks

The "Do Not Work on Russia" Norm

Russian cybercriminal forums have maintained an informal but consistently enforced norm prohibiting attacks on Russian-speaking targets. This norm predates the modern ransomware era; it was present in the early 2000s carding forums that were the precursors to today's ransomware operations. Violation of the norm has historically been grounds for being banned from forums and, in some documented cases, reported to Russian law enforcement.

The persistence of this norm is itself evidence of state influence, even where no formal control exists. An underground forum that routinely bans members for attacking Russian targets and never bans them for attacking American ones is not behaving the way a purely commercial criminal enterprise would. It is behaving the way a community behaves when it knows that one type of conduct has official consequences and the other does not.

The invasion of Ukraine in 2022 complicated this norm. Many ransomware groups with Ukrainian members refused to follow Conti's Russia endorsement, which directly contributed to the Conti chat leak. Some operators took sides; others tried to stay neutral. The norm has been under strain since 2022 as Ukrainian-affiliated hackers (state and freelance) have explicitly targeted Russian infrastructure. But the underlying enforcement mechanism, Russian law enforcement acting on forum norms, has not fundamentally changed.

Part Nine

The Money Pipeline: How Russian Ransomware Actually Cashes Out

Financial Plumbing of the Russian-Aligned Ransomware Ecosystem

The financial trail is the most actionable part of the Russian ransomware problem. You cannot easily arrest a GRU officer in Moscow or shut down an FSB-protected criminal by filing a diplomatic note. But every ransomware payment has to travel through a conversion pipeline before it becomes something spendable, and that pipeline has nodes you can attack. The challenge is that those nodes are mostly inside Russia or in jurisdictions that do not cooperate with Western law enforcement. The opportunity is that they are identifiable, traceable, and in some cases vulnerable to coordinated international pressure.

Step One: The Ransom Payment

Ransomware victims pay almost exclusively in Bitcoin (BTC) or Monero (XMR). Bitcoin is the default because it is the most liquid and widely understood cryptocurrency, and most victims' finance departments can acquire it quickly. Monero is the privacy coin of choice for operators who want to minimize blockchain traceability from the start: unlike Bitcoin, Monero uses ring signatures and stealth addresses that make transaction tracing significantly harder even with sophisticated blockchain forensics.

The choice of currency tells you something about the operator. Groups with established laundering infrastructure and OTC relationships are less worried about Bitcoin traceability because they have the back-end to handle it. Groups that demand Monero, or offer a discount for Monero payment, are either more technically sophisticated about their exposure or specifically trying to avoid the blockchain trail that has gotten other operators caught. One tactical development from 2022 onward: some ransomware operators began accepting payment in stablecoins (USDC, USDT) in specific cases, particularly where the victim is a crypto-native company. Stablecoin issuers (Circle, Tether) can freeze specific wallet addresses, and have done so in law enforcement-requested situations.

Step Two: Obfuscation Before the Off-Ramp

Once a ransom payment is received, the first priority is making the transaction history harder to follow. Techniques have evolved significantly as blockchain forensics capabilities have improved.

Mixers: The Old Method

Cryptocurrency mixers pool funds from multiple users and redistribute them, breaking the transaction trail between input and output wallets. ChipMixer was the most significant Bitcoin mixer used by ransomware operators, processing an estimated $3 billion in Bitcoin before

German and US authorities seized its infrastructure in March 2023. Sinbad was its successor, sanctioned by OFAC in November 2023. Tornado Cash was the dominant mixer for Ethereum-based transactions, sanctioned in August 2022. The wave of mixer takedowns and sanctions has worked: blockchain analytics firms report a significant decline in mixer usage for ransomware cashout since 2022 to 2023.

Cross-Chain Bridges: The Current Method

As mixer usage declined, ransomware operators shifted to cross-chain bridges, which swap cryptocurrency from one blockchain to another. Blockchain forensics tools are generally better at tracing within a single chain than across multiple chains. If you convert Bitcoin to Ethereum, then to a Binance Smart Chain token, then to USDT on Tron, then to Bitcoin again, you have created multiple analytical discontinuities that require different forensics tools for each step. TRM Labs identified cross-chain bridges as the dominant obfuscation method for ransomware operators in 2024, replacing mixers. The bridge layer is harder to sanction than a mixer because many bridges are decentralized protocols without a central operator. This is a genuine gap in current regulatory architecture.

Step Three: The Russian Exchange Ecosystem

After obfuscation, ransomware proceeds need to reach an exchange that will convert cryptocurrency to spendable currency. For Russian-aligned operators, the preferred destination has consistently been Russian-nexus exchanges with minimal KYC/AML controls, willingness to process transactions that compliant Western exchanges would flag, and implicit or explicit protection from Russian regulatory enforcement.

Exchange	Years Active	Volume / Scale	Known Links	How It Ended
BTC-e	2011-2017	$4B+ processed	Mt. Gox hack proceeds; Silk Road; multiple ransomware groups	Domain seized July 2017; founder Alexander Vinnik arrested Greece; extradited France (convicted); extradited US 2024; $110M penalty
WEX	2017-2018	BTC-e successor	Inherited BTC-e user base and criminal connections	Collapsed 2018 after operator disputes; no enforcement action
Hydra Market	2015-2022	$5.2B in crypto processed	Dominant laundering venue for Russian darknet and ransomware ecosystem; offered ruble cashout via couriers	German/US seizure April 2022; $25M Bitcoin seized; operator Pavlov indicted; most significant single disruption action in Russian crypto-crime history
Garantex	2019-2025	$100M+ illicit transactions documented	Conti, Black Basta, LockBit, Ryuk, NetWalker proceeds processed	First sanctioned OFAC April 2022; continued operating 3 years; domain seized March 2025, $26M frozen; rebuilt as Grinex; Grinex sanctioned August 2025
Bitzlato	2018-2023	$700M-$1B illicit flows	Hydra Market counterpart; darknet vendors and	Coordinated US/EU/EUROPOL action January 2023; founder Anatoly Legkodymov arrested

Exchange	Years Active	Volume / Scale	Known Links	How It Ended
			ransomware; 46% of assets from illicit sources	Miami; first FinCEN primary money laundering concern for crypto firm
PM2BTC / UAPS	2013-2024	$1.15B handled; 32% from criminal sources	Genesis Market fraud shop; ransomware groups; initial access brokers	OFAC sanction + FinCEN primary money laundering concern Sept 2024; domains seized by US Secret Service and Dutch FIOD; operator Sergey Ivanov charged
Cryptex	~2018-2024	$51.2M+ directly from ransomware	Direct ransomware proceeds; connected to Ivanov network	OFAC sanction September 2024; domains seized US/Netherlands; part of same coordinated action as PM2BTC
Grinex / A7A5	2025-ongoing	Garantex operational successor	Direct successor: same infrastructure and staff per Chainalysis	Sanctioned OFAC August 2025; may still be operating via additional successor infrastructure per ICIJ reporting

The Garantex Pattern: Why Sanctions Alone Are Not Enough

Garantex was first sanctioned in April 2022. It continued operating for nearly three years. It processed hundreds of millions of dollars in illicit funds during that period. The sanctions changed the legal risk for any Western entity interacting with Garantex, but did nothing to prevent Russian clients from using it through Russian banking infrastructure. The exchange only stopped after a physical domain seizure in March 2025. Designation without enforcement access to the infrastructure is a partial measure. Physical seizure is necessary.

Step Four: The OTC Broker Layer

Not all ransomware cashout flows through formal exchanges. A significant portion moves through over-the-counter (OTC) brokers, individuals or small operations who match cryptocurrency buyers and sellers directly without using exchange order books. In the Russian cybercrime context, OTC desks allow operators to convert cryptocurrency to rubles without the paper trail that even a compliant exchange's records would create. Russian-nexus OTC desks largely operate through Telegram channels, private Telegram bots, and invitation-only forums. The transaction model is straightforward: the operator sends crypto to the broker's wallet; the broker sends rubles to a specified Russian bank account, often via peer-to-peer payment apps (SBPay, Tinkoff, Sberbank transfers). No KYC. No records. Commission of 1-5%.

OTC desks are more vulnerable to blockchain forensics than they appear, because they necessarily aggregate transactions. An OTC broker who handles ten criminal clients is funneling their funds through a limited number of wallet addresses and exchange accounts. That aggregation creates a detectable cluster in blockchain analytics tools. The challenge is attribution: identifying the person behind the wallet cluster and connecting them to a sanctionable identity. The most productive approach combines blockchain analytics (wallet clustering, transaction graph analysis) with OSINT on Telegram channels, forum posts, and payment app usernames.

Step Five: The Fiat Off-Ramp

The critical vulnerability in any ransomware cashout is the conversion from cryptocurrency to fiat currency. Cryptocurrency has no direct utility until it can be converted to something that pays rent, buys cars, or funds operations. The dominant cashout mechanism for Russian-aligned operators is direct conversion to Russian rubles through Russian financial infrastructure. PM2BTC was specifically documented by FinCEN as providing crypto-to-ruble exchange services using OFAC-sanctioned Russian financial institutions. That is the specific mechanism: the exchange converts crypto to rubles and transfers to a Russian bank account, using Russian correspondent banking that has no Western visibility.

Russian cybercriminal leaders have historically converted significant criminal proceeds into high-value real assets. Maksim Yakubets of Evil Corp drove a customized Lamborghini with a vanity plate reading "Thief" in Russian through Moscow streets. Common real-asset conversion patterns based on open-source reporting and sanctions documentation include Moscow and St. Petersburg residential real estate held through corporate structures, high-end vehicles, business investments in Russia's hospitality and service sectors, and holding cryptocurrency in long-term wallets without conversion while waiting for enforcement pressure to pass.

Financial Pressure Points: Assessment

Node	Who Controls It	Applicable Pressure Tool	Effectiveness
Russian-nexus crypto exchanges	Russian operators, sometimes offshore registered	OFAC SDN designation; coordinated domain seizure; secondary sanctions on processing banks	MEDIUM: Designation alone insufficient (Garantex operated 3 years post-sanctions). Physical seizure together with designation is more effective. Successor creation is rapid.
Cryptocurrency mixers	Centralized operators	OFAC SDN; FinCEN Section 311; DOJ prosecution of operators	HIGH for centralized mixers (ChipMixer, Sinbad successfully disrupted). LOW for decentralized protocols (Tornado Cash). Centralized targets are shrinking.
Cross-chain bridges	Often decentralized protocols	Limited: sanctioning smart contracts has legal basis but uncertain practical effect	LOW to MEDIUM: Forensics tools are still catching up to cross-chain bridge tracing. Current enforcement gap.
OTC brokers (individual)	Individual operators via Telegram and forums	Blockchain forensics plus OFAC designation of named individuals; third-country arrest if travel occurs	MEDIUM for identified operators. OTC market fragments rapidly when individual desks are targeted.
Russian bank accounts receiving crypto-to-ruble	Russian domestic banks	Secondary sanctions on banks processing illicit crypto conversions;	LOW to MEDIUM: Post-2022 secondary sanctions have reduced some correspondent banking but

Node	Who Controls It	Applicable Pressure Tool	Effectiveness
		correspondent banking pressure	domestic ruble transactions have no Western visibility.
Stablecoin off-ramps (USDT/USDC)	Tether, Circle (issuers)	Direct issuer freeze request	HIGH when applicable: both issuers have cooperated with law enforcement. Limitation: most Russian ransomware ops prefer Bitcoin, not stablecoins.
Ransomware affiliate payment infrastructure	RaaS operators controlling payment portals	Infrastructure takedown (Operation Cronos model); payment portal seizure	HIGH when executed: LockBit takedown disrupted payment flows and published operator identities. Groups rebuilt but at reduced capacity.

Part Ten

Levers and Effects: How to Exploit the Ecosystem (Lawfully)

A Cross-Cutting Framework for Disruption

The preceding sections of this document describe the Russian cyber ecosystem from the inside: how it is structured, who the key actors are, how they relate to each other, and where the documented cases provide the best evidence of state-criminal overlap. This section inverts the perspective. It asks: given what we know about the ecosystem's structure, which external actions have the most leverage, against which parts of the system, and with what realistic probability of effect?

The framework below covers eight categories of lever. For each, it describes what the lever is, which Russian institutions and criminal actors it affects most, what documented examples demonstrate its use and effectiveness, and what its limitations are. The section concludes with a matrix mapping lever to state organ to criminal actor type.

A preliminary note on goals: disruption of the Russian cyber ecosystem is not the same as elimination. The ecosystem is resilient because it is distributed and because the state actively maintains conditions that allow it to reconstitute after disruption. The realistic goal is sustained attrition, meaning operations that increase costs, degrade specific capabilities, expose specific actors, and reduce the effective operational tempo of the most dangerous elements. Measured against that goal, several levers show genuine sustained effect.

Lever 1: Indictments and Public Attributions

What it is: DOJ criminal indictments naming specific foreign intelligence officers or cybercriminals, combined with allied government attribution statements linking specific operations to specific Russian services.

Which institutions it targets: Primarily GRU and FSB officers who are named individually. Secondarily, the entire Russian services by creating public accountability for state-directed operations that Russia officially denies.

Which criminal actors are most affected: Operators who are named individually (Yakubets, LockBitSupp/Khoroshev), whose ability to operate internationally is constrained by arrest risk. Less effect on anonymous operators.

Concrete examples: Mueller indictment (July 2018) naming 12 Unit 26165 officers; Sandworm indictment (October 2020) naming six Unit 74455 officers; Yahoo/FSB indictment (2017); Evil Corp sanctions and indictment (2019 and 2024). The Bellingcat-style OSINT methodology applied to GRU officers in the Salisbury case demonstrates that named indicted individuals face real consequences: their travel is permanently constrained, their family members become collateral exposure, and allied services can develop CI targeting based on the public record.

Limitations: Named officers remain at large in Russia. No GRU or FSB officer indicted for cyber operations has been extradited. The deterrent effect on future operations is disputed. The

primary value is accumulating accountability, constraining travel, enabling allied sanctions, and creating an evidentiary record for civil litigation and reparations claims.

Lever 2: Sanctions (OFAC SDN and Targeted Financial Measures)

What it is: US Treasury OFAC designations of individuals and entities on the Specially Designated Nationals list, blocking their access to the US financial system and prohibiting US persons from transacting with them. UK, EU, and Australian parallel designations expand the geographic coverage.

Which institutions it targets: Most effective against actors with international financial exposure: contractors (Positive Technologies), exchange operators (Garantex, PM2BTC), and criminal organizations with overseas assets (Evil Corp). Less effective against Russia-based entities with no international financial footprint.

Which criminal actors are most affected: Exchange operators who need international banking relationships to maintain liquidity. Contractors who need to import Western technology or maintain European banking. Ransomware operators who have diversified assets in sanctionable jurisdictions (UAE, Cyprus, Turkey).

Concrete examples: Evil Corp designation (December 2019) effectively barred US companies from paying ransoms to Evil Corp affiliates, forcing Evil Corp to rebrand through third-party tools. Positive Technologies designation (April 2021) excluded it from NATO-member government markets. Garantex designation (April 2022) created legal risk for Western exchanges transacting with it. The October 2024 Evil Corp sweep sanctioning Ryzhenkov and Benderskiy by name targeted the FSB connection specifically.

Limitations: Sanctions without enforcement access to the sanctioned entity's infrastructure show limited effectiveness against Russia-internal entities. Garantex operated for three years under OFAC designation. Successor entities can be created rapidly (Grinex followed Garantex within weeks). The most effective use of sanctions is as part of a multi-tool action that includes physical seizure, criminal indictment, and secondary sanctions pressure simultaneously.

Lever 3: Contractor Exposure

What it is: Targeting the private sector contractor layer that provides engineering capacity and operational support to GRU, FSB, and SVR. This includes sanctions, export controls, reputational exposure, and employee-level OSINT investigation.

Which institutions it targets: GRU contractor ecosystem (NTC Vulkan and similar); FSB contractor relationships (SyTech, others); infosec vendors with dual-use relationships (Positive Technologies).

Which criminal actors are most affected: Contractors themselves. Indirectly, any criminal operation that depends on contractor-provided infrastructure or tooling.

Concrete examples: The Vulkan Files leak demonstrated that contractor employees are viable insider threat vectors. NTC Vulkan's exposure forced public acknowledgment of contracts with all three major intelligence services simultaneously. Positive Technologies OFAC designation excluded it from Western markets. Export control enforcement against technology inputs to Russian cyber contractors (semiconductors, cloud services) directly limits their engineering

capability. The SyTech leak (2019) exposed another FSB contractor's project portfolio through an anonymous hack, suggesting the contractor layer has multiple viable access points.

Limitations: Russia can create new contractors relatively quickly, though with degraded vetting and technical talent post-2022 brain drain. Export controls have the most sustained effect because they degrade the physical technology inputs that contractors need; sanctions have less effect against contractors whose primary market is Russian government contracts denominated in rubles.

Lever 4: Telecom and Control Infrastructure Pressure

What it is: Sanctions and export controls targeting suppliers, vendors, and integrators of SORM and TSPU hardware; public naming of the telecom control architecture in diplomatic and legal contexts; using documented TSPU capabilities to rebut Russian claims of inability to disrupt domestic criminal infrastructure.

Which institutions it targets: Roskomnadzor vendors (RDP.RU and similar); indirectly, the FSB through SORM coverage arguments; Russian telecom infrastructure broadly.

Which criminal actors are most affected: Indirectly, all Russia-based criminal infrastructure whose continued operation depends on state non-disruption. Directly, telecom vendors that have Western technology dependencies.

Concrete examples: The 2019 Sovereign Internet Law and TSPU deployment created an internationally documented record of Russia's fine-grained internet control capability. This record directly undercuts Russian claims that it lacks the means to identify or disrupt domestic cybercriminals. Export control enforcement against Western-origin components in TSPU hardware raises costs for Russia's control infrastructure maintenance.

Limitations: Russia has been actively domesticizing its telecom supply chain precisely because of export control risk. RDP.RU and successor suppliers are reducing Western technology dependence. The primary leverage from this sector is argumentative and diplomatic rather than technically disruptive.

Lever 5: MLAT Non-Cooperation Records

What it is: Systematic documentation of Russian non-responses to formal legal assistance requests, Interpol Red Notices, and bilateral cooperation requests, analyzed over time and presented as evidence of deliberate state shielding.

Which institutions it targets: MVD/Department K as the formal cooperation interlocutor; indirectly FSB and the overall state protection apparatus. Used in diplomatic demarches, sanctions rationale documents, and civil litigation.

Which criminal actors are most affected: This lever does not directly disrupt criminal actors. It builds the evidentiary record that supports sanctions, indictments, and legal arguments about state responsibility.

Concrete examples: The gap between the Garantex OFAC designation (April 2022) and any Russian regulatory action against Garantex (never), sustained across a 35-month period in which Russian authorities received US cooperation signals and did nothing, is the clearest

recent MLAT non-cooperation pattern. The Evil Corp non-response pattern (no Russian cooperation after December 2019 indictment, despite Yakubets's known Russian location) is the canonical individual-level example.

Limitations: MLAT records are not public. Building an analytically useful dataset requires systematic cooperation between law enforcement agencies across multiple requesting countries, consistent documentation, and a common analytical framework. This is a sustained intelligence and legal work product, not a single action.

Lever 6: Crypto and Financial Tracing and Seizures

What it is: Blockchain forensics-based identification of criminal financial flows, combined with law enforcement seizure actions when funds can be reached. Includes identification of OTC brokers, exchange operators, and money laundering nodes; OFAC designation of identified entities; physical seizure of exchange infrastructure and cryptocurrency wallets.

Which institutions it targets: The entire financial conversion layer of the criminal ecosystem: exchanges, mixers, cross-chain bridges, OTC desks, and the fiat off-ramp infrastructure. Does not reach Russian state institutions directly, but degrades the usability of ransomware proceeds for state-linked criminal actors.

Which criminal actors are most affected: Exchange operators and OTC brokers who are identified through blockchain forensics. Ransomware operators who rely on specific mixing or laundering infrastructure. Carders and financial fraud actors who use marketplace payment channels.

Concrete examples: The Hydra Market takedown (April 2022) was the single most disruptive action against the Russian criminal financial ecosystem: average daily darknet market revenue fell from $4.2 million to $447,000 overnight. ChipMixer seizure (March 2023) and Sinbad sanction (November 2023) materially reduced the mixer layer. Colonial Pipeline ransom recovery ($2.3 million of $4.4 million) demonstrated that early-stage blockchain forensics can recover funds before conversion. PM2BTC/Cryptex coordinated action (September 2024) combining OFAC, FinCEN Section 311, domain seizure, and criminal charges against Ivanov is the current model for effective multi-vector financial disruption.

Limitations: Cryptocurrency can be moved rapidly. Decentralized protocols (cross-chain bridges, decentralized exchanges) have no central operator to sanction. Recovery requires that funds remain in accessible wallets before the operator converts them. The forensics arms race is real: as tracing improves, obfuscation techniques evolve. Sustained investment in forensics capability is required to maintain effectiveness.

Lever 7: Infrastructure Takedowns

What it is: Coordinated international law enforcement seizure of criminal cyber infrastructure: ransomware operator leak sites, payment portals, affiliate management platforms, botnet C2, and bulletproof hosting infrastructure.

Which institutions it targets: Criminal ransomware operations and their supporting infrastructure. Does not directly reach state actors, but degrades criminal operations that state actors benefit from or use as proxies.

Which criminal actors are most affected: RaaS operators (LockBit, ALPHV/BlackCat) whose affiliate model depends on centralized infrastructure. Botnet operators (Cyclops Blink, Emotet, QakBot) whose C2 can be seized or disrupted. IABs whose forum presence provides their market access.

Concrete examples: Operation Cronos (February 2024) against LockBit disrupted payment flows, published operator identities (LockBitSupp identified as Dmitry Khoroshev), and seized decryption keys that were distributed to victims. LockBit rebuilt at reduced capacity. Operation Endgame (May 2024) targeted major dropper and loader infrastructure used across multiple criminal groups. CISA/FBI Cyclops Blink disruption (April 2022) took down a 1,000+ device Sandworm botnet before it could be weaponized.

Limitations: Groups rebuild. LockBit was operational within weeks of Operation Cronos. Infrastructure takedowns without concurrent criminal prosecution of operators produce temporary disruption, not permanent elimination. The most durable effect comes from combining infrastructure takedown with public naming of operators (increasing their personal risk profile) and financial seizure (degrading their ability to fund rebuilding).

Lever 8: Public Naming and Information Operations

What it is: Public attribution statements from allied governments, investigative journalism exposures (Bellingcat, The Insider, Vulkan Files consortium), and strategic use of criminal indictments as public accountability documents rather than just criminal process.

Which institutions it targets: GRU and FSB primarily (most named officers). Indirectly, the political cost borne by the Kremlin for acknowledged state-criminal overlap.

Which criminal actors are most affected: Those named publicly, particularly those with identifiable public profiles (Yakubets's Lamborghini, named LockBit operators). Criminal actors who rely on anonymity for operational protection face permanent exposure when publicly named.

Concrete examples: Bellingcat's GRU officer identification methodology (Salisbury poisoners, developed 2018) has been adapted to identify cyber operation officers. The Vulkan Files publication forced NTC Vulkan and its employees into the public record, enabling downstream OSINT investigation. Evil Corp operator Maksim Yakubets's lifestyle documentation (Lamborghini, wedding) built the evidentiary basis for the 2019 sanctions package.

Limitations: Russian state media has sophisticated counter-narrative capabilities. Named officers face no domestic consequences. Information operations work best when they are designed to reach specific audiences (technical researcher community, third-country policymakers, potential contractor employees) rather than mass audiences, and when they are sustained over time rather than episodic.

Lever-to-Target Matrix

The following matrix maps each lever to the Russian state institution and criminal actor category it most directly affects. Effectiveness ratings are based on documented outcomes in the public record.

Lever	FSB	GRU	SVR	Ransomware Groups	Exchanges / Mixers	Contractors	OTC Brokers
Indictments / Attribution	MEDIUM (Yahoo, Snake named officers)	HIGH (18+ named officers; travel constrained)	LOW (no named officers)	MEDIUM (LockBit operators named)	LOW	MEDIUM (NTC Vulkan documentation)	LOW
OFAC Sanctions	MEDIUM (Evil Corp FSB link sanctioned)	MEDIUM (named officers; contractor firms)	LOW	HIGH (Evil Corp operational disruption)	HIGH (Garantex, PM2BTC, Cryptex)	HIGH (Positive Technologies)	MEDIUM (Ivanov case)
Contractor exposure	MEDIUM	HIGH (Vulkan; Scan-V, Amezit programs)	MEDIUM	LOW direct	LOW	HIGH	LOW
Telecom/Control pressure	MEDIUM (SORM argument)	LOW direct	LOW	LOW direct	LOW	MEDIUM (TSPU vendors)	LOW
MLAT non-cooperation records	HIGH (Center 18 non-cooperation documented)	LOW	LOW	HIGH (Evil Corp, Garantex patterns)	HIGH (exchange non-action patterns)	LOW	LOW
Crypto/Financial tracing + seizures	LOW direct	LOW direct	LOW direct	HIGH (payment disruption)	HIGH (exchange seizures)	LOW	HIGH (OTC identification)
Infrastructure takedowns	LOW direct	MEDIUM (Cyclops Blink disrupted)	LOW direct	HIGH (Operation Cronos)	MEDIUM (mixer seizures)	LOW	LOW
Public naming / Info ops	HIGH (Yahoo, Center 18 exposure)	HIGH (GRU officer exposure; Bellingcat methodology)	LOW	HIGH (LockBitSupp, Yakubets)	MEDIUM	HIGH (Vulkan Files)	MEDIUM

Part Eleven

Futures: Brain Drain, War, and What Comes Next

Scenarios for the Russian Cyber Ecosystem

The Russian cyber ecosystem in April 2026 is under more structural pressure than it has been at any point since 2014. The brain drain triggered by the February 2022 invasion removed a significant portion of Russia's commercial technical talent pool. Sanctions have degraded access to Western technology inputs required for both offensive and defensive cyber operations. Attribution accumulation has constrained named officer mobility. And sustained international law enforcement coordination has produced a series of significant disruptions to the criminal financial infrastructure.

At the same time, the ecosystem remains broadly functional. Russia is still conducting active espionage operations (APT29 cloud operations, Center 16 Turla campaigns). Ransomware operators with Russian protection continue to extract payments from Western victims. GRU destructive operations continue against Ukrainian infrastructure. The ecosystem is resilient precisely because it is distributed: no single disruption is terminal.

The following three scenarios represent plausible trajectories over a 3-to-5 year horizon, based on current trends and structural factors. They are not predictions; they are analytical frameworks for thinking about which indicators to monitor.

Scenario A: Baseline Continuity with Gradual Capability Erosion

In the baseline scenario, Russia's cyber ecosystem continues to function broadly as it does today, with sustained but gradually degrading capability in specific areas due to compounding structural pressures. The brain drain effect becomes more visible as the cohort of officers and contractors who were technically trained before 2022 ages and is not replaced at the same depth. Export controls continue to limit access to advanced semiconductor technology, slowing toolset development. Attribution accumulation continues to constrain named officers.

Indicators to watch: Turla/Snake operational tempo (declining operational pace or increased technical mistakes would indicate capability erosion). GRU unit 74455 malware sophistication (if Industroyer-class tools are not updated or replaced, capability plateau is occurring). Contractor recruitment patterns (increased reliance on junior personnel or reduced security vetting visible in leaked documents or forum discussions).

Implications for Western investigators and policy: In the baseline scenario, sustained pressure continues to produce incremental results. The forensics arms race remains active but manageable. Indictment and sanctions pipelines continue to produce accountability even without arrests. The primary risk is complacency: the baseline looks like stability, but the compounding structural degradation is real even if slow.

Scenario B: More Criminal, Increasing Reliance on Protected Criminal Actors

In this scenario, the post-2022 officer talent shortage and ongoing technological constraints push the FSB and GRU toward greater reliance on protected criminal actors to supplement uniformed officer capacity. The model that the Yahoo case documented (officers directing criminal assets for intelligence collection) becomes more common as the professional officer corps thins. The contractor layer also expands, accepting more employees with weaker security vetting.

Indicators to watch: New documented cases of criminal actors receiving collection tasking from FSB or GRU handlers. Ransomware operations that show intelligence collection behaviors alongside financial extortion (targeting patterns consistent with SVR or FSB collection priorities). Increased forum discussion among criminal actors of state contact or protection arrangements. Contractor employee social media profiles showing rapid career changes into defense sector from criminal adjacent backgrounds.

Implications for Western investigators and policy: The more criminal scenario creates more access points for Western services. Criminal actors are more susceptible to CI recruitment, financial pressure, and third-country arrest than uniformed officers. A more criminal-dependent Russian cyber ecosystem is a more vulnerable one, though it is also potentially less predictable and less controllable by the state, which creates escalation risk.

Scenario C: More Isolated, Runet Fragmentation and Domestic Consolidation

In this scenario, Russia accelerates the "sovereign internet" project toward practical isolation of the Russian internet from the global internet, creating a domestic digital environment that is more surveilled, more filtered, and more controlled, but also more isolated from Western technical dependencies and Western intelligence visibility. TSPU capabilities are extended and deepened. Domestic technology substitution accelerates. Foreign platforms are systematically excluded.

Indicators to watch: Formal Runet isolation tests becoming operational exercises rather than tests. Domestic Russian technology companies winning government contracts previously held by foreign vendors. Significant reductions in Russian internet traffic visible at international exchange points. Domestic certificate authority expansion reducing dependence on Western root CAs.

Implications for Western investigators and policy: A more isolated Runet creates both advantages and disadvantages for Western investigators. Advantages: reduced surface area for Russian services to conduct operations requires them to route through more visible international infrastructure when operating against Western targets. Disadvantages: reduced Western intelligence visibility into domestic Russian criminal and state activity; domestic criminal infrastructure harder to reach through coordinated ISP action; more difficult for allied services to maintain passive collection inside Russian network space. Overall, the more isolated scenario tends to be bad for Western visibility while not fundamentally changing Russian offensive capability against Western targets, which is conducted through foreign infrastructure anyway.

Part Twelve

Research Agenda: What to Build and What to Monitor

Datasets to Maintain and Ongoing Monitoring Tasks

This section is a working reference for the sustained research and monitoring work needed to keep the analysis in this document current. It describes specific datasets to build and maintain, specific monitoring tasks to run on an ongoing basis, and specific trigger events that should prompt an immediate analytical update.

Core Datasets

Dataset	Fields to Track	Update Frequency	Primary Source
Officer / individual actor table	Name, service/unit, rank, role, indictment/sanction status, date, specific attribution, travel restrictions, last known location, family/associate network	On each new indictment, sanction, or public attribution	DOJ indictments, OFAC designations, Bellingcat OSINT, allied government statements
MLAT and cooperation log	Request date, requesting country, crime type, actor profile, state linkage, response type, response latency, outcome, geopolitical context at request time	On each documented request and response	Public DOJ reports, allied government disclosures, journalist reporting on specific cases
Vendor and contractor network	Company name, ownership, government contracts, FSTEC/FSO certification status, sanction status, technology dependencies, key personnel, intel service relationships	Quarterly or on new public disclosure	FSTEC certification database, Russian government procurement records, OFAC designations, Vulkan Files and similar leaks
Sanctions and indictment matrix	Actor name, entity type, sanctioning jurisdiction, date, stated basis, current status, successor entities, measured effect on operations	On each new sanction or indictment	OFAC SDN list, UK HMT list, EU consolidated list, DOJ press releases, FinCEN advisories
Crypto exchange and laundering node registry	Exchange name, registration jurisdiction, owner/operator, sanction	Monthly or on each new sanction/seizure	OFAC designations, FinCEN Section 311 orders, Chainalysis/TRM Labs reports, ICIJ reporting

Dataset	Fields to Track	Update Frequency	Primary Source
	status, documented illicit transaction volume, ransomware groups served, successor entities, seizure status		
Criminal group and RaaS tracker	Group name, lineage, state connection confidence level, key operators (named/anonymous), estimated victims, estimated ransom volume, current operational status, law enforcement actions	Monthly or on significant operational news	DOJ press releases, OFAC designations, commercial threat intelligence, blockchain forensics reports

Ongoing Monitoring Tasks

- New OFAC SDN designations involving Russian actors: Review narrative language in each designation for new factual information about state-criminal relationships, exchange operations, and officer connections. OFAC designation narratives often contain specific intelligence that is not available elsewhere in open source.
- DOJ indictments and criminal complaints: Read the full factual section, not just the press release. Mueller-style indictments contain officer names, unit addresses, malware authorship attributions, and operational method descriptions that are primary source intelligence documents.
- FinCEN advisories and Section 311 designations: The primary money laundering concern designations are more analytically detailed than OFAC designations. They contain entity-level transaction pattern analysis, percentage of illicit flows, named ransomware groups, and specific financial mechanisms.
- Allied government attribution statements (UK NCSC, CISA, Australian ASD): Joint attribution statements often contain technical detail not available in US-only publications. The February 2024 cloud-targeting advisory is a good example.
- Chainalysis and TRM Labs annual and quarterly reports: The most comprehensive synthesis of blockchain analytics data on ransomware payment volumes, laundering techniques, and exchange ecosystem. Cross-check figures between the two firms.
- Leaked documents (Conti, Vulkan, SyTech, Black Basta model): When large-scale document leaks occur, prioritize analysis of: (1) personnel lists and communications that can populate the officer/actor table; (2) infrastructure documentation that can update the vendor/contractor network; (3) operational communications that reveal state-criminal liaison relationships.
- Russian domestic legislation and regulatory actions: Roskomnadzor blocking orders, FSTEC certification updates, Yarovaya Law amendments, and Central Bank of Russia crypto regulation changes all have direct bearing on the operational environment for both state actors and criminal actors.

- Brain drain indicators: Russian GitHub contribution data, university enrollment statistics, emigration figures from the Russian Statistical Service (Rosstat), and Russian IT sector employment reports track the talent pipeline that feeds both the services and the criminal ecosystem.

Trigger Events Requiring Immediate Analytical Update

- New major ransomware infrastructure takedown: Update criminal group tracker, assess successor formation, track blockchain flows from seized wallets.
- New DOJ indictment of Russian state cyber actors: Update officer table, assess travel restriction implications, identify new evidential basis for sanctions actions.
- New OFAC designation of Russia-nexus exchange or mixer: Update exchange registry, assess whether predecessor-successor entity pattern applies, track post-designation operational continuity.
- New documented Russian-state attribution from allied government: Add to attribution accumulation record, assess implications for specific officers or units, identify new leverage for allied policy coordination.
- Significant document leak from Russian contractor or criminal group: Prioritize personnel list extraction and cross-referencing; infrastructure documentation for vendor network update; financial information for exchange registry update.
- Significant change in Russia-West diplomatic or sanctions relationship: Assess implications for MLAT cooperation probability; update geopolitical context field in cooperation log; adjust effectiveness assessments for diplomatic levers.

Part Thirteen

Sources, Reading List, and How to Go Deeper

Sources and Reading List

This section is organized by format and purpose, not alphabetically. The goal is to give a practical path from "read this first" to "go here when you need operational detail."

Essential Books

Andrei Soldatov and Irina Borogan have written the most consistently useful body of work on Russian intelligence services available in open source. Their books are narrative-driven, sourced in primary documents and interviews, and written for people who want to understand how these institutions actually function.

- "The New Nobility" (2010): The essential FSB book. Covers the service's evolution from KGB successor to Putin's primary domestic power instrument. Especially good on institutional culture, internal rivalries, and how the FSB accumulated political authority through the 2000s.
- "The Red Web" (2015): The essential Russian internet book. Covers SORM, TSPU precursors, Roskomnadzor, and the history of state control over Russian digital infrastructure. Directly relevant to the enabling institutions chapter.
- "Our Dear Friends in Moscow" (2025): Their most recent book, covering the generation of Russian professionals who came of age under Putin. Relevant for understanding the talent pool and cultural context from which the services recruit.

Mark Galeotti runs the Mayak Intelligence newsletter and the "In Moscow's Shadows" blog, which are the best ongoing open-source resources for Russian security service analysis. His ECFR paper "Putin's Hydra: Inside Russia's Intelligence Services" (2016) is the best concise structural overview of the full inter-service landscape.

Kevin Riehle's "Russian Intelligence: A Case-Based Study" (NI Press, 2022) is more academic but extremely well-sourced and uses case studies to illustrate how the services operate. Available through the National Intelligence University.

Andy Greenberg's "Sandworm" (2019, Doubleday) is the most readable deep-dive on Unit 74455 and the Ukraine power grid attacks. It reads like a thriller but is thoroughly reported. Essential background for anyone working on GRU destructive operations.

Primary Sources: Read These Directly

US DOJ indictments are underused by analysts who are not lawyers. They are primary-source intelligence documents that contain officer names, unit addresses, malware authorship

attributions, and explicit descriptions of operational methods. Reading the full text, not just the press release, almost always provides more detail than any secondary source.

Document	Date	What It Contains
US v. Netyksho et al. (GRU/APT28)	July 2018	12 Unit 26165 officers named by name, rank, and specific role. Full description of DNC hack, DCCC targeting, and Podesta operation. Read the full factual allegations section.
US v. Andrienko et al. (Sandworm)	October 2020	Six Unit 74455 officers named. Covers NotPetya, Olympic Destroyer, French election targeting, and Novichok false-flag deception campaign.
US v. Belan, Dokuchaev, Sushchin, Baratov (Yahoo/FSB)	2017	The canonical state-criminal hybrid case document. Describes case officer structure, asset payment, dual-purpose operation, and institutional protection mechanism in legally precise terms.
OFAC SDN Designation: Evil Corp / Yakubets	December 2019	Read the full SDN narrative, not just the names. The language about FSB relationships is explicit. Key evidentiary document for state-criminal overlap argument.
OFAC SDN Designation: Evil Corp expansion	October 2024	Covers Ryzhenkov, Benderskiy, and the LockBit connection. Extends the FSB-criminal link to include LockBit affiliate relationship.
FinCEN Section 311: PM2BTC	September 2024	Most detailed financial institution-level analysis of a Russian crypto laundering operation available in open source. Contains transaction pattern analysis, illicit percentage breakdown, and named ransomware group connections.
CISA/NSA/FBI/NCSC Advisory AA24-057A (APT29 cloud TTPs)	February 2024	Joint advisory summarizing APT29's evolved cloud targeting tactics. Practical technical guidance alongside attribution. Best current open-source summary of SVR cloud operations.
CISA Advisory AA23-129A (Snake/Turla)	May 2023	Most comprehensive single open-source document on Turla's technical infrastructure. Published in conjunction with Operation Medusa.

Ongoing Sources: Where to Keep Up

Source	Type	Best For
Recorded Future / Insikt Group	Paid intelligence; free reporting	Infrastructure analysis, actor tracking, dark web coverage; their annual Russia reports are comprehensive baseline reading
Bellingcat	Open-source investigation	Officer identification (GRU Salisbury model applied to cyber), travel tracking, OSINT methodology; reproducible techniques that analysts can apply
The Insider (theins.ru)	Russian investigative journalism	Internal FSB/GRU reporting; strongest on officer identities and internal service dynamics; primary source for Russian-language intelligence
Meduza (meduza.io)	Russian independent media	Political context, criminal cases with Russian government angles, domestic enforcement stories; publishes in Russian and English

Source	Type	Best For
Krebs on Security (krebsonsecurity.com)	Cybercrime journalism	Best English-language reporting on specific criminal actors, forum ecosystems, and case follow-ups; consistently accurate and operational
The Record (Recorded Future News)	Cyber news	Fast, well-sourced coverage of indictments, sanctions, operations; strong on the criminal side and law enforcement actions
CISA Advisories (cisa.gov)	US government	Technical attribution, malware analysis, defensive guidance; primary source for US government attribution statements
Agentura.ru	Soldatov/Borogan site	Ongoing FSB and security service monitoring; primary documents and Russian-language sources; direct access to original research
Mandiant / Google TAG reporting	Commercial threat intelligence	APT tracking, malware analysis, campaign attribution; their named actor reports are comprehensive and well-sourced
Galeotti's Mayak Intelligence	Expert analysis	Best single source for security service structural analysis and political context; weekly newsletter format
Chainalysis Crypto Crime Report	Annual research report	Most comprehensive annual synthesis of blockchain analytics data; covers ransomware payment volumes and laundering techniques
ZachXBT (Substack / X)	Independent blockchain investigation	Identifies specific OTC brokers, exchange accounts, and laundering clusters not yet formally sanctioned; investigations often precede official actions
Elliptic blog (elliptic.co)	Commercial blockchain analytics	Strong technical coverage of specific sanctions actions, DeFi and bridge-based laundering; current on cross-chain bridge usage by ransomware

For Deeper Work on Specific Topics

On Turla / Center 16 / Snake

The May 2023 CISA joint advisory on Snake malware (AA23-129A) is the most comprehensive single document on Turla's technical infrastructure. MITRE ATT&CK's Turla entry (G0010) aggregates all published research with technique mappings. Kaspersky's early Turla research (2014 to 2015) remains technically relevant for historical context.

On Sandworm / Unit 74455

Greenberg's "Sandworm" (2019) is the most readable deep-dive on Unit 74455 and the Ukraine power grid attacks. The October 2020 DOJ indictment is the primary legal document. ESET's research on Industroyer and Industroyer2 is technically definitive.

On APT29 / SVR

The joint CISA/NSA/FBI/NCSC advisory AA21-008A on SolarWinds (January 2021) is the primary government statement. Microsoft's Threat Intelligence Center reporting on Midnight

Blizzard (January and February 2024) covers the most recent cloud-targeting evolution. Volexity's original Dark Halo reporting is technically detailed on the SolarWinds detection story.

On the Criminal Ecosystem

Brian Krebs' multi-part Conti series ("Conti Ransomware Group Diaries," March 2022) is essential reading on the internal operations of a major ransomware organization. Chainalysis annual crypto crime reports track money flows. FinCEN advisories on ransomware contain detailed typology analysis that is underused by non-financial analysts.

On the Contractor / NTC Vulkan Model

The original Vulkan Files reporting consortium (Der Spiegel, Guardian, WaPo, Paper Trail Media, iStories, Le Monde) published in March 2023. Mandiant published concurrent analysis of the Vulkan documents with additional context. The full consortium reporting is free online. The SyTech contractor leak (2019) provides an earlier data point on the same contractor model.

A Final Note on Confidence

This document draws on confirmed public reporting, government documents, and well-sourced journalism. Where confidence on specific claims is lower (analyst inference, single-source reporting, circumstantial connections), it has been noted in context. The structural picture, how these services are organized and how they interact with the criminal ecosystem, is HIGH confidence. The operational details of specific officer relationships and current tasking arrangements remain partially obscured, and that is a known limitation of open-source analysis on this topic. The most analytically durable product of this kind of research is not the specific claims about current operations but the structural model: who has what authority, which institutions have which incentives, and where the documented vulnerabilities are located.