RANSOMWARE ECOSYSTEM DISRUPTION FRAMEWORK

Framework Overview and Reader's Guide

Version 0.2 | June 2026 | Working Document
Developed by Reno

READ THIS FIRST

This document is the entry point to the Ransomware Ecosystem Disruption Framework suite. It explains what the framework is, why it was built, how the documents relate to each other, and where to start based on your role. If you have received any document in this suite, read this one first.

SECTION 1 | WHAT THIS FRAMEWORK IS

The Russia-linked ransomware ecosystem does not reconstitute because it is resilient by accident. It reconstitutes because the criminal infrastructure, financial rails, and state protection relationships that sustain it are left intact after episodic disruption operations. Takedowns create friction. They do not create degradation unless the friction compounds over time across multiple layers simultaneously.

This framework is a structured system for producing that compounding effect. It defines the ecosystem, identifies its structural leverage points, assigns operational pressure across interagency lanes, measures the effects of that pressure, and maintains accountability for whether actions are producing the degradation they claim to produce.

THE SINGLE MOST IMPORTANT PRINCIPLE

Episodic takedowns are not the objective. Sustained ecosystem degradation is. Success is measured by compounding friction over time: actors spending more on security and reconstitution, Russian institutions treating criminals as liabilities rather than assets, protection relationships dismantled, ransom volume and operational tempo declining across multi-quarter windows.

Any operation that cannot demonstrate its contribution to that trajectory is operational activity, not strategic progress. This framework exists to make that distinction visible and defensible.

1.1 What This Framework Is Not

- A policy document or legal authority. Nothing in this framework constitutes operational authorization.
- A targeting directive. KPI outputs are measurement and accountability tools, not targeting panels.
- A static product. The ecosystem adapts. This framework must evolve with it.
- A leadership optics scorecard. Every metric traces to concrete underlying data. Undocumented operations do not count.
- A global ransomware framework. All documents are scoped to Russia/CIS-linked ransomware and associated enabling infrastructure unless explicitly stated otherwise. Do not apply to global ransomware without revisiting design assumptions.

1.2 The Strategic Logic

The Russia-linked ransomware ecosystem has three structural dependencies that, when pressured simultaneously, produce compounding friction:

Dependency	What It Enables	What Breaks It
Financial rails	Ransom proceeds converted to spendable fiat. Without cash-out, criminal income exists only on-chain.	OTC broker designation, exchange KYC pressure, mixer disruption, mule network friction (Nodes 01/02/08/09)
Operational infrastructure	Attacks conducted, payloads delivered, victims managed, data published. Without infrastructure, operational tempo collapses.	BPH takedowns, botnet sinkholing, leak site disruption, IAB market pressure (Nodes 03/04/05/06)
State protection	Elite actors insulated from Russian domestic enforcement. Without protection, domestic risk rises and	Krysha relationship disruption, FSB factional exploitation, FNS exposure, officer liability operations (Protection

Dependency	What It Enables	What Breaks It
	criminal-state bargain erodes.	Layer)

Pressure on any single dependency creates friction. Pressure on all three simultaneously creates degradation. The framework is designed to impose all three simultaneously, compounding over time.

SECTION 2 | THE FRAMEWORK SUITE

The framework consists of twelve documents and one Excel workbook. They are grouped into three tiers based on audience and operational sensitivity.

DISTRIBUTION TIERS

Tier 1 (Leadership): Strategic overview, macro KPI outputs. No individual officer names. For senior IC/LE leadership and STRAT offices.

Tier 2 (Operational): Full framework, node playbooks, measurement architecture, case studies, tracking tools. For interagency working groups and operational/analytic leads.

Tier 3 (Controlled Annex): Protection relationship inventory with individual officer detail, cooperation output from debrief records. Restricted to analytic teams with appropriate authorities.

2.1 Foundation Documents (Read in Order)

00 ALL TIERS

Framework Overview and Reader's Guide (this document)

Entry point. Explains what the framework is, how documents relate, and where to start by role. Read before any other document.

Who reads this: Everyone who receives any document in this suite.

01 ALL TIERS

Glossary of Terms

Defines all terms used across the suite, grouped by category with operational context. Covers framework-specific terms, ecosystem node terms, Russian institutional terms, legal/regulatory terms, technical terms, and partner/platform terms.

Who reads this: Anyone new to this material. Reference throughout.

2.2 Strategic and Institutional Documents

02 TIER 2

Ecosystem Disruption Playbook (Flagship)

The strategic framework for sustained disruption operations. Covers the four-phase model (Mapping, Pressure Alignment, Cost Imposition, Sustainment), engagement triggers to avoid, protection layer disruption methodology, affiliate strategy, and third-country arrest framework. The document all other operational documents reference.

Who reads this: Operational and analytic leads. Senior leadership for the Operator Snapshot section.

03 TIER 2

Dependency Map (Refined)

Priority-weighted disruption reference across all 16 ecosystem nodes. Orders nodes by disruption priority tier (CRITICAL/HIGH/MEDIUM), assigns partner lanes, defines disruption methods, and identifies backfire risk. The structural foundation from which the node playbooks were built. Note: Nodes 01-11 have companion playbooks and KPI tracking. Nodes 12-15 are mapped but not yet tracked at the meso layer.

Who reads this: Operational leads for workstream assignment. Analytic leads for ecosystem mapping.

04 TIER 2

Russian Government Protection and Exploitation Framework

Examines seven Russian government entities (FSB, MVD, Rosfinmonitoring, CBR, FNS, GRU, SVR) through a single lens: how each protects cybercriminals, what breaks that protection, what to do about it, and what will blow back. The institutional exploitation layer that underpins the protection layer strategy.

Who reads this: Analytic leads and operational teams working the protection layer track.

2.3 Node Disruption Playbooks

05 TIER 2

Phase A: Critical Node Playbooks (Nodes 01-03)

Operational playbooks for OTC Crypto Brokers (Node 01), High-Risk Exchanges (Node 02), and Bulletproof Hosting (Node 03). The financial backbone and primary infrastructure layer. Build first. Eight-section format: ecosystem role, structural vulnerabilities, pre-action requirements, action sequence, partner lanes, reconstitution monitoring, KPIs, and engagement triggers.

Who reads this: Operational teams with OTC/financial and infrastructure lanes. Treasury/OFAC, FBI/NCA, Chainalysis.

06 TIER 2

Phase B: High Node Playbooks (Nodes 04, 07, 08)

Operational playbooks for IAB Markets (Node 04), Underground Trust Infrastructure (Node 07), and Mixing/Obfuscation Services (Node 08). The operational engine and financial obscuration layer. Designed to run in parallel with Phase A and compound its effects.

Who reads this: Operational teams with access intelligence, underground monitoring, and financial obfuscation lanes.

07 TIER 2

Phase C: High Node Playbooks (Nodes 05, 06, 09)

Operational playbooks for Botnet/Loaders (Node 05), Leak Site Hosting (Node 06), and Mule Networks (Node 09, dual-track: Russia-domestic and third-country). Highest coordination complexity. Benefits directly from Phase A and B groundwork. Node 09 dual-track requires reading each track independently.

Who reads this: FBI/NCA/Europol (botnet), FVEY LE (leak sites), Rosfinmonitoring channel and FVEY LE/Europol (mule networks).

2.4 Measurement and Tracking Documents

08 TIER 2

KPI Measurement Framework

The complete measurement architecture. Three-layer system (micro/meso/macro), three macro themes (domestic enforcement, FSB strife, ecosystem economics), confidence labeling system, maturity levels, WAIS scoring guide, internal strife architecture, node cluster metrics, per-operation log template, ownership map, and governance. The analytic backbone of the suite.

Who reads this: Framework coordinator, interagency working group leads, operational teams responsible for metric population.

09
TIER 2

KPI Tracking Workbook (Excel)

The operational measurement instrument. Seven tabs: Instructions, WAIS Scorer (auto-calculating), Macro KPI Dashboard, Node Pressure tracker, Leak Site Signals, Group Pressure Tracker, and Operation Log. Compatible with Excel 97-2004 and later. No macros. Drop-down fields throughout.

Who reads this: All teams populating metrics. One workbook per reporting period or per active operation.

2.5 Reference and Training Documents

12
TIER 2

Historical Case Studies

Five real-world operations and events scored against the KPI framework: Conti collapse (2022), QakBot/Operation Duck Hunt (2023), LockBit/Operation Cronos (2024), BlackCat/ALPHV (2023-24), and Black Basta leak (2025). Demonstrates the framework works, calibrates WAIS scoring, and trains analysts on how to connect node-level pressure to macro ecosystem effects. All analysis is open-source only.

Who reads this: New analysts and operational teams onboarding to the framework. Reference for WAIS calibration.

11
TIER 2

Group Pressure Tracking Template

The operational instrument for sustained pressure campaigns against specific target groups. Seven sections: group profile, baseline metrics, pressure action log, observed effects tracker, WAIS log, strife event log, and 90-day assessment. One template per active target group. Pre-populated RansomHub annex included as a worked example.

Who reads this: Operational teams running sustained campaigns against specific actors or brands.

SECTION 3 | HOW THE DOCUMENTS CONNECT

The documents are not independent. Each feeds the others. Understanding the connections is required to use the suite effectively.

If you want to...	Start with...	Which feeds...
Understand the overall strategy and mission	Ecosystem Disruption Playbook (Doc 02)	Everything. Doc 02 is the strategic reference all other documents presuppose.
Understand Russian institutional behavior and exploitation	RU_GOV Protection Framework (Doc 04)	Protection layer strategy in Doc 02. KPI A-3 protection relationship inventory in Doc 08.
Understand ecosystem structure and node priorities	Dependency Map (Doc 03)	Phase A/B/C playbooks (Docs 05/06/07). Node cluster metrics in Doc 08.
Plan a specific node pressure action	Relevant phase playbook (Docs 05/06/07)	Micro-layer log in Doc 08/09. Group Pressure Tracker (Doc 11).
Measure whether actions are working	KPI Framework (Doc 08) and Workbook (Doc 09)	Leadership reporting. Interagency accountability. Pressure-effect ledger.
Score an arrest event	KPI Framework Section 6 (WAIS guide)	WAIS Scorer tab in Excel (Doc 09). Micro-layer log.
Track a sustained campaign against a specific group	Group Pressure Tracking Template (Doc 11)	Group Pressure Tracker tab in Excel (Doc 09). Micro-layer log.
Understand how past operations scored	Historical Case Studies (Doc 12)	WAIS calibration. Reconstitution benchmark setting. Training.
Look up a term	Glossary (Doc 01)	Any document where the term appears.

3.1 The Causal Chain

The framework is built on a single causal chain. Operations at the micro level must feed metrics at the meso level, which must explain movements at the macro level. If any link in the chain is missing, the macro numbers are not defensible.

Layer	Document	What It Requires From The Layer Below
MACRO: Ecosystem outcomes	KPI Framework (Doc 08), Excel Dashboard (Doc 09)	Meso-layer node metrics must explain why macro indicators moved. Without meso evidence, macro claims are narrative.
MESO: Node pressure	KPI Framework Section 3 (Doc 08), Node Pressure tab (Doc 09)	Micro-layer operation logs must document which specific actions produced which node-level effects. Without micro logs, meso metrics have no causal basis.
MICRO: Per-operation logging	KPI Framework Section 4 (Doc 08), Operation Log tab (Doc 09)	Every disruption action must have a log entry before acting (expected effects) and at 30/90/180 days (observed effects). Undocumented operations do not count.

SECTION 4 | WHERE TO START BY ROLE

Different roles require different entry points. This section gives a direct reading path for each.

Senior Leadership / STRAT Offices

- Read this document (Doc 00) for framework orientation.
- Read the Operator Snapshot section of the Ecosystem Disruption Playbook (Doc 02) for mission and four-phase summary.
- Review the Macro KPI Dashboard tab in the Excel workbook (Doc 09) for current ecosystem status.
- The KPI Framework document (Doc 08) Section 2 covers what each macro metric means and how to interpret it.
- Do not read node playbooks or the protection layer annex at this entry point. Those are Tier 2 operational documents.

Operational Leads (New to Framework)

- Read the Glossary (Doc 01) first. Many terms are framework-specific or used in non-standard ways.
- Read the Ecosystem Disruption Playbook (Doc 02) in full. This is the strategic foundation.
- Read the RU_GOV Protection Framework (Doc 04) for the institutional exploitation layer.
- Read the Dependency Map (Doc 03) for node priority and partner lane assignments.
- Then read the relevant phase playbook for your assigned node lane.
- Read the KPI Framework (Doc 08) to understand measurement obligations before any action.

Analytic Leads (Measurement and Reporting)

- Read the KPI Framework (Doc 08) in full. This is your primary reference document.
- Set up the Excel workbook (Doc 09) for your reporting cycle.
- Read the Historical Case Studies (Doc 12) to calibrate WAIS scoring and understand what framework-scored events look like in practice.
- Maintain the Group Pressure Tracking Template (Doc 11) for each active target group.
- The strife event log (KPI Framework Section 5.2) is your primary IC-value product. Own it.

Interagency Partners (Receiving Suite for First Time)

- Read this document (Doc 00) for full suite orientation.
- Read the Glossary (Doc 01).
- Identify your node lane from the Dependency Map (Doc 03) partner lane matrix.
- Read the relevant phase playbook for your assigned nodes.
- Review the Ownership Map in the KPI Framework (Doc 08, Section 7) to understand what metric population your agency is responsible for.
- Contact the framework coordinator to confirm your agency's ownership assignments and establish reporting cadence.

SECTION 5 | KNOWN GAPS AND SCOPE BOUNDARIES

This section is explicit about what the framework does not yet cover. Gaps are not failures. They are the next coordination agenda.

5.1 Nodes 12-15

The Dependency Map identifies 16 ecosystem nodes; Node 16 (Exploit/Vulnerability Brokers, CRITICAL) was added per the Module 06 assessment and does not yet have a playbook phase or meso-layer tracking. The node playbooks (Phase A/B/C) cover Nodes 01-11. Nodes 12-15 (Gray-Market VPS Networks, Domain/DNS Ecosystems, Data Exfiltration Staging Infrastructure, and Operational Proxy/Anonymization Services) are mapped in the Dependency Map but do not yet have companion playbooks or meso-layer KPI tracking. These nodes are designated MEDIUM priority with lower standalone disruption value. They will be incorporated into meso-layer tracking in a future framework update.

5.2 GRU-Nexus and SVR-Adjacent Actors

Actors with confirmed GRU operational nexus or SVR infrastructure overlap are explicitly outside this framework's scope. The institutional leverage logic (FSB factional exploitation, FNS exposure, MVD referrals) does not apply to state employees conducting military operations. These actors require separate analytic frameworks and different authority structures. If GRU nexus indicators are observed during operations within this framework, flag separately through appropriate channels.

5.3 Non-Russia CIS Actors

Actors operating under Kazakh, Belarusian, or other non-Russian CIS state protection require jurisdiction-specific analysis. This framework's institutional pressure points (FSB, MVD, FNS, CBR) are Russian. Belarus is operationally equivalent to Russia for framework purposes. Kazakhstan has functioned as an actual enforcement partner on specific cases and its dynamics differ meaningfully. Other CIS jurisdictions require case-by-case assessment.

5.4 L2 Ownership Gaps

Several high-value metrics in the KPI framework are designated Level 2 (Requires Buy-In) because they require formal interagency ownership or classified collection feeds that are not yet assigned. The most critical unresolved gap is the micro-layer operation log aggregator: without a designated agency or team responsible for collecting and maintaining per-operation logs across all active operations, the causal chain from micro to macro cannot be maintained. This gap is identified in the KPI Framework ownership map (Doc 08, Section 7) and is the highest-priority interagency coordination item.

5.5 Protection Layer Intelligence Products (Tier 1 Analytic Gap)

The protection layer disruption track (Doc 02, Section 9) is this framework’s primary strategic differentiator from prior disruption approaches. Its core premise is that FSB officer protection relationships are load-bearing ecosystem nodes, and that disrupting the officer’s financial exposure and internal FSB standing produces more durable ecosystem degradation than disrupting the protected criminal actor alone. This premise is analytically sound and well-supported by the institutional dynamics documented in Doc 04.

The intelligence products the track requires do not currently exist. Doc 02, Section 9.3 explicitly notes: “All deliverables in this section are proposed; none currently exist.” The three minimum deliverables required to execute the protection layer track are: (1) an anomalous outflow registry for the top 20 protected actors, identifying protection payment candidates from crypto-to-fiat financial maps; (2) officer financial exposure profiles built from open-source property registries, corporate registries, and lifestyle inconsistency analysis; and (3) a cash-out graph covering the top 20 OTC and broker nodes with end-to-end case exemplars. None of these products are built. Until they are, the protection layer disruption track is a documented methodology without an executable intelligence base.

This is the framework’s highest-priority analytic production gap. The intermediary cash-out mapping program and protection layer financial exposure capability are identified as the top two investment priorities in the Dependency Map (Doc 03, Section 3). Neither requires classified collection. Both are open-source and financial registry analytic tasks executable with existing blockchain forensics tools and OSINT methodology. The gap is one of resource allocation and tasking authority, not methodology.

5.6 Group Tracking vs. Actor Targeting

The Group Pressure Tracking Template (Doc 11) and Group Pressure Tracker tab in the Excel workbook (Doc 09) track group-level pressure effects. They do not constitute targeting directives for individual actors. Individual actor-level data (named operator identities, protection officer relationships, cooperation output from specific debriefs) is maintained in the Tier 3 controlled analytic annex under existing foreign-intelligence minimization rules, not in Tier 2 framework documents.

SECTION 6 | DOCUMENT REGISTRY

Current status of all documents in the framework suite as of June 2026.

Doc	Title	Version	Status	Distribution	Companion
00	Framework Overview and Reader's Guide	0.2	Working Document	All Tiers	All documents
01	Glossary of Terms	0.1	Working Document	All Tiers	All documents
02	Ecosystem Disruption Playbook	0.3	Working Document	Tier 2	All playbooks, Doc 08
03	Dependency Map (Refined)	1.0	Working Document	Tier 2	Docs 05/06/07
04	RU_GOV Protection and Exploitation Framework	3.0	Working Document	Tier 2	Doc 02, Doc 08
05	Phase A: Critical Node Playbooks (Nodes 01-03)	1.0	Working Document	Tier 2	Doc 03, Doc 08
06	Phase B: High Node Playbooks (Nodes 04/07/08)	1.0	Working Document	Tier 2	Doc 03, Doc 08
07	Phase C: High Node Playbooks (Nodes 05/06/09)	1.0	Working Document	Tier 2	Doc 03, Doc 08
08	KPI Measurement Framework	0.2	Working Document	Tier 2	Doc 09, Doc 11
09	KPI Tracking Workbook (Excel)	0.1	Working Document	Tier 2	Doc 08
10	KPI Sourcing Plan	1.0	Working Document	Tier 2	Doc 08, Doc 09
11	Group Pressure Tracking Template	0.1	Working Document	Tier 2	Doc 08, Doc 09
12	Historical Case Studies	0.1	Working Document	Tier 2	Doc 08, Doc 11

VERSION CONTROL NOTE

All documents in this suite are Working Documents subject to revision. Version tracking is maintained by the framework coordinator. Recipients should confirm they hold the current version before acting on this analysis. Changes to any document require interagency working group concurrence. The framework is reviewed quarterly at the metric level and annually at the structural level.

SECTION 7 | GOVERNANCE SUMMARY

Full governance detail is in the KPI Framework document (Doc 08, Section 8). This section provides the key rules for all users.

What This Framework Authorizes

- Measurement and accountability for disruption operations.
- Analytic input for operational planning.
- Interagency coordination on metric ownership and reporting.
- Strategic-level reporting to leadership on ecosystem degradation.

What This Framework Does Not Authorize

- Operational authorization for any specific action. Agency-specific authorities and approval processes govern operational decisions.
- Targeting of specific individuals. The framework tracks counts and trendlines of cases and relationship states, not a targeting panel.
- Use of macro KPI movements to justify new operational authorities without corresponding micro and meso evidence. A macro number moving in the right direction is not sufficient basis for expanded authorities. The causal chain must be shown.
- Distribution of Tier 3 controlled annex content (protection relationship inventory with individual officer detail) beyond analytic teams with appropriate authorities.

THE MOST IMPORTANT GOVERNANCE RULE

The protection-layer KPIs and strife event log entries involving officers are analytic products, not targeting directives. Any operational use of protection-layer analytic outputs must go through existing agency authorities and approval processes. At the leadership level, report counts and status categories only. Individual officer-level data stays in the Tier 3 controlled annex.