Category	Organisation / Provider	Key Data / Capability	Why Approach for HornetStrike	Typical Access Path
Telecoms / Tower Dumps / CDR	Vodacom South Africa	CDRs, tower dumps, IMSI/IMEI, subscriber (RICA) data	Core mobile footprint; essential for location/timing reconstruction in serious cases	Via SAPS / OIC lawful directions under RICA; no direct "open API"
	MTN South Africa	Same as above	Second major national MNO; different subscriber base and coverage	Same as above (RICA / s205-type processes)
	Cell C	CDRs, tower data, RICA	Smaller but still materially relevant subscriber base	Same as above
	Telkom Mobile	CDRs, tower data, RICA	Fixed–mobile blend, useful for edge cases and broadband-linked phones	Same as above
	Rain	Data-only mobile, CDR/tower info	Fills coverage gaps, data SIMs in IoT / routers	Same as above
	Major MVNOs (e.g. FNB Connect, Standard Bank Mobile, etc.)	Subscriber metadata, some CDR mirrored from host MNO	Banking-linked SIMs; useful correlation with financial data	Typically via host MNO + bank / MVNO contracts, not standalone LI
Vehicle & Traffic Registers	RTMC / NaTIS & eNaTIS	National register for vehicles, driver licences, contraventions, accidents – official traffic information system(RTMC)	Backbone for plate → vehicle → owner → licence resolution	Formal agreements via RTMC; case-by-case queries for LE; tightly governed by POPIA/NRTA
	SANRAL (Toll & gantry systems)	Toll/gantry passage records, some LPR/ANPR imagery	Historical movement of vehicles across tolled routes; links to VOI lists	MoUs with SANRAL; usually via SAPS lead for serious matters
	Provincial Transport Depts (e.g. Gauteng, KZN, WC)	Provincial traffic offences, local registers, sometimes accident data	Fill gaps in provincial enforcement/contravention history	Inter-gov MoUs; LE-led requests
	Metro traffic & metro police (JMPD, TMPD, EMPD, Cape Town, eThekwini, etc.)	Fixed cameras, speed-over-distance, local LPR, traffic violations	City-level movement and offence datasets; useful for route reconstruction	Direct MoU with each metro + SAPS collaboration
LPR / ANPR – National & Private	Vumacam (SafeCity)	City-wide CCTV and LPR; VOI hits, crime-fighting integration with private security and LE(Vumacam)	One of the biggest urban camera/LPR grids; ideal for real-time and historical vehicle traces	Commercial integration agreements; LE vetted access models
	NAVIC – National Vehicle Intelligence Cloud	National ANPR/LPR network; plate reads, VOI checks, SAPS/ICB integrations(NAVIC™)	Massive volume of plate reads; very mature vehicle-intel ecosystem	Commercial/API integration for vetted security/LE partners
	SNIPR	ANPR/LPR network linked to SAPS stolen/suspicious vehicle databases(SCP SECURITY V4White)	National LPR hits and alerts, widely used by CPFs and security firms	Commercial/API integration plus LE partnerships
	Estate / mall / gated-community LPR vendors (Chromesoftware, etc.)	Local ANPR streams at estates, malls, truck stops	Case-specific movements in small, high-value areas	One-off MoUs per site or via their LPR platform partners (NAVIC/SNIPR, etc.)
Financial Crime & Payments	SABRIC – SA Banking Risk Information Centre	Banking fraud intel, modus operandi, shared incident data, aggregated loss stats(SABRIC)	Central node for bank fraud intel; ideal for HornetStrike fraud typology feeds + alerts	Membership/MoU with SABRIC; data-sharing frameworks with banks & LE
	PASA – Payments Association of South Africa	Scheme rules, systemic payment data view, scheme-level risk controls	Bridges between individual banks and national payment mechanisms	Policy-level MoU; not a raw log pump, but key for access to scheme-level intel
	BankservAfrica	Interbank switching/clearing; rich transaction metadata patterns	Essential to correlate inter-bank flows in advanced fraud/mule networks	Strategic MoU for investigative exports; might pilot specific HornetStrike integrations
	South African Reserve Bank – NPS & Prudential Authority	Oversight of banks & payment system, AML/CFT supervision of banks(Reserve Bank of South Africa)	Regulatory perspective on high-risk institutions, FATF/FIC compliance	Policy-level collaboration; no bulk operational feed, but key for governance & escalation
	Major retail & challenger banks (ABSA, FNB, Standard Bank, Nedbank, Capitec, Tyme, Discovery, etc.)	Internal fraud alerts, transaction logs, KYC/KYB, device & behavioural intel	Direct case datasets when bank is victim or partner; supports HornetStrike pilots	Bilateral MoUs; often via SABRIC umbrella + case-specific legal orders
	Card schemes (Visa, Mastercard, etc.)	Cross-border card fraud intel, BIN/IIN data, chargeback patterns	Critical for international card fraud and cross-border mule routes	Scheme-level agreements; may tie into global fraud platforms HornetStrike consumes
Identity, Address, Ownership & Bureaus	Department of Home Affairs – National Population Register & new ID verification service	South African ID, birth, death, citizenship records; NPR/NIS verification APIs(SA News)	Core person identity ground-truth; binds all other datasets to real identities	API / verification service contracts for authorised entities; LE access via standing frameworks
	Credit bureaus: Experian, TransUnion, Compuscan (Experian), XDS	Credit history, addresses, employers, contact details, trace/skip-trace data(RCS Group)	Fast enrichment from ID/number/phone to addresses, employers, and related parties	Commercial contracts + strict FIC/POPIA compliance; often already integrated with banks
	CIPC – Companies and Intellectual Property Commission	Company registrations, directors, beneficial ownership proxies, IP registers(Wikipedia)	Maps suspects to companies, directorship networks and shell vehicles	API / bulk data or structured queries under contract; public search is too limited for HornetStrike scale
	Deeds Registries (Dept of Agriculture, Land Reform & Rural Development)	Property ownership, bonds, historical transfers	Asset-tracing and network-mapping for suspects and entities	Bulk/batch data agreements and case-driven queries
	Vehicle finance & insurance data providers	Asset finance, insured assets, policyholders	Links vehicles and assets to real people/companies beyond NaTIS	Contracts via banks/insurers; regulatory constraints apply
Financial Intelligence & AML	FIC – Financial Intelligence Centre	STR/SARs, cash threshold reports, terrorism financing intel, AML risk views(FIC)	Goldmine for network-level financial intelligence, especially if HornetStrike is positioned as an analysis surface	Policy and system-to-system integration under FIC Act; highly controlled
	SARB / Prudential Authority (again)	AML/CFT supervision, FATF linkage, bank-level risk supervision(Reserve Bank of South Africa)	Ensures HornetStrike aligns with national AML strategy and FATF expectations	Strategic MoU, not operational firehose
Law Enforcement, Intelligence & Prosecution	SAPS (including Crime Intelligence)	Case files, dockets, seized data (phones, PCs), crime registries	Primary operational user and source of case-level data (tower dumps, LPR exports, etc.)	National- and provincial-level MoUs, plus project-specific agreements
	DPCI (Hawks)	Serious commercial crime, organised crime, cybercrime investigations	High-value cases where HornetStrike can prove itself quickly	Dedicated integration at national unit level; joint task teams
	NPA & Asset Forfeiture Unit (AFU)	Prosecution case records, restraint/forfeiture data	Required for end-to-end trace from intel → prosecution → asset recovery	MoUs to support evidence-grade reporting and disclosure workflows
	State Security Agency (SSA)	Signals and strategic intelligence	Only relevant at Gov-core tier; overlaps with SIGINT and strategic investigations	Political/strategic engagement; extremely closed environment
	INTERPOL NCB Pretoria / AFRIPOL / SARPCCO	Notices, stolen vehicle & document databases, cross-border intel	Cross-border validation for IDs, vehicles, passports, and fugitives	Access via SAPS / DPCI; HornetStrike as an analytic consumer, not direct member
Traffic & Local Safety (Overlap with LPR)	Metro police & city CCTV units (Joburg, Tshwane, Cape Town, eThekwini, etc.)	City CCTV, intersection cameras, some LPR and traffic offences	Local movement, assaults/robberies, hijack routes connected to financial crime	City-level MoUs; often already interlinked with Vumacam/NAVIC/SNIPR
Universities & Academic / Data Partners	Universities South Africa (USAf)	Umbrella body for 26 public universities; coordination and policy for HE sector(Universities South Africa)	Single point to broker sector-wide partnerships (research, data-sharing frameworks, ethics)	MoU with USAf; then bilateral deals with individual universities
	Key individual universities: UNISA, Wits, UP, UJ, UCT, Stellenbosch, NWU, UKZN, TUT, CPUT, etc.	Large student and staff datasets; internal fraud and cyber incidents; research capacity (data science, cybercrime, criminology)	1) Data sources in specific fraud cases (NSFAS, registration scams, etc.) 2) R&D partners for analytics, ML and intel models	Case-specific agreements (for investigations) + long-term research MoUs
Other Strategic Data Sources	NSFAS and major bursary / funding schemes	Beneficiary, payment, and academic-link data	Connects education fraud to banking and ID fraud networks	MoUs plus FIC-aligned data-sharing where financial crime is involved
	Large private security groups (Fidelity, ADT, etc.)	Incident logs, response data, some local LPR/CCTV	On-the-ground intel, especially for hijackings, robberies and ATM attacks	Commercial integrations + SABRIC / SAPS-aligned JOCs
	Major retail groups & digital platforms (Pick n Pay, Shoprite, Takealot, etc.)	Loyalty, transaction, delivery address and device data	Useful in card-not-present fraud, mule purchasing, and address correlation	Bilateral agreements per investigation domain