

MARIE LANDRY'S SPY SHOP ♦ LANDRY INDUSTRIES

The Cyber-Physical Intelligence *Manifesto*

*Deploying lawful tactical hardware for epistemic ground truth in
an age of synthetic information.*

MARIE-SOLEIL SESHAT LANDRY

FOUNDER & SPYMASTER • LANDRY INDUSTRIES INC.
MONCTON • ACADIAN REGION • NEW BRUNSWICK • CANADA

RESEARCH DRAFT V1.0 — LAWFUL OPERATIONS EDITION

PREFACE

An intelligence model is only as strong as the evidence it can defend — in court, in print, and against an adversary who is trying to fool you.

The digital-only intelligence paradigm is under strain. Deepfakes, data poisoning, synthetic identities, and confabulating language models have made it cheap to manufacture a convincing digital reality. This book argues for a corrective: **Cyber-Physical Intelligence (CPI)**, the disciplined fusion of a lawful physical-collection layer with an open-source digital layer, adjudicated by structured analytic technique. Hardware anchors; open sources contextualize; the analyst decides.

A retail inventory of cameras, recorders, and trackers is not a distraction from serious intelligence work — handled correctly, it is the physical ingestion layer that grounds it. But "correctly" is the entire argument. The strength of CPI does not come from covert collection against unsuspecting targets. It comes from rigorous, lawful capture of records you are entitled to make, hashed and time-synced into evidence, and fused with open sources under a method that can survive scrutiny. Rigor, not trespass, is the edge.

SCOPE & LEGALITY

Every collection method described in this book is scoped to lawful operation under Canadian law. That means hardware deployed on premises you control, communications you are a party to (one-party consent), client sites under written authorization, assets you own, and consent-based monitoring. The covert interception of third parties — bugging conversations you are not part of, planting trackers on vehicles you do not own, recording into others' private spaces — is treated here as a legal hazard to be avoided, not a tradecraft to be taught. Chapter 3 sets out the law in detail.

AI-ASSISTANCE & VERIFICATION DISCLOSURE

This manuscript was developed with AI assistance and edited under the author's fact-checking discipline. The legal propositions in Chapter 3 are grounded in the primary Canadian statutes and the leading authority cited in the References. The technical and academic citations inherited from earlier strategy drafts were audited via live search for this edition: confirmed sources are cited in the References, mis-citations have been corrected, and unverifiable entries removed — see the Verification Note.

FRONT MATTER — FOUNDATIONS

The Hardware Axiom

A physical sensor converts the world into a record that is *costly to forge*. Photons strike a CMOS array; acoustic pressure waves move a diaphragm; radio-frequency timing reaches a satellite constellation. These are not magic. They can be spoofed, edited, or fabricated — GPS spoofing is real, video is editable, metadata can be altered. What they are is **expensive to fake convincingly**, far more so than a social-media post or a synthetic identity that can be conjured at near-zero cost.

THE AXIOM

Prefer the evidence that is most expensive to falsify — then spend your effort proving that this particular piece was not.

This reframes the old slogan that hardware is "un-falsifiable." It is not. The honest and more defensible claim is that physical capture raises the adversary's cost and complexity of

deception above the digital baseline. CPI exploits that asymmetry — and, crucially, never assumes it. Every anchor is validated before it is trusted.

The CPI Framework

Cyber-Physical Intelligence rests on three moving parts. First, a **lawful physical-collection layer**: sensors you are entitled to operate, producing timestamped, hashed records. Second, an **open-source digital layer**: the public reporting, registries, imagery, and documentation that supply context and scale. Third, an **adjudication discipline**: a structured method — here, the Analysis of Competing Hypotheses — that resolves conflicts between the two, deferring to the higher-integrity source only after that source's integrity has itself been checked.

The remainder of this book builds each layer in turn, states the legal boundaries that make it usable, adds the defensive counterpart (technical surveillance countermeasures), and closes with the ethics of putting lawful sensing in more hands.

CONTENTS

PART I — THE CASE FOR GROUND TRUTH

01 The Failure of Digital-Only Intelligence ▶

PART II — THE LAWFUL COLLECTION LAYER

02 The Tactical Edge: Hardware as the Lawful Ingestion Layer ▶

03 The Legal Architecture of Lawful Collection ▶

04 Technical Surveillance Countermeasures as Threat Modeling ▶

PART III — FUSION, PROVENANCE & MATERIALS

05 Fusing Hardware Streams with Deterministic OSINT ▶

06	Supply-Chain Verification & Material Provenance	▶
----	---	---

07	Advanced Materials as Hardware Solutions (<i>Research Program</i>)	▶
----	--	---

PART IV — SOVEREIGNTY & ETHICS

08	Sovereign Security & Ethical Frameworks	▶
----	---	---

—	Conclusion: The Lawful CPI Doctrine	▶
---	-------------------------------------	---

A	Appendix A — The CPI Operating Loop	▶
---	-------------------------------------	---

§	References	▶
---	------------	---

01

PART I — THE CASE FOR GROUND TRUTH

The Failure of Digital-Only Intelligence

An intelligence pipeline that draws only from digital sources has a single point of failure: the medium itself can be authored by your adversary. The collector sees what the network shows it, and the network is increasingly a curated, partly synthetic surface. This chapter sets out three failure modes that justify reaching for an anchor outside the manipulable medium.

1.1 The Virtual Illusion

Sophisticated actors no longer merely hide in digital noise; they manufacture it. Data poisoning seeds the open record with planted artifacts. Networks of synthetic identities generate coordinated, mutually corroborating "evidence." Search and recommendation surfaces can be gamed so that the most visible account of an event is the most engineered one. An all-digital collector that treats volume and consensus as signal is precisely the collector such operations are designed to defeat.¹⁰

1.2 Cognitive Over-Reliance

The second failure is human. Analysts under time pressure default to the dashboard — the platform-reported metric, the tidy figure, the document that arrives already formatted. Physical anomalies that contradict the digital story (a site that is busy when the records say it is idle, a shipment that moves when the manifest says it is parked) get discounted because they are inconvenient and hard to quantify. Automation bias compounds the problem: a number on a screen feels more authoritative than a contradiction in the world.

1.3 The Generative Hallucination Crisis

The third failure is new in degree. Large language models can fabricate fluent, plausible context — including citations and quotations that never existed — and a product built on unverified model output silently inherits those confabulations. The danger is not that models are useless; it is that they break the chain of evidence by inserting confident fiction into a workflow that assumes its inputs are real. An intelligence claim must trace back to something an adversary did not author and a model did not invent.

Conclusion to Part I: digital collection is necessary but not sufficient. The remedy is not to abandon it, but to anchor it — to fuse it with records drawn directly from the physical world under conditions the analyst controls and the law permits.

02

PART II — THE LAWFUL COLLECTION LAYER

The Tactical Edge: Hardware as the Lawful Ingestion Layer

Hardware you are entitled to operate produces records grounded in physics and stamped in time. This chapter treats three sensor classes as data sources — optical, acoustic, and telemetric — and the discipline that turns a raw capture into defensible evidence.

DEPLOYMENT SCOPE

Throughout this chapter, "deploy" means: on premises you own or control; in communications you are a party to; on client sites under written authorization; on assets you own; or with the documented consent of the person or owner concerned. Collection outside these bounds is addressed — as a prohibition — in Chapter 3.

2.1 Optical Capture (CMOS Integrity)

A digital image sensor records the light that actually reached it at the moment of capture, together with embedded metadata — timestamp, device, and often coordinates. Deployed on property you control or under authorization, a camera supplies a timestamped baseline against which digital claims can be cross-referenced: did the activity the documents describe actually occur, when they say, where they say? The evidentiary value depends on integrity, not just capture — which is why footage should be hashed at acquisition and its handling logged.

2.2 Acoustic Capture

Audio recording is governed tightly, and the boundary is the whole point. You may record conversations you are a party to, and environments you are authorized to record. Within that boundary, an audio record corroborates or contradicts a written account and preserves nuance a transcript discards. Outside it — recording a conversation between others to which you are not a party and to which no party has consented — the activity is a criminal offence, not a technique (see §3.1). Local capture integrity (hashing, secure storage, no onward interception) is the only kind worth building.

2.3 Telemetric Capture (GPS & Movement)

Location and telemetry data, gathered from assets you own or under a consent-based arrangement (for example, a fleet your organization operates and discloses), turns logistics from assertion into observation. Movement data is a powerful corroborant: it exposes the contradiction between what a supply-chain document claims and what a vehicle actually did. The lawful basis is ownership or consent; covert tracking of vehicles you do not own is treated in §3.3 as a hazard, not a capability.

2.4 The Integrity Discipline

A capture becomes evidence only when its provenance is defensible. That means calibrated devices, synchronized clocks, cryptographic hashing at the point of acquisition, tamper-evident storage, and a documented chain of custody. The discipline is unglamorous and decisive: an adversary's first move against physical evidence is to attack its integrity, and disciplined acquisition is what makes that attack fail.

03

PART II — THE LAWFUL COLLECTION LAYER

The Legal Architecture of Lawful Collection

The CPI model only works if its evidence is admissible and its collector is not committing an offence. This chapter states the relevant Canadian law as it actually is. It is the most important chapter in the book, because it is the difference between an intelligence capability and a criminal liability.

3.1 Interception of Private Communications

Under the *Criminal Code*, wilfully intercepting a private communication by means of any electro-magnetic, acoustic, mechanical, or other device is an indictable offence carrying up to five years' imprisonment.¹ Canada follows a **one-party consent** rule: the consent exception applies where the originator of the communication, or the person it was intended to reach, consents.¹ In practice this means you may record a conversation you are a participant in, or one in which a participant consents.

What the exception does not cover is the scenario the early strategy drafts treated as routine: planting a device to capture a conversation between other people, to which you are not a party and for which no party has consented. That is the core offence, not an edge case — and the "deploy hardware to intercept a target" framing is exactly what the section prohibits.¹

3.2 Recording Images & Voyeurism

Visual capture has its own boundary. The voyeurism offence reaches surreptitious recording where there is a reasonable expectation of privacy, and the Supreme Court has held that such an expectation can persist even in some public and semi-public settings.² Cameras on your own property are generally permissible, but they must not be aimed to capture areas where others retain that reasonable expectation — for instance, into a neighbour's home.

3.3 Tracking & Telemetry

The statutory tracking-warrant power authorizes a *peace officer* or *public officer* to obtain tracking data; it does not extend to private actors.³ There is therefore no equivalent lawful

route by which a private operator may covertly track a vehicle. Secretly placing a tracker on a vehicle you do not own, without consent, risks prosecution for criminal harassment or mischief, complaint to the Office of the Privacy Commissioner, and civil liability.⁴ The lawful basis for telemetry is ownership of the asset or the documented consent of the owner.

3.4 Licensing in New Brunswick

Providing investigative or security services for others is a regulated activity. In New Brunswick, the *Private Investigators and Security Services Act* requires a licence to act as a private investigator or to provide security services, ordinarily through a licensed agency, with liability insurance and a bond.⁵ Selling surveillance hardware is a distinct, unregulated commercial activity; deploying that hardware on a client's behalf is not. The line between "retailer" and "investigator" is a licensing line, and crossing it without a licence is itself an exposure.

3.5 Data Protection

Any personal information collected in the course of commercial activity engages federal private-sector privacy law, which requires consent for collection, use, and disclosure, limits collection to identified purposes, and imposes safeguarding and retention discipline.⁶ Sensor programs that gather identifiable data inherit these obligations from the moment of capture.

PRACTICE NOTE

Lawful collection is a precondition, not a finishing touch. Confirm your basis — ownership, party status, written authorization, or documented consent — *before* a device is deployed, and record that basis alongside the evidence it produces.

STANDING DISCLAIMER

This chapter describes the general statutory landscape and is not legal advice. Statutes are amended and interpreted over time; verify the current text and case law, and obtain advice from qualified counsel before relying on any proposition here in an operational or commercial context.

04

PART II — THE LAWFUL COLLECTION LAYER

Technical Surveillance Countermeasures as Threat Modeling

If physical capture is your ground truth, then protecting your own environment from hostile capture is the defensive half of the same discipline. Technical Surveillance Countermeasures (TSCM) — lawful, defensive bug-sweeping — is how an organization secures its own facts.

4.1 RF Spectrum Awareness

A portable spectrum analyzer establishes a baseline of the radio-frequency environment in a space and surfaces anomalies against it: an emitter that should not be there, a leak that should not exist. Spectrum awareness converts an invisible attack surface into an inspectable one, and a documented baseline makes future deviations obvious.

4.2 Non-Linear Junction Detection

Some threats do not transmit. Non-linear junction detection identifies the semiconductor junctions present in electronic devices regardless of whether they are powered or emitting, allowing dormant or quiescent electronics concealed in structures and furnishings to be located. It complements spectrum work by covering the threats that spectrum work alone would miss.

4.3 Corporate Vulnerability Auditing

A sweep is most valuable as an intelligence product: not merely "is there a device here," but "where is this organization exposed, and what would an adversary learn." For a research-driven firm, that audit protects proprietary R&D — the asset most worth stealing. Note that, depending on how such services are offered to others, provincial security-services licensing (see §3.4) may apply.

05

PART III — FUSION, PROVENANCE & MATERIALS

Fusing Hardware Streams with Deterministic OSINT

Collection is not analysis. This chapter sets out how lawfully-gathered physical records are fused with open-source material into a single, defensible picture.

5.1 Fact-Constant Synthesis

Treat a validated physical record — a hashed timestamp, a coordinate from an owned asset, a calibrated reading — as a *constant*: a fixed point against which narrative-driven digital inputs are measured. Open-source claims that conflict with a validated constant are flagged for scrutiny rather than averaged in. This is the operational form of separating what is fixed from what is merely asserted.

5.2 Zero-Leakage Local Architecture

Sensitive fusion belongs in a local-first architecture: a database that integrates sensor inputs with open-source collection without exfiltrating the underlying material to third-party services. The design goal is that the most sensitive correlations exist only where you control them, reducing both the attack surface and the privacy footprint of the work.

5.3 Structured Validation (Analysis of Competing Hypotheses)

When digital and physical sources disagree, the Analysis of Competing Hypotheses provides the adjudication frame.⁷ Candidate explanations are listed, each item of evidence is tested against all of them, and the hypothesis that survives the most disconfirmation prevails. The physical anchor is weighted heavily — but only after its own integrity has been validated, never on the assumption that "hardware cannot lie."

06

PART III — FUSION, PROVENANCE & MATERIALS

Supply-Chain Verification & Material Provenance

The same fusion discipline applies to provenance: corroborating where a thing came from and whether a chain of custody is intact. The framing here is commercial verification and audit — not interdiction against unconsenting parties.

6.1 Verifying the Organic Claim

Provenance claims — "organic," "single-origin," "unadulterated" — are assertions until corroborated. Consent-based and commercial sensing (environmental sensors on participating sites, owned tracking on your own consignments) can substantiate or undermine those claims with physical observation, supporting honest producers and exposing fraud against them. This is the verification spine of the broader organic-economy work the author has long pursued.

6.2 Chain-of-Custody Validation

Physical logging maps naturally onto recognized chain-of-custody concepts, for which international standards provide a common vocabulary and a set of custody models.⁸ Aligning your logging to those models makes your provenance evidence interoperable with auditors, certifiers, and counterparties rather than a private artifact only you can read.

6.3 Countering Adulteration

Where substitution or blending is suspected, marker identification and transit verification can expose the discrepancy between declared and actual material. Conducted as a commercial audit — with the cooperation or contractual rights that make it lawful — this turns provenance from a marketing claim into a tested fact.

07

PART III — FUSION, PROVENANCE & MATERIALS

Advanced Materials as Hardware Solutions

EDITOR'S NOTE — RESEARCH PROGRAM, NOT PRODUCT

This chapter describes a forward-looking materials research program (the author's Hempoxies line of work). The performance characteristics discussed are **hypotheses and design targets**, not validated specifications of a shipping product. Each claim requires experimental confirmation before it is represented as established.

7.1 Vitrimer Casings

Dynamic bio-based polymer networks (vitrimers) are an active field of academic research,¹¹ attractive in principle for enclosures because their reversible bonds suggest reworkable, lower-footprint hardware.¹³ The author's program explores hemp-derived vitrimer chemistries toward casings that could, in theory, be reshaped or decommissioned cleanly. The maturity level here is research, and the chemistry is a hypothesis under development.

7.2 Molecular Provenance

A complementary research direction is embedding traceable markers into a part so that the component can, in effect, attest to its own origin and history through spectrometric inspection. As a concept this aligns hardware with the provenance discipline of Chapter 6; as a capability it remains to be demonstrated.

7.3 Structural Integrity by Simulation

Molecular and mechanical simulation offers a path to designing rugged sensor housings before committing to fabrication.¹² The proposed use is to model candidate composites under operational stress and iterate in silico — a standard engineering approach, presented here as the intended method rather than a completed result.

08

PART IV — SOVEREIGNTY & ETHICS

Sovereign Security & Ethical Frameworks

Capability carries obligations. This closing chapter sets out where lawful CPI serves the public interest — and the ethic that keeps a decentralized model legitimate.

8.1 Agricultural Sovereignty

Field-deployable sensing, used lawfully on one's own or a cooperative's land, lets independent growers monitor and defend their operations — protecting greenhouse cooperatives and food-sovereignty efforts with their own ground truth rather than depending on external attestation. This is the protective application of the author's PhytoIntelligence work.

8.2 Mitigating Institutional Bias

Deterministic, auditable physical capture can act as a check on opaque predictive analytics. Where automated systems risk encoding social and administrative bias, a transparent record of what actually happened — collected lawfully and open to inspection — offers a corrective grounded in observation rather than inference. International guidance on the ethics of artificial intelligence frames the responsibilities such systems carry.⁹

8.3 Decentralizing the Intelligence Grid

Equipping citizen scientists and independent organizations with lawful sensing capability reduces the concentration of situational awareness in a few hands. But the decentralized model must be the *lawful* model, or it discredits the very cause it serves. A network that normalizes unlawful collection becomes the abuse it claims to counter; a network disciplined by consent and legality becomes a durable public good.

CLOSING ETHIC

Capability without legality is not power — it is liability wearing the costume of power.

CONCLUSION

The Lawful CPI Doctrine

The argument of this book reduces to a short doctrine. Anchor on the evidence that is costliest to fake, and validate it rather than trusting it. Collect only what you are entitled to collect — by ownership, party status, authorization, or consent. Fuse physical anchors with open sources under a structured method, and adjudicate conflicts by disconfirmation, not by volume. Protect your own ground truth with defensive countermeasures. Report with full provenance and a clear legal basis.

None of this depends on trespass, and that is the point. The competitive advantage of Cyber-Physical Intelligence is not access to the forbidden; it is the rigor and integrity of the lawful. A spy shop's inventory, in this frame, is not a catalogue of ways to break the law — it is the toolkit of a decentralized, lawful, ground-truth network.

APPENDIX A

The CPI Operating Loop

A ten-step sequence for running a Cyber-Physical Intelligence cycle within lawful bounds. Step 4 is the gate: nothing is deployed until its legal basis is confirmed and documented.

01 Observe the anomaly

Identify a conflict between the digital record and what appears to be happening in the physical world.

02 Define intelligence requirements

State precisely what physical observation — visual, acoustic, telemetric — is missing from the picture.

03 Hypothesize manipulation vectors

Map how the digital record might be spoofed, poisoned, or misreported by the relevant parties.

04 Design a lawful collection plan

Select appropriate hardware and confirm the legal basis for each capture — ownership, party status, written authorization, or documented consent. Record that basis.

05 Collect verbatim, hashed, time-synced records

Acquire the physical evidence with calibrated devices, synchronized clocks, and hashing at the point of capture.

06 Fuse the layers

Integrate the validated physical anchors with open-source collection in a controlled, local-first workspace.

07 Adjudicate by competing hypotheses

Resolve digital-versus-physical conflicts via ACH; weight the anchor heavily, but only after validating its integrity.

08 Formulate the conclusion

Synthesize the verified picture into an actionable intelligence product.

09 Replicate & calibrate

Re-test sensor calibration against known controls to confirm the evidence is sound.

10 Report with provenance

Publish findings with their full chain of custody and a stated legal basis for every collection step.

REFERENCES

The sources below were confirmed via live search against primary statutes, the leading authority, and the publishers of record. Where citations inherited from earlier strategy drafts contained errors, the corrected details are given here; the residual set that could not be confirmed is listed in the verification note that follows.

- [1] Criminal Code, RSC 1985, c C-46, s 184 (interception of private communications; one-party consent exception at s 184(2)(a); maximum penalty five years), and related ss 184.1–184.2.

Justice Laws Website – laws-lois.justice.gc.ca/eng/acts/c-46

- [2] R v Jarvis, 2019 SCC 10 (reasonable expectation of privacy and the voyeurism offence, Criminal Code s 162).

Supreme Court of Canada

- [3] Criminal Code, RSC 1985, c C-46, s 492.1 (tracking-device warrant; authority limited to peace and public officers).

Justice Laws Website

- [4] Criminal Code, RSC 1985, c C-46, ss 264 (criminal harassment) and 430 (mischief); see also the Personal Information Protection and Electronic Documents Act re: privacy complaints.

Justice Laws Website; Office of the Privacy Commissioner of Canada

- [5] Private Investigators and Security Services Act, RSNB 2011, c 209 (licensing of private investigators and security services in New Brunswick; agency, insurance, and bonding requirements).

CanLII – canlii.org/en/nb/laws/stat/rsnb-2011-c-209

- [6] Personal Information Protection and Electronic Documents Act, SC 2000, c 5 (PIPEDA) (consent, purpose limitation, safeguarding of personal information in commercial activity).

- [7] R J Heuer Jr & R H Pherson, *Structured Analytic Techniques for Intelligence Analysis (Analysis of Competing Hypotheses)*.
CQ Press / Pherson Associates
-
- [8] ISO 22095:2020, *Chain of custody — General terminology and models (Amendment 1 published 2026)*.
International Organization for Standardization
-
- [9] UNESCO, *Recommendation on the Ethics of Artificial Intelligence (2021)*.
UNESCO
-
- [10] A Yadav, A Kumar & V Singh, "Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security", *Artificial Intelligence Review*, 2023, 56:12407–12438, DOI 10.1007/s10462-023-10454-y.
Springer – corrected attribution (source draft mis-credited this DOI to "Al-Asadi et al.")
-
- [11] E Albertini, S Dalle Vacche & A Vitale, "Bio-based vitrimers: chemistry, performance and applications", *RSC Applied Polymers*, 2026 (advance article), DOI 10.1039/D5LP00408J.
Royal Society of Chemistry
-
- [12] "Molecular Simulation of Covalent Adaptable Networks and Vitrimers: A Review", *Polymers*, 2024, 16(10):1373, DOI 10.3390/polym16101373.
MDPI
-
- [13] "Pultrusion and Vitrimer Composites: Emerging Pathways for Sustainable Structural Materials", *Journal of Composites Science*, 2025, 9(10):559, DOI 10.3390/jcs9100559.
MDPI – corrected journal (source draft cited this as "Polymers")
-

VERIFICATION NOTE — LIVE-SEARCH AUDIT

The bibliography inherited from the earlier (Gemini-generated) strategy draft was checked source by source. **Confirmed genuine and now cited above:** the RSC bio-based vitrimers review, the *Polymers* molecular-simulation review, the *Journal of Composites Science* vitrimer-composites review, the *Artificial Intelligence Review* OSINT survey, ISO 22095, and the legal authorities. **Genuine but mis-cited in the source, now corrected:** the composites review was labelled "Polymers" when it is the *Journal of Composites Science*; and the OSINT survey was credited to "Al-Asadi et al." when its authors are Yadav, Kumar & Singh. **Not verifiable, and removed:** the Zenodo record cited as "Landry, 2025, Hemp Bionanocomposites" (DOI 10.5281/zenodo.15091234) does not resolve to that work and has been dropped pending a correct identifier. **Not authorities:** the TSCM-equipment and other vendor pages cited in the source draft are real commercial sources but not scholarly references, and are not listed. A few additional inherited items (specific institutional reports) were not independently confirmed and were left out rather than cited unverified.

M A R I E L A N D R Y ' S S P Y S H O P ◆ L A N D R Y I N D U S T R I E S

THE CYBER-PHYSICAL INTELLIGENCE MANIFESTO

RESEARCH DRAFT v1.0 — LAWFUL OPERATIONS EDITION

M A R I E - S O L E I L S E S H A T L A N D R Y · M O N C T O N , N E W B R U N S W I C K , C A N A D A

Developed with AI assistance under the author's fact-checking discipline. Legal propositions grounded in primary Canadian statutes; citations verified via live search, with corrections noted in the References. Not legal advice — consult qualified counsel before operational or commercial reliance.