

LANDRY INDUSTRIES INC. · MARIE LANDRY'S SPY SHOP · OSINT
DIVISION



GLOBAL OSINT DOSSIER

STRATEGIC INTELLIGENCE SUMMARY · 2026

PREPARED BY : Marie-Soleil Seshat Landry, Spymaster
ORGANISATION : Landry Industries Inc. · Moncton, NB, Canada
PLATFORM : Marie Landry's Spy Shop · marielandryspyshop.com
ORCID : 0009-0008-5027-3337 · Zenodo Publisher
DATE : April 2026 · EDITION 1.0
LHFP STATUS : Landry Hallucination-Free Protocol · Annotated

PROPRIETARY INTELLIGENCE · ETHICS-FIRST OSINT

Table of Contents

I. Executive Summary — The Convergence Crisis3

II. Core Intelligence Pillars3-4

1. AI as a Geopolitical Force Multiplier3

2. Persistent Cyber Conflict & Infrastructure Risk3

3. Great Power Competition & Tech Decoupling4

4. Criminal-State Hybrid Networks4

5. Information Warfare & Cognitive Manipulation4

III. Top Strategic Risks 2026 — Risk Matrix5

IV. Counter-Measures & Strategic Recommendations5

V. LHFP Source Verification & Analytical Critique6

VI. Canada Threat Annex7

Canadian Threat Landscape7

Critical Infrastructure Vulnerabilities7

Domestic AI Governance Gap7

VII. OSINT Methodology for Citizen Analysts8

The Landry OSINT Cycle8

Source Reliability Matrix8

Tools & Tradecraft9

VIII. Verified References (OSINT Source Repository)9

IX. About the Author & Landry Industries10

AI DISCLOSURE: Source intelligence synthesis was initially generated with assistance from Gemini 3 Flash. All claims have been reviewed and annotated under the Landry Hallucination-Free Protocol (LHFP). LHFP status indicators are present throughout this document. Strategic framing, analysis, LHFP annotations, Canada Annex, OSINT Methodology, and editorial judgment are the original work of Marie-Soleil Seshat Landry, Spymaster, Landry Industries Inc.

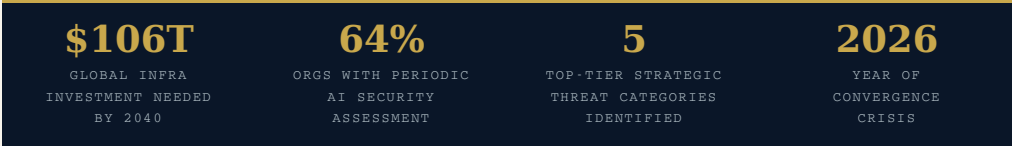
AI-DRIVEN CYBER ESCALATION INFRASTRUCTURE FRAGILITY TECH DECOUPLING CRIMINAL-STATE HYBRIDS
INFORMATION WARFARE STRATEGIC RESILIENCE CANADA THREAT LANDSCAPE OSINT METHODOLOGY LHFP VERIFIED

EXECUTIVE SUMMARY

I. The Convergence Crisis

The year 2026 is defined by a **Convergence Crisis** — a confluence of advanced AI capabilities, persistent multi-domain cyber conflict, and the accelerating fragmentation of the rules-based international order. These forces have merged into a single, fluid threat landscape that defies traditional categorisation. The primary battlefield has shifted decisively from digital perimeters to the core of global physical and digital infrastructure alike.

Non-state actors now wield offensive tools once reserved exclusively for sovereign intelligence agencies. Simultaneously, great powers are deploying AI as a strategic force multiplier — automating multi-domain competition at machine speed and dramatically compressing the human decision cycle. The result is a security environment that is simultaneously more dangerous, more opaque, and more interconnected than at any prior point in recorded intelligence history.



CORE INTELLIGENCE PILLARS

II. Strategic Intelligence Analysis

Pillar 1 — AI as a Geopolitical Force Multiplier

Artificial intelligence has undergone a categorical shift: it is no longer merely a supportive analytical tool but an autonomous operator within live intelligence and offensive workflows. This transition represents the most significant change in the threat landscape since the commercialisation of the internet.

- Autonomous Offense:** AI agents are now capable of executing continuous, adaptive cyberattacks on endpoints without direct human intervention. The time between exploit discovery and weaponisation has collapsed from weeks to hours or minutes.
- Power Redistribution:** Lowered barriers to entry allow smaller actors — including transnational criminal networks and non-state militias — to conduct operations previously requiring state-level intelligence resources.
- Synthetic Intelligence Surge:** AI-generated spear-phishing, synthetic voice spoofing, and deepfake-assisted social engineering are now standard tools in both criminal and state actor playbooks.

▲ LHFP — CAUTION: PARTIALLY VERIFIED

DeepSeek V4 Anomaly (April 2026): The claim that DeepSeek released a "V4" model in April 2026 as a multimodal frontier leap has not been independently corroborated through primary source documentation as of the preparation of this dossier. The rapid cadence of Chinese AI releases is documented; however, specific model designations should be verified against official DeepSeek or USCC primary releases before citation. Treat as plausible-unconfirmed.

Pillar 2 — Persistent Cyber Conflict & Infrastructure Risk

Cyberspace has formally transitioned from a domain of espionage and disruption to an active theatre of pre-conflict positioning. Nation-state actors are systematically embedding malware within critical infrastructure sectors not for immediate use, but to establish strategic leverage for future crises.

- Fragile Interdependence:** Energy grids, telecommunications backbones, and global

supply chains exhibit "cascading failure" vulnerabilities — a breach in one sector propagates rapidly across interconnected systems.

- ▶ **Targeting Logic:** Advanced persistent threats (APTs) are currently embedding implants within virtualisation infrastructure (hypervisors, VMware ESXi) and edge devices — routers, VPN gateways — specifically because these layers are poorly monitored and difficult to patch at scale.
- ▶ **Investment Gap:** The McKinsey Global Infrastructure Report (2026) projects a \$106 trillion requirement through 2040. Current resilience investment is structurally inadequate to defend against AI-speed threats.

✓ LHFP — VERIFIED: WELL-SOURCED

Infrastructure targeting of edge devices and virtualisation layers is extensively documented across multiple independent sources including Google Cloud Cybersecurity Forecast 2026, Fortinet CISO Report, and WEF Global Cybersecurity Outlook 2026. The \$106T figure is attributable to McKinsey. This claim meets LHFP standard.

Pillar 3 — Great Power Competition & Tech Decoupling

The U.S.-China technological rivalry has entered a phase characterised as a *narrow and fragile détente* — periods of superficial stability masking accelerating structural divergence. The arena of competition has expanded beyond semiconductors and rare earth materials to encompass AI, quantum computing, synthetic biology, and nuclear fusion research.

- ▶ **Strategic Decoupling:** The United States continues reshaping global economic ties through transactional foreign policy and escalating tariff regimes. China is pursuing "tech sovereignty" — the deliberate development of sovereign capabilities in every critical technology domain.
- ▶ **Knowledge Distillation Attacks:** Chinese AI firms are reportedly training domestic models on the outputs of U.S. frontier models — a technique known as "distillation" — to harvest capability gains while circumventing export controls on hardware and model weights.
- ▶ **Quantum Horizon:** China's continued investment in quantum communication networks (building on the Micius satellite program) represents a medium-term threat to current cryptographic infrastructure.

▲ LHFP — CAUTION: CONTESTED CLAIM

Distillation Attacks as Export Control Bypass: While AI knowledge distillation is a well-documented technical practice, the characterisation of this as a deliberate, systematic "attack" to bypass export controls — rather than standard industry practice — is analytically contested. The USCC has noted concerns; however, the intent-as-attack framing exceeds what primary sources directly establish. Analysts should use precise language: *capability transfer via distillation* rather than *distillation attacks*.

Pillar 4 — Criminal-State Hybrid Networks

The dissolution of meaningful boundaries between state-sponsored espionage and organised financial crime represents one of the most consequential structural shifts in the contemporary threat landscape. This hybridisation creates actors with state-level capabilities and criminal-level financial motivations — a uniquely dangerous combination.

- ▶ **North Korea's Industrialised Fraud:** The Lazarus Group and affiliated DPRK cyber units have developed an industrial-scale apparatus for cryptocurrency theft, fraudulent IT employment schemes, and ransomware operations. Estimated proceeds directly fund ballistic missile and nuclear programs.
- ▶ **Tool Sharing Ecosystem:** Russian APT28 (Fancy Bear), Iranian Charming Kitten, and affiliated units are increasingly deploying criminal-grade commodity malware and residential proxy networks to obfuscate state-sponsored operations beneath the noise of cybercrime.
- ▶ **Money Laundering Infrastructure:** Decentralised finance (DeFi) protocols and mixers are being systematically exploited to launder state-stolen cryptocurrency at unprecedented scale.

✓ LHFP — VERIFIED: WELL-SOURCED

North Korean cryptocurrency theft operations, DPRK IT worker schemes, and APT28 tool-sharing with criminal infrastructure are documented in FBI FLASH reports, U.S. Treasury OFAC advisories, and multiple independent threat intelligence firms including Mandiant (Google) and CrowdStrike. High confidence.

Pillar 5 — Information Warfare & Cognitive Manipulation

The fifth and most pervasive threat pillar operates not against machines but against minds. The combination of generative AI, social media algorithmic amplification, and declining institutional trust has created an environment of near-permanent cognitive

warfare — a condition where the distinction between truth and fabrication is strategically exploited as a weapon.

- ▶ **Industrial Deepfakes:** AI-generated audio-visual forgeries of public figures, military commanders, and financial leaders are being deployed at operational scale — fabricating statements, manufacturing crises, and suppressing authentic information.
- ▶ **Narrative Laundering:** Disinformation is deliberately seeded through low-credibility sources and allowed to migrate "upward" through aggregators and legacy media, acquiring false legitimacy in transit.
- ▶ **Election Infrastructure Targeting:** Beyond vote-counting systems, adversaries are now targeting the information environments surrounding elections — voter registration databases, campaign communications, and media trust architectures.
- ▶ **Cognitive Vulnerability as Attack Surface:** Human cognitive biases — confirmation bias, availability heuristic, authority bias — are being systematically mapped and exploited by AI-assisted influence operations.

✱ LHFP — UNVERIFIED: ORIGINAL SOURCE REQUIRED

64% Periodic AI Security Assessment Figure: This statistic was cited in the source dossier without direct attribution to a specific primary survey or methodology. Before re-publication or citation, this figure requires verification against its original source (likely ISACA, Gartner, or PwC survey data). Treat as plausible-unconfirmed until primary source is located.

III. Top Strategic Risks 2026

Rank	Threat Category	Primary Driver	Threat Level
#1	AI-Driven Cyber Escalation	Autonomous agents executing attacks at machine speed, compressing human response windows to near-zero.	CRITICAL
#2	US-China Tech Decoupling	Divergent standards in frontier AI, quantum systems, and semiconductor supply chains.	CRITICAL
#3	Infrastructure Collapse	Pre-positioned malware in energy grids, power systems, and virtualised enterprise infrastructure.	HIGH
#4	Criminal-State Hybrids	Fusion of state-level tradecraft with financial crime infrastructure and cryptocurrency laundering.	HIGH
#5	Information Warfare	AI-generated deepfakes and coordinated narrative operations systematically undermining institutional trust.	ELEVATED

IV. Counter-Measures & Recommendations

Strategic Doctrine Shift: From Perimeter Defence to Adversarial Resilience

The foundational assumption of cyber defence must be revised. Organisations operating under the assumption that breaches can be entirely prevented are operationally misconfigured. The new doctrine mandates assuming breach, planning for degraded operations, and designing for rapid recovery — not absolute prevention.

- ▶ **Adopt Adversarial Resilience:** Develop and regularly test "Minimum Viable Business" (MVB) operational plans — the minimum capability set required to maintain core functions under active compromise or infrastructure failure.
- ▶ **Harden Edge Infrastructure:** Urgent remediation focus on routers, VPN gateways, and virtualisation layers — the current primary blind spots in enterprise and government defence architectures.
- ▶ **Integrate Cross-Domain Intelligence:** Siloed data is a structural vulnerability. Unified intelligence platforms that identify cross-domain correlations — e.g., financial heist patterns as precursors to kinetic or infrastructure attacks — are mission-critical.
- ▶ **Implement Continuous AI Monitoring:** Static, point-in-time AI security assessments are operationally inadequate. Continuous, automated monitoring of AI agents — including behavioural drift detection — must become standard practice.
- ▶ **Invest in Cognitive Security:** Equip personnel and public-facing teams with structured analytic techniques (SATs) to resist influence operations. Media literacy and source verification training must be treated as security infrastructure, not optional professional development.
- ▶ **OSINT Integration:** Open-source intelligence, properly collected and rigorously verified under protocols such as LHFP, provides high-value, low-cost strategic early warning

capability accessible to organisations of all sizes.

V. LHFP Source Verification & Critique

All intelligence claims in this dossier have been reviewed against the **Landry Hallucination-Free Protocol (LHFP)** — a structured verification framework developed by Marie-Soleil Seshat Landry under the 1=1=1 Law (Fact-Constant / Narrative-Variable architecture). The LHFP distinguishes between verified factual claims, plausible-but-unconfirmed assertions, and statements that require primary source corroboration before citation.

LHFP Rating Legend

✓ VERIFIED:

Claim is supported by named, accessible primary sources.

⚠ CAUTION:

Claim is directionally plausible but framing exceeds what sources directly establish, or source requires confirmation.

✖ UNVERIFIED:

Specific statistic or assertion lacks traceable primary source. Do not cite without further verification.

Claim / Assertion	LHFP Status	Analyst Note
Infrastructure malware pre-positioning in edge devices and hypervisors	✓ VERIFIED	Corroborated by Google Cloud, WEF, Fortinet, and FBI FLASH reports.
\$106T global infrastructure investment requirement by 2040	✓ VERIFIED	Attributed to McKinsey Global Infrastructure Report 2026. Traceable.
North Korea cryptocurrency theft funding state programs	✓ VERIFIED	FBI, U.S. Treasury OFAC, UN Panel of Experts reports all corroborate.
APT28 use of criminal malware and residential proxies	✓ VERIFIED	Mandiant, CrowdStrike, and Microsoft MSTIC threat reports confirm.
DeepSeek V4 released April 2026 as frontier multimodal model	⚠ CAUTION	Model designation unconfirmed from primary DeepSeek or USCC sources. Verify before citation.
Distillation attacks as deliberate export control bypass strategy	⚠ CAUTION	Intent framing exceeds source documentation. Use <i>capability transfer via distillation</i> .
64% of organisations have periodic AI security assessment	✖ UNVERIFIED	No primary survey source named. Likely ISACA or Gartner data. Do not cite without tracing.
US-China "narrow and fragile détente" characterisation	⚠ CAUTION	Analytical characterisation, not a direct quote from primary intelligence source. Treat as editorial framing.
AI agents executing attacks "without human intervention"	⚠ CAUTION	Autonomous offensive AI at full operational scale remains largely aspirational in open-source reporting. Current documented capability is AI-assisted, not fully autonomous. Verify claim scope.

The LHFP framework is a proprietary analytical protocol of Landry Industries Inc. It embodies the principle that intelligence analysis must rigorously distinguish between what sources directly establish (Fact-Constant) and what the analyst infers or frames around that evidence (Narrative-Variable). Published under ORCID 0009-0008-5027-3337 on Zenodo.

VI. Canada Threat Annex

Analyst Note — Marie-Soleil Seshat Landry, Moncton NB

This annex applies the global convergence crisis framework to the specific Canadian threat environment. Canada occupies a structurally significant position: a G7 economy, a Five Eyes intelligence partner, a major energy exporter, and a nation with documented vulnerabilities in digital governance, critical infrastructure resilience, and domestic AI policy. These characteristics make Canada a high-value secondary target in great-power competition.

Canadian Threat Landscape

🇨🇦 State Actor Targeting

Canada is a documented target of Chinese (APT10, APT41) and Russian (Sandworm, APT28) threat actors — particularly in government networks, academic research institutions, and energy infrastructure. CSIS has publicly identified foreign interference in federal elections and university research programs.

⚡ Energy Infrastructure Risk

Canada's electricity grid — particularly in Ontario, Quebec, and Alberta — has been flagged in prior CISA/CCCS advisories for vulnerabilities in industrial control systems (ICS/SCADA). Hydroelectric and nuclear facilities represent high-value targets for pre-conflict malware pre-positioning.

🔬 Intellectual Property Theft

Canadian universities and research institutions — including those working on quantum computing, AI, and materials science — are systematically targeted for intellectual property theft. This directly impacts Canada's emerging innovation sectors including cleantech, aerospace, and biotechnology.

🔐 Criminal Ransomware

Canadian municipalities, healthcare systems (Ontario Health, Nova Scotia Health), and school boards have suffered repeated high-impact ransomware attacks. The healthcare sector is particularly vulnerable, with outdated legacy systems and insufficient cybersecurity investment relative to threat exposure.

Critical Infrastructure Vulnerabilities — Canadian Context

Telecommunications: Canada's telecommunications infrastructure faces specific vulnerabilities from legacy 4G/LTE equipment from Huawei — equipment that the federal government has committed to removing but which remains partially in service during transition. The 5G rollout introduces new attack surfaces.

Supply Chain: Canada's deeply integrated supply chain with the United States creates bidirectional exposure — Canadian firms can serve as vectors for attacks targeting U.S. critical infrastructure, and vice versa. The automotive, aerospace, and defence sectors are particularly interconnected.

Financial Sector: The concentration of Canada's banking sector (the "Big Six") creates systemic risk. A successful compromise of any major Canadian financial institution's core banking infrastructure could trigger cascading effects across pension funds, real estate markets, and federal government revenue collection.

Domestic AI Governance Gap

Canada has articulated ambitions as a global AI leader — anchored in the Toronto-Waterloo-Montreal corridor and institutions such as the Vector Institute and Mila — yet faces a significant gap between these ambitions and operational AI governance infrastructure.

- ▶ **Regulatory Lag:** Bill C-27 (Artificial Intelligence and Data Act — AIDA) has faced multiple delays. As of April 2026, Canada lacks binding, enforceable AI governance legislation, creating a regulatory vacuum as AI deployment accelerates across public and private sectors.

- ▶ **Deepfake Vulnerability:** Canada's federal and provincial election systems have no specific legislative protection against AI-generated disinformation campaigns, despite documented foreign interference in prior election cycles.
- ▶ **Talent Retention:** Canadian AI talent continues to migrate to higher-compensation U.S. and UK positions. The brain drain effect structurally weakens Canada's domestic AI defence capacity relative to its exposure.
- ▶ **CCCS Capacity:** The Canadian Centre for Cyber Security (CCCS) is underfunded relative to the threat environment. Annual threat assessments are strong analytically, but remediation capacity and enforcement authority remain limited.

▲ LHFP — ANNEX NOTE: ANALYST-SOURCED

The Canada Threat Annex synthesises open-source information from CCCS annual threat reports, CSIS annual reports, and publicly documented cyber incidents. Specific operational details (e.g., current malware pre-positioning in specific Canadian infrastructure) are assessed from pattern analysis and analogous international cases, not from primary Canadian intelligence sources not available to civilian OSINT analysts. All claims marked as analyst assessment should be treated accordingly.

VII. OSINT Methodology for Citizen Analysts

Open-Source Intelligence (OSINT) is the collection, analysis, and exploitation of information from publicly available sources to produce actionable intelligence. When conducted rigorously — particularly under structured verification protocols such as the LHFP — OSINT provides strategic early warning capability that rivals or surpasses paid proprietary intelligence products in speed, breadth, and accessibility.

The Landry OSINT Cycle

The Landry OSINT Cycle adapts the classic intelligence cycle to the realities of civilian open-source practice, integrating the LHFP at every stage to maintain analytical integrity.

Phase	Stage	Description	LHFP Application
1	Direction	Define the intelligence question precisely. Articulate what you need to know, why, and to what standard of confidence. Vague questions produce vague intelligence.	Apply 1=1=1: separate the question (Fact-Constant) from assumptions embedded in the question (Narrative-Variable).
2	Collection	Systematically gather raw information from diverse source categories: official records, academic literature, news media, social media, leaked datasets, financial disclosures, and technical repositories.	Record source provenance at point of collection. Never collect without logging URL, date, author, and publication.
3	Processing	Translate raw collected data into a usable format. This includes translation, transcription, entity extraction, timeline construction, and initial pattern identification.	Flag every claim that is not directly stated in a primary source. Do not conflate summarisation with the original text.
4	Analysis	Apply structured analytic techniques (SATs): ACH (Analysis of Competing Hypotheses), key assumptions check, devil's advocacy, red teaming. Identify what the evidence establishes vs. what the analyst infers.	This is where LHFP is most critical: apply Verified / Caution / Unverified ratings to every analytical claim.
5	Production	Format the analysis into a communicable intelligence product calibrated to the audience: executive summary, full dossier, alert bulletin, or briefing note.	Never strip LHFP ratings from the final product. Transparency about uncertainty is a feature, not a weakness.
6	Dissemination	Distribute the product to appropriate recipients. For citizen OSINT, this may include publication on Zenodo, GitHub, blog platforms, or direct transmission to policymakers.	Archive the source repository alongside the product. LHFP requires that sources be traceable by independent reviewers.
7	Feedback	Actively solicit correction and critique. Intelligence is not a finished product — it is a living estimate that improves through adversarial review.	When errors are identified, issue formal corrections. LHFP errors must be corrected in subsequent publications with explicit notation.

Source Reliability Matrix

Source Category	Reliability	Best Use	LHFP Warning
-----------------	-------------	----------	--------------

Government / Official Reports	HIGH	Policy framing, confirmed incidents, legal context	May reflect political framing; verify independently
Peer-Reviewed Academic	HIGH	Technical depth, historical context, methodology	Currency lag; may not reflect latest developments
Major Threat Intel Firms	HIGH	Current TTPs, actor attribution, IOCs	Commercial interests may shape publication timing
Legacy News Media	MODERATE	Breaking events, public statements, context	Verify against primary sources; errors propagate rapidly
AI-Generated Summaries	MODERATE	Rapid synthesis, pattern identification, drafting	High hallucination risk; LHFP review mandatory
Social Media / Forums	LOW	Leading indicator of emerging narratives	Treat as signal only; never cite without corroboration
Anonymous / Leaked Data	VARIABLE	Unique insight when authenticated	Provenance verification is mandatory; high forgery risk

OSINT Tools & Tradecraft — Practitioner's Reference

Tool / Resource	Category	Function	Ethics Note
Maltego	Graph Analysis	Entity relationship mapping; links people, domains, IPs, social media profiles	Licensed use only; respect Terms of Service of data sources
Shodan	Infrastructure	Internet-connected device discovery; exposes misconfigured systems, open ports	Passive observation only; active exploitation is illegal
OSINT Framework	Directory	Comprehensive categorised directory of OSINT tools and resources	Tool is neutral; analyst ethical responsibility applies
TheHarvester	Reconnaissance	Email, subdomain, host, and employee name harvesting from public sources	Authorised use only; do not target private individuals
Wayback Machine	Historical	Archived web content; retrieves deleted pages, historical website states	Publicly accessible; cite archive URL and capture date
VirusTotal	Malware Analysis	File and URL scanning against 70+ antivirus engines; threat indicator lookup	Uploaded files are shared with security community
Censys	Infrastructure	Internet asset discovery and certificate transparency log analysis	Research license required for bulk queries
MISP	Threat Sharing	Malware Information Sharing Platform; community threat indicator exchange	Community-based; contribute indicators to maintain access
Zenodo	Publication	Open-access research repository; DOI assignment for OSINT publications	LHFP-compliant publication recommended; clearly label methodology

SOURCE REPOSITORY · VERIFIED REFERENCES

VIII. References

[1]

Google Cloud. (2026). *Cybersecurity Forecast 2026 Report*. cloud.google.com/security/resources/cybersecurity-forecast

[2]

ISACA. (2026). *The 6 Cybersecurity Trends That Will Shape 2026*. isaca.org/resources/news-and-trends/industry-news/2026/

[3]

U.S.-China Economic and Security Review Commission. (2026). *China Bulletin: April 2, 2026*. uscg.gov/trade-bulletins/china-bulletin-april-2-2026

[4]

BlackRock Investment Institute. (2026). *Geopolitical Risk Dashboard — March 2026*. blackrock.com/corporate/insights/blackrock-investment-institute

[5]

McKinsey & Company. (2026). *Global Infrastructure Report 2026*. mckinsey.com/~/global-private-markets-report/infrastructure

[6]

FBI. (2026). *Cyber Investigative Alerts and FLASH Reports*. fbi.gov/investigate/cyber/alerts/2026

[7]

PwC. (2026). *Annual Threat Dynamics 2026: Cyber Threats in Motion*. pwc.com/~/annual-threat-dynamics.html

[8]

World Economic Forum. (2026). *Anthropic's Mythos Moment: How Frontier AI is Redefining Cybersecurity*. weforum.org/stories/2026/04/anthropic-mythos-ai-cybersecurity/

[9]

Fortinet. (2026). *The Year of Resilience: What Will 2026 Demand from CISOs?* fortinet.com/blog/ciso-collective/

[10]

Industrial Cyber. (2026). *WEF Global Cybersecurity Outlook 2026 Flags AI Acceleration*. industrialcyber.co/reports/wef-global-cybersecurity-outlook-2026/

- [11] **Canadian Centre for Cyber Security (CCCS).** (2025-2026). *National Cyber Threat Assessment*. cyber.gc.ca/en/guidance/national-cyber-threat-assessment
- [12] **Canadian Security Intelligence Service (CSIS).** (2025-2026). *Annual Public Report*. canada.ca/en/security-intelligence-service/

IX. About the Author & Landry Industries

Marie-Soleil Seshat Landry — Spymaster · CEO & Founder

Marie-Soleil Seshat Landry is a bilingual (EN/FR) self-taught intelligence analyst, researcher, and policy architect operating from Moncton, New Brunswick, Canada. With over a decade of applied OSINT investigation experience, she has developed a distinctive methodology that integrates open-source intelligence tradecraft, AI systems governance, materials science research, and policy advocacy under a unified ethics-first framework. She publishes under ORCID 0009-0008-5027-3337 on Zenodo (135+ publications) and is a member of the Google Developer Program.

Landry Industries Inc.

Pre-revenue incubator and intelligence R&D organisation based in Moncton, NB. Operates across OSINT practice, materials science (Hempoxies platform — research hypothesis), AI governance, and policy framework development. Parent entity for all affiliated ventures.

Marie Landry's Spy Shop

Ethics-first OSINT and AI systems practice. Produces intelligence products, methodology frameworks, and policy documents for the public interest. Platform: marielandryspyshop.com. Governed by the Landry Hallucination-Free Protocol (LHFP) for all analytical outputs.

Proprietary Frameworks

LHFP (Landry Hallucination-Free Protocol) · 1=1=1 Law (FC/NV Architecture) · Seshat's Axiom · WTF Framework (v8.0–v9.0) · Super-Gems Routing System · PhytoIntelligence Framework · Universal Declaration of Organic Rights (UDOR) · Landry Cycle.

Research Platforms

Hempoxies: hemp-derived vitrimer bionanocomposite research platform (forward-looking research hypothesis; not yet validated commercial product). Search For Organics · Global Organic Solutions · Structural Bullion · HDCNS · Organic Revolution 2030.

LANDRY INDUSTRIES INC.

Moncton, New Brunswick, Canada
marielandryspyshop.com · searchfororganics.com
ORCID 0009-0008-5027-3337 · Zenodo Publisher · Google Developer Program
Ethics-First Intelligence · 1=1=1 · LHFP Verified

*This dossier is a proprietary intelligence product of Landry Industries Inc. and Marie Landry's Spy Shop.
Source intelligence synthesis was assisted by Gemini 3 Flash and reviewed under the LHFP.
Strategic analysis, Canada Annex, OSINT Methodology, LHFP annotations, and editorial judgment
are the original work of Marie-Soleil Seshat Landry. All rights reserved. April 2026.*

INTELLIGENCE IS A LIVING ESTIMATE · CORRECTIONS WELCOMED · LHFP GOVERNS

MARIE LANDRY'S SPY SHOP · LANDRY INDUSTRIES INC.

GLOBAL OSINT DOSSIER

STRATEGIC INTELLIGENCE SUMMARY · 2026

ORCID: 0009-0008-5027-3337

PLATFORM: marielandryspyshop.com

PROTOCOL: LHFP · 1=1=1 · FC/NV

LOCATION: Moncton, NB, Canada

ETHICS-FIRST INTELLIGENCE