

CIA-GPT: The Comprehensive Guide

Marie Seshat Landry
Marie Landry's Spy Shop
marielandryspyshop.blogspot.com

1. Overview

CIA-GPT is a custom-trained AI model developed by Marie Seshat Landry using OpenAI's platform. It is designed to generate high-quality Open Source Intelligence (OSINT) reports in alignment with the IC OSINT Strategy 2024–2026. CIA-GPT helps CIA allies produce professional-grade intelligence reports with accuracy, clarity, and ethical integrity.

2. Core Objectives

- Support OSINT production for CIA allies and partners.
- Align with U.S. Intelligence Community (IC) directives.
- Streamline data collection, validation, and analysis.
- Enhance tradecraft with generative AI.

3. Custom Instructions

1. **Define the Objective** — Clearly articulate purpose, targets, and scope.
2. **Data Collection** — Collect from news, social media, public records, etc.
3. **Validation** — Cross-reference sources and filter irrelevant data.
4. **Analysis** — Use contextual, sentiment, and pattern analysis.
5. **Structure Reports** — Include:
 - Executive Summary
 - Introduction
 - Findings
 - Conclusion
 - Recommendations

- Appendices

6. **Clarity & Precision** — Maintain professional tone and formatting.
7. **Ethical Compliance** — Respect laws and privacy.
8. **Strategy Alignment** — Match IC OSINT Strategy 2024–2026.

4. **IC OSINT Strategy 2024–2026 Highlights**

- Coordinate Open Source Data Acquisition & Expand Sharing
- Establish Integrated Open Source Collection Management
- Drive OSINT Innovation (AI, ML, NLP, Automation)
- Develop the Next-Generation OSINT Workforce and Tradecraft
- Foster governance and partnerships across IC, academia, industry

5. **CIA-GPT Integration with IC Strategy**

- Employs AI to enhance collection and analytical speed.
- Enables federated collaboration via open-access datasets.
- Reduces redundancy through smart prompt templates.
- Provides actionable insights for warfighters and policymakers.

6. **100 OSINT Prompt Templates with Placeholders**

1. Investigate [Name] for [allegation] using OSINT and search.
2. Profile online activity of [User Handle].
3. Map financial records connected to [Target].
4. Track disinformation campaigns in [Country].
5. Monitor protest activity in [Location].
6. Analyze hate speech trends involving [Group].
7. Conduct pattern analysis on [Data Set].
8. Scan darknet forums for mentions of [Keyword].
9. Reverse-image search [Image Description].

10. Validate origin of viral content about [Topic].
11. Analyze influence network of [Public Figure].
12. Compile timeline of [Person]'s public appearances.
13. Profile Telegram channels used by [Extremist Group].
14. Extract metadata from video titled [Video Name].
15. Investigate cryptocurrency wallets linked to [Entity].
16. Map shell companies associated with [Business].
17. Analyze recruitment language in [Platform] by [Group].
18. Predict escalation timeline for [Conflict].
19. Locate satellite imagery confirming [Event].
20. Detect speech patterns in public addresses by [Name].
21. Investigate voter manipulation in [Region].
22. Compile aliases used by [Suspect].
23. Audit donations linked to [NGO].
24. Identify extremist symbolism in media from [Source].
25. Detect keyword surge for [Hashtag].
26. Analyze sentiment on [Event] across [Platforms].
27. Track hate group migration to [Platform].
28. Evaluate AI-generated content trends by [Author].
29. Identify key influencers in [Niche].
30. Detect psyops campaigns targeting [Group].
31. Extract court records involving [Individual].
32. Profile the digital footprint of [Organization].
33. Forecast threats against [Embassy or Facility].
34. Review past manifesto statements from [Name].
35. Trace public patents owned by [Scientist].
36. Compile data leaks mentioning [Company].

37. Analyze real estate purchases in [City] by [Nationality].
38. Track narrative framing in [Newspaper].
39. Compile public procurement by [Contractor].
40. Track coordinated hashtag campaigns in [Country].
41. Assess TikTok threats against [Entity].
42. Monitor militia chatter in [Forum Name].
43. Detect foreign agents' digital activity in [Agency].
44. Search public court rulings mentioning [Name].
45. Analyze ideology shifts in [Political Faction].
46. Monitor supply chain links tied to [Sector].
47. Investigate VPN exit node patterns for [IP Range].
48. Conduct IP traceback on [Website].
49. Evaluate foreign media narratives about [Topic].
50. Detect war crime indicators in footage from [Area].
51. Investigate known safe houses in [Region].
52. Profile violent lone actors tied to [Ideology].
53. Track youth radicalization on [App].
54. Analyze bot activity in [Hashtag].
55. Compare sentiment shifts before and after [Event].
56. Map misinformation clusters around [Subject].
57. Track digital signatures in malware linked to [Group].
58. Analyze Telegram exfiltration channels for [Leaks].
59. Forecast civil unrest in [Location].
60. Monitor travel patterns of [Suspect].
61. Identify propaganda dissemination through [Media].
62. Analyze subreddit content tied to [Theme].
63. Profile hacking operations of [Hacker Group].

64. Track refugee displacement from OSINT in [Conflict Zone].
65. Search job listings tied to [Military Group].
66. Audit social influencers spreading [Ideology].
67. Trace use of open-access AI tools by [Faction].
68. Detect insider threat signals in posts from [Employee].
69. Analyze game forums for recruitment language.
70. Extract anti-West narratives from [Platform].
71. Scan phishing domains targeting [Industry].
72. Investigate ghostwriting by intelligence-linked authors.
73. Map extremist graffiti patterns in [City].
74. Monitor student groups aligned with [Terrorist Entity].
75. Review anti-satellite weapon tests posted online.
76. Analyze fake NGO activity in [Region].
77. Validate drone footage over [Conflict Zone].
78. Compile satellite overpass timestamps for [Location].
79. Scan crowd-sourced reports in [Emergency].
80. Investigate public signal jamming in [Area].
81. Detect telecom manipulation in [Region].
82. Track visual meme trends after [Event].
83. Predict regime stability using [OSINT Signals].
84. Cross-verify casualties from [Attack].
85. Detect real-time sentiment changes in crisis tweets.
86. Map crowd movement via live cameras in [City].
87. Detect water contamination chatter online.
88. Analyze targeting doctrine of [Terrorist Group].
89. Profile cults emerging in [Online Community].
90. Audit GAI hallucinations influencing reporting.

91. Extract facial data from public security cams.
92. Scan open source code leaks from [Firm].
93. Evaluate cross-border smuggling indicators.
94. Compile livestream propaganda schedules.
95. Map black market medicine sales in [Region].
96. Assess rumor credibility about [Event].
97. Detect extremist TikTok trends post [Incident].
98. Audit crowd funding for terrorism in [Currency].
99. Investigate crash reports on suspicious drones.
100. Trace panic-buying indicators before [Disaster].
101. Detect violent incel forum activity upticks.
102. Validate nuclear testing OSINT from [Date].
103. Profile AI-generated content promoting [State Actor].
104. Scan for protest logistics posts on [App].
105. Investigate foreign surveillance gear in [Marketplace].
106. Review live police scanner transcripts for [Event].