

CIA-GPT: The Comprehensive OSINT AI Assistant Guide

Marie Seshat Landry
Marie Landry's Spy Shop
marielandryspyshop.blogspot.com
CIA-GPT on ChatGPT: g-scjrJgpFd-cia-gpt

July 26, 2025

1. Introduction

CIA-GPT is an advanced, custom-configured AI assistant designed for allies of the United States Intelligence Community (IC). Developed by Marie Seshat Landry, it empowers users to create professional-grade Open Source Intelligence (OSINT) reports that adhere to the highest intelligence standards, as defined in the IC OSINT Strategy 2024–2026.

This guide outlines the origin, configuration, usage instructions, and 100 versatile prompt templates for CIA-GPT, equipping analysts, researchers, and national security partners with a tool capable of transforming open data into actionable intelligence.

2. Purpose and Objectives

CIA-GPT was built with the following key objectives:

- Provide a streamlined framework for OSINT report generation.
- Equip non-governmental analysts with IC-aligned tradecraft.
- Enable faster, smarter, and ethically compliant investigations.
- Support decision-making processes for allied policymakers.

3. Custom Configuration Instructions

CIA-GPT operates under a custom GPT instruction set to ensure alignment with professional intelligence tradecraft:

1. **Define the Objective:** Identify targets, outline scope, and define aims.

2. **Data Collection Parameters:** Utilize web, social, academic, and government sources.
3. **Validation:** Cross-reference and verify source credibility.
4. **Analysis:** Extract insights using pattern, sentiment, and contextual analysis.
5. **Report Structuring:** Format using:
 - Executive Summary
 - Introduction
 - Findings
 - Conclusion
 - Recommendations
 - Appendices
6. **Precision:** Ensure factual, grammatically correct, and objective language.
7. **Legal Compliance:** Uphold privacy, ethical, and legal standards.
8. **Strategic Integration:** Align with IC OSINT Strategy 2024–2026.

4. Alignment with IC OSINT Strategy 2024–2026

CIA-GPT was developed in direct alignment with strategic focus areas outlined by the Office of the Director of National Intelligence:

- **Coordinate Open Source Data Acquisition and Expand Sharing**
- **Establish Integrated Open Source Collection Management**
- **Drive OSINT Innovation To Deliver New Capabilities**
- **Develop the Next-Generation OSINT Workforce and Tradecraft**

5. Use Cases

CIA-GPT supports a wide array of missions, including:

- Tracking online extremism and radicalization trends.
- Geolocating and timestamping disinformation content.
- Uncovering shell companies and illicit financial networks.
- Monitoring geopolitical risks and cyber threat actors.
- Verifying the authenticity of videos, images, and audio.

6. 100 OSINT Prompt Templates

1. Investigate the digital footprint of [Name] for ties to [Organization].
2. Identify cryptocurrency transactions linked to [Wallet Address] over the past 12 months.
3. Track public social media content from [Username] indicating radicalization.
4. Compile a timeline of suspicious real estate acquisitions in [City] by [Entity].
5. Analyze images and videos posted by [Group] for geolocation clues.
6. Scrape public records to identify shell companies tied to [Individual].
7. Search hacker forums for mentions of upcoming campaigns by [Threat Actor].
8. Detect influence operations linked to [Country] targeting [Event].
9. Monitor Telegram channels discussing protests in [Location].
10. Investigate extremist memes circulating among [Target Audience].
11. Analyze Reddit threads related to [Topic] for sentiment shifts.
12. Track disinformation narratives about [Subject] in [Language].
13. Review public procurement data for unusual contracts involving [Company].
14. Profile OSINT indicators of foreign surveillance equipment sales in [Region].
15. Identify digital signatures in leaked malware samples by [Group].
16. Assess satellite imagery of [Area] for activity changes since [Date].
17. Monitor forums for recruitment messages by [Paramilitary Group].
18. Track changes in Google Trends for terms related to [Ideology].
19. Reverse image search propaganda posters used by [Extremist Group].
20. Analyze protest logistics coordination via WhatsApp leaks.
21. Review Twitter/X posts for rising hostility against [Minority Group].
22. Investigate donations to NGOs operating in [Conflict Zone] for links to [Nation].
23. Compile a dossier of journalists targeted by disinformation in [Country].
24. Detect deepfake audio attributed to [Political Leader].
25. Scrutinize online stores selling tactical gear to [Radical Network].
26. Extract metadata from drone footage posted by [Militant Group].

27. Map hate crime incidents shared in local online communities in [City].
28. Analyze financial filings of [Tech Company] for indirect ties to [Entity].
29. Locate origin of viral false claim about [Incident].
30. Audit TikTok content pushing anti-[Country] propaganda.
31. Track location-tagged images from combat zones in [Region].
32. Identify fake news sites registered in [Country Code Top-Level Domain].
33. Detect indicators of cyberattacks in GitHub repositories from [Username].
34. Trace stolen passport scans being sold on forums linked to [Market].
35. Map IP ranges commonly used by disinformation botnets in [Region].
36. Monitor livestreams promoting insurgency in [Territory].
37. Identify journalists who have been targeted with online harassment campaigns.
38. Audit airline manifests for suspicious travel patterns of [Person of Interest].
39. Extract indicators of military movement from civilian satellite imagery.
40. Analyze backlash to sanctions on [Country] in domestic social media.
41. Review metadata of PDFs shared by [Propaganda Outlet].
42. Assess risks of insider threats at [Critical Infrastructure Company].
43. Identify training materials shared in jihadist forums.
44. Compile data on assassination threats posted in forums tied to [Group].
45. Detect cyberwarfare escalation patterns from open source chatter.
46. Track online militia fundraising efforts in [Cryptocurrency].
47. Search classified leaks mentioned on [Paste Site].
48. Extract public evidence of bio-lab activity near [Coordinates].
49. Verify authenticity of battlefield footage shared by [Actor].
50. Map suspicious domain registrations related to [Vaccine Disinfo Campaign].
51. Analyze sentiment about [Treaty or Policy] in non-Western media.
52. Investigate online chatter on retaliatory attacks for [Military Operation].
53. Detect online precursors to lone-wolf attacks in [City].

54. Audit TikTok micro-influencers spreading extremist ideology.
55. Cross-reference mugshots in law enforcement leaks with public data.
56. Track user migration from Facebook to encrypted apps after [Event].
57. Profile content creators who romanticize war for propaganda.
58. Analyze eBay and Etsy sales of restricted military gear.
59. Scan for rumors of coups or uprisings in [Unstable Region].
60. Detect public hacking guides shared on [Forum] for [Critical Sector].
61. Map censorship circumvention tool usage spikes in [Country].
62. Monitor Twitch streams promoting violent extremism.
63. Assess OSINT indicators of human trafficking networks in [Border Area].
64. Trace fake charities raising funds for terrorist organizations.
65. Search stolen ID leaks used for financial fraud in [Banking Sector].
66. Review patterns in phishing lures targeting [Gov Department].
67. Track defacement campaigns of Western sites by [Hactivist Group].
68. Analyze patriotic trolling campaigns originating in [Region].
69. Detect proxy server use from state-sponsored troll farms.
70. Identify misinformation spread during humanitarian disasters.
71. Review censorship laws used to suppress dissent in [Regime].
72. Profile deepfake technology distributors selling tools on [Marketplace].
73. Audit open Discord servers fostering incel radicalization.
74. Compile chatter about upcoming armed standoffs in [Location].
75. Analyze child exploitation risk from rogue influencers in [Country].
76. Trace passport scam networks using social ads in [Language].
77. Identify buyers of satellite phones linked to rebel groups.
78. Audit meme culture spread via political subreddit networks.
79. Track militia roadblocks reported via crowdsourced apps.
80. Search online hate forums for real-world violence announcements.

81. Monitor religious radicalization in diaspora communities.
82. Detect threats against polling stations from open channels.
83. Track info-ops against peacekeeping missions in [Conflict Zone].
84. Analyze calls to violence against scientists in [Research Area].
85. Compile images of civilian injuries for atrocity documentation.
86. Audit crowd movement data in authoritarian cities after protests.
87. Monitor propaganda livestreams on TikTok from war zones.
88. Assess OSINT indicators of diplomatic expulsions after [Incident].
89. Search aliases used in darknet narcotics marketplaces.
90. Trace ex-military personnel training paramilitary actors abroad.
91. Analyze trends in piracy operations on coastal regions.
92. Monitor drone usage patterns in terrorist reconnaissance missions.
93. Search patent filings that signal military dual-use potential.
94. Trace influencer networks supporting violent separatists.
95. Review state-controlled news footage metadata for fabrication.
96. Audit training camp locations using satellite archives.
97. Analyze voice biometrics for suspects using public podcasts.
98. Trace violent group coordination during sports events.
99. Identify covert messaging in online radical music videos.
100. Detect civil unrest signal peaks before regime changes.
101. Track OSINT indicators of cross-border smuggling networks.
102. Map education curriculum changes supporting extremist ideology.
103. Verify public birth records used in identity forgery.

7. Conclusion

CIA-GPT represents a leap forward in decentralized OSINT capabilities. Whether investigating extremist networks, cyber actors, or geopolitical threats, this AI-powered assistant enables rapid, reliable, and IC-compliant intelligence production.

For direct access, visit: **CIA-GPT on ChatGPT**.