Transnational Cyber Intelligence-Driven Cybercrime and Crimeware Analyst

Analyst training for the digital battlefield. Engage scenario-driven simulations against global crimeware actors and disrupt AI-augmented, financially integrated ecosystems with structured methods and Europol-aligned competencies.

Start Now (https://checkout.teachable.com/secure/209647/checkout/order_tngb7bzl)

Preview Syllabus

Delivery Mode

Online · Instructor-Supported · On-Demand Access

Course Length

Self-Paced · ~52 CPE Credits

Audience

Law enforcement, cybercrime analysts, prosecutors, CERT units, cryptocurrency investigators, intelligence professionals

Course Overview

Cybercriminal networks cross borders. Training follows them. Work real-world cases through structured analytic techniques blended with Europol competency frameworks. Track ransomware-as-a-service, infiltrate darknet

networks, analyze cross-border laundering, and think like the adversary to stop them.

Self-Paced · On-Demand · Online

You Will Master

Cybercrime Intelligence Methodology

- ✓ **Adversary modeling with 14 structured analytic methods**
- ✓ **Red teaming, pre-mortem thinking, estimative forecasting**
- ✓ **Crimeware ecosystems—operation, evolution, evasion**
- ✓ **Integration of SIGINT, OSINT, and AI-derived intelligence**

Crypto-Enabled Criminal Economies

- ✓ **Tracing illicit finance across decentralized platforms**
- ✓ **Exploiting blockchain transparency for seizures and attribution**
- ✓ **Typologies—fake arbitrage exchanges, scam-as-a-service, wallet drainers**
- ✓ **Links among laundering, hybrid warfare, and sanctions evasion**

Cognitive Tradecraft and Structured Thinking

- ✓ **Debiasing with AI-powered tools**

- ✓ **Alternative futures, indicators of warning, deception detection**
- ✓ **Adversary cultural profiles using Hofstede's dimensions**
- ✓ **Visual logic maps that turn data into action**

Simulations & Injects

- ✓ **Tabletops based on Europol and INTERPOL disruptions**
- ✓ **Actor-specific injects—Russia, Cartels, Southeast Asia, CaaS, Port Corruption Rings**
- ✓ **Case studies—malware-as-a-service and AI-generated deepfakes**
- ✓ **Crisis response drills for ransomware tied to geopolitical actors**

Course Modules

Full Module Outline

#	Module Title	Summary	Assignment / Activity
1	Foundations of Intelligence and OSINT in Transnational Cybercrime	Define intelligence operationally; treat OSINT as structured insight. Focus on reconnaissance phases, linguistic layering, pseudonym tracking, and surface-to-darknet transitions. Launch task-based outputs.	Tool-based OSINT lab and first-stage intelligence report
2	Stakeholder Analysis and Strategic Intelligence Framing	Map criminal ecosystems through stakeholder domains and influence modeling. Link actors to infrastructure, illicit finance, and logistics. Build adversary profiles with prioritization.	Stakeholder map and adversary profile
3	Data Provenance, Collection Discipline, and Digital OPSEC	Build evidentiary workflows with legal admissibility in mind. Operationalize browser capture, dark web monitoring, timestamping, and persona protection.	OPSEC simulation and chain-of-custody validation
4	Cultural Profiling and Behavioral Mapping	Apply Hofstede's dimensions to regional behavior and cyber activity. Analyze TTPs, deception patterns, and organizational logic across regions.	Behavioral mapping and deception signal detection

#	Module Title	Summary	Assignment / Activity
5	STEMPLES + Indicators of Change and Predictive Signatures	Track shifts in tradecraft, cadence, and volatility. Build predictive models to spot inflection points before escalation.	Predictive dashboard and volatility mapping
6	Adversary Targeting and Actor Ecosystem Mapping	Move from recognition to targeting. Model internal economies and hierarchies. Prepare disruption-ready targeting packages.	Targeting package with hierarchy map
7	Hybrid Threats, State Proxies, and Geopolitical Overlay	Assess cybercrime as geopolitical activity. Trace overlaps among ransomware, sanctions evasion, and proxy coordination.	Hybrid threat assessment and attribution simulation
8	Structured Analysis and Competing Hypotheses in Cybercrime	Apply ACH, red teaming, and futures methods to incomplete cases. Address mirror imaging and deception signals through structured output.	ACH matrix and futures projection

#	Module Title	Summary	Assignment / Activity
9	Cognitive Tradecraft and Bias Elimination	Confront bias and overconfidence. Calibrate estimative language, write under pressure, and deliver measurable products.	Bias mitigation report and writing drill
10	Applied Analysis Types and Behavioral Intelligence Structuring	Apply fourteen analysis types to behavioral patterns. Select models under constraint and brief escalation chains.	Escalation model and method matching
11	Intelligence Writing and Operational Report Development	Produce CIIR-style reports, simulation debriefs, and decision briefs. Move from interpretation to recommendation.	CIIR report and live brief simulation
12	Insider Threats and Elicitation Methods	Test claims under pressure, force impostors off-script, and treat video calls as forensic tests. Run liveness checks, workspace scans, and stress-tested interviews.	Elicitation lab with interview stressors

#	Module Title	Summary	Assignment / Activity
13	Case Studies	Full-spectrum adversary simulations close the course. Track actors, respond to injects, coordinate across jurisdictions, and deliver debriefs.	Capstone simulation and final debrief

Tools & Outputs

- ✓ AI-augmented writing templates for structured reports
- ✓ Visual maps that track laundering pathways
- ✓ Inject library aligned with IOCTA 2024 and Europol's cTCF
- ✓ Forensic readiness packs for investigative teams

Why Enroll?

- ✓ Real case files and operational blueprints
- ✓ Europol-compatible competencies that raise readiness
- ✓ Certification respected across task forces and intelligence units
- ✓ Mindset training that anticipates modern adversaries

Course Specifications

Prerequisites	**Basic intelligence tradecraft or prior experience in cyber or financial investigations recommended**
Learning Objectives	**Model adversary ecosystems with fourteen techniques; trace illicit finance; build Hofstede-based cultural profiles; apply bias-mitigation tools; plan OSINT and darknet collection with chain-of-custody; map actor networks and payment paths; integrate SIGINT, OSINT, and AI-derived intelligence; run tabletops; deliver field-ready structured reports.**
Format	**Recorded instructor-led video/audio modules on-demand with scheduled live web meetings, office hours, and direct messaging**
Technical Requirements	**Internet access; modern browser with extension permissions; ability to install required software on a PC or laptop**
Assignments & Assessments	**Scenario exercises per module; inject labs; quizzes on method application; final structured assessment in a full-spectrum simulation**
Resources & Readings	**Europol IOCTA 2024 and cTCF materials; AI-augmented writing and mapping templates; darknet forensic packs; 50+ downloadable guides and white papers**
Schedule & Timeline	**Self-paced with unlimited on-demand access**

Certification & Credits	**Approximately 52 CPE credits and Europol-compatible certification in transnational cybercrime intelligence**

Lead Instructor

Forty years of intelligence experience are built into this online recorded course with the availability for instructor office hours or email/text Q&A

-

Flexible Pricing

Access on-demand modules, templates, injects, and support. Progress at your pace and deliver operational outcomes.

Enroll Now (https://checkout.teachable.com/secure/209647/checkout/order_tngb7bzl)

Start Now (https://checkout.teachable.com/secure/209647/checkout/order_tngb7bzl)

Questions? Write info@treadstone71.com.

Your Instructor

Treadstone 71

Treadstone 71 is a woman and veteran-owned small business exclusively focused on cyber and threat intelligence consulting, services, and training. We are a pure-play intelligence shop.

Training dates and locations here (https://www.treadstone71.com/index.php/cyber-intelligence-training/training-event-listings)

Since 2002, Treadstone 71 delivers intelligence training, strategic, operational, and tactical intelligence consulting, and research. We provide a seamless extension of your organization efficiently and effectively moving your organization to cyber intelligence program maturity. Our training, established in 2008, follows intelligence community standards as applied to the ever-changing threat environment delivering forecasts and estimates as intelligence intends. From baseline research to adversary targeted advisories and dossiers, Treadstone 71 products align with your intelligence

requirements. We do not follow the create once and deliver many model. We contextually tie our products to your needs. Intelligence is our only business.

- We use intuition, structured techniques, and years of experience.
- We supply intelligence based on clearly defined requirements.
- We do not assign five people to do a job only one with experience.
- We do not bid base bones only to change order you to overspending.

We do not promise what we cannot deliver. We have walked in your shoes. We understand your pressures.

We are known for our ability to:

- Anticipate key target or threat activities that are likely to prompt a leadership decision.
- Aid in coordinating, validating, and managing collection requirements, plans, and activities.
- Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives as related to designated cyber operations warning problem sets.
- Produce timely, fused, all-source cyber operations intelligence and indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).
- Provide intelligence analysis and support to designated exercises, planning activities, and time-sensitive operations.
- Develop or recommend analytic approaches or solutions to problems and situations for which information is incomplete or no precedent exists.
- Recognize and mitigate deception in reporting and analysis.
  Assess intelligence, recommend targets to support operational objectives.
- Assess target vulnerabilities and capabilities to determine a course of action.
- Assist in the development of priority information requirements.
- Enable synchronization of intelligence support plans across the supply chain.
- ...and Review and understand organizational leadership objectives and planning guidance non-inclusively.

❓ Frequently Asked Questions

How long do I have access to the course?

The course is self-paced for up to 12 months.

COURSE EULA

Course EULA - REQUIRED Treadstone 71 LLC ("T71") IS WILLING TO LICENSE THE T71 Cyber Intelligence Training (COLLECTIVELY, "COURSE") UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS NON-COMMERCIAL VERSION LICENSE AGREEMENT ("AGREEMENT"). PLEASE READ THESE TERMS CAREFULLY BEFORE MOVING AHEAD WITH THIS COURSE. BY INSTALLING OR USING THE INFORMATION ON THE PROVIDED USB, YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, T71 IS UNWILLING TO LICENSE THE COURSE TO YOU ("YOU"), AND YOU SHOULD NOT INSTALL OR USE THE COURSE. NON-COMMERCIAL VERSION LICENSE To qualify for a Non-Commercial Version License, You must: (1) use the Course for non-commercial purposes as defined herein. The term "Non-Commercial Version License" is limited to using the concepts, methods, processes, procedures, and plans for internal organizational use. Entities are not allowed to teach this course or semblance of this course without express permission from Treadstone 71 LLC. Organizations are not allowed to deliver commercial services based upon this course that compete directly or indirectly with Treadtone 71 LLC. If You do not qualify for a Non-Commercial Version License, then you should discontinue the COURSE. GRANT OF LICENSE Provided that you qualify for a Non-Commercial Version License as specified above, and subject to the terms and conditions contained herein, T71 hereby grants You, an end user, a personal, non-transferable, non-exclusive, non-sublicensable license to install and use the

COURSE, free of charge, for non-commercial purposes only. In addition, subject to the terms and conditions contained herein and provided that You meet the requirement specified above for an Non-Commercial Version License, T71 hereby grants to You, an end user, a non-transferable, non-exclusive, non-sublicensable license, free of charge, to (1) use the COURSE for the intent of building or expanding a cyber intelligence program within your organization. For the avoidance of doubt, the following are considered examples of commercial uses of the COURSE: (1) use for financial gain, personal or otherwise; (2) use by government agencies without recompense to T71; (3) use by a telecommunication or Internet service provider company with recompense to T71; (4) use in connection with administering a commercial web site; (5) use in connection with the provision of professional service for which you or your company or organization are compensated (including paid administration); (6) bundling or integrating the COURSE with any other product, service, or another COURSE product for commercial use. (7) teaching this course in a seminar, online, commercial or academic setting. T71 and/or its licensors reserve all rights not expressly granted to You herein. This license is not a sale of the COURSE or any copy of the COURSE. The COURSE contains valuable trade secrets of T71 and its licensors. All worldwide ownership of and all rights, titles and interests in and to the COURSE, and all copies and portions of the COURSE, including without limitation, all intellectual property rights therein and thereto, are and will remain exclusively with T71. The COURSE is protected, among other ways, by the copyright laws of the United States and international copyright treaties. All rights not expressly granted herein are retained by T71 and its licensors. USE RESTRICTIONS You may not: (i) use the COURSE, except under the terms listed above; (ii) create derivative works based on the COURSE (e.g. incorporating the COURSE in a commercial product or service without a proper license). (iii) copy the COURSE (iv) rent, lease, sublicense, convey, distribute or otherwise transfer rights to the COURSE; (v) remove any product identification, copyright, proprietary notices or labels from the COURSE; or (vii) use any T71 trademarks in any manner other than their presence within Your copy of the COURSE without written permission of T71. Any and all copies made by You as permitted hereunder must contain all of the original COURSE's

copyright, trademark and other proprietary notices and marks. MAINTENANCE, SUPPORT AND UPDATES T71 is under no obligation to maintain or support or update the COURSE in any way, or to provide updates or error corrections CONFIDENTIALITY The COURSE and any license authorization codes are confidential and proprietary information of T71. You agree to take adequate steps to protect the COURSE and any license authorization codes, if any, from unauthorized disclosure or use. You agree that You will not disclose the COURSE, in any form, to any third party, except as otherwise provided herein. WARRANTY T71 EXPRESSLY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS, AND ANY WARRANTY THAT MAY ARISE BY REASON OF TRADE USAGE, CUSTOM, OR COURSE OF DEALING. WITHOUT LIMITING THE FOREGOING, YOU ACKNOWLEDGE THAT THE COURSE IS PROVIDED "AS IS" AND THAT T71 DOES NOT WARRANT THAT THE COURSE WILL RUN UNINTERRUPTED OR ERROR FREE NOR THAT THE COURSE WILL OPERATE WITH HARDWARE AND/OR COURSE NOT PROVIDED BY T71. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THE AGREEMENT. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU, AND YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE. TERMINATION This Agreement will terminate immediately and automatically without notice if You breach any provision in this Agreement. Upon termination You will remove all copies of the COURSE or any part of the COURSE from any and all computer storage devices and destroy the COURSE. At T71's request, You or your authorized signatory, will certify in writing to T71 that all complete and partial copies of the COURSE have been destroyed and that none remain in your possession or under your control. The provisions of this Agreement, except for the license grant and warranty, will survive termination. U.S. GOVERNMENT RIGHTS If You use the COURSE by or for any unit or agency of the United States Government, this provision applies. The COURSE shall be classified as "TRAINING COURSE", as that term is defined in the Federal Acquisition

Regulation (the "FAR") and its supplements. T71 represents that the COURSE was developed entirely at private expense, that no part of the COURSE was first produced in the performance of a Government contract, and that no part of the COURSE is in the public domain. (1) If the COURSE is supplied for use by DoD, the COURSE is delivered subject to the terms of this license agreement and either (i) in accordance with DFARS 227.7202-1(a) and 227.7202-3(a), or (ii) with restricted rights in accordance with DFARS 252.227-7013(c)(1)(ii) (OCT 1988), as applicable. (2) If the COURSE is supplied for use by a Federal agency other than DoD, the COURSE is restricted computer COURSE delivered subject to the terms of this license agreement and (i) FAR 12.212(a); (ii) FAR 52.227-19; or (iii) FAR 52.227-14(ALT III), as applicable. RESTRICTED RIGHTS Use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth in this agreement and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995),DFARS 252.227-7013(c)(1)(ii) (OCT 1988), FAR 12.212(a) (1995), FAR 52.227-19, or FAR 52.227-14 (ALT III), as applicable. Manufacturer is Treadstone 71 LLC, 11864 Izarra Way, 7206, Fort Myers, FL 33912 EXPORT LAW You acknowledge and agree that the COURSE may be subject to restrictions and controls imposed by the United States Export Administration Act (the "Act") and the regulations thereunder. You agree and certify that neither the COURSE nor any direct product thereof is being or will be acquired, shipped, transferred, or re-exported, directly or indirectly, into any country, except pursuant to an export control license under the Act and the regulations thereunder, or will be used for any purpose prohibited by the same. By using the COURSE, You are acknowledging and agreeing to the foregoing, and You are representing and warranting that You will comply with all of the United States and other applicable country laws and regulations when either exporting or re-exporting or importing the COURSE or any underlying information technology. Further, You represent and warrant that You are not a national of Cuba, Iran, Iraq, Libya, North Korea, Russia, Sudan or Syria or a party listed in the U.S. Table of Denial Orders or U.S. Treasury Department's list of Specially Designated Nationals. GOVERNING LAW This Agreement is governed by the laws of the State of Florida without regard to conflict of laws rules and principles. Application of the United Nations Convention on Contracts for the International Sale of

Goods is expressly excluded. MISCELLANEOUS If any provision hereof shall be held illegal, invalid or unenforceable, in whole or in part, such provision shall be modified to the minimum extent necessary to make it legal, valid and enforceable, and the legality, validity and enforceability of all other provisions of this Agreement shall not be affected thereby. No delay or failure by either party to exercise or enforce at any time any right or provision hereof shall be considered a waiver thereof or of such party's right thereafter to exercise or enforce each and every right and provision of this Agreement. This Agreement will bind and inure to the benefit of each party's permitted successors and assigns. You may not assign this Agreement in whole or in part, without T71's prior written consent. Any attempt to assign this Agreement without such consent will be null and void. This Agreement is the complete and exclusive statement between You and T71 relating to the subject matter hereof and supersedes all prior oral and written and all contemporaneous oral negotiations, commitments and understandings of the parties, if any. In the case of any conflict between the terms of this Agreement and the provisions of any purchase order for the COURSE, the terms of this Agreement shall control. Please contact the Director of Business Development at T71 11864 Izarra Way, 7206, Fort Myers, FL 33912 888.714.0071 – info@treadstone71.com

Once I enroll, what happens?

You receive an invitation email from Teachable.com, the online portal hosting our training classes. The email requires your registration into the course. One week before the course starts, we send you information on course requirements, what you will receive, links to other information, proper email addresses for books and other course information.

Course Cancellation Policy

If you wish to cancel your course registration, your registration fee will be fully refunded when written notification is received 30 days before class start. After that date, if you need to cancel your registration, please email info@treadstone71.com with the reason why you need to cancel. If you

have accessed the content (i.e., the class has started) we will be unable to refund your registration fee. Refunds will be issued back to the original payment method used within 5-7 business days minus platform registration fees.

Get started now!

Enroll in Course for $4,699