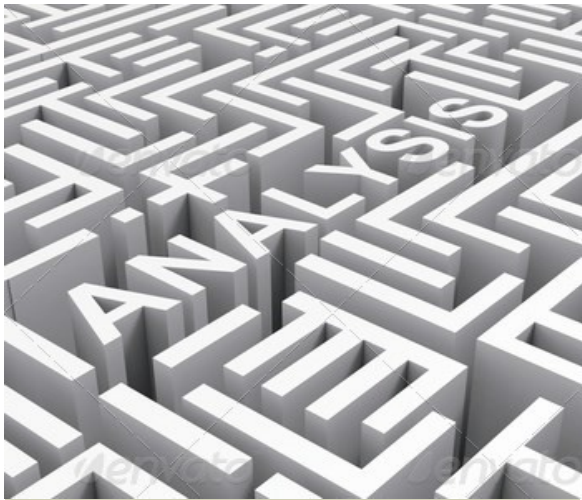


# Cyber Intelligence Program Development



We see what others cannot

Treadstone 71 Proprietary and Confidential



## Intelligence Training

- ANONYMITY AND CYBER PERSONAS
- INTRODUCTION TO INTELLIGENCE
- BASICS OF EFFECTIVE ANALYSIS
- ANALYSIS AND CRITICAL THINKING
- ERRORS IN and TYPES OF ANALYSIS
- CLANDESTINE CYBER HUMINT
  - Tor, Tails, Maltego, Oryon,
- CYBER COUNTERINTELLIGENCE
  - Perception as Deception, Social Psychology, Differences in Culture, Diversity, Hofstede Dimensions, Social Psychology, Reciprocity, Consistency, Social validation
- STRUCTURED ANALYTIC TECHNIQUES
- CRITICAL THINKING - COGNITIVE BIAS
- ANALYTIC WRITING AND REPORTING
- BRIEFINGS – DISSEMINATION
  - International Association for Intelligence Education Standards for Intelligence Analyst Initial Training



## Delivering the right information at the right time to the right people

The program and included courses examine Sherman Kent's Analytic Doctrine from the cyber perspective following traditional tradecraft and lifecycle activities. We assist and drive the building of intelligence strategic and program plans as well as methods to validate and communicate the plans. Laying the groundwork for an accepted and understood program requires leadership approvals and buy-in. Our program ensures these activities are successful. The Treadstone 71 Cyber Intelligence Program includes:

- ◊ Strategic Plan development, acceptance and dissemination
- ◊ Program Plan development, acceptance, dissemination, and implementation
- ◊ SoPs—Tradecraft focused, Hunt and Detect Mission Guidance, Incident Response Support, Campaign Analysis, Confidence Levels, Likelihoods
- ◊ Priority Intelligence Requirement development
  - ◊ Passive Intelligence Collection, Collection Planning, Mission Mgmt
  - ◊ Organization, Production Management, Processing - Decomposition
  - ◊ Structured Analytic Techniques - Analytic Writing and Dissemination
- ◊ Intelligence Lifecycle Development
- ◊ Virtual HUMINT Creation and Management
- ◊ Internet Exposure Assessment - Attack Surface Analysis - Perception Management - Sentiment Analysis
  - ◊ Deep Web, Forums, Social Networking, Closed Sites
  - ◊ Deception Detection and Credibility and Reliability Analysis
  - ◊ Pattern, Trends and Tendency Analysis – Campaign Analysis
  - ◊ Denial and deception identification
  - ◊ Serialized and Ad-Hoc Reporting
- ◊ Competitive Intelligence Assessment and Program Analysis
- ◊ Situational Awareness, Predictive and Preventive Analytics
- ◊ Campaign Analysis with Recommendations and Opportunities

The Treadstone 71 Program ensures support for organizational mission and objectives while strengthening intelligence across the enterprise. The program validates intelligence vision, mission, goals, objectives and intelligence requirements. Treadstone 71 incorporates both revolutionary and evolutionary methods. We work with you to establish the framework for creating, improving and measuring your program. Strategic goals and objectives are created and assigned. The program creates metrics, performance goals, milestones, and roadmaps. Treadstone 71 guides you through the journey anticipating modifications and shifts. The program helps you advance the enterprise intelligence program. Standardize intelligence oversight, peer reviews and governance as well as clear roles, responsibilities and job families. We also integrate with customer facing organizations providing advice and guidance on competitive intelligence. The bottom line:

*The Treadstone 71 program applies in-depth, substantive expertise, corporate and organizationally specific information and tough minded tradecraft to product and provide distinctive value-added recommendations and opportunities advancing corporate leadership's needs while improving organizational business interests.*



## PROGRAM AND TRAINING COMMENTS

“The Cyber Intelligence Training delivered and created by Jeff Bardin will add rapid returns to both Cyber Intel Analysts, and your Security Operations. This very thorough class prepares the student for your Cyber Intelligence function. This class starts with the history of intelligence as a tradecraft and the evolution to the digital corporate world. Along the way, each student receives quality instruction and hands on experience with today’s OSINT tools. This is necessary for anyone new to Cyber Intelligence, and complimentary to any Security Operations within your enterprise. This 4.5-day class provides the student with the resources and fundamentals needed to establish cyber intelligence as a force as both a proactive offensive step, and a counter intelligence-contributing arm of your larger team.”

“The class was very detail orientated with a strong focus on the work of Cyber threats and how to better secure your assets against potential attacks. He was able to answer each and every question asked with specific details, and then some. I would sign up again right away for any other classes offered by Jeff”

Anonymity—Personas—Measurement—  
Social Networking Intelligence—Traditional  
Tradecraft—Intelligence—  
CounterIntelligence—Cybercrime

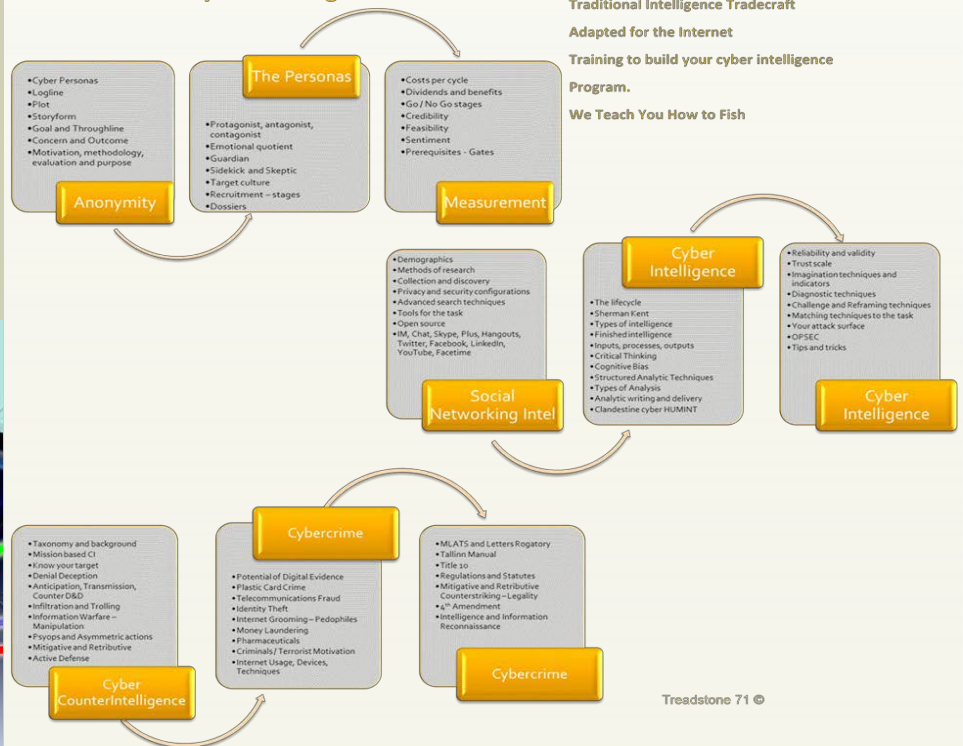


Program initiatives provide overall structural management, governance, risk, Intelligence operations, oversight, and compliance with applicable organizational regulations and statutes. Creating an Intelligence Center of Excellence helps facilitate the cyber intelligence, counterintelligence and cybercrime functions through the following areas:

- ◇ Open Source data collection
- ◇ Adversary actor dossier development
- ◇ Fraud detection and analysis, Fusion analysis
- ◇ Technical capabilities to protect collection activities
- ◇ Operational Threat Vector Analysis
- ◇ Threat Intelligence based upon proper basic and research intelligence
- ◇ Access to the proper tools necessary to manage the program
- ◇ Rules of engagement and escalation
- ◇ Continued training and understanding of tradecraft
- ◇ Methods of Analysis and Structured Analytic Techniques
- ◇ Analytic writing, peer review, bottom-line-up-front (BLUF) delivery
- ◇ Organizational attack surface situational awareness
- ◇ Global regulatory and statutory awareness

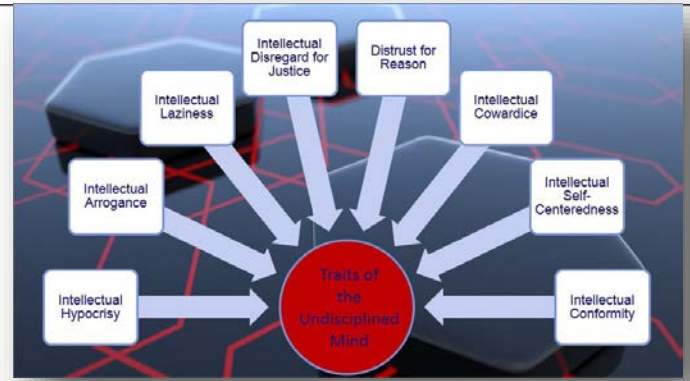
Each of these functional areas works in federation with corporate leadership and corresponding marketing, physical Intelligence and stakeholder functions. It is intended that this program integrates with and extracts requirements from all levels within your organization thus ensuring continuous improvement in Cyber Intelligence consistent with our mission statement.

### Treadstone 71 Cyber Intelligence



The Treadstone 71 Cyber Intelligence Program builds the foundation for and drives the actions needed to create a mature practice.

- Build skills and capabilities in OSINT tools for data collection
- Move from see, detect and arrest to prevention and prediction
- Align technical with social networking data.
- Create information of value
- Deliver actionable intelligence that is correct and complete
- Understanding link, trend, pattern, tendency, and anomaly analysis
- Develop capabilities that anticipate adversarial actions
- Reduce analytic cycle time
- Provide leadership with recommendations and opportunities
- Deliver the bottom line up front each time, every time



The Treadstone 71 Cyber Intelligence Program expands beyond traditional cyber intelligence and cover action tradecraft. We focus on understanding the actors, their capabilities, motivations, methods, and educational backgrounds. A true red team activity may only be performed if you fully understand and can replicate each nuance and detail of the adversary's methods. In contrast, using the same methods with the same technical footprint to penetrate adversary virtual organizations leaves a signature bound to be found.

Though the Program teaches highly structured methods in collection, organization, analysis, facilitation and dissemination, the patterns and trends showed by actual collection and technical footprints is consistently varied to demonstrate an ad hoc approach to the adversary.

The Program provides an understanding of the challenges of investigating cybercrimes and an awareness of the multitude of legal, ethical, and privacy related issues. The Program compares various theoretical and social perspectives use to explain cybercrime while analyzing the impact cybercriminals can create on your organization and your staff. We help you apply the proper cyber laws, regulations and cybercrime related legal concepts to tradecraft execution and infiltration activities.

Reach out to Treadstone 71 to learn more about the Cyber Intelligence Program and how we can lead your organization to a mature, effective and business driven intelligence program. 888.714.0071—[info@treadstone71.com](mailto:info@treadstone71.com) —[www.treadstone71.com](http://www.treadstone71.com)

We see what others cannot



TREADSTONE 71

888.714.0071 Office  
508.519.0363 Fax  
[info@treadstone71.com](mailto:info@treadstone71.com)  
[www.treadstone71.com](http://www.treadstone71.com)  
[www.cybershafarat.com](http://www.cybershafarat.com)  
[@treadstone71lc](https://twitter.com/treadstone71lc)

Treadstone 71 Proprietary and Confidential