Countering Disinformation and Foreign Influence Operations Training Course

Professional Development Training Course Outline

Category	Defense and Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In an era of rapid digital communication, the spread of disinformation, coordinated foreign influence campaigns, and manipulative online narratives has become a pervasive threat to national security, public trust, electoral integrity, and institutional stability. Governments, media institutions, private organizations, and civil society groups increasingly face sophisticated information warfare strategies that exploit social media, artificial intelligence, digital platforms, and psychological operations to distort facts, provoke division, and undermine democratic processes. Countering Disinformation and Foreign Influence Operations Training Course provides participants with deep, practical insight into identifying, analyzing, and countering modern disinformation tactics through strategic communication, intelligence-led analysis, and multi-stakeholder coordination.

Participants will learn how to integrate digital forensics, threat intelligence, behavior analytics, and narrative mapping to detect and disrupt influence operations in real time. The course emphasizes proactive countermeasures including resilience-building, strategic messaging, rapid response frameworks, and public awareness. Through structured case studies, practical exercises, and scenario-based simulations, learners will gain the competencies needed to safeguard information ecosystems and strengthen organizational capacity against manipulation, misinformation, and hostile foreign influence.

Programme Curriculum

Countering Disinformation and Foreign Influence Operations Training Course

Introduction

In an era of rapid digital communication, the spread of disinformation, coordinated foreign influence campaigns, and manipulative online narratives has become a pervasive threat to national security, public trust, electoral integrity, and institutional stability. Governments, media institutions, private organizations, and civil society

groups increasingly face sophisticated information warfare strategies that exploit social media, artificial intelligence, digital platforms, and psychological operations to distort facts, provoke division, and undermine democratic processes. Countering Disinformation and Foreign Influence Operations Training Course provides participants with deep, practical insight into identifying, analyzing, and countering modern disinformation tactics through strategic communication, intelligence-led analysis, and multi-stakeholder coordination.

Participants will learn how to integrate digital forensics, threat intelligence, behavior analytics, and narrative mapping to detect and disrupt influence operations in real time. The course emphasizes proactive countermeasures including resilience-building, strategic messaging, rapid response frameworks, and public awareness. Through structured case studies, practical exercises, and scenario-based simulations, learners will gain the competencies needed to safeguard information ecosystems and strengthen organizational capacity against manipulation, misinformation, and hostile foreign influence.

Course Objectives

1. Understand the foundations, motivations, and strategic goals of disinformation and foreign influence operations.
2. Identify digital platforms, channels, and ecosystems commonly exploited for influence activities.
3. Analyze disinformation tactics, bots, trolls, and coordinated inauthentic behavior using trending analytical frameworks.
4. Conduct threat intelligence assessments on influence actors, networks, and digital narratives.
5. Apply advanced OSINT techniques to detect early signs of coordinated influence campaigns.
6. Evaluate the psychological, cognitive, and social engineering techniques used in modern information warfare.
7. Build narrative mapping structures to track and counter harmful information flows.
8. Develop strategic communication responses to mitigate the impact of disinformation.
9. Strengthen institutional resilience through proactive policy, training, and monitoring systems.
10. Coordinate cross-sector collaboration between government, media, civil society, and technology platforms.
11. Integrate cybersecurity, data analytics, and digital forensics into counter-disinformation work.
12. Develop early-warning systems and rapid-response protocols for emerging influence threats.
13. Apply ethical, legal, and regulatory frameworks to counter-disinformation operations effectively.

Organizational Benefits

- Enhanced capacity to detect and mitigate disinformation campaigns
- Strengthened institutional resilience against influence threats
- Improved rapid-response coordination and communication strategy
- Reduced reputational and operational risk from misinformation
- Better situational awareness through advanced intelligence analysis
- Stronger cross-sector collaboration and crisis management
- Increased digital literacy and analytical capacity among staff
- Improved strategic communication and public engagement
- Enhanced protection of organizational credibility and trust
- Strengthened compliance with legal and regulatory information standards

Target Audiences

- Government communication and intelligence officers
- Media and public information professionals

- National security and defense personnel
- Civil society and non-profit governance teams
- Corporate risk management and crisis communication units
- Researchers, analysts, and policy advisors
- Digital security and cybersecurity teams
- Regulatory bodies and oversight institutions

Course Duration: 5 days

Course Modules

Module 1: Understanding Disinformation Ecosystems

- Define disinformation, misinformation, malinformation, and foreign influence
- Explore global trends shaping information manipulation
- Identify actors, motivations, and geopolitical drivers
- Examine digital platforms exploited for influence operations
- Assess societal vulnerabilities and psychological triggers
- Case Study: Election-related disinformation campaign in a developing democracy

Module 2: Digital Tactics, Tools, and Amplification Techniques

- Understand bot networks, troll farms, and coordinated inauthentic behavior
- Analyze algorithmic amplification and virality engineering
- Track hashtag hijacking, meme warfare, and micro-targeting
- Identify synthetic media and AI-generated content
- Map influence operations across cross-platform networks
- Case Study: Coordinated botnet amplification during a national crisis

Module 3: Threat Intelligence for Disinformation Detection

- Conduct OSINT investigations for influence tracking
- Apply digital forensics to identify false narratives
- Use threat intelligence tools for pattern detection
- Build profiles of hostile information actors
- Monitor emerging narratives and early-warning indicators
- Case Study: Intelligence analysis of a foreign propaganda network

Module 4: Psychological and Behavioral Dynamics of Influence

- Explore cognitive biases exploited in disinformation
- Understand emotional manipulation and narrative framing
- Examine culture, identity, and group polarization
- Analyze psychological warfare techniques
- Design awareness strategies to strengthen cognitive resilience
- Case Study: Psychological impact of disinformation during a public health crisis

Module 5: Strategic Communication for Counter-Narratives

- Create strong, credible counter-messaging frameworks
- Develop proactive communication strategies for crisis periods
- Build audience-specific engagement tools

- Apply narrative correction and inoculation strategies
- Integrate data analytics in communication planning
- Case Study: Counter-narrative campaign that successfully neutralized a false claim

Module 6: Cybersecurity and Platform Governance in Influence Operations

- Explore the intersection of cybersecurity and disinformation
- Identify platform-level vulnerabilities and policy gaps
- Examine regulatory frameworks for digital platforms
- Strengthen internal cyber hygiene and monitoring
- Coordinate with platforms for threat reporting and mitigation
- Case Study: Cyber breach used to seed disinformation across social media

Module 7: Institutional Resilience and Policy Frameworks

- Develop internal policies for information integrity
- Establish governance structures for influence management
- Build staff training programs for disinformation awareness
- Implement monitoring, evaluation, and reporting tools
- Strengthen coordination with national and regional partners
- Case Study: Government resilience model for countering national-level influence threats

Module 8: Crisis Response and Rapid Mitigation Strategies

- Develop incident-response protocols for information attacks
- Activate cross-sector collaboration in crises
- Conduct real-time monitoring and situational assessment
- Establish communication clarity during high-risk periods
- Integrate feedback mechanisms for adaptive response
- Case Study: Rapid response to a viral false narrative during an emergency

Training Methodology

- Instructor-led presentations and expert briefings
- Scenario-based simulations reflecting real-world influence events
- Case study review and analytical group exercises
- Practical OSINT, threat intelligence, and narrative mapping activities
- Hands-on communication strategy development
- Reflection sessions and action planning for institutional implementation

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
02 Nov 2026	06 Nov 2026	Online	$1,000
02 Nov 2026	06 Nov 2026	Physical	$1,500
02 Nov 2026	06 Nov 2026	Physical	$3,000
02 Nov 2026	06 Nov 2026	Physical	$3,000
02 Nov 2026	06 Nov 2026	Physical	$6,000
02 Nov 2026	06 Nov 2026	Physical	$4,500
02 Nov 2026	06 Nov 2026	Physical	$6,000
02 Nov 2026	06 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com