Accredited Africa Training Institute for Capacity Development
Unit FO409, Hatfield Plaza · 1122 Burnett St, Hatfield 0028 · Pretoria, Gauteng · South Africa
Tel: +27 12 004 8389 · Mobile: +27 65 077 6310
Email: apply@aaticd.co.za · Website: www.aaticd.co.za

COURSE BROCHURE

Operational Counterintelligence Planning And Management For Military Operations Training

Law, Military Science and Security / Sovereignty of the State

Unit Standard 117365 · NQF Level 6 · 40 Credits · 37 Days

COURSE OVERVIEW

This course equips military and security personnel with the competencies to plan, coordinate, and manage operational counterintelligence activities within a military operational environment. It focuses on integrating counterintelligence into operational planning cycles, threat assessment, and protective measures to safeguard mission-critical information and assets.

Category	Law, Military Science and Security
Subfield	Sovereignty of the State
Unit Standard	117365
Accreditation	SAQA Accredited · NQF Level 6 · 40 Credits
Duration	37 days
Training Method	Online, On-Campus, In-House
Certificate	Issued via AATICD LMS — verifiable online

LEARNING OUTCOMES

- Apply counterintelligence planning principles to support military operational objectives.
- Analyze threats to operational security and develop countermeasures to mitigate risks.
- Evaluate the effectiveness of counterintelligence operations within a joint operational framework.
- Design a counterintelligence support plan aligned with the military decision-making process.
- Implement counterintelligence collection and reporting procedures in accordance with legal and ethical guidelines.
- Demonstrate the ability to manage counterintelligence resources and coordinate with other intelligence disciplines.

WHO SHOULD ATTEND

- This course is designed for military intelligence officers, counterintelligence practitioners, and operational planners involved in joint or combined military operations.
- It is also suitable for security managers and defence force personnel responsible for operational security and intelligence management.

COURSE OUTLINE

Day 1: Introduction to Operational Counterintelligence

- Overview of counterintelligence concepts
- Historical context and evolution
- Legal basis: Constitution, Defence Act, and relevant policies
- Roles of military intelligence, security, and command
- Ethical considerations and rules of engagement

Day 2: The Threat Landscape

- Classification of threats: foreign intelligence services, insiders, non-state actors
- Intelligence collection methods: HUMINT, SIGINT, OSINT
- Case study: Soviet and post-Soviet CI operations
- Vulnerability assessment frameworks
- Threat indicators and warning signs

Day 3: CI Planning Fundamentals

- CI planning cycle: assess, plan, execute, evaluate
- Input to commander's estimate and OPORDs
- IPB and CI: enemy, terrain, civil considerations
- Planning for offensive vs. defensive operations
- Risk management in CI planning

Day 4: CI Operations Management

- CI operational cycle: collection, analysis, dissemination
- Investigation procedures: interviews, evidence handling
- CI operations: surveillance, counter-surveillance, deception
- OPSEC: identifying critical information, indicators analysis
- Coordination with military police and security forces

Day 5: Counterintelligence Analysis and Reporting

- Analytical methodologies: structured analytic techniques
- Link analysis and network mapping
- Writing CI reports: format, classification, dissemination
- Briefing command on CI findings
- Feedback and updating CI assessments

Day 6: Insider Threat Detection and Management

- Insider threat categories: malicious, negligent, compromised
- Behavioural indicators and red flags
- Personnel security: vetting, access controls
- Investigation of insider incidents
- Legal and privacy considerations

Day 7: CI in Peace Support Operations

- CI in UN and AU missions
- Information sharing with coalition partners
- Dealing with non-state actors and local populations
- CI in humanitarian and reconstruction operations

- Case studies: African Union missions

Day 8: CI in Counterinsurgency Operations

- Insurgent intelligence collection methods
- CI operations: source operations, double agents
- Disruption of insurgent communications
- Fusion with PSYOPS and CIMIC
- Case study: CI in Afghanistan and Iraq

Day 9: Technical Counterintelligence

- Types of technical surveillance devices
- Cyber counterintelligence: malware, phishing, network defence
- TEMPEST and emission security
- TSCM survey procedures
- Technical security policies and standards

Day 10: Deception and Counter-Deception

- Principles of military deception
- Deception techniques: camouflage, feints, disinformation
- Planning deception in support of CI
- Counter-deception: identifying denial and deception
- Case studies: Operation Bodyguard

Day 11: CI in Cyber Operations

- Cyber threat actors: nation-states, hacktivists, insiders
- CI collection in cyberspace: OSINT, honeypots
- Network defence and incident response
- Attribution challenges
- Legal aspects of cyber CI

Day 12: CI and Force Protection

- Force protection principles: deter, detect, defend
- CI threat assessments for bases and convoys
- Physical security measures
- CI support to personal security details
- Case studies: attacks on bases

Day 13: CI Source Operations

- Source types: walk-ins, defectors, double agents
- Recruitment approaches and handling
- Source validation and reliability assessment
- Debriefing techniques
- Legal and ethical considerations

Day 14: Counterintelligence in Joint and Combined Operations

- Joint CI doctrine and coordination
- Multinational CI: challenges and solutions
- Information classification and releasability
- CI in SADC and African Standby Force
- Case studies: multinational exercises

Day 15: CI Legal and Policy Framework

- Constitution, NIA Act, Defence Act
- Ministerial directives and policy
- Rules of engagement for CI operations
- Oversight: Joint Standing Committee on Intelligence
- International law: Geneva Conventions

Day 16: CI Risk Management

- Risk assessment methodologies
- CI risk matrix: likelihood, impact
- Mitigation strategies: avoidance, reduction, transfer
- Continuous monitoring and review
- Reporting risk to command

Day 17: CI Training and Awareness

- Training needs analysis
- CI awareness: briefings, posters, exercises
- Scenario-based training
- Evaluation and feedback
- Building a CI culture

Day 18: CI in Information Operations

- Information operations pillars: OPSEC, MILDEC, PSYOPS, EW
- CI support to OPSEC and MILDEC
- Countering adversary propaganda
- Coordination with public affairs
- Case studies: information warfare

Day 19: CI Evaluation and Lessons Learned

- Evaluation metrics and criteria
- After-action review process
- Documenting lessons learned
- Updating CI doctrine and procedures
- Continuous improvement cycle

Day 20: Capstone Exercise and Course Review

- Capstone exercise: scenario-based planning
- CI input to OPORD
- Briefing command
- Course review and Q&A;
- Feedback and certification

ASSESSMENT & CERTIFICATION

Delegates are assessed through exercises and a final test. A mark of **50% or above** earns an **AATICD Certificate of Completion**, issued digitally with a unique verification code. This course carries **40 NQF credits** at **NQF Level 6**.

PRICING (PER DELEGATE, EX-VAT)

Delegates	Training Method	Price per Delegate	Total
1	Online	R 115,500.00	**R 115,500.00**
1	In-House	R 150,200.00	**R 150,200.00**
1	On-Campus (Pretoria)	R 173,200.00	**R 173,200.00**

UPCOMING SESSIONS

Start	End	Method	Venue
10 Aug 2026	29 Sep 2026	On-Campus	Abu Dhabi, UAE
11 Aug 2026	30 Sep 2026	On-Campus	Durban, South Africa
11 Aug 2026	30 Sep 2026	On-Campus	Mauritius
12 Aug 2026	01 Oct 2026	On-Campus	Cape Town, South Africa
13 Aug 2026	02 Oct 2026	On-Campus	Dubai, UAE
14 Aug 2026	05 Oct 2026	On-Campus	Pretoria, South Africa
17 Aug 2026	06 Oct 2026	On-Campus	Durban, South Africa
18 Aug 2026	07 Oct 2026	On-Campus	Shenzhen, China

Contact us if no suitable date is listed — on-demand sessions can be arranged for groups.

HOW TO GET A QUOTE OR APPLY

1. **Get an instant quotation online:** visit **www.aaticd.co.za**, open the page for this course (Unit Standard 117365) and click **Get A Quote / Apply**. Select your training method and number of delegates — your quotation is generated immediately and emailed to you with the course brochure attached.
2. **Apply by email:** send the course title, your preferred training method (Online, In-House or On-Campus Pretoria), the number of delegates and your preferred dates to **apply@aaticd.co.za** — our team will reply with a formal quotation.
3. **Apply by phone or WhatsApp:** call **+27 12 004 8389** or WhatsApp **+27 65 077 6310** and we will prepare your quotation and reserve your seats.
4. **Confirm your booking:** accept the quotation and settle the invoice. As soon as payment is confirmed your delegates are enrolled and receive their AATICD LMS login details by email, along with joining instructions for their chosen training method.

Group discounts apply automatically — the more delegates you enrol, the lower the price per delegate. No payment is required to request a quotation.

Accredited Africa Training Institute for Capacity Development
Unit FO409, Hatfield Plaza, 1122 Burnett St, Hatfield 0028, Pretoria, Gauteng, South Africa
Tel: +27 12 004 8389 · WhatsApp: +27 65 077 6310 · apply@aaticd.co.za · www.aaticd.co.za