Counterterrorism and National Security Training Course

Professional Development Training Course Outline

Category	Political Science and International Relations	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Counterterrorism and National Security Training course offers an immersive, hands-on learning experience designed to equip professionals with the essential skills and knowledge to combat contemporary security threats. This comprehensive program delves into the complex and evolving landscape of **global terrorism**, exploring key concepts such as **radicalization**, **extremist ideologies**, and the strategic use of **emerging technologies** by hostile actors. Participants will gain a deep understanding of the intricacies involved in **threat analysis**, **intelligence-led operations**, and the legal frameworks governing **national security policy**, fostering a proactive mindset essential for effective **preventive counterterrorism**.

This specialized training provides a practical foundation for developing and executing robust **counterterrorism strategies**. The curriculum focuses on building competence in critical areas like **critical infrastructure protection**, **cybersecurity defense**, and **crisis management**. Through a blend of theoretical instruction and practical exercises, attendees will learn to identify, assess, and mitigate a wide range of threats, from **violent extremism** to **transnational organized crime**. The course emphasizes inter-agency cooperation and information sharing, crucial for a unified and resilient response to both domestic and international security challenges.

Programme Curriculum

Counterterrorism and National Security Training Course

Introduction

Counterterrorism and National Security Training course offers an immersive, hands-on learning experience designed to equip professionals with the essential skills and knowledge to combat contemporary security

threats. This comprehensive program delves into the complex and evolving landscape of **global terrorism**, exploring key concepts such as **radicalization**, **extremist ideologies**, and the strategic use of **emerging technologies** by hostile actors. Participants will gain a deep understanding of the intricacies involved in **threat analysis**, **intelligence-led operations**, and the legal frameworks governing **national security policy**, fostering a proactive mindset essential for effective **preventive counterterrorism**.

This specialized training provides a practical foundation for developing and executing robust **counterterrorism strategies**. The curriculum focuses on building competence in critical areas like **critical infrastructure protection**, **cybersecurity defense**, and **crisis management**. Through a blend of theoretical instruction and practical exercises, attendees will learn to identify, assess, and mitigate a wide range of threats, from **violent extremism** to **transnational organized crime**. The course emphasizes inter-agency cooperation and information sharing, crucial for a unified and resilient response to both domestic and international security challenges.

Course Duration

5 days

Course Objectives

1. **Analyze** the evolving nature of **global terrorist threats** and their operational methodologies.
2. **Evaluate** various **extremist ideologies** and the processes of **radicalization** and recruitment.
3. **Apply** foundational principles of **threat assessment** and **risk management** to national security contexts.
4. **Develop** and implement effective **counter-radicalization** and **de-radicalization** programs.
5. **Master** the techniques of **intelligence collection** and **threat fusion analysis** for proactive counterterrorism.
6. **Formulate** and execute **critical infrastructure protection** plans against physical and cyber threats.
7. **Identify** and disrupt **terrorist financing** and logistical networks.
8. **Design** and manage **crisis response** and **incident management** protocols.
9. **Utilize** open-source intelligence (OSINT) and digital forensics for **cyber threat intelligence**.
10. **Comprehend** the legal and ethical frameworks surrounding **counterterrorism law** and human rights.
11. **Enhance** skills in **inter-agency collaboration** and international partnerships.
12. **Prepare** for and respond to **WMD (Weapons of Mass Destruction)** and chemical, biological, radiological, and nuclear (CBRN) incidents.
13. **Conduct** post-incident analysis and develop lessons-learned for continuous improvement in **homeland security**.

Target Audience

- Law Enforcement Officers
- Military Personnel
- Intelligence Community Analysts
- Government Officials
- Corporate Security Managers
- First Responders (Fire, EMS, etc.)
- Critical Infrastructure Operators
- International Relations Professionals

Course Outline

Module 1: Foundations of Counterterrorism

- History and evolution of terrorism and political violence.
- Typologies of terrorism: ideological, state-sponsored, and lone-wolf.
- Understanding the terrorist attack cycle.
- International and national legal frameworks for counterterrorism.
- **Case Study:** The 9/11 attacks and the resulting changes to global security and intelligence.

Module 2: Threat Assessment and Risk Management

- Principles of threat identification, vulnerability analysis, and consequence evaluation.
- Methodologies for conducting comprehensive risk assessments.
- Identifying indicators of suspicious activity and pre-attack surveillance.
- Developing mitigation strategies for high-risk targets.
- **Case Study:** The 2013 Boston Marathon bombing and the role of open-source intelligence in post-incident investigation.

Module 3: Intelligence and Information Sharing

- The intelligence cycle: collection, analysis, and dissemination.
- The role of human intelligence (HUMINT) and signals intelligence (SIGINT).
- Fusion centers and inter-agency cooperation.
- Ethical and legal considerations in intelligence gathering.
- **Case Study:** The intelligence failures leading to the 2004 Madrid train bombings and subsequent reforms.

Module 4: Counter-Radicalization and Prevention

- Understanding the psychological and sociological drivers of radicalization.
- Community-based counter-radicalization programs.
- Strategies for intervening with at-risk individuals.
- The use of social media and online platforms for extremist propaganda.
- **Case Study:** An examination of efforts to counter ISIS recruitment on social media platforms.

Module 5: Critical Infrastructure and Physical Security

- Identifying and protecting critical infrastructure sectors.
- Threats to transportation, energy, and communication systems.
- Implementing multi-layered physical security measures.
- Hostile vehicle mitigation techniques.
- **Case Study:** The 2008 Mumbai attacks and their lessons for protecting crowded places and hotels.

Module 6: Cybersecurity and Cyber-Terrorism

- The landscape of cyber threats, from state-sponsored attacks to cyber-terrorism.
- Protecting networks and data from malicious actors.
- Digital forensics and attribution of cyber-attacks.
- Responding to and recovering from a cyber-attack.
- **Case Study:** The Stuxnet attack and its implications for national infrastructure.

Module 7: Crisis and Incident Management

- Command and control systems.
- Developing effective crisis communication strategies.
- Managing a coordinated multi-agency response to a major incident.
- Hostage negotiation and active shooter protocols.
- **Case Study:** The 2015 Paris attacks and the challenges of coordinating a response across multiple agencies and jurisdictions.

Module 8: Emerging Threats and Future Trends

- The proliferation of WMDs and CBRN threats.
- The use of drones and other unmanned systems by terrorist groups.
- The nexus between terrorism and transnational organized crime.
- Future challenges and a look at the next generation of security.
- **Case Study:** The use of chemical weapons in the Syrian civil war and the international response.

Training Methodology

- Instructor-Led Sessions: Expert-led discussions and presentations.
- Case Study Analysis: Detailed examination of real-world events.
- Practical Exercises & Drills: Hands-on simulations of crisis scenarios.
- Group Discussions: Collaborative problem-solving and idea-sharing.
- Scenario-Based Learning: Participants apply learned skills in realistic, evolving situations.

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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 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