Course Curriculum at a Glance

Day 1
Introduction to UAS and their use by state and non-state actors
The UAS threat spectrum: terrorism, espionage, sabotage, subversion, and organized crime
Drone detection methods and sensing technologies
Passive drone mitigation in peacetime

Day 2
Active and passive drone mitigation in operational environments
Emerging UAS concepts and resulting challenges for countermeasures
C-UAS planning and table-top exercise

Day 3 (venue-dependent)
Live flight demonstration of various drone models

© JAPCC

Team blue explains their Counter-Unmanned Aircraft Systems plan during the tabletop exercise.

Who Should Attend

The C-UAS Fundamentals Training Course is designed for the entire NATO C-UAS community but is particularly relevant to uniformed and non-uniformed NATO and EU personnel, military and civil law enforcement agencies, academia, defence industry stakeholders, and those working at critical civil or military infrastructure.

Why You Should Attend

Small UAS are cost-effective, highly adaptable, and easily weaponized. As such, security professionals must understand both the evolving threat landscape and the full spectrum of counter-UAS measures. Over an intensive two-day programme, participants will explore UAS threats through NATO's TESSOC framework, assess the capabilities and limitations of current detection and engagement technologies, design a layered C-UAS architecture, and test their plan during a tabletop exercise. Participants will leave with a deeper understanding of C-UAS challenges and the knowledge required to help protect themselves, their teams, and their assets.

Please visit
www.japcc.org/training
for course dates, locations, and registration.

Joint Air Power Competence Centre
Römerstraße 140, 47546 Kalkar, Germany
Phone: +49 (0) 2824 90 2201
Email: contact@japcc.org

Follow us on Social Media:

COUNTER-UAS

FUNDAMENTALS

Training Course

NATO
OTAN

Joint Air Power
Competence Centre

Small, unmanned aircraft are rapidly transforming the landscape in force protection. For less than the cost of a laptop, an adversary can deploy a GPS-guided quadcopter equipped with sensors to collect sensitive data or carry payloads with lethal explosives. Whether targeting a military base, critical infrastructure, or a crowded sports venue, these threats can emerge with little or no warning.

The Counter-Unmanned Aircraft Systems (C-UAS) Fundamentals Training Course is a focused, two-day classroom programme designed give professionals a clear understanding of adversary UAS threats and the tools available to counter them. The course emphasizes C-UAS theory and moves beyond simply tracking the latest sensors or jammers. Attendees will analyse specific C-UAS challenges, assess different systems and capabilities, and integrate countermeasures into a comprehensive security plan. The course consists of 16 hours of instructor-led discussions and scenario-based exercises, structured in three phases: threat awareness, detection options, and mitigation planning.

Day One: Basics. A primer on UAS platforms, control systems, and payloads provides attendees with a common vocabulary, regardless of background. The course then introduces the Terrorism, Espionage, Sabotage, Subversion, and Organised Crime (TESSOC) framework to analyse real-world incidents and identify gaps in current defences. Finally, attendees evaluate detection methods, including visual observation, acoustic trian-

gulation, radio-frequency sensing, and radar. By the end of day one, attendees will understand the strengths and limitations of various techniques and how the legal constraints affect available tools and sensors.

Day Two: Countermeasures. The morning session covers passive tactics, such as camouflage, deception techniques, physical hardening, and organizational measures, to degrade UAS effectiveness without kinetic force. The course then examines active defeat measures, including jamming, spoofing, physical interceptors (ranging from shotguns and net-guns to advanced air defence systems), and the emerging directed-energy systems. Course instructors align each tool with the threat scenarios introduced on day one, guiding attendees to analyse cost, collateral-damage implications, and national legal constraints. The course culminates in a tabletop exercise, where mixed teams plan for a realistic attack scenario. Budget, terrain, and rules of engagement must be balanced to create a layered defence, with plans subsequently simulated and tested in a virtual environment.