Advanced Drone Security and Counter-UAS Strategies Training Course



23 - 27 Nov 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #SM3337_131504

Course Introduction / Overview:

The proliferation of Unmanned Aerial Systems (UAS), commonly known as drones, presents a significant and evolving threat to the security of critical infrastructure, government facilities, and public spaces. This training course provides a comprehensive exploration of drone security and Counter-UAS (C-UAS) strategies, designed to equip security professionals with the knowledge to protect vital assets. Moving beyond theoretical concepts, this program delves into the practical realities of drone threat assessment, detection, and mitigation. As detailed by security expert P.W. Singer in works like "Wired for War," the accessibility of advanced technology has democratized new forms of threat, making proactive defense essential. Participants will gain a deep understanding of the C-UAS technology landscape, from RF analysis and radar to kinetic and non-kinetic effectors. BIG BEN Training Center has structured this course to build a strategic mindset, enabling attendees to develop and implement a robust, layered C-UAS defense plan that is legally compliant and operationally effective. This course is the definitive guide for any organization seeking to neutralize the aerial threats of the modern age and secure their airspace against unauthorized drone activity.

Target Audience / This training course is suitable for:

- Security Directors and Managers.
- Critical Infrastructure Protection Specialists.
- Law Enforcement and Public Safety Officers.
- Government and Military Security Personnel.
- Corporate Security and Loss Prevention Professionals.
- Risk and Compliance Managers.
- Aviation and Airport Security Staff.
- Emergency Response Planners.
- Security Consultants and System Integrators.
- Facility Managers of high-security sites.

Target Sectors and Industries:

- Energy Sector (Oil & Gas, Nuclear Power Plants, Electrical Grids).
- Transportation and Logistics (Airports, Seaports, Rail Yards).
- Government, Defense, and Homeland Security Agencies.
- Critical Manufacturing and Industrial Facilities.
- Public Venues (Stadiums, Arenas, Event Spaces).
- Telecommunications and Data Centers.
- Correctional Facilities.
- Chemical and Petrochemical Plants.
- Financial Institutions and Corporate Headquarters.

Target Organizations Departments:

- Corporate Security Department.
- Physical Security Operations.
- Risk Management and Assessment.
- Emergency Management and Response.
- Compliance and Regulatory Affairs.
- Information Technology and Cybersecurity (related to drone data).
- Facilities Management.
- Legal and General Counsel.
- Operations and Control Center Teams.

Course Offerings:

By the end of this course, the participants will have able to:

- Analyze the full spectrum of drone-based threats to critical sites.
- Evaluate the capabilities and limitations of various C-UAS detection technologies.
- Differentiate between kinetic and non-kinetic drone mitigation techniques.
- Develop a comprehensive, layered C-UAS security strategy.
- Understand the complex legal and regulatory frameworks governing C-UAS operations.
- Formulate a drone incident response plan for effective crisis management.
- Integrate C-UAS systems with existing physical security infrastructure.
- Conduct a drone vulnerability assessment for their specific facility.
- Assess future trends in both drone and anti-drone technologies.
- Make informed, vendor-neutral decisions on C-UAS procurement and deployment.

Course Methodology:

The training methodology at BIG BEN Training Center is designed for maximum knowledge retention and practical application. This course employs a blended learning approach that combines expert-led instruction with highly interactive and participatory sessions. Participants will engage with complex material through a variety of methods, including detailed presentations, real-world case study analyses of significant drone security incidents, and facilitated group discussions that encourage peer-to-peer learning. A key component of the course involves interactive workshops where attendees will work on practical exercises, such as developing a draft C-UAS policy or designing a layered defense for a hypothetical facility. We emphasize a problem-solving approach, challenging participants to think critically about the unique security challenges they face. The learning environment is collaborative and supportive, with continuous opportunities for feedback and direct interaction with the instructor. This ensures that participants not only grasp the theoretical concepts but also gain the confidence to apply these advanced strategies effectively within their own operational contexts.

Course Agenda (Course Units):

Unit One The Evolving Drone Threat Landscape

- Introduction to Unmanned Aerial Systems (UAS) technology.
- Anatomy of a drone and its core components.
- Categorization of drone threats from nuisance to hostile.
- Historical review of significant drone security incidents worldwide.
- Assessing drone vulnerabilities at critical infrastructure sites.
- Understanding the adversary's perspective and attack vectors.
- The role of open-source intelligence in drone threat analysis.

Unit Two C-UAS Detection, Tracking, and Identification

- Principles of a layered C-UAS detection strategy.
- Radio Frequency (RF) detection and spectrum analysis.
- Radar systems for drone detection and tracking.
- Electro-Optical (EO) and Infrared (IR) camera systems.
- Acoustic sensors and their operational limitations.
- Data fusion and sensor integration for a common operating picture.
- Techniques for identifying and classifying detected drones.

Unit Three Drone Mitigation and Neutralization Strategies

- An overview of kinetic and non-kinetic countermeasures.
- RF jamming and its effects on drone command and control.
- GPS spoofing and protocol manipulation techniques.
- High-Power Microwave (HPM) systems.
- Drone takeover and cyber-based mitigation methods.
- Kinetic solutions including nets, projectiles, and directed energy.
- Developing Rules of Engagement (ROE) for C-UAS operations.

Unit Four Legal, Regulatory, and Policy Frameworks

- Navigating national and international laws on C-UAS.
- Legal authorities for drone detection and mitigation.
- Privacy considerations and civil liberties implications.
- Coordination with aviation authorities and law enforcement.
- Developing a legally compliant C-UAS operational policy.
- Liability and insurance considerations for C-UAS deployment.
- Case studies on legal challenges in C-UAS operations.

Unit Five C-UAS Integration, Operations, and Future Trends

- Integrating C-UAS into a Security Operations Center (SOC).
- Developing a comprehensive Drone Incident Response Plan (DIRP).
- Post-incident procedures and digital drone forensics.
- Training and drills for C-UAS security teams.
- The threat of drone swarms and advanced autonomous systems.
- The impact of AI and machine learning on C-UAS technology.
- Future-proofing your C-UAS strategy against emerging threats.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As counter-drone technologies become more autonomous, what ethical frameworks must be established to govern their use in civilian airspace and prevent unintended consequences?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by adopting a holistic and strategic approach to drone security, moving far beyond a simple technical overview of C-UAS hardware. While many programs focus narrowly on equipment, our curriculum emphasizes the critical integration of technology, policy, and human factors. We provide a vendor-neutral perspective, empowering participants to critically evaluate and select the right solutions for their specific threat environment, rather than promoting any single product. The course content is uniquely structured around a strategic decision-making framework, teaching participants not just what the technologies do, but how to build a resilient, legally compliant, and scalable C-UAS program from the ground up. It places significant emphasis on the legal and regulatory complexities, a crucial aspect often overlooked, ensuring that organizations can act decisively and lawfully. By integrating comprehensive incident response planning and future-proofing against emerging threats like autonomous swarms, this training equips leaders with the foresight and strategic depth needed to master airspace security in a rapidly evolving technological landscape.