Surveillance Operator Survival Course

Cost: $2999.00

Duration: 5 days (Class minimum size is 4 persons)

Schedule: This course is a 5 day course, based on years of training and real world operations, as well as overseas and domestic high risk surveillance operations. *This course is Monday through Friday. The sixth day, Saturday, is a free day. We will open up the studio for the afternoon for those who want to practice and further familiarize them selves with the technical gear.*

What separates us from the others is the addition of familiarization / hands on use of real world technical surveillance devices and methods, as well as the same in counter eavesdropping equipment and techniques.

Surveillance Operator Course introduction: (5 days) The "Art of War" by Sun Tzu, Section 13, The Use of Spies... "what enables the wise and sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is ***Foreknowledge***." Surveillance has been used as a vigorous tool for centuries and even to this day forms an integral aspect of the security and intelligence market. The principles and new types of surveillance have progressed over the years with technology breakthroughs, requiring real world professional training. We review the lessons learned from surveillance incidents such as "Bader Meinhoff," "Kidnapping of General James Dozier," "1986 Berlin Discotheque," "1996 Khobar Towers," 1998 Nairobi" and the Israeli Mercaz Harah Massacre incident.

Surveillance has become a fast emergent part of the Private Security Industry and we provide the skill sets to recognize and identify surveillance operations and personnel. This course covers the basic to advanced protocols necessary for gathering evidence and intelligence by covert means. We provide realistic scenario training where students works as part of a team in a high pressure practical surveillance environment where split second decisions regularly need to be made.

Core Group is not only continuously involved in on-going surveillance operations, but training others to do so as well. Our surveillance specialists have extensive expertise in state of the art surveillance equipment, psychological techniques, and strategic planning. As an Air Force Electronic Warfare Officer, Major Jones is a specialist in the detection and location of eavesdropping devices, otherwise known as Technical Surveillance Countermeasures, or T.S.C.M., which is part of the curriculum. He has also been trained by the leading TSCM company in the world - Research Electronics International.

Each day, we start out in the classroom with presentations and hands on equipment practicum's, then move onto daily scenarios which place exercises in a realistic environment where students are required to clearly understand the objectives, manage the appropriate equipment, manage team members, formulate plans, conduct briefings, and then put those plans into action, then debrief the missions. Instructors teach how to carry out surveillance while on foot, in a vehicle and also from a static point. We bring out the best in each team member and improve their skills, not only in gathering information and intelligence by covert means but their ability to work as a close knit team under stressful conditions.

Surveillance: OODA Loop. Observe, Orientate, Decide & Act. OODA Loop & Leadership responsibilities. Team leadership & Delegation. Assertion skills & Time Management. Managing Conflict & Group Dynamics. Surveillance case studies & profiles. Surveillance as corporate leverage. Target selection & identification. Phases of criminal & terrorist surveillance. Pretext & undercover operations. Cover & disguises. Static surveillance. Foot surveillance techniques. Mobile surveillance techniques. Vehicle surveillance techniques. Stake out, pick up and follow. Trash pulls, reconstruction & story boarding. Penetration testing as part of the planning cycle.

Technical Surveillance: Electronic surveillance device history. Various ways to "Bug" a room. How devices are operated and their limitations. Corporate competitive intelligence. Signal attenuation & limitations. Improvised bugging methods. Methods of audio and telephone monitoring. Cell phones as monitoring devices. Cell phone cameras, videos, and recording. Covert methods of computer monitoring. Wireless networks and vulnerabilities. Digital voice recorders as monitoring devices. Satellite vehicle tracking equipment and systems. Tagging vehicles with GPS and monitoring them. Practicum reviewing dozens of devices for familiarization. Legal issues related to electronic surveillance.

Surveillance Detection: Surveillance as the visible hand of the opponent. Detection as the early warning event. Skills used to detect and confirm surveillance. Your physical security as the weak link. Surveillance detection techniques. Seeing, observing and comparing. Target identification & description. Identification sequences - characteristics. Common methods for detecting surveillance. Foot passive and active methods. Vehicle passive and active methods. High risk escape methodologies. Morphic resonance and fields.

Counter Surveillance: Counter surveillance - The threat of surveillance. CS as the actions taken once surveillance has been detected. Intelligence gathering and research. Use of comparative surveillance logs. Operation planning (briefing , debriefing). What your enemy is looking for. Early warning - K.O.C.O.A. What to look for when conducting surveillance. Active and passive measures for C.S. False starts, eye contact, sweep car, etc. Surveillance detection routes.

Technical Surveillance Counter Measures: TSCM Counter measures & bugging equipment. Cost of illegal eavesdropping. Physical examination analysis. Radio frequency analysis. Various deployment kits. OSCOR, CPM-700 and ORION overview. Frequency detectors, field detectors & scanners. Camera hunters, spyfinders & ICOM receivers. Wireless mics, cassette & digital recorders and cell phones. Improvised bugging devices & baby monitors. High tech listening devices. 110v powered, phone line powered & battery powered. Cell phones, laptops, key loggers, and computer monitoring.