



Staff Attack the Network



Fort Benning, Home of the MCoE

- No Cost to Unit.
- 2 & 3 Day Courses.
- 15 to 30 students
- Minimal site requirements.
- Expanding soldiers knowledge base.
- Flexible scheduling.
- Practical Exercises integrated into lessons
- Unclassified, no clearance required
- Synchronizes Staff training within BDE and BN.
- Reinforces doctrinal skills set.
- Combines multiple WFF into a seamless method of network engagement
- FORSCOM AtN Pre-deployment Training Requirements, Annex B 9.B(1)



Staff Attack the Network Personnel



Fort Benning, Home of the MCoE

The AtN MTT provides training to Active, Reserve and National Guard units on the current and applicable Staff Attack the Network Training Support Package that reflects the TRADOC Commander's guidance for conducting staff training on targeting network activities. The TSP consists of 10 lessons integrated with 4 to 5 practical exercises that introduce BDE/BN Staffs to the fundamentals of collecting and analyzing data in order to disrupt or destroy enemy networks. The objective being to synchronize lethal and Non-lethal actions to neutralize threat networks while simultaneously supporting friendly networks, influencing neutral networks and shaping the operational environment. The AtN course introduces student to the six pillars of attack the network methodology.



ATTACK THE NETWORK PROJECTS



Fort Benning, Home of the MCoE

EDGE - Enhanced Dynamic GeoSocial Environment

- Intended to provide a virtual domain (simulation) in which Soldiers can exercise their AtN knowledge/skills within a defined scenario
- Focuses on 4 of the 6 pillars of AtN
 - Understand the Mission
 - Frame the OE
 - Understand the Networks
 - Interact with and Engage the Networks
- Early design phase and its intended use is both as a PE for MTT and eventually as a standalone web-based exercise simulation
- Funded by JIDA and TRADOC G2
- Built by Simulation Training and Technology Center (Contractor)



Six pillars of AtN



Fort Benning, Home of the MCoE

- Understand the Mission
- Frame the Operational Environment
- Understand the Networks
- Organize for the fight
- Interact with and Engage the Networks
- Assess the Effort

The following lessons each fall under one of the pillars



ATTACK THE NETWORK LESSONS



Fort Benning, Home of the MCoE

Introduction to Attack the Network (AtN)

This lesson provides the student with a clear definition of a threat, friendly and natural network. Additionally, the three operational approaches (Supporting, Influencing and Neutralizing) and the three contributing factors that feed the AtN Methodology (Event, Intelligence and Enablers) are covered in the lesson. The students are introduced to the six pillars of AtN as well.

Define the Operational Environment (OE)

This lesson uses the six interrelated operational variables: (PMESII-PT) to conduct a comprehensive analysis of any operational area prior to beginning a campaign and is continuously updated during operation. While PMESII-PT is conducted at campaign level, ASCOPE is conducted at the tactical level and in many ways compliments PMESII-PT. The variables provide a view of the operational environment that emphasizes its human aspects. Since land forces operate among populations, understanding the human variables is crucial. The Operational Variables helps commanders appreciate how the military instrument complements the other instruments of national power.

Network Concepts.

The lesson is designed to show the types of networks, their components, bonds and characteristics. It addresses adaptive network threats, elements that make up a network and conditions for network formation. It also discusses Adaptive Networked Threats in Unified Land Operations

Intelligence and Analytical Tools

This lesson is designed primarily for educating non-Intelligence personnel, it teaches to recognize how intelligence contributes to the attack the network process, Identify the four steps of the IPB process, Correlate how IPB processes contribute to the attack the network planning process and determine the PIR/CCIR process as it relates to attack the network planning process.



ATTACK THE NETWORK LESSONS



Fort Benning, Home of the MCoE

Exploitation

This lesson describe the contribution of technical exploitation, forensic exploitation, biometric exploitation, document exploitation, and site exploitation to Attack the Network operations. Identify the three types of captured enemy documents significant to document exploitation. Describe the site exploitation framework and the biometric enabled intelligence.

AtN Enablers and Staff Organization

This lesson is designed to give Battle Staff members a fundamental understanding of the different types of Enablers and at what command level those enablers operate. Secondly, the lesson introduces staff members to specific bureaus, boards, centers, cells, and working groups (B2C2WG) and how they apply to the staff organizational structure to target a specified threat network.

Information Collection and Joint ISR

This lesson covers understanding the principles of Information collection operations as a Staff member. Describe the fundamentals of Information collection and Joint ISR synchronization and integration as well as recognize and understand ISR supportive role to Targeting.

Engage the Network

This class describes the AtN targeting process by identifying the four targeting methodologies (D3A, F3EAD, the Joint Targeting Cycle and F2T2EA). Also identify the working groups that occur at brigade and battalion level during the targeting cycle and focuses on the considerations for AtN COA development.

Assessment

This lesson describes how Measures of Effectiveness (MOE) are used to assess Attack the Network (AtN) Operations, it also describe the assessment framework and the steps of the assessment process. In addition it identifies the guidelines for writing MOEs and Describe methods for evaluating and presenting the status of an MOE.



ATTACK THE NETWORK LESSONS



Fort Benning, Home of the MCoE

Understand the Narcotics Network

The lesson is designed to show how other threat networks operate. It provides the student ability to look at networks other than an IED, Snipers or Mortar Networks. The six pillars of AtN are utilized during this lesson in order to identify, target, engage and defeat the Narcotics Network.