

The Terrorism Industry”: An Al-Qaeda Course in Security and Intelligence

Part Six

Part Six

This is the sixth segment in the series “The Terrorism Industry” by Sheikh Abu Ubaydah Abdallah al-Adam, who was until his death a prominent leader of Al-Qaeda responsible for its intelligence and security operations. The series was published by the Al-Fajr Media Institution, which is responsible for disseminating the written, audio and visual materials of Al-Qaeda and its affiliates.



Continuation - Recruiting People to the Organization

The military training undergone by those who are recruited into the organization must be precisely tailored to their classification and the role that they are selected to perform. This is also the case in various intelligence agencies around the world, in which employees undergo lengthy, goal-oriented training.

The Fifth Stage: Continued Surveillance

By this stage, the comrade has already been selected, trained and prepared for jihad activities, and the group’s leadership trusts that he will join its operations. However, the comrade must be observed in order to make sure that he is indeed carrying out his role in a satisfactory manner. Several factors should be noted during this observation:

1. Emotional stressors that are liable to influence the comrade and cause him to act in a hasty and reckless manner, which could potentially harm the overall jihadist interest. For example, a comrade may rush to carry out a revenge attack after a member of the group is killed, thereby bringing himself to the attention of intelligence agencies.
2. Each and every member of the organization must be given the most updated security guidelines and should conduct themselves accordingly.
3. A comrade’s mistakes should be examined in order to be sure that he was placed in the appropriate job role; if it is determined that the job role is not suitable, he should be moved to a different role.
4. Checks should be frequently carried out to determine if a comrade working undercover has been discovered; if he has been discovered, the situation must be dealt with immediately and the comrade must be transferred to a visible job role.
5. If a comrade is found to be involved in activities unbecoming of jihad or the group, he must be dismissed. However, he should not be killed (which is what intelligence agencies do when they want to get rid of an agent), but rather relieved of his duties. Nevertheless, if a member of the organization is discovered to be an enemy spy then he

will be dealt with in a different way.

6. The comrade should be encouraged as needed; if he makes a mistake his punishment should be proportionate.
7. Keep distance from anyone who was convicted of an improper act.

Security of Documents

Every jihadist group is in possession of important documents, such as war plans, and the enemy invests a great deal of resources in trying to obtain these documents. As many safety precautions as possible should be taken in order to safeguard both classified and unclassified documents. Documents that are important to a jihadist group generally include letters exchanged between group leaders, documents regarding operational activities and CD-ROMs with group members' personal details. It is important to remember that if these kinds of confidential documents are leaked, it can cause great harm to jihad by disrupting operations, exposing many group members and even endangering the lives of the group's fighters.

Risks associated with documents

The risks associated with documents (letters, files, CDs, computers, etc.) include loss, theft and duplication. In addition, the careless discussion of information included in such documents is liable to lead to their discovery.

Levels of confidentiality pertaining to documents

Just as intelligence agencies around the world assign their documents various levels of confidentiality in accordance with their importance, jihadist groups must do the same and indicate the level of confidentiality on the back of each page. The highest level, "sensitive", refers to strategic information that no one is permitted to see unless his name is written on the document. The second level, "top secret", refers to information concerning the organization's security. The third level, "very confidential", refers to information regarding the security of activities within the organization but not the security of the organization itself. The fourth level, "confidential", refers to information and secrets passed among senior members of the organization. The lowest level of confidentiality, "regular", refers to information that is publicly available and does not pose a threat to the organization.

Saving documents

Documents should be saved according to the "need to know" principle – only the relevant people need to receive the information. In addition, documents should be saved in secure places designed for this purpose, according to their level of confidentiality.

Transfer of documents

When information is transferred from place to place, its level of confidentiality must be taken into account. For example, information classified as “top secret” must not be sent in the mail but rather should be passed in person from one leader to another. When information is being transferred, one must make sure that the messenger is trustworthy, the addresses of recipients are correct and precise, the number of copies is exact, all of the signatures appear in the designated areas, and classified information is not sent via regular mail. In today’s Internet age, the mujahideen can share all information with one another online, making the process more efficient, but extreme caution should be used when using computers.

Disclosure of information

A highly classified document must include the list of the people who are permitted to view it, and they should be informed if leakage of the document would constitute a security risk. A person must never look at information that he is not authorized to view, and a document must not be transferred from one person to the next without the knowledge of its original author. In addition, classified documents must not be sent to private homes.

Destruction of documents

Documents, or portions thereof, must not be destroyed without the knowledge of the original author. Classified documents must be destroyed using a shredding device and leftover materials that can be used to write documents must be disposed of.

The loss of documents

If a document is lost, management must be informed and the lost document must be searched for carefully.

ABOUT THE ICT

Founded in 1996, the International Institute for Counter-Terrorism (ICT) is one of the leading academic institutes for counter-terrorism in the world, facilitating international cooperation in the global struggle against terrorism. ICT is an independent think tank providing expertise in terrorism, counter-terrorism, homeland security, threat vulnerability and risk assessment, intelligence analysis and national security and defense policy. ICT is a non-profit organization located at the Interdisciplinary Center (IDC), Herzliya, Israel which relies exclusively on private donations and revenue from events, projects and programs.

ABOUT THE JIHADI MONITORING GROUP

The Jihadi Websites Monitoring Group (JWMG) is a specialized research and analysis team at the International Institute for Counter-Terrorism (ICT). Composed of researchers fluent in Arabic, the JWMG monitors websites that support and serve the Global Jihad organizations. The unique characteristic of JWMG publications is the team's integration of diverse materials from a wide variety of Arabic sources. JWMG connects each source to larger trends, providing a complete understanding of events on both a local and a global scale.

[Click here for a list of online JWMG publications](#)

For tailored research please contact us at JWMG@ict.org.il.