IDC HERZLIYA

ICT
International Institute
for Counter-Terrorism
With the Support of Keren Daniel

ICT Jihadi
Monitoring Group

Insights

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

Part Three

Part Three

This is the third 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 –General Security Principles

The Fourth Principle: Transfer Information to Relevant Parties Only

Every piece of information must only be shared with those who need it in order to carry out their mission. There must be compartmentalization within the organization and information must not be shared with those who are not directly affected by it. The more people who are privy to the information, the greater the risk that it will be leaked or discovered during the course of investigations by intelligence organizations. Similarly, the more information that a person knows, the greater the risk that he poses to himself and to the organization in the event that he is taken captive. Intermediaries may be used to transfer information between various members of the organization. Information must be securely stored as well as compartmentalized. Every activist [within the organization] must see to it that as few people as possible are aware of his identity and job role, in order to minimize the circle of people that might incriminate him. It is important to remember that intelligence organizations investigate people and connect pieces information that they receive from each investigation. In this manner, they paint a reliable picture of the mujahideen and use the information to catch new suspects by surprise, by pretending to already know everything in an effort to get them to confess more details.

Sometimes people share information with comrades who do not need to know it for several reasons: to make them feel good in thinking that they are trusted; to put them at ease and cause them to take pride in the organization's capabilities; and to encourage those who feel despair and depression. While this may provide short-lived satisfaction, it is important to avoid it because anyone who is taken captive is liable to break and reveal everything he knows under severe torture by intelligence agents. It is important to understand that the commander of the group is responsible for all of the information at its disposal and he is the one who determines which members will be privy to which details. Therefore, the commander is in charge of compartmentalization and confidentiality [within the organization].

The Fifth Principle: Deliver Information Based on Need and Timing

Information should be only be shared with a member of the organization who really needs to know it and only at the necessary time, not before. For example, when a commander presents his men with a mission, he must not flood them with information by telling them what their next mission will be, even if the goal is to motivate them. Such information must not be publicized, especially not far in advance of the relevant operation; such carelessness enables intelligence agencies to gather information about Islamist organizations and thwart their planned operations. Of course, it is permissible to create ruses in order to dupe the intelligence agencies; for instance, to carry out regular military drills in order to get the enemy accustomed to the routine and then turn one of the drills into a surprise military attack. However, even in such instances it is important to maintain secrecy and share relevant information with those participating in the operation only once it is about to take place.

There are many advantages to sharing information on a need-to-know basis. First, when a member of the organization sees that his commander only gives him information as needed, he learns to do the same, thus imparting good security habits. Second, when all of the information is well-guarded and operations are successful, the commander's credibility grows as does his soldiers' faith in him, leading them to trust him and carry out his orders without hesitation. Third, when information is only relayed as needed, mistakes can be easily handled; if the information becomes widespread it is more difficult to correct the faulty impression that was created. The proper transfer of information enables the continuity of operations and the future surprise factor. When information is not transferred properly, it becomes easier for the enemy to gather information about the group. Subsequently, the group's operations are met with failure, and its leader loses the trust of his soldiers and ceases to serve as an example to them. Many operations have failed due to unnecessary chatter before or after they were carried out, which led to the capture of soldiers and the cessation of the group's operations.

The Sixth Principle: One Mistake Brings Immediate Danger

One security mistake by one member of the group is enough to expose the entire group to immediate danger. The first mistake is liable to cause confusion and chaos, resulting in additional mistakes that lead to greater danger. There are mistakes that, once committed, cannot be rectified (for instance, when a comrade is captured by the enemy it is reasonable to assume that he will divulge everything he knows once he is imprisoned). These are referred to as "first and last" mistakes since they create a predicament from which it is difficult to extricate oneself. For example, if a fighter betrays his group and discloses information to the enemy but later regrets it and asks to re-join the group, it would be a terrible mistake to take him back; one must beware of traitors and double agents, and remember that they pose an enormous risk.

The Seventh Principle: Stay Put in an Emergency Situation

In an emergency situation, a fighter should stay put and not move around. Some intelligence organizations operate according to the principle that, in an emergency, the mujahideen will begin to advance and so they begin to advance as well and end up meeting in the middle. Erratic behavior during an emergency only makes things easier for the enemy and, therefore, [the mujahideen] should remain in one place in order to avoid detection. In an emergency situation, there are many factors that could cause a person to want to move from his location, such as the desire to make sure that his family is ok, or to communicate with his comrades to see how they are and to formulate a plan of action. Since one must not move around too much during an emergency one must try to take care of such matters ahead of time: to make sure that one's family is in a safe location and to formulate a clear plan of action with one's comrades before the operation even begins. If contact with one's comrades is lost during an emergency situation, the fighter must not contact anyone – he needs to remain at his post and await instructions. In addition, every fighter in the operation needs to appoint a replacement for himself who can take his place if need be without any communication between them during the operation.

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.