Updates

7/11/2013
OPCW Verifies Inaccessible Syrian Site

The Organization for the Prohibition of Chemical Weapons (OPCW) has verified one of the two sites in Syria previously reported has having been inaccessible to the organization's team

6/11/2013
Wounded Syrians Treated in Israeli Hospitals

Several Syrian civilians wounded during fighting in Syria, including a teenager and a baby who suffered

Defense Industries Index

AEROMAOZ Ltd.
Aeromaoz is a world leader in ruggedized...

Elmo
has more than 25 years' experience in...

Emtan Karmiel
has long been a leader in firearms parts...

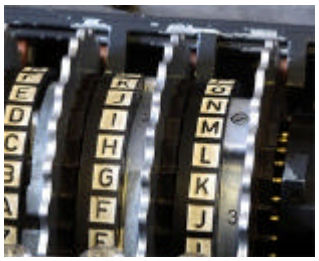
Home Page » More Headlines

"Cryptography is a Strategic Element"

Brig. Gen. Danny Bren, Commander of the IDF Lotem unit, in an exclusive interview to IsraelDefense about the activity of the National Cryptography Unit and the importance of cryptography in the age of cyber warfare

Ami Rojkes Dombe 3/1/2014

Recommen



The fact that cyberspace has evolved into a combat zone for all intents and purposes (and the IDF currently regards it as such) has heightened the importance of cryptography. In this arena, the Code, Cipher & Security Unit of the IDF C4I Directorate plays a major role: it constitutes the primary defensive layout of the IDF and other security agencies against attempted enemy attacks.

Generally, the CSC (Cryptography & Security Center) is one of the IDF's most confidential units. It is so secret that its very existence has only been revealed to the media in recent years. CSC provides encryption codes to the IDF and other security services and government agencies. It also serves as a critical node for strategic and tactical decisions made within the Israeli defense establishment, against the background of the emergence of cyberspace as a combat zone and the ever-increasing dependence of the military on computer-based technology. The IDF personnel authorities staff this unit with a collection of geniuses, selected through a particularly stringent screening process prior to their recruitment.

"Codes and ciphers as a strategic element are thoroughly implanted among commanders at battalion commander level and higher; the importance of the role played by codes and ciphers in the management of operations at these echelons is critical," says Brig. Gen. Danny Bren, commander of the Lotem Unit at the IDF C4I Directorate, in an exclusive interview to *IsraelDefense*.

Lotem is the primary technological unit of the IDF C4I Directorate and one of the IDF's largest technological units – if not the largest. CSC operates under this unit. Bren, 44, began his military service at IDF Intelligence Unit 8200, graduated with a master's degree from the Technion and returned to military service. He previous served as a research project officer with the CSC and advanced within the ranks, until he eventually became the commander of the CSC. The Lotem unit at the IDF C4I Directorate is in charge of the CSC, among other things, as well as of the central computer unit (Mamram) and the Directorate's electronic warfare unit.

As the former commander of the CSC, Bren has a unique concept regarding the role of cryptography in the military context. If, to some readers, the word "code" invokes associations of technology or mathematics, Bren suggests that cryptography be regarded as a strategic element.

"This is one of the reasons why the IDF C4I Directorate and the Ground Forces have introduced classes on cyber and cryptography into the syllabus of the IDF Tactical Command College. IDF commanders are provided with information about the importance of cryptography as early as during the basic officers training course. On the ground, the communication officers provide information security solutions," says Bren.

"The fact that cyberspace now constitutes a battlefield for all intents and purposes has only helped clarify the importance of cryptography once more. However, this is an ancient field. Evidence of the use of ciphers and encryption has been interwoven in human history since the days of ancient Egypt, through biblical times (Atbash substitution cipher) and Julius Caesar, who developed an encryption method known as 'Caesar's Shift Cipher', and, naturally, to the world wars of the 20th century (the 'Zimmermann Telegram'/Enigma). Only recently, we have witnessed the affair of the monitoring effort by the NSA, in which cryptography was used."

A National Unit

CSC deals with cryptography and the decoding/deciphering of transmitted confidential information during reception, on-going data communication, establishment and troubleshooting of data communication networks, operating and loading data cryptographic devices through advanced communication transceivers, troubleshooting cryptographic devices and various other activities.

The unit is a part of the IDF, but it is regarded as a national unit and as the provider of cryptographic services to other organizations as well. In other words, the CSC provides the solution and means to encrypt any bit of information that is to be transmitted through radio communication and needs to be encrypted, in Israel or by an Israeli organization.

The servicemen accepted by the National Code & Cipher Unit undergo a training period of several weeks.

This training prepares them for a service term with the goal of keeping the secrets of the IDF on the strategic level, between command centers, and on the tactical level, between combat forces on the ground. Academic reservists possessing various occupational skills that are associated with the unit's field of activity also serve with the unit. CSC alumni hold key positions in Israeli high-tech industry.

"Codes and ciphers were a strategic element used by warlords since the dawn of history. If you know what the other side plans, it takes out the sting of the planned operation. This is the reason why warlords always wanted to conceal their strategy by using codes and ciphers," says Brig. Gen. Bren.

"The first time the world was introduced to an automated cipher was during World War II, with the 'Enigma' machine previously developed by Germany. Prior to then, manual measures had been used. The story of the 'Enigma' tipped the balance in favor of more frequent use of encryption. Before the 'Enigma' had been cracked by former members of Polish intelligence, Germany succeeded in neutralizing supply convoys to US forces in Europe, and the eventual cracking of this encryption system helped the Allies win the war. It was all a matter of strategy."

Cryptography in the Tactical Realm

Bren reveals that the history of cryptography in Israel, at least the properly documented history, began at the IDF base in Tzrifin. Initially, a simple manual code was employed by using printed tables through which the codes were converted. The breakthrough in the use of cryptography by the IDF occurred after the Yom-Kippur War. "No one cracked the Israeli code in 1973. They did monitor it, but they did not crack it," says Bren.

According to Bren, the IDF Signals Corps entered the war in a high state of readiness, owing to a decision by the IDF Chief Signals Officer at the time, Maj. Gen. Shlomo Inbar. He decided to place the corps on alert three weeks before the start of the war, owing to a personal feeling that something was about to happen. Indeed, the surprise attack notwithstanding. The Israeli forces managed to maintain uninterrupted communication from the first day to the last day of the war at the Suez Canal forts, at the command centers and among the tactical elements.

"During the Yom-Kippur War, the prevailing thought was operational – to win. In such atmosphere, cryptography was not conceived as an element that can contribute to the tactical moves, and therefore it was used by command centers primarily. If you take into consideration the cumbersome operation of the cryptographic systems that were in use back then (in the early 1970s), you will understand why no one wanted to use cryptography unless they were obliged to do so.

"Although there are no empirical findings that indicate that Egypt had cracked the IDF code and monitored all of the Israeli communication networks, including those used by the command centers, something changed among the IDF supreme command following that war. They realized that enemy monitoring had probably taken place, and one of the conclusions was that cryptography should be used to protect the tactical realm of the fighting as well. This led to the establishment of a technical body that would deal with cryptography and develop an automated process," states Bren. "Could full encryption of the tactical communication change the course of the war and the number of casualties? Possibly. I do not know. We may have succeeded in reducing the number of losses among our troops."

Bren served as commander of the CSC during the Second Lebanon War, and according to him, it was the first time the unit had to change its operational strategy. Pursuant to the events of that war, Bren still takes part in the IDF discourse, even though it is not directly associated with the technological-professional aspects.

"It is not a part of the job description of the commander of the Lotem unit, but the outcome of circumstances, and it has to do with the role played by cryptography in the context of cyber defense in the IDF."

There are several reasons why cryptography currently plays a major role in the IDF concept, and according to Bren one of the primary reasons is the fact that IDF Chief of Staff Benny Gantz, personally understands the importance of this issue. "When Gantz was division commander at the Lebanon Liaison Unit and IDF Northern Command, he wanted to have cryptography without 'feeling' it. He understood the importance of cryptography from an operational point of view," stresses Bren.

Another reason for the importance of cryptography has to do with the technological changes the IDF underwent over the last few years. Like other military organizations around the world, the IDF has also become a technology-based military and as such, communication and data networks became a primary tool of the tactical echelon. One example is the Digital Army Program adopted by the IDF Grand Forces, which provides infantry, armored and artillery forces with improved command and control capabilities. It is unnecessary to mention what would happen to the IDF during combat operations if the enemy succeeded in cracking the encryption of this system. The CSC tries to prevent that scenario, as well.

Terms of Service RSS Sitemap Register

© All rights reserved, content and design by Arrowmedia Israel Ltd. Daronet Web Building