Cyber tools are no substitute for human intelligence

America can keep on playing with its technological toys despite the reality that is slapping it in the face. In Israel the price of making mistakes is much higher.

The IDF's battle against terrorism also means soldiers using computers - but this does not suffice to thwart every attack. / Photo by Moti Milrod

By Gabi Siboni

HAARETZ, 02.07.14

In recent years, the use of cyber tools has taken a central and sometimes exclusive role in the work of many intelligence agencies throughout the world. The documents exposed by Edward Snowden show how willing the Americans are to invest in technological systems to collect information and gather as much intelligence as they can using cyber tools. This almost exclusive reliance on the collection and analysis of intelligence using technology comes at the expense of the human element as a basic component of intelligence-gathering.

Israel’s intelligence community is also conducting a technological race. The agencies have diverted intelligence gathering resources to cyberspace at the expense of human intelligence-gathering, on the assumption that most of the information there is available and the main challenges are the accessibility of information and the technology of gathering, analysis and use of the relevant intelligence it contains. The transition to such tools also owes its existence to pressure from the industries that develop advanced technologies and want to sell their products.

Unfortunately, reality is not cooperating with this phenomenon, and the kidnapping of Gilad Shaar, Naftali Fraenkel and Eyal Yifrah should serve as a warning signal. This was a planned operation that was carried out under the cybernetic radar of the security agencies, which had difficulty putting together a relevant picture of the situation.

Like Israel, the United States is also having difficulty coping with organizations that keep a low cyber profile. The Islamic State (known until recently as ISIS) works with knives and rifles, leaving American intelligence with its sophisticated technology capabilities yet unable to sketch out a precise and profound picture of the complex reality in the Middle East. We cannot assume that the kidnappers and members of the Islamic State are ignorant of technology. It is more likely that they are well aware of the limitations of technology and work cleverly to minimize their exposure.

The intelligence agencies need to stop and reexamine their quest for the magical solutions of cyber tools. The accomplishments in the war on suicide terror a decade ago were the result of a balance between technology and the human element – a balance that has been broken in recent years. Not everything that is appropriate in America is appropriate in Israel. America can keep on playing with its technological toys despite the reality that is slapping it in the face, while in Israel the price of making mistakes is much higher.

The diversion of the effort to build integrated intelligence-gathering capability will be complex, and will mean having to deal with opposition from the industry. But the development of the threats on the eastern front and in the Sinai peninsula demand that the intelligence discipline keeps up to date. The creation of an intelligence picture of high quality – which is a condition for prevention and effective operational performance – must not rely on cyber tools alone.

Dr. Siboni, a colonel (res.) in the IDF, is a senior research fellow at the Institute for National Security Studies, where he serves as director of the Military and Strategic Affairs and Cyber Security programs.