ing the reduction of Lebanon's external debt in the first quarter of 2004 by about $746 million, and its stabilization at the end of March this year at about $33.5 billion.

9. *Al-Safir*, July 26, 2003.
10. Al-Arabiyah television, Dubai, October 11, 2003 (FBIS translation).
11. *Al-Nahar*, June 13, 2004.
12. *Al-Intiqad*, June 11, 2004.
13. *Al-Nahar*, June 9, 2004.
14. *Al-Mustaqbal*, June 9, 2004.
15. Interview with author, August 19, 2003, Tel Aviv.
16. *Al-Mustaqbal*, July 30, 2004.
17. In the "Politics" program, Channel 1, September 9, 2003.
18. *Al-Mustaqbal*, August 21, 2003. According to the paper's commentator, Nassir al-Assad, the IAF attack in Lebanon, which violated the blue line, "shifts the confrontation to the blue line." According to him, Hizbollah succeeded in establishing a new equation, more convenient in his opinion than anti-aircraft fire, or in other words, "the battle for the blue line has begun."
19. *Bamahane*, August 22, 2003.
20. *Ma'ariv*, November 7, 2003.
21. *Ha'aretz*, December 10, 2003.
22. *Ha'aretz*, January 20, 2004.
23. *Al-Safir*, January 22, 2004.
24. *Ha'aretz*, January 20, 2004.
25. *Al-Safir*, January 23, 2004.
26. *Al-Mustaqbal*, February 16, 2004.
27. *Al-Nahar*, May 12, 2003.
28. *Al-Mustaqbal*, February 21, 2004.
29. *Al-Safir*, Beirut, May 13, 2004.
30. *Al-Intiqad*, May 21, 2004. In a speech delivered by Nasrallah on June 30 he again denied that Hizbollah was involved in the Palestinian attacks, and said that "the fighters are Palestinian, the weapons are Palestinian, the bodies are Palestinian, and the direction is Palestinian. Hizbollah merely formed the model."
31. See, for example: Arik Mirovsky, "They Left Lebanon and Came Home," *Ha'aretz*, Real Estate Supplement, June 13, 2004.

Technology in the Fight against Terrorism

Uzi Eilam

Introduction

In the twentieth century modern technology was a key component of power buildup in the preparations for war, and even more so in the inter-bloc struggle following World War II. Today, terrorism is the main threat to the world, and it is clear that the fight against it is *the war* for which the world must prepare. Technology has already emerged on both sides of the battlefield: terrorist organizations generally use existing technology, which they can obtain with relative ease, while the countries on the defensive are also developing advanced technologies and investing considerable efforts and resources in them. Thus, technology should be regarded as an essential weapon in the war against terrorism, not only in the need to confront "simple" terrorism of explosives and suicide bombers, but also in preparing for future threats involving technology-intensive terrorism.

However, even today the fight against terrorism has yet to realize the full potential of its technological capabilities. Moreover, it seems that the planning in this sphere suffers from a lack of clear analysis and definition of the terror threat, as well as from a tendency to react rather than be proactive in developing anti-terrorism capabilities. It is not enough to give a static assessment of the situation or describe the present, regardless of how clear that description may be. What is required is a twofold approach involving anticipation of future threats alongside advancements in future solutions and technologies currently unavailable.

This article charts a course of action for the proper use of technology in the war against terror. It outlines the principles for building the defense system by mapping the capabilities required for this war. It also stresses the need to expand the use of current military technologies and the development of capabilities for needs that cannot be met by existing technology.

Terrorism and Technological Capability

In principle, there is an asymmetry between terrorist organizations and the countries that, defending themselves against many diverse threats, are forced to diffuse their efforts across many theaters. The terrorist organizations, for their part, can focus on a limited number of targets and ensure success in pinpointing the Achilles' heel of each. True, terrorist

organizations have neither the well-established technological infrastructure nor the budget to develop sophisticated and advanced systems, but that does not prevent them from carrying out successful attacks using low-tech methods. Thus, for example, they can threaten civil aviation with simple ground-to-air missiles (Strela) and use shoulder launched anti-tank missiles (LAW), which they can buy on the global arms market.

Terrorist organizations have demonstrated the easy ability to use a small amount (a few kilograms) of explosives and relatively primitive detonation means to carry out suicide attacks using human bombs, car bombs, or roadside bombs or bombs inside buildings that are activated by remote control. Since these attacks create such tremendous spectacles and cause damage and stress among the civilian population, they figure high on the list of preferred methods. Shooting at moving vehicles or into crowds with automatic weapons or sniping at selected human targets with a rifle is a threat of much lower priority than the use of explosives. In addition, organizations have the ability to perpetrate cyber terror, with the world's most advanced communications technology accessible to them, including the use of the internet. The probability of such events occurring is still low, but the significance of the threat is not.

Finally, there are non-conventional terrorism capabilities, including chemical, biological, radiological, and even nuclear means. For years North Korea and Iran have been developing non-conventional means such as long-range missiles, and it is well known that Syria has a chemical and biological arsenal. Even Pakistan, which is ostensibly at the forefront of the war on terrorism, is suspected of providing other countries with know-how and technology for developing nuclear weapons. Each of these countries has a past rich in covert activity involving the support of terrorist organizations and the unchecked supply of weapons systems.

Biological terrorism is perceived as the greatest of these threats, closely followed by chemical terrorism. A nuclear threat developed by the terrorist organizations themselves is regarded lower on the threat scale because the probability of their achieving such capability is low. A more tangible danger is the acquisition of "out-of-the-box" capability by terror organizations, which offers "a shortcut" to instant operability.

Building a Defense System

The weakness of the defense system is reflected in the lack of a comprehensive situation assessment vis-à-vis the threat. There is no defense plan based on identification of the threats, analysis of their significance, and prioritization of the ways to deal with them. Without such a plan, it is impossible to define the operational needs and required capabilities that would lead us to pinpoint technologies already existing in military and security systems. These are technologies that thus far were reserved for the element of surprise in an all-out war that can be converted for use in anti-terror systems without security or secrecy restrictions.

The war on terror requires formulation of a defense plan for handling the immediate threats that cannot be met using existing capabilities, and, simultaneously, preparations for combating future threats. The immediate threats will be handled by special units (some are already in place in countries such as the US, France, Germany and Israel) and by the use of means dependent on current technological capabilities. This sphere will benefit greatly from the ability to transplant existing technologies into the systems to be used. Future threats will be handled with systems to be developed as well as by new modi operandi. The plan must incorporate a means of prioritization for handling the threats, which will be determined according to the severity of the threat and the options for formulating a solution.

The second stage is identification of existing technologies in military and security systems that can be converted, with minor changes, to meet the needs of the war on terror. This includes optic sensors and advanced radar, data processing systems, advanced electronic warfare means, command and control systems, and others. Critical here are the technologies that thus far have been compartmentalized and incorporated in weapon systems designed as surprise weaponry for gaining a military edge in an all-out war. Their conversion will provide an important addition to the development of the defense systems' capability against terrorism.

Another stage entails analyzing

the gap between technologies available for immediate use and technologies required for meeting future threats. This analysis will also be based on the initial threat identification and prioritization and will allow formulation of a comprehensive research and development plan. The fourth stage involves the allocation of suitable budgets. Lacking a comprehensive plan, it is not surprising that the budgets channeled into technology conversion and technology development are much lower than allocations in many countries where an all-out war figures at the top of their security threat agenda. Thus, countries that have not yet allocated sufficient budgets will either have to rely on the achievements of others or formulate an emergency plan in order to narrow the gaps with those who have made important technological advances.

The goal is to launch a coordinated, multinational effort involving research and development of defense and warfare systems. In the near future, it will likely be possible to initiate several bi-national projects. Use of technologies that are not very sensitive in terms of security will aid in shortening the timetable at this stage of the effort. Nevertheless, it is clear that only multinational cooperation in advanced technology research and development will bring about a comprehensive defense strategy.

Mapping the Required Capabilities

It is clearly impossible to confront the threat of terrorism by means of one technology, one group of people, or one line of defense. The requisite concept, therefore, must be based on "layers of defense." It is also clear that there is no possibility of "immunizing" the entire global population against all the threats; thus, the emphasis must be placed on the most dangerous threats and on finding a "vaccine" against them. This evaluation will make it possible to pinpoint the capabilities required and determine the ways to achieve them. Following are some examples of the required capabilities:

The challenge in converting existing capabilities does not lie only in planning these means, but in their production at affordable prices as well.

- ***Detection and identification of people*** – it is necessary to adapt these capabilities to a wide range of situations, including organization and preparations in advance of terrorist activity, movement between or within countries, entrances to public places, entrances to airports, and other stages leading up to the attack.
- ***Detection and identification of materials*** – materials used in terrorism itself, particularly explosives, metals, and non-conventional warfare material.
- ***Defense capability*** – varied capabilities, primarily physical protection of people, sites, and facilities. Materials technology and advanced systems must be mobilized to recognize, pinpoint, and actively thwart the specific threat. In this context it should be noted that defending communication networks against cyber terror requires special technological capabilities.
- ***Intelligence capability*** – pinpointing centers of organization and preparations, monitoring the range of terrorist activities in progress, and identifying groups or individual active members of terror organizations. This type of intelligence gathering will require the use of electronic intelligence technologies and the application of surveillance satellite capabilities.
- ***Defense of air travel*** – the use of biometric means for identifying passengers, specifically, systems based on cuttingedge sensors for improved luggage checks and cockpit defense. For the airport as a whole, layers of peripheral defense are needed, including preemption of the use of shoulder launched anti-aircraft missiles.
- ***Protection of sea routes*** – to this end, it is imperative to expand the security zone. Security means will be activated as far away as thousands of miles from the destination ports, that is, even before containers are loaded onto ships. Beyond the intelligence cooperation and the adoption of international procedures and regulations, this sphere should make broad use of new technologies, both in

multilevel x-ray screening of the cargo and in a sensor complex for identifying explosives and even non-conventional warfare material.[1]

■ *Land defense* deals with a different range of threats – there are thousands of kilometers of borders with various topographies, and it is impossible to seal them hermetically. This will require a scan of the communication means and, as discussed below, use of the internet to monitor communication within terrorist organizations.

Expanding the Use of Existing Technologies

Among the many diverse technologies developed for armies since the end of World War II are assets that can be incorporated into the war on terrorism.

Over many decades of the twentieth century, electro-optic and electronic sensors, radar, lasers, odor detectors, and other devices were developed and incorporated into anti-aircraft missile warheads, air-to-air missiles, anti-tank missiles, and aircraft, ship, and tank defense systems. These systems and many others, such as the sensors in the warhead of the Arrow missile, can recognize, pinpoint, and respond to their targets quickly even in very complex situations. The challenge in converting these capabilities does not lie only in planning these means, which will lead to detection of objects in the new battlefield, but rather in their development and production at affordable prices.

Various materials, particularly ceramic materials (for protective purposes) and composite materials are used in bulletproof vests and vehicles and in aircraft (specifically helicopters) protection systems. The goal is to expand the use of lighter materials whose weight will satisfy the requirements. In this sphere as well, the main challenge is to reduce costs.

Identification capabilities using software that can simultaneously process output of the various sensors have long been used in advanced weapon systems. The terrorism battlefield necessitates a larger conversion effort in order to provide the ability to identify a person and the systems used for an attack early enough to prevent or reduce the damage. A certain degree of freedom regarding false alerts, to which the defensive system will reconcile itself, will enable countries to lower warning system costs and shorten the timetables for developing the systems and becoming equipped with them.

Command and control systems for land battle are already in use. These systems are capable of receiving data from various sources, be it air or land, and give all command echelons a complete picture of both enemy and friendly forces at any given moment. With a minimal conversion effort, these capabilities will provide multifocal monitoring of the terror organizations' activity as well as real-time coordination among the command centers of the countries involved in the anti-terror campaign. Systems for localized defense, e.g., defense by means of a ground-to-air missile system or with the aid of a powerful laser, will be used primarily to protect infrastructure facilities and government centers. These systems are expensive, but since the number of targets they must protect is small, they are quite worthwhile. This category includes the Nautilus system for defense against short- and medium-range rockets. Nautilus is based on advanced radar sensors and a powerful laser, and is at an advanced stage of development by the US army in cooperation with the IDF.

Electronic intelligence systems (ELINT, SIGINT) – some of which have already been "unfrozen" for use against terrorism – have been strongly adopted by many armies on the conventional battlefield. The challenge of mobilizing a larger portion of these capabilities for the war on terror lies primarily in lowering the security classification of the systems requiring conversion.

Space technologies were applied during the superpowers' struggle for satellites and a range of sensors in space and in high-altitude drones. This represents a real reversal in thinking, whereby a capability that was once used only for strategic purposes is redirected for new ends such as monitoring terror organizations' activities.

New Technological Capabilities Required

There are certain needs that are not adequately met by current technologies. For example, in the category of explosive materials, high-sensitivity sensors that are not yet available will be required to detect explosives re-

motely (at a distance of 100 meters or even more). In addition to the new sensing technologies, early identification of the explosive materials will require integration of various methods in a complete system affording detection and identification as well as immediate activation of preventive means. Similarly, a combination of sensing capability and cross-referencing sensing results from sensors operating according to various physical principles is also required in the area of sea and land charges. The ability to scan 100 percent of the containers at reasonable times and costs requires a considerable development effort.

Costs also make it difficult to provide protection for passenger aircraft. In this case, the problem does not stem from the lack of a proper solution. Select military and civilian aircraft (e.g., the aircraft of heads of state) are already equipped with defense means. The required technological breakthrough involves the development of inexpensive sensors and their integration into a warning system on the aircraft. This system must provide protection for all civilian aircraft at a reasonable price.

Data cross-referencing and the integration of disciplines are also essential to pinpoint and monitor terror activity preparations. The capability required here is remote voice and visual recognition of humans. A computerized database of voices and facial features, which can be created with existing technology, can help develop pattern recognition capability. This capability will provide the system with the required effectiveness and reliability. The integration of data cross-referencing with sensitive sensors is also essential for quick detection and identification of biological and chemical warfare materials. The principle of using a range of sensors, as in the case of explosive material identification, will imbue the system with a high degree of reliability and a low false alarm level. Another required capability will be communication pattern recognition for identifying and monitoring the communication of terrorist organizations via the internet and other means.

The following capabilities will be needed as early as possible in order to guarantee the advantage to the defenders in the war against terror:

- ***Detection and identification of explosives***. The capability for remote explosives detection (100 meters away) is a formidable challenge, yet essential for achieving a range of new, effective responses to a threat that now appears to have no response. The goal is to achieve remote neutralization of bomb detonation mechanisms by integrating various sensors that support and complement each other. The multiple sensors will imbue the system's performance with a high level of reliability.
- ***Intelligence Means***. Database technology is likely to contribute to both defensive and offensive capabilities. Intended are software and methodologies that develop the capability to respond to queries and update requirements from a large mass of data.[2] This capability will be used for automatic detection of unusual patterns of movement between countries by terrorist organization members and in financial transactions within the international banking network. Multi-media technology, such as identification of facial features and image matching, will add an important dimension to the data retrieval capability. Text retrieval technology is another means of automatic monitoring of free texts for the purpose of indicating, classifying, and ultimately finding the paper trail left by terror organizations while preparing for their activities.[3]
- Developing a response to terrorism in ***computer communications***. This area requires defense of national infrastructure facilities, including national communication systems, energy systems, the banking system, and the transportation infrastructure. The way to develop a proper defense against this threat is by defining the critical national systems and pinpointing the weaknesses in these systems. A worthy achievement would be to develop reliable, self-learning, self-improving defense systems that adapt themselves to changes and threat developments. Another important capability is immediate pinpointing of the "communication hazard" – which would make it possible to respond quickly and neutralize both the threat and the hazard itself.

Thus far, the world "knows" how to deal with the non-conventional threat vis-à-vis countries through institutional channels, such as the International Atomic Energy Agency (IAEA), the UN, the EU, and a large number of research institutes. On the other hand, there is no focused attempt to harness the technology for

monitoring and preventing the use of non-conventional terror by the organizations that are threatening to use it. Undoubtedly, the "stick" of the war on non-conventional terror must be held at both ends, meaning that there must be effective supervision of countries liable to supply materials alongside an effort to prevent the acquiring organizations from transferring and activating these means.

Monitoring nuclear facilities or clandestine shipping of fissile material necessitates the development of systems for identifying these materials. These systems will be based on technologies that utilize the clear physical signatures of the nuclear materials. Biological terrorism is on the agenda of the United States Department of Homeland Security. The department has initiated a project called Project Bio Shield,[4] which is intended to significantly upgrade US self-defense capability in the area of biological terror. What is required today is a technological effort producing means for quick detection of the composition of biological material and preparation of immunization in advance of a biological attack, as well as the means for treating the population following an attack.

Summary

Technology is obviously not the only means for fighting terrorism, and does not supplant the social, psychological, economic and political aspects. However, it will contribute to more effective action in this war. Launching the technological activity required to convert existing military systems for use in the war on terror and to develop new systems must begin immediately, and not wait for the formulation of a comprehensive defense concept. Each localized advance will contribute to the overall improved defense capabilities against terrorism.

Israel has technologies that are ripe for conversion – technologies whose security bans can be removed – and development capability for future needs. As such, it can serve as an example of a country making the most of its technological capability in the fight against terrorism.

Notes

1. The twofold terrorist attack on the Port of Ashdod in March 2004 highlights the need for comprehensive handling of the problem of the use of containers. In addition to the procedures and the organization required for using the existing (and expensive) methods to search containers with x-rays, it is necessary to develop advanced and inexpensive systems in order to attain maximal control of the movements of containers worldwide.
2. This refers to the ability to store and search multimedia data, such as images, sounds, voice, graphics and video, and to retrieve data from the databases.
3. The use of databases and monitoring personal communications raises three topics worthy of examination and regulation: (a) the violation of the right to privacy and human rights, which gives rise to constitutional and legal questions both within the various countries and at the international level; (b) the entry into the inner sanctum of military technologies, and into the databases in the domains of intelligence in particular, which is not a matter of course for all countries that perceive this a strategic capability of the highest order; and (c) coordination between the various organizations within countries and at the international level, which is difficult to achieve due to their own various ingrained structures and behavioral patterns.
4. In his speech at the Biological Conference in June 2003, President Bush provided Congress with an incentive to approve the legislation on the subject of biological defense. In this framework the government intends to invest $1 billion over the next decade in research and development of effective vaccines and treatments for the effects of biological terror.