Multi-Layered Defense and Initiated Attack in Defending the Homeland

Uzi Eilam

Introduction

The end of the twentieth century witnessed a dramatic transformation of the battlefield, and classical warfare between armies and states became relatively rare. Warfare on the modern battlefield is usually asymmetrical, fought between a state and a non-state enemy, or between two non-state entities. Armed groups target civilians in order to change a state's modus operandi and policies. This type of warfare is commonly known as terrorism.[1] The shock of the 9/11 attacks in the United States, and subsequent attacks in Europe, Iraq, and many other places around the world have thrust the world into a new reality. The threat of explosive devices and suicide attacks has been joined by the threat of rockets and missiles and the threat of cyberspace warfare. This new reality demands an improved response to the complex and dynamic threats of terrorism, specifically, a comprehensive approach and the investment of significant resources that can generate an effective response.

Over the years Israel experienced waves of attacks resulting in many casualties. Terrorism was on the rise elsewhere in the world as well, especially in Western Europe, but until recently did not reach the point where it was defined as a threat requiring special measures. France, which for many years thought it was immune to Islamic terrorism, learned the hard way that it too was a terrorism target. The attacks on March 19, 2012 in Toulouse, in which four Jews – a teacher and three schoolchildren – were killed and three French soldiers were murdered by one terrorist showed the French that the threat, in all of its severity, is present there as well. Unlike

Brig. Gen. (ret.) Uzi Eilam is a senior research fellow at INSS.

other European countries, the United Kingdom, which for many years was the target of Irish Republican terrorism, developed its own methods for domestic use to confront the threat. On the other side of the Iron Curtain, Russia failed in its war in Afghanistan, which it invaded in late 1979. The blood-soaked campaign against guerilla fighters who adopted terrorism as a successful method ended with Russia's humiliating withdrawal from Afghanistan. The 9/11 attacks were based on the creative notion of training terrorist pilots. The hijackings of the planes were accomplished without the use of firearms, and the hijackers, who boarded those planes in groups of five, aroused no suspicion.

Security services have long been aware that the various terrorist organizations help one another. The Irish underground, the Japanese Red Army, the German Bader-Meinhof gang, Fatah, and other Palestinian organizations found a common denominator and made use of the same training camps in Libya and Lebanon, and later also in Afghanistan.

In recent years, terrorists have also used the threat of nonconventional terrorism − atomic, biological, and chemical. The chemical threat was realized when canisters filled with the nerve gas sarin were used in the March 20, 1995 attack on the Tokyo underground.[2] The attack, carried out by the Aum Shinrikyo (literally "the unadulterated truth"), killed 12 and injured many. Nonconventional terrorism hangs like a sword of Damocles above the head of humanity.

At first, the fight against terrorism focused on tactical and ad hoc solutions. Israel built a defensive line through the Jordan Valley and put the Jordan Valley Brigade in charge. The response to the threat of Israeli airplanes being hijacked was the creation of a whole network of physical security on the planes themselves, including specially trained security personnel. Until the 9/11 attacks, the United States did not see the need for physical security and skilled security personnel on aircraft, methods adopted by Israel following the years of airplane hijackings.

If indeed the world is engaged in a global war on terrorism, what is the optimal way to defend against it? Should the response be focused on defensive aspects or should offensive ones augment defensive measures? Who are the enemies and where is the battle zone? This essay examines these questions from an historical perspective in order to draw conclusions and attempt to formulate some insights about the right strategy and most

effective tactics involving technology as a critical component in the response to this type of warfare.

The Terrorism Threat

An examination of the terrorism threat reveals a dizzying array of fields and methods. Some have been around for many years but have not yet been met with an appropriate response. The future is sure to bring threats that today are unimaginable. Here is a short survey of known threats:

a. *Aerial attacks*: Attacks on airplanes and attacks using airplanes offer a host of possibilities. The American aircraft that crashed into the Twin Towers in New York and the Pentagon in Washington on September 11, 2001 are extreme examples. As a lesson learned from those attacks, the United States now operates the Federal Air Marshal Service to secure passengers and airplanes. Firing shoulder-borne missiles at planes, as in the 2002 attempt to down an Arkia flight in Kenya, has not yet led to a decision to equip all passenger planes in the world – not even in Israel – with anti-missile defense systems. By contrast, passengers' shoes get special attention at many airports as the result of a foiled attempt to blow up a trans-Atlantic flight en route from Paris to Miami in December 2001 using explosives hidden in the soles of a terrorist's shoes. The world has not yet experienced damage to airplane systems via cyber attacks, but such a possibility is no longer in the realm of science fiction.

b. *Suicide attacks*: Suicide attacks by means of vehicles laden with explosives were seared into public consciousness beginning with Hizbollah's 1983 attacks in Beirut. Now, almost 30 years later, the same method of action is still used successfully in Iraq, Afghanistan, and elsewhere. In Israel, suicide attacks were the weapon of choice during the 1990s and early 2000s. Attacks on buses can be considered a special category of suicide attacks.

c. *Roadside bombs*: Roadside bombs are a familiar tool used by terrorist organizations. The wide range of bombs, locations, and methods of detonation (booby traps with sensors, manual detonation from afar, or electronic detonation from afar) make it difficult to develop a comprehensive response to this threat.

d. *Nonconventional terrorism*: For decades, the use of chemical and biological agents has been discussed as a possible terrorism threat;

the most prominent attack was Aum Shinrikyo's use of sarin on the Tokyo subway. The anthrax envelopes mailed in the United States in 2001, after the 9/11 attacks, brought the potential of the biological threat by terrorist groups to the fore. Because the investigation showed that the envelopes were mailed by a lone "bizarre" American scientist, the panic over chemical and biological attacks ebbed and preparedness for these sorts of attacks has dwindled.

e. *High trajectory weapons*: Rockets, artillery, and missiles are obvious means of terrorism and represent the firepower of terrorist organizations. The Russians began to sell their Katyusha rockets, developed during World War II, and Grad missiles, with a range of dozens of kilometers, all over the world.[3] The Qassam rocket, manufactured in local Hamas workshops, now has a range of more than 10 km. The Second Lebanon War showed Israel and the world at large the impact of high trajectory weapons used massively by a non-state entity against a civilian population. Iran and Syria have worked to restock Hizbollah's arms depots with an arsenal of rockets and missiles of all sorts and ranges, and this is currently one of the most important challenges facing Israel.
f. *Cyberspace terrorism*: Today most civilian activity is communications and computer based, from simple economic and social transactions, through emergency and medical services, to basic infrastructures of water, electricity, gas, and communications. Almost all activities are computerized and linked in one way or another to communications networks and the internet. The potential for damage in the realm of cyberspace, already colossal, is only growing as the technology develops further. Information security is currently an inseparable part of using the internet. Cyberspace terrorism capabilities are becoming more sophisticated all the time, and defending computer systems from harm has become a matter of exerting continuous, daily efforts.

Special attention must be paid to threats that could result in severe strategic damage, e.g., harm to infrastructure facilities, the paralysis of financial centers, the shutting down of energy installations and governmental centers, and damage to communications networks and databases. Such damage could be created through physical means, such as explosives, or by cyber attacks, liable to be much more dangerous and comprehensive. Interfering with transportation routes has significant economic implications, and to no small degree means the undermining

of world order. Terrorist activity can occur on the ground at the airport soon after takeoff using shoulder borne anti-aircraft missiles, or in the air, during the flight. The same is true of naval routes, the theater of most international trade; it too constitutes a strategic threat. Such activity, should it expand and succeed, is liable to entail paralysis of the global economy. The threat of high trajectory weapons – starting from ranges of several kilometers and ending with ranges of hundreds and even thousands of kilometers – is considered a strategic threat that will exist in the future. On the basis of Israel's experience, an almost certain outcome of the success of this threat is a significant paralysis of the economy and serious damage to the routines of all civilians in the nation under attack.

Learning the lessons after the shock of 9/11 while also considering the range of threats and challenges outlined above leads to the assessment that the threat is much greater than it was in the past and requires a systematic, comprehensive response.

The Response

In terms of the terrorism threat, the current situation may be likened to a global epidemic. Some would define the widespread reach of terrorism and the war on it as World War III. The French philosopher and sociologist Jean Baudrillard has even claimed that the war on terrorism is World War IV (Baudrillard considered the Cold War to be World War III).[4] Current methods of action to combat terrorism must confront the inherent asymmetry of the battle. The process of formulating the response must involve a sober, realistic analysis of the threats and identification of those that lack an adequate response. The response must consist of a combination of offensive and defensive components, based to a large degree on technological initiatives and capabilities. The decision by the United States and its allies to act in Afghanistan, America's targeted assassinations, and the ongoing effort that resulted in the elimination of Osama Bin Laden are evidence of the change that has occurred in thinking about the response. The use of offensive components requires the formulation of different tactics than those used in the past and reliance on technologies that will help confront various situations in the war on terrorism in the coming years.

Similarly, it is necessary to reexamine one of the IDF's fundamental premises – to move the war onto enemy territory – and consider whether

this principle remains relevant in this type of warfare. When speaking of a non-state organization operating out of defined territory, it is still possible to apply this principle, and examples in Israel are Operation Defensive Shield, the Second Lebanon War, and Operation Cast Lead. However, by contrast, fighting against decentralized terrorist organizations and cells is more complex. Moving the fight onto the court of an enemy using rockets and missiles requires different approaches when the threat is short range (dozens of kilometers) or when the threat is long range (hundreds of kilometers). We are already witnessing differences in the various components of the tactical response, e.g., the use of unmanned and armored combat vehicles against anti-tank missiles. Warfare against terrorism within the country's own borders is prosecuted primarily by means of focused intelligence. The use of bombs at roadsides and inside buildings, where forces are likely to operate, requires early identification of preparations to place these bombs in order to foil such attacks. It is crucial to attain relatively safe passage in the face of anti-tank and explosive device threats in enemy territory on the way to neutralizing the enemy's networks of artillery rockets and missiles. Contemporary urban warfare requires the identification of the enemy while maintaining the safety of troops moving through the urban landscape. Wars of the future will make extensive use of unmanned platforms to gather intelligence, operate ammunition, and identify enemy systems by drawing enemy fire at unmanned tools. An important component in these systems of warfare will be encrypted communications systems adapted to the new type of urban warfare, including use on the ground of effective systems to distinguish between friend and foe.

Technology for Defensive Systems

The need to supply a response requires the full use of technological capabilities. In this field, states usually have a relative advantage over terrorists and non-state entities. Some of the critical capabilities needed are:

a. *Means of discovery and sensing*: Sensors, especially those capable of identifying explosives at a distance, are an important need still awaiting a full response. At border crossings and airports in the United States advanced imaging technologies and X-rays systems operating on the backscatter method are already in use.[5] In addition, millimetric

wave imaging systems are also in use. These systems do not identify explosives but do identify suspicious objects carried by people. It seems that the use of trained dogs is a reliable method to discover certain types of explosives. Distance sensing of materials that power explosive devices is still awaiting a solution. An inseparable part of future sensor systems is to be found in cheap, reliable moving robots that would carry the sensors to wherever they are needed. Neutralizing explosive devices used by terrorist organizations leads to a search for alternatives to the chemicals used to put the explosive devices together. The challenge is to develop pesticides, insecticides, and herbicides based on chemicals that would be useless in constructing explosives.

b. *Identification and incrimination*: In recent years the use of biometric identification has expanded. The traditional opposition to the use of the range of biometric measures, such as fingerprints, retinal scans, and facial recognition, has to a large extent receded. The United States has changed its approach, followed by European nations and other countries around the world, all of which have decided that it is impossible to avoid conceding some personal rights for the sake of general safety.[6] This decision could lead to the establishment of biometric databases, which in the future could allow quick, reliable identification of terrorist suspects. A combination of technological developments based on understanding of human behavior in defensive systems could constitute a new component in the war on terrorism. An example of a system designed to identify malicious intent is the FAST project developed by the US Department of Homeland Security.[7] The system resembles a polygraph. A high intensity laser sensor reads people's rate of breathing and pulse, while another sensor identifies the shifting of body weight – the litmus test for behavior with malicious intent. Today, the warnings received by this system are not yet reliable and the errors are liable to result in false positives or the failure to pick up on real threats. Further means of development are needed for these systems before they can be declared operational.

c. *Cyber defense*: The development of countermeasures to cyber attacks must be founded on the assumption that this type of warfare knows no geographical boundaries. In such warfare, terrorist organizations exploit the freedoms of the democratic world and global communications. This war is characterized above all by the asymmetry in the ability of very

few to cause massive damage to central national systems. Preparing for defense against this threat requires ongoing tracking and unceasing efforts to develop countermeasures needed to defend against a threat that is constantly evolving.[8]

d. *Intelligence gathering*: Improving intelligence about the organizations, teams, and isolated individuals engaged in terrorism is a huge challenge. This challenge has many aspects, and in order to make progress, far reaching technological efforts are needed. A wide array of intelligence means are required, as are technological developments (eavesdropping, surveillance, decryption in real time) that will allow a leap in terms of future intelligence capabilities. It is necessary to increase the synergy between the intelligence and security institutions operating within and between nations. The Israeli attempt to combine the efforts of the General Security Service, the IDF, the Israel Police, and the Border Police in the war against terrorism is a good example of such synergy.

e. *Defense against high trajectory weapons*: The response to the high trajectory threat requires the construction of defensive systems with high rates of success of interception. Defensive systems in Israel – those already existing and those under development – clearly demonstrate the levels approach. The response to short range threats is now embodied by the Iron Dome system. For mid-range threats, there are the Arrow 1 missile, which has been operational for several years, and the Arrow 2 system, whose development is almost complete. In addition, the David's Sling system (also known as Magic Wand) is now under development. The Arrow 3 is being developed to confront long range missile threats, and will become operational once the necessary budgets are allocated and it demonstrates effectiveness in testing. In a limited area in Iraq, the American army used Vulcan Phalanx cannons to defend against high trajectory weapons.[9] Israel investigated the possibly and decided against the system. Simple calculations concluded that the Phalanx provides a response that requires the use of a very large number of cannons. In addition, the budgets for cannon purchases and, even more so, the allocation of manpower needed to operate them indicated their negative cost-benefit ratio. Nonetheless, it may have been worthwhile, especially in terms of the public and political aspects of defending the home front, to purchase several such systems and place them in certain locations, such as Sderot. This would also have afforded an opportunity

to test in practice both the solution itself and the justification for rejecting it from a public perspective.

f. *Laser interceptors*: A second field in defending against high trajectory weapons is the use of the powerful laser system, Nautilus, whose development encountered several crises. The development of the chemical laser based system was interrupted when the American army decided to withdraw from the project. A fierce and bitter argument erupted because there was no response to the short range high trajectory weapons threat and the growing public pressure exerted by the residents of Sderot and the settlement adjacent to the Gaza Strip. A sober analysis of the situation demonstrates that at present there is no archetype of a chemical laser system operating on the Nautilus principle in the United States. Because of the system's limitations, its effective range is at most 10 kilometers. Furthermore, its inability to function in rain and fog makes it an unreliable defense. The system's rate of fire is not at the speed of light, because the laser beam has to rest for several seconds on the rocket head before exploding it. The budgets required for these systems are much larger than the data published in the press.[10] Nonetheless, it would be right to accelerate the development of anti-missile laser systems, solid-state laser technology, that would be safer, more reliable, and perhaps even significantly cheaper.

The important challenges facing defensive weapon systems are their cost and improved interception rates for each of the levels. Laser weapons must find their proper place within the short range defensive systems while using safe laser technologies and finding a solution for a compact, inexpensive system. The response to the high trajectory weapons threat by means of ground attack also requires tactical solutions, in part new ones, and technological solutions. These must give the operational forces the ability to destroy missiles effectively in the launching areas while providing survivability and defense to forces moving towards the target.

Defense in Layers

The principle of levels of defense can be adopted and implemented in many areas of the war on terrorism. Layers of defense against the rocket and missile threat provide a response to different threats and supply backup for the defensive levels next to them. Defending against suicide bombers will improve as the result of adding measures and actions preventing the

first stages of preparing an attack. These are the distant levels in terms of time and distance from the attack itself.

One can generate levels of defense against arenas of explosive devices and booby-trapped buildings. The technological goal of sensing explosives from a distance could serve as a basis for adding an important layer in confronting the threat. The layers would consist of a combination of tactical preparation with technological support and sensors and the use of existing and still to be developed robotic tools.

Defending against weapons used at border crossings and air routes is a classic example of layers. Even now, a range of sensors, comprehensive defensive systems, and innovative technological means that have reached operational status are used at border crossings. Layers in systems of biometric scans allow backup for instances in which there are no values in databases using methods of identification currently in use (fingerprints, retinal scans, and facial recognition). Additional layers are supposed to identify changes in breathing, pulse rate and voice, body motions, eye movements and changes in body heat, the rate of speech and intonation. The higher the number of layers available to the defending side, the better the chances of picking out those suspected of terrorist activity. Developing layers of systems and backup and redundant measures would also benefit defense against cyber terrorism. Defense would start with internet providers and continue through the computers themselves and the internal networks of the defending organizations.

The principle of layers does not in and of itself represent a magic solution to the war on terrorism. Examining every threat listed above together with searching for an additional layer of defense or attack will eventually lead to the construction of a system that provides a better – if not hermetic – response to the threats of terrorism.

Conclusion

Today, homeland security is a vastly different battlefield than the theater of the World Wars, Korea, Vietnam, and the Yom Kippur War in Israel. The lessons of the war against terrorism bespeak the need to adopt an approach of constructing layers of defense in every realm. One cannot of course remain only with smart defense systems, no matter how effective. In order not to leave the initiative in the hands of the terrorists, it is necessary to improve the offensive capabilities.

Will the repeated stings of targeted assassinations of senior terrorists decide this war? Apparently not. On the other hand, a nation's capabilities to hold onto the territory of another nation and continue fighting manpower and resource-intensive wars on terrorist cells are also limited. It is not necessary to stay in enemy territory for long. The lesson learned from the IDF's 18-year stay in Lebanon after 1982 and the lessons learned by the American army after its wars in Iraq and Afghanistan show that the use of surprising tactics and innovative technologies help in a war everyone understands is an ongoing one. The secret of containing threats lies in the ability to continue acting in the war while maintaining a bearable ratio of losses.

Thus, what is needed is an approach that allows significant foiling of terrorist activity at a cost that will not entail an unbearable budgetary burden. Such an approach would rely on old and new technologies that allow missions to be accomplished at a tolerable casualty cost. This approach, in which every action is of short duration, would prevent most of the risks of going about one's routine while staying for an extended time in occupied areas. At the same time, multi-layered defenses would be given to civilians against the range of threats inherent in the war on terrorism. This defense must allow life in the civilian sector to carry on without too much disruption. This will allow the active operating forces sufficient time – within the limits of the always-ticking political clock – to undertake their missions properly.

Notes

1 It is difficult to come up with a universally accepted definition of terrorism. Among the dozens of alternatives is the Security Council's 2004 definition: "criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act," United Nations Security Council Resolution 1566, October 2004.

2 K. B. Olsen, "Aum Shinrikyo: Once and Future Threat?" *Emerging Infectious Disease Journal* 5, no. 4 (1999).

3 Zvi Magen, Yiftah Shapir, and Olena Bagano-Moldavski, "Russian Arms Exports to the Middle East," *Strategic Assessment* 13, no 2 (2010): 83-95.

4 Jean Baudrillard, "The Spirit of Terrorism," *Le Monde*, November 2, 2001.

5 J. Sarah Caygill, Frank Davis, and Seamus P. J. Higson, "Current Trends in Explosive Detection Techniques," *Talanta* 88, January 15, 2012, pp. 14-29.

6 Jeffery A. Larsen and Tacha L. Pravecek, *Comparative U.S.-Israeli Homeland Security*, The Counter Proliferation Papers, Future Warfare Series, No. 34, USAF Counter Proliferation Center 46-47, pp. 25-35, and http://cpc.au.af.mil/PDF/monograph/comparativeusisraeli.pdf, and also *Inquiry into the EU-US Passenger Name Record Agreement*, CEPS Policy Brief, No. 125, March 2007.

7 Samantha Michaels, "Department of Homeland Security Develops New Technology to Detect Terrorist Intent," March 11, 2010, http://nationalsecurityzone.org/site/department-of-homeland-security-develops-new-technology-to-detect-terrorist-intent.

8 "DoD Cyberstrategy Unveiled; Critical Attack Revealed," *National Defense Magazine*, July 14, 2011 , http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=467.

9 "Air Defense: Phalanx Marches through Afghanistan," *Strategy Page*, March 2012, www.strategypage.com/htmw/htada/20120313.aspx.

10 Shmuel Mittelman, "Petition to the High Court of Justice: Iron Dome Selected with Whitewashing and Debacles," *Maariv*, July 14, 2010; and Oded Amichai, "Opinion," July 21, 2010.