

Tools for Countering Future Terrorism

Eric Herren

Researcher, International Policy Institute for Counter-Terrorism

Introduction

Today's terrorist activities are becoming increasingly interdisciplinary and flexible. Future terrorist attacks will be built on past experience in terms of psychological effects, planning time and lethality.

If we are discussing tools for countering future terrorism, we of course have to think of the shape and form of such attacks. To understand the history of a possible future attack we have to try to anticipate the terrorist as networking organizations, misusing our weakest points and trying to find the Achilles heel of modern western society.

They will use favourable tactics like suicide attacks, multiple attacks involving conventional and most possibly WMD as well. As we learned from the past, terrorists are willing to study our defensive measures and update their operational strategy as well as use our repressive actions in favour of their psychological warfare. Terrorists will go into joint ventures and improve the dynamics of "terror networking". Attacks targeting the international audience will compete with local acts of terror, less professional in terms of tactics, but still effective in aiming at the psychological balance of the suffering victims.

This article wants to highlight the multilevel activities on both sides. Existing terrorist strategies and tactics on one side. And the interdisciplinary approach of the counterterrorist community on the other side. Each actor in a comprehensive counterterrorism policy is focussing into the structure of a possible terrorist attack.

Do we at all see the whole dimension of modern terrorism? To find ways and measures to deal with future terrorism, each player of the targeted society has to improve its understanding of the phenomena, the reactions to it, as well as the level of preparedness for upgraded terrorist activities.

The article will discuss in short six levels of counterterrorist activities. To each player in this counterterrorist structure, some basic recommendations are made concerning the threat of "Future Terrorism"

The structure of terrorism

Let us take closer look at the ingredients of a terrorist attack. I will concentrate on only few important aspects, taking a “top-down” approach, from the general to the specific. This list can be thought of as a kind of “infrastructure” for a terrorist attack.

Ideological / religious / political movement – Here we find the hotbeds of future terrorist organisations.

Terrorist organisation – Included in the terrorist organization are radical supporters, the leadership, the masterminds, economic support activities—both legal and illegal, and all logistic cover operations and institutions. More and more we see organizations networking with other terrorist organisations espousing the same cause.

Strategic planning – Terrorist organisations invest significant efforts in “meta activities,” such as public relations, and often use sophisticated tools to steer internal public opinion. Extensive efforts are also directed toward influencing the world audience through psychological warfare. Strategic planning also includes logistics and basic training. Terrorist organisations need to maintain and continually upgrade their arsenals, and to fill the ranks of fighters. Fundraising is another characteristic operation on this level.

Operational activities – In order to be effective, terrorist organizations need to have an intelligence-gathering capability. The use of open sources like the internet aide in target selection. Terrorists also seek to get information by simply monitoring the grey area around private security organisations. The increasing tendency to outsource police and law enforcement tasks to the private sector may also allow terrorists to access information on vulnerabilities.

Tactical preparation – This includes recruiting operatives and planning terrorist attacks. A terror attack is a complex operation. The “shahid,” or suicide attacker, is surrounded by several circles of activists who select and arm the human bomb, and send him on his mission. A successful attack is based on intelligence and the processing of real time information, knowledge management, and a certain degree of “dumb luck.”

Attack – From the standpoint of the terrorist organizations, an attack is successful if it produces a high body count and maximum destruction, followed by extensive media coverage.

The structure of counter terrorism

Here too, I will touch on only a few of the relevant factors in the counter-terrorism “infrastructure,” again, going from the general to the specific. Keep in mind that this list is far from complete.

Public opinion – Terrorism is a kind of psychological warfare; its aim is to undermine the morale of the targeted nation as well as to influence international public opinion. Thus, counter-terrorism must start at the true frontline—the level of the general public

The media – The media is of crucial importance for both terrorist and counter terrorist strategies.

Political leadership – The leadership of the nation forms the policies and guidelines for counter terrorist organisation and operations.

Think tanks – Interdisciplinary think factories can play a role in advising decision-makers and enhancing counter terrorist strategies.

Intelligence – Intelligence is of central importance in the war against terrorism.

Special operations – Special operations are the spearhead of counter terrorist efforts. They include rescue operations as well as law enforcement, security and military operations.

Counter-terrorism tools

I would like to point out that counter-terrorism begins with a strong and determined counter-terrorist community. In order to effectively fight terrorism, it is necessary to build a community of interest that is single-minded and solutions-oriented. This organisation needs an efficient internal communication system; it needs a common language, and a sense of trust and responsibility among members of the community.

Effective counter-terrorism requires the establishment of operational platforms to exchange views, create training scenarios and set up red-teams.

All of the foregoing applies equally to the national and the international levels.

It is also necessary to invest extensive efforts into ensuring that new terrorist organizations don't sprout as quickly as we uproot the ones we now face. In other words, it isn't enough to fight the alligators; we must drain the swamp.

We will now examine the dilemmas and difficulties of each aspect of counter terrorism in relation to the terrorist infrastructure. I will tackle this from the bottom-up, beginning with the more specific and working up to the most general ingredients of counter-terrorism.

Special operations

Special operations are the fundamental activities of counter-terrorism. As an example of the various factors involved, let us take as an example the type of operations that may come into play in the case of a suicide terror attack.

Rescue operations – Once the human bomb is within his chosen target area, special operations will be limited to reducing the impact of the attack. Professional rescue operations will need to take into account that the attack may be a compound one, with secondary attacks planned to target rescue forces. Medical personnel are an integral part of the security plan and play the greatest role in mitigating the effects of the attack.

Security measures – Increased security measures can lead to the discovery of the attacker before he or she can reach the target zone, thus reducing the damage or preventing the attack altogether. Successful security measures include the designation of different security zones ranging from non-target to pre-target and target zones. Each zone is characterized by different security activities, ranging from electronic surveillance to physical barriers.

Defensive activities – This includes special operations against planning and recruiting efforts by specialised cells within the terrorist organisations. Defensive measures must be continually upgraded by constantly re-examining and testing security arrangements. Nothing is more dangerous in security operations than the establishing of routine procedures which lose their sensitivity.

Offensive strikes – Offensive counter-terror operations are special operations directed against the close circle surrounding the suicide bomber—those who recruit the human bombs, equip them with the deadly explosives, instruct them about favourable targets, harbour them before sending them into action and try to cover their footprints. Many nations that strike back at terrorists base such operations on the right to self defence. The rationale is that the person who “arms and aims” the human bomb is no less culpable than the bomber, and must be held responsible.

Surgical operations – This aspect of counter-terrorism includes counterintelligence activities, as well as special operations against logistics and training infrastructure. Terrorists often hide their activities within legal business or social – even medical or international organisations. Bomb factories have been found in the same building as nursery schools and hospitals. By the same token, weapons procurement may take place under the legal auspices of a third state support and fundraising for terrorist organisations may be covered by legal business activities. This type of interaction between terrorist infrastructure and civilian institutions makes special operations against such activities extremely difficult and risky.

Coordinated strategies – Among the most important special operations are those that seek to stem the flow of sympathy and support to terrorist organizations. These operations attempt to knock the wind out of public outrage and hate, the glorification of suicide bombers, and the misleading of young men and women by religious indoctrination.

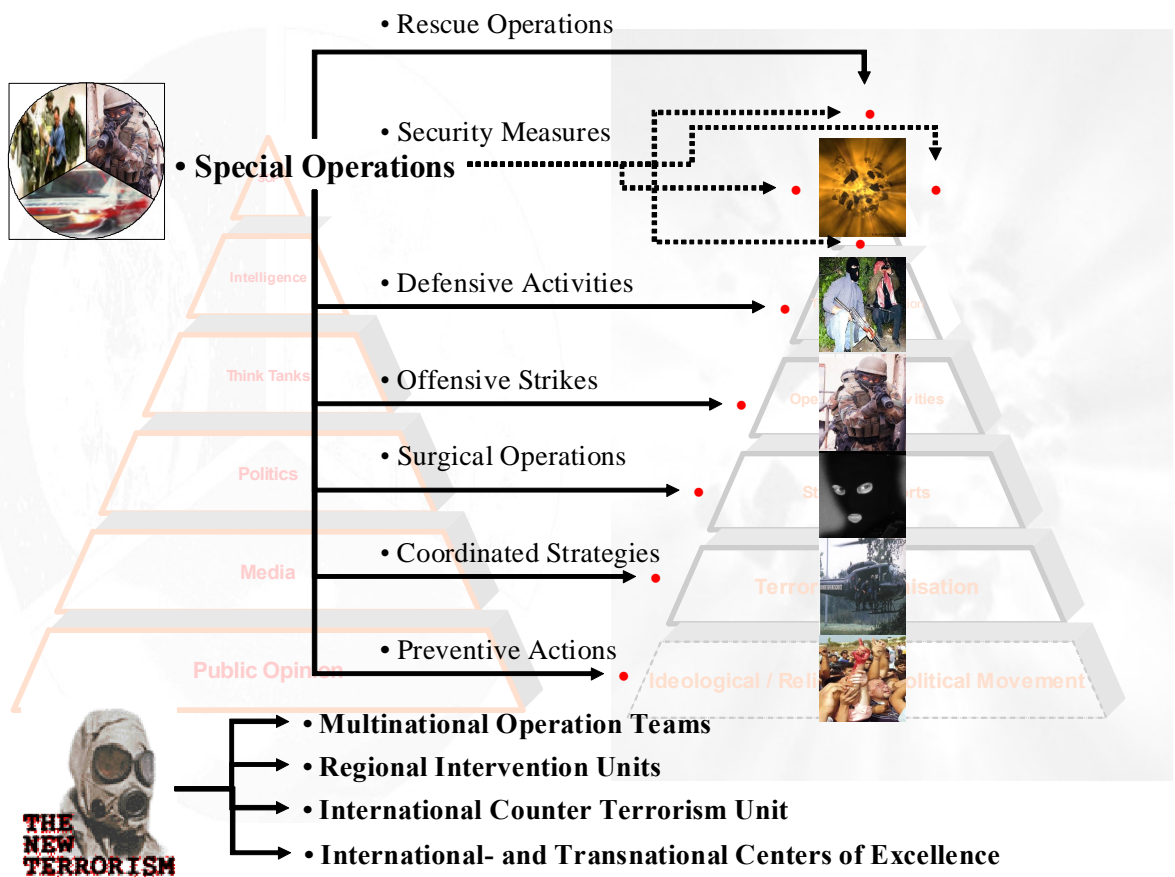
Counter-terrorism at the highest levels must counter disinformation and psychological warfare. Long-term counter-terrorist strategies must include the winning of hearts and minds to successfully win the war against terrorism.

Preventive actions in the virtual world – Lastly, we come to preventive counter-terrorist “street work,” carried out by units specifically trained to deal with the “virtual infrastructure” of terrorism. Here intelligence is derived from the continual monitoring of internet forums, websites, and other forms of digital communications. The goal is to enter the virtual battlefield to pick out potential future terrorists and attempt to open a window for them to integrate back in our society.

Conclusion for Future terrorism

To deal with the threat of future terrorism, we will need to create multinational special operation teams. These teams will include regional intervention units, who will be first on scene to stabilize the situation and preparing the field for take-over units.

It would be useful to establish an international counter-terrorist unit, which would bring together the best counter-terror solutions from around the world. At the same time, we must establish international and transnational centres of excellence, and create think factories and knowledge-management organisations.



Intelligence

Intelligence is the sense-organ of the counter-terrorist organism—the faculty that takes in and processes incoming information. As we did above, we will analyze the components of intelligence using the example of the threat of suicide attacks.

Identification of the threat – Intelligence is the key factor in preventing the attack. Once the potential suicide bomber is identified, security measures can be directed in a purposeful direction. The time factor here is critical; information processing procedures must work quickly and forward their analysis to the end users at special operations level.

Counterintelligence – Intelligence communities must upgrade their for counterintelligence capabilities. Data security is vital to prevent terrorists from gaining access to information that could help in target selection. Intelligence agencies should be able to provide specific recommendations and advise to private institutions seen as at risk of information theft, in order to prevent sensitive information falling into the hands of terrorists.

Humint / Sigint / Elint – Intelligence gathered from the inner circle of the activists surrounding the “shahid” is based mainly on human sources. The running of such cells is a sensitive and risky business.

In many countries, human Intelligence is very much a neglected artform. Too many efforts have been, and are being, invested to other means of intelligence gathering. We must come back to the human sources within our own organisations, including police and customs officers and other government employees. The police officer on his own beat must be successfully integrated into the information-gathering process; he has intimate knowledge of his own area, and will be the first to know of any unusual activity.

Unfortunately the flow of information is often blocked by obstacles within the system. At the same time that we are collecting the best resources from our peripheries and bringing them together in federal institutions, we may be missing some of the best resources that are already available in our midst.

Psy Ops – Psychological operations involving the intelligence community should be directed not only against public relation efforts of the terrorist organisation, but should also aim to disrupt the flow of communications within the levels of the terrorist organizations. This kind of activity can help to keep the terrorist organisation busy with preserving their own structures and the risk to make mistakes will increase.

Multinational intelligence community – Intelligence aimed at terrorist organisations and their strategic efforts includes humint, sigint, and elint. The most important factor in this kind of activity is international cooperation. Often this part of the game is played on the international stage far from the “hot spots” and well-protected from unwanted attention. Examples are operations to prevent terrorist fundraising and weapons procurement.

Thermostat – Intelligence agencies need to establish sensors within ideological, religious and political movements that can sense the “temperature” of the more radical elements and put into play preventive activities. Dilemmas in the struggle against terrorist organisations often include the lack of cooperation between all the agencies involved. While healthy competition is part of the game on the national as well as the

international level, it is clear that success in the war against terrorism is only reached through partnership and trust. Intelligence agencies are notorious for spreading their efforts far and wide. In order to avoid this, the intelligence community should be gathered under a common umbrella, coordinated and guided by political decisions.

Needless to say, intelligence is crucial to the success of special operations of all kinds. But more than this, it is the job of intelligence to create a round table for the exchange of views and should strive as far as possible to achieve an interdisciplinary approach.

I would like to highlight an issue often seen within intelligence communities: who is the end-user for all these sensitive products? Too often intelligence has been, and is created, merely to support old institutions and infrastructure within the intelligence agency.

Intelligence must be used by political decision-makers as part of their consultancy tools.

In many countries the relation between intelligence and media are like cat- and-mouse, with the “right to know” and censorship producing a lot of frictions. Public opinion and intelligence are sometimes strange bedfellows; in times of threat, the public calls for visible results from the agencies. Here the dilemma is to explain what is being done without jeopardizing the success of intelligence operations.

Conclusion for Future terrorism

The threat of future terrorism will force the intelligence community to establish multinational intelligence databases, with reasonable access for partner states. This will naturally lead to the dilemma of protecting the sources of the intelligence and establishing who gets access, and how much access. One simple rule could be: the more a state gives, the greater its access.

It will also be necessary to upgrade our ability to successfully process information under time pressure. It makes no sense to become a vacuum cleaner, sucking in all kinds of information, if the means of analyzing and interpreting this information are lacking. Analyzed information must be able to flow back to the end users and other sensors of the counter terrorist community:

Here we will need to learn about and integrate better knowledge management processes. Do we fully recognize the power of open sources? We will need specialists analyzing open sources in all languages and in every open forum.

Human intelligence will be the main resource for effective intelligence gathering. The human factor must become our main concern. Intelligence officers will need purposeful career planning and feedback for successful activities. To be proud of his or her job is one of the main sources of motivation in a career that has little open reward or glory.

Think tanks

One of the most neglected of counter-terrorist tools is the think tank. Academic “think factories” are helpful in providing a broader view of the phenomena of terrorism. They are removed from the actual stage of combat and are able to focus on the problem from all possible views and positions.

Think tanks should concentrate on the actual threats, as well as learning from the overall history of terrorism. Their task should include attempting to foresee the future and “think the unthinkable.”

Members of think tanks should include former and present members of the counter-terrorism community, as well as anyone who can contribute to the vision. Think tanks should become consultants and critical observers supplying feedback to the counter-terrorism community, and providing forecasts and partnership in solution-oriented task forces. We will also have to learn to accept them as teachers and instructors.

Conclusion for Future terrorism

What is needed is a successful networking of think tanks. These organizations are probably the only ones that can keep up with the pace of terrorist networking. Official governmental operations and coordinated strategies are often held back by office procedures, unnecessary bureaucracy, and political interests.

Think tanks create the possibility of online brainstorming forums, bringing together huge resources of intellectual potential—a kind of creative solution-seeking that can be extremely helpful.

We will need interdisciplinary institutions whose activities are devoted to finding global strategies and are willing to be part of a whole. We need international centers of competence, which will concentrate on specialized tasks as an interdisciplinary contribution to the fight against terror. An example is the recently established Center for the Study of Militant Islam.

Regarding future terrorist threats—it is likely enough that science fiction will become a relevant part of mental preparedness for future terrorism.

Politics

Politics and counter-terrorism are at the head of virtually every national agenda today. Let me just point out several key issues with regard to successful measures against terrorism.

Political will – Political commitment to combat terrorism is the fundamental motor behind all counter-terrorist activities. The will to fight terrorism—and especially to confront the gray zones where terrorism and organized crime meet—are crucial tasks for political decision-makers. But let us not be dreamers; today in many countries the gray zones are an integral part of the economic infrastructure of the nation. It will be hard to get countries to cut off funding to terrorists when this funding is seen as a legitimate part of the national economy.

Leadership – National and international leadership in the war against terrorism is necessary to concentrate the efforts of all relevant sources.

Definitions – An international definition of terrorism is crucial and fundamental. Such a definition will serve as a basis for counter-terrorist activities, and an operational tool to expand our ability to combat terrorism on the international level. Too many groups that employ terrorism are still hiding behind expressions like “freedom fighters” and “insurgents.”

Laws – Based on the political will of the leaders and supported by international definitions, nations must create and change their laws to be better prepared to meet the emerging threat of terrorism and organized crime.

Clear political decisions – We must demand that political leaders to make difficult decisions; in the absence of political guidance, counter-terrorism organizations all too often become notorious institutions for managing problems rather than solving them. Politics is an important partner in counter-terrorism, and is responsible for controlling and supporting counter-terrorism tools.

Politicians must impress not only public opinion by their determination to fight terrorism, but also must send clear signals to extremist groups. We further expect from politics a professional handling of the media.

Conclusion for Future terrorism

The fight against future terrorism will demand political courage, as well as perseverance to overcome the impact of future attacks. Future terrorism will also entail great political flexibility and the need to adapt. We will need political vision and most of all our leaders will need the ability to learn and integrate reality into their decision-making process.

Media

Most of the public knowledge about terrorism is transmitted through the media. Many international media outlets concentrate only on the most obvious stage of terrorist activities—the attack itself. In fact, it is often the media that is the first responder to a terrorist attack.

Using the example of a suicide attack, the media will home in on the scene of the attack, broadcasting images of the death and destruction. These pictures are the strongest weapon in the hands of terrorist organizations. They show results on the targeted population and play to an international audience. These images prove the success of the operation to the terrorist organization, while at the same time satisfying their sick motivation to kill innocents.

But where is the media's interest in backstage terrorist activities? Such activity is the real “bread and butter” of terrorism, and deserves at least as much coverage as do terror attacks. However, this kind of coverage requires intensive investment, professionalism and journalistic expertise, and the success of such TV documentaries is not guaranteed.

Many media agencies are using the term of “Info-tainment.” The average audience wants to know who is the bad guy and who is the good guy without investing too much thought. Information must be cut into small, tasty pieces which can be swallowed easily and cause no stomach ache.

Modern terrorists try to influence decision-makers through public opinion. This kind of psychological warfare is often supported by the media by the lack of professionalism of on-scene journalists. They themselves become part of the action and lose their sense of objectivity. The terrorists' message is transmitted through the good offices of the international media. The effects of this reportage could be mitigated by paying the same attention to backstage terrorist activities.

Conclusion for Future terrorism

It is in our interests to educate the media to their responsibilities as a first responder to terrorist attacks. Media can be used and / or misused as part of psychological operations. The media can become a partner in counter-terrorism if we learn how to cooperate and if we strictly draw the borders between responsible journalism and playing into the hands of terrorists.

Future terrorism may well include “media terrorism”—information channels could be hijacked and panic spread by pre-prepared pictures and scenes and fake political statements. This too, is something for which we need to be prepared.

Public opinion

Today’s terrorist attacks target public opinion in several ways. First: a successful suicide attack aims to lower the morale and weaken the resistance of the targeted population. The terrorists’ goal is to create a feeling of general vulnerability among the citizens. This psychological warfare results in enormous pressure on the government to take action (or over-reaction) and thus forces international condemnation of the targeted nation.

Secondly, the attack is also used by terrorist organizations to spread their message to the whole world. Unlike the old forms of terrorism, which sometimes had very clear political messages, today’s terrorist strategy is twofold: it sends shockwaves through the civilized world; and it uses its “successes” to call for sympathizers to join the jihad. Each successful attack is another page written in the terrorist handbook used to teach a coming generation of extremists.

A successful counter-terrorist strategy must include a powerful effort to educate and teach citizens about the dangers of terrorist manipulation and the impact of psychological warfare.

Security measures –Increased security measures can only be implemented if public opinion supports these actions. It is the general population that suffers from security checks and the loss of privacy. Therefore much more attention should be directed to this most vital part of counter-terrorist strategy—with an emphasis on education. Terrorism is an attack on the public morale and the emotional balance of each individual. We must do all we can to strengthen this most important partner in counter-terrorism.

Conclusion for Future terrorism

Public support is critical for any long-term counter-terrorist strategy. As Boaz Ganor has said, “Counter terrorist forces can win the battle but loose the war the moment that citizens are afraid to use public transportation or to go to public places.”

Summary

Of course this discussion of counterterrorism measures has to be upgraded especially with political issues such as poverty and globalization, as well as diplomatic tools and economic sanctions.

It is also a fact that each and every state has its own agenda and follows the political guidelines of the ruling parties.

Still, we have to acknowledge that terrorism and especially “Future Terrorism” needs to be dealt with in the most professional way possible. This attitude will lead us to the conclusion, that counterterrorism can only be effective if we upgrade the common knowledge of the people in terms of terrorist strategies and goals. Public support and understanding will pressure both, the media as well as our politicians, to deliver the best possible solutions to deal with the phenomena.

The most effort will be on the shoulders of our intelligence community. National as well as international “power games” will destroy the most needed energy to focus on the real picture. A network will only be as strong as its weakest partner ! Let’s accept new, unfamiliar partners at the round table to open the spectrum of understanding.

The spearhead of the counterterrorist community, special forces, rescue teams and many others are forced by the daily routine to integrate new methods and abilities. What has to be done here, is concentrate the expertise and let others participate in the operational learning process of real time experience.

If we want to be ready to confront the threat, we have to stay open minded, sharpen our sensors and become part of a never-ending learning process which will demand a lot of determination and effort.