



Intelligence and its Operationalisation

Mr. Eric Herren, ICT Associate
November, 2013

ABSTRACT

Intelligence is the main pillar of successful counter terrorist operations. Successfully detected, carefully selected and efficiently processed information, tactical knowledge and the understanding of your opponent puts any counter terrorist organization into the pole position.

So how come, that terrorist are still launching deadly attacks and responding forces are sometimes lost with inactivity and helplessness? Does the structure and set up of counter terrorist organizations allow the best possible answer to the threat? This article disputes and analyses the interface between intelligence and operational forces. How can operational behavior be supported by relevant information and guidance towards success? What is the role of operational learning? Can we adapt to the shift of terrorist tactics and their success in learning our responses?

* The views expressed in this publication are solely those of the author(s) and do not necessarily reflect the views of the International Institute for Counter-Terrorism (ICT).

Intelligence and its Operationalisation

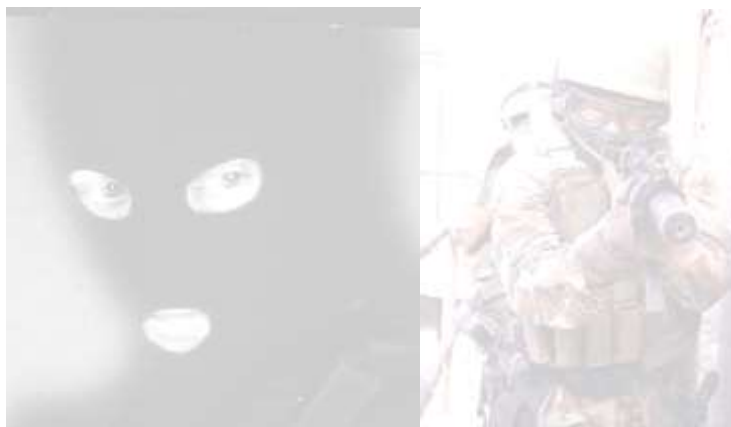
Preface:

Intelligence is the main pillar of successful counter terrorist operations. Successfully detected, carefully selected and efficiently processed information, tactical knowledge and the understanding of your opponent puts any counter terrorist organization into the pole position.

So how come, that terrorist are still launching deadly attacks and responding forces are sometimes lost with inactivity and helplessness? Does the structure and set up of counter terrorist organizations allow the best possible answer to the threat? This article disputes and analyses the interface between intelligence and operational forces. How can operational behavior be supported by relevant information and guidance towards success? What is the role of operational learning? Can we adapt to the shift of terrorist tactics and their success in learning our responses?

Counter terrorist operations are based on the awareness of a certain threat to the stability and well being of a community. Accurate analysis of the situation should then trigger actions to avoid, deter or minimize the aftermath of this threat.

Three major factors are influencing the outcome of counter terrorist activities.



The most important of them is the “**human factor**”. The skills of the human beings involved are absolutely crucial. Careful selection, ongoing training and testing are basics. Furthermore it needs determination, courage and the will to overcome all obstacles on the way to success. Especially if we discuss the interface between Intelligence and operational forces we will learn about the inalienability of the human factor.

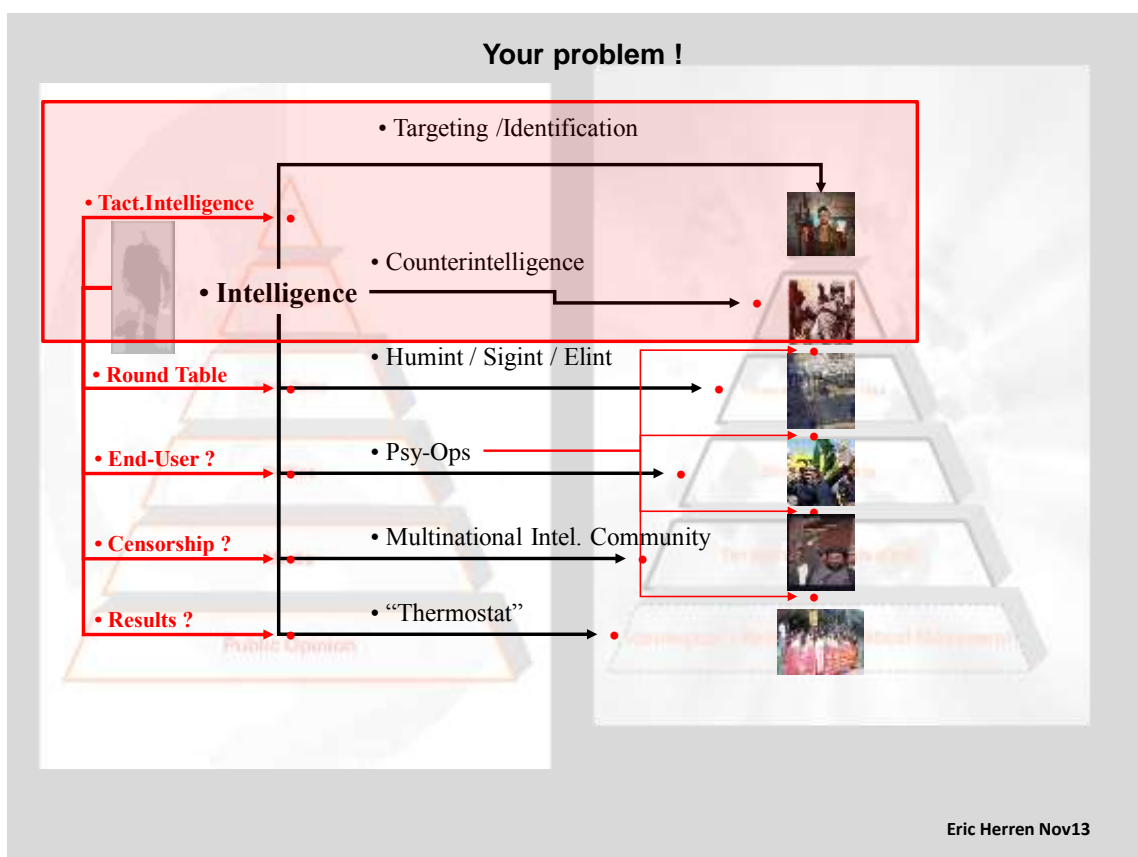
Technology and **processes** are the second and third factor influencing the result of many counter terrorist operations.

This paper attempts to highlight the gaps emerging between knowledge and ability, analysis and action. How can operational behavior be upgraded and optimized for successful accomplishment of the given task or mission. The advantage of knowing your enemy, anticipating his next steps and building up the best possible response are essential for success.

The protagonists:

Terrorist organizations are difficult to structure. Sometimes they have no structure at all and are just a group of individuals put together by opportunity.

But almost all have something in common. They are acting on different levels of interest. On top of all activities is the wish to launch successful attacks to undermine the stability of their enemies and create a mystic aura of success against the alleged superior opponent.



Eric Herren Nov13

Based are such groups often in the nourishing ground floor of political, religious or ideological inspired radical movements. Here they are looking for a point of crystallization to share the

common ideas and dreams. Often the dust particles of radicalization are spread by the Internet or other media to reach out for counterparts to align with.

Another level of activities includes strategic or operational activities such as networking, procurement and financing efforts. Additional levels of operations are tactical preparations including recruitment, training and intelligence gathering. The top level of terrorist doings concentrates on different kind of attack missions.

On the side of the counter terrorist organization we should find multilevel activities and strategies as well. An interdisciplinary community of professional bodies should simultaneously target the whole spectrum of terrorist efforts.

A basic partner has to be public opinion. The citizens are key to any successful counter terrorism policy. The CT community has to integrate the media, politics, and academic institutions as well as homeland security related organizations and not only rely on basic pillars such as intelligence and special operations forces.

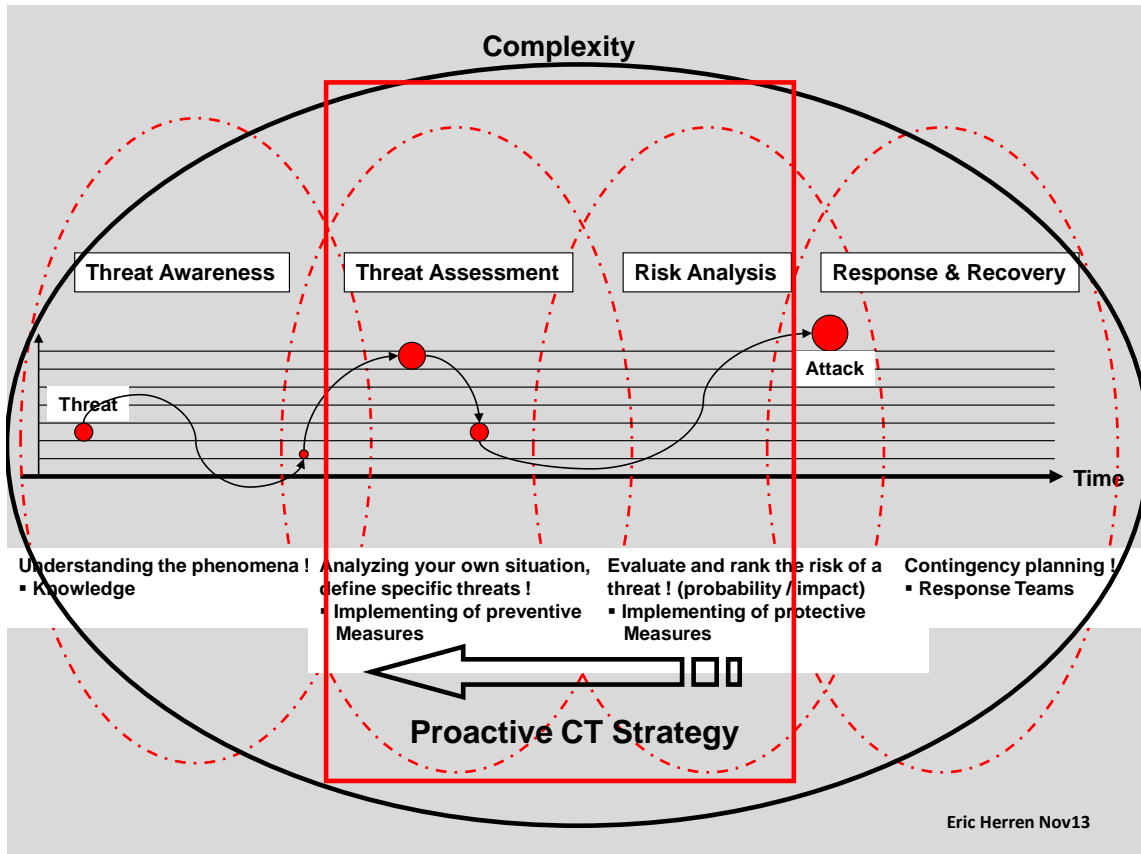
To keep the discussion focused this paper concentrates on only two partners in the struggle against terrorism. Intelligence and special operation forces! The findings can be adapted to both, military and civilian organizations.

To elaborate the dilemmas evolving from this more or less close relationship between intelligence and special operation forces we have to define the classic role of each one of them.

Proactive counter terrorism strategy

Counter terrorism is often a victim of time! Mostly there is not enough time to implement all necessary sensors to get a complete picture. If time is not of urgency, many of the problems could be solved after intensive analysis and exploration. Unfortunately it is in the nature of terrorism that time is frequently a rare article in the arsenal of counter terrorist organizations.

Also the nature of a threat is a variable factor. Terrorists are planning and executing their attacks not in a linear cycle. If we look at the time line from the planning to the attack, threats are emerging complementary to a certain constellation and opportunity. The planners of an attack often suit their time table according to the intelligence and security efforts of the targeted community. The famous saying of a arrested IRA terrorist makes the point:” Law enforcement has to be successful and lucky all the time; we only have to be once!”



In a proactive counter terrorism strategy, intelligence is responsible for threat awareness and threat assessment. This includes the understanding of the phenomena of terrorism and the fabrication of specific information and knowledge for strategic end users such as politicians and other decision makers. Furthermore, intelligence is assigned to assess emerging and future threats. Analyze global-national- and regional situations, suggest and implement preventive measures to name only few of the tasks.

As we follow the time line towards a potential attack or confrontation, analyzed intelligence is transformed into a risk assessment. The evaluated risk of a threat is ranked according to its probability and impact. Protective measures are implemented. Here we often find the critical interface between intelligence and operation. The whole complexity and dynamic of such processes are constantly underestimated. Modern technology is providing huge flow of information and data that has to be processed and integrated in to tactical behavior.

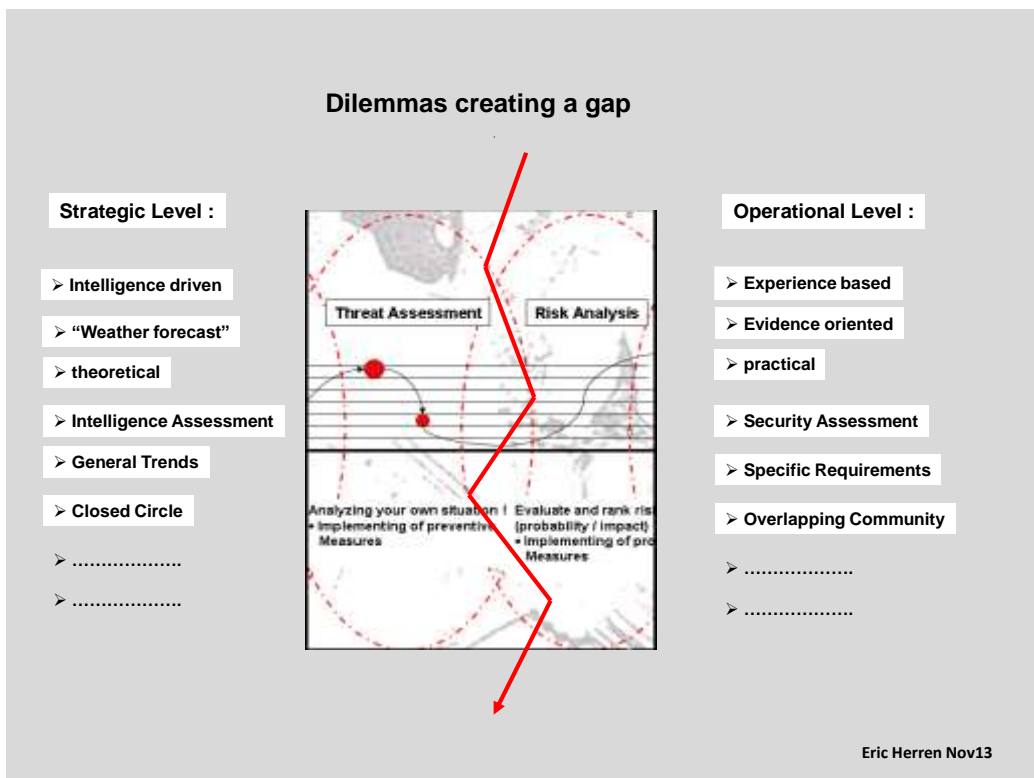
Let's take the example of a potential suicide attack. Intelligence is usually working intensively to monitor activities and all movements of potential terrorist groups or affiliated movements. Successful threat awareness should guide the services to potential hotbeds of radicalization. Here intelligence activities should include "counter terrorism street working" trying to lead away mostly young people from being captured by the gravitation of successful recruitments efforts of

terrorist organizations. Intelligence should be able to emplace kind of thermostat to measure the degree and success of radicalization.

In many cases Intelligence services do have information and knowledge of this kind but face enormous difficulties in transforming it to operational references. For example the killing of a potential suicide attacker by operational forces counts as a big success. To capture him/her alive would even boost this outcome. The so revealed close circle of a suicide bomber could initiate a much larger and comprehensive intelligence operation. One could for example not only follow the operational trail of the terrorist group but also try to discover the masterminds in terms of knowhow and technology. Foot soldiers are recruited more frequently; people who have the knowhow of assembling explosive charges are in the other hand quite limited. Here the challenge is to monitor a potential suicide bomber and his supporters in order to pinpoint the right moment for intervention. Such operations need an extremely high degree of cooperation and understanding of the involved counter terrorism organizations.

Dilemmas creating a gap

In general one can argue that the obstacles for closer cooperation are as follows. On a strategic level, involving activities of a rather proactive, analytical nature, lots of decisions are intelligence driven. Turning to the operational theatre, most of the moves are experience based. Two different mentalities, often two different languages and mind sets confront each other.

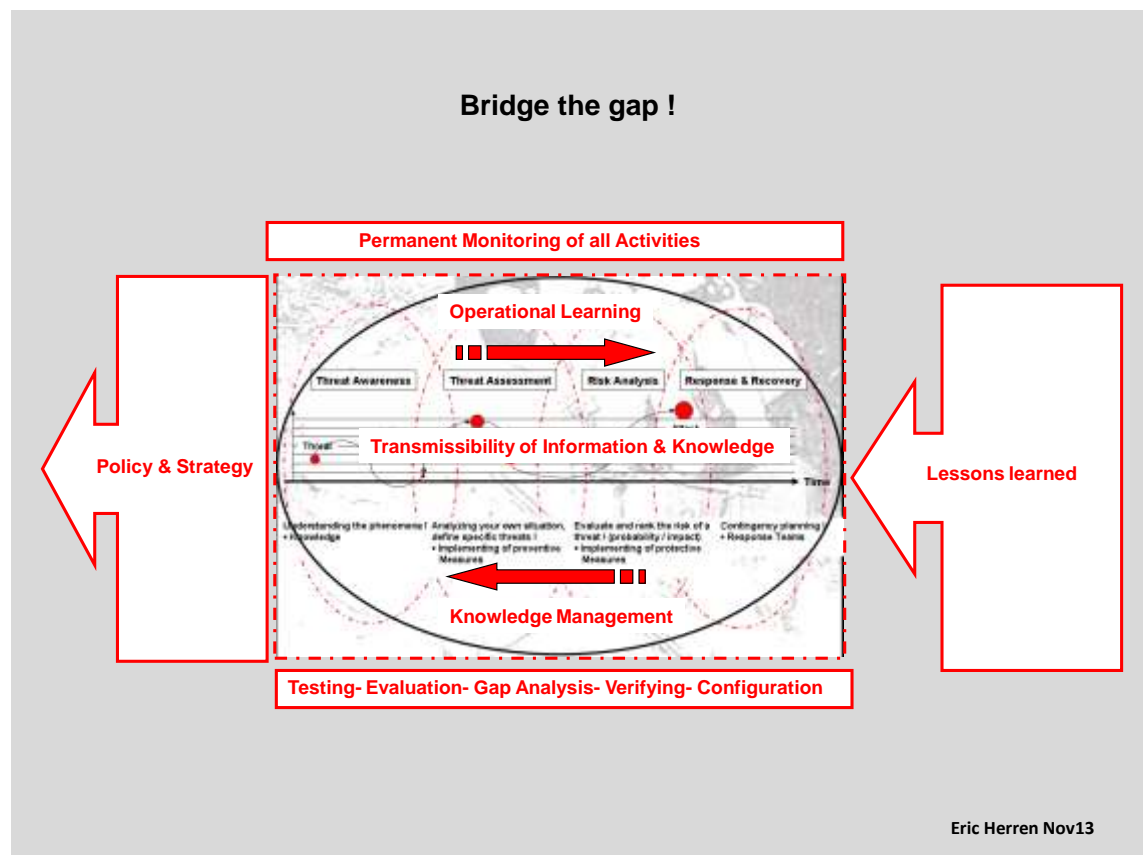


The operational theater is more evidence oriented with many practical guidelines. Intelligence is often theoretical and similar to a weather forecast. Organizations involved with risk assessment and implementing protective measures are in favor of specific requirements and security related arguments. General trends frequently provided by intelligence services are less appealing than concrete data and selected indications.

Another dilemma is the “closed circle” mentality of many intelligence communities in contradiction to the overlapping, interdisciplinary operational level, including many partners such as police, fire brigades and rescue units and others.

Can we bridge the gap?

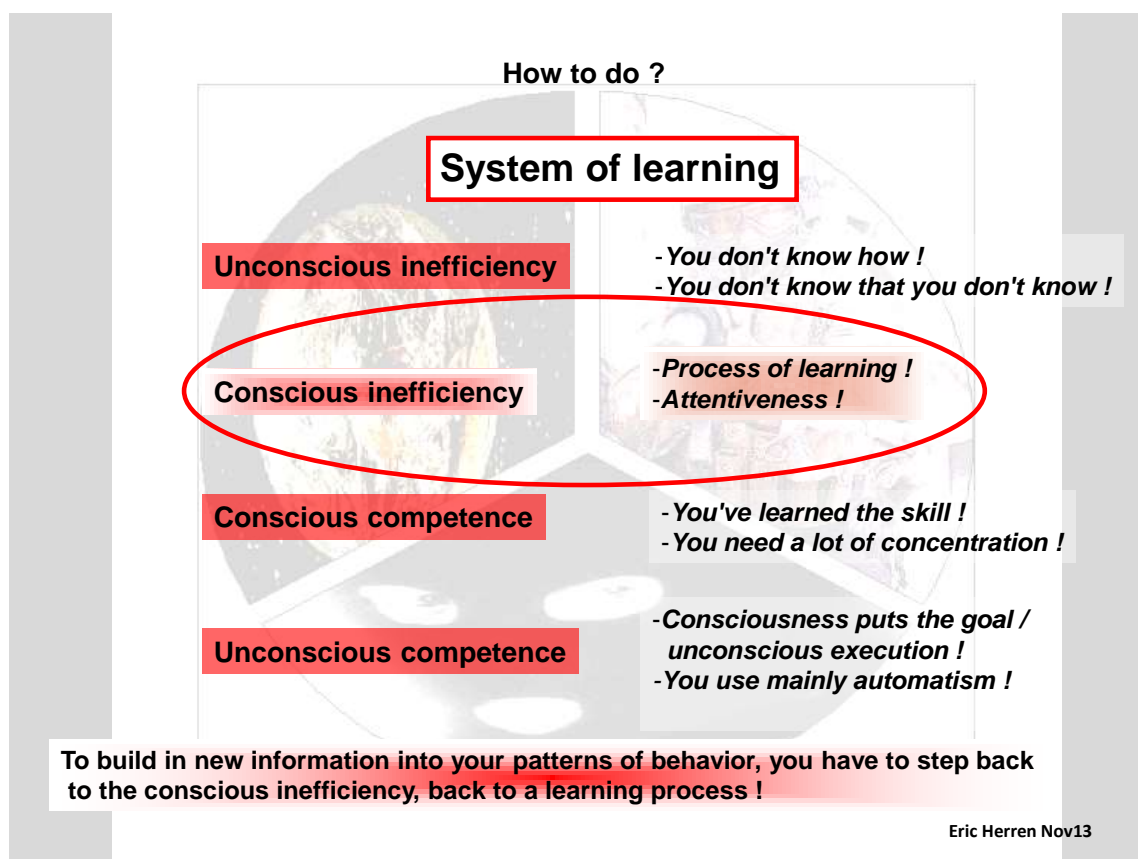
To bridge the gap one has to permanently to analyze the full complexity of the involved measures and actions. We need a permanent monitoring of all counter terrorist activities that are targeting the different multilevel initiatives and moves of radical groups. We have to test and evaluate permanently our reactions and planned operations. A mayor part in a successful policy and strategy has to be the implementation of lessons learned.



But in the end of the day, the gaps can only be bridged by a certain transmissibility of information and knowledge. Modern counter terrorist strategies have to include successful knowledge management and the ability of operational learning. The next pages should allow an insight in how human beings are dealing with information and how operational attitude can be manipulated and guided by perception behavior. We cannot allow having a piece of information somewhere within the counter terrorist community that could be decisive for the outcome of an action somewhere on the other end of the stage. All available resources have to be included to allow the best possible outcome of any activity. We will later on discuss the many obstacles that still prevent this unconditional cooperation.

How can we do it?

A first step is the understanding of the system of learning. It is essential to differentiate between the different levels of efficiency and competence. Unconscious inefficiency is the first stage. Here one can say that you don't know how to do a certain challenge or job. And furthermore you don't even know, that you don't know. This level in any counterterrorism business would be more than critical.



The second stage is the conscious inefficiency. You are in a process of learning and all your senses are enabled. Attentiveness is dominating your condition. The concentration capacity is limited.

Later on you reach the stage of conscious competence. You have learned the skill but you still need a lot of concentration. You act smoothly but slowly. You know what you are doing and the ongoing, permanent consciousness demands its price.

Unconscious competence is dominating the top level. Consciousness put the goal; you execute the complex system of different actions mainly unconscious by using automatism. This level of training increases the speed of action and relieves the consciousness for other challenges. Many special operation forces are functioning in this degree of training mode. Movements are fast and smooth, even complex patterns of action are executed with tremendous speed and accuracy. But one has to accept, that this high state of action is less beneficial in terms of integrating new and different information. Automatically executed structures of action are difficult to stop and divert. Your behavior is predictable and conducted in a closed environment. Once the complex action is triggered, it is difficult to penetrate the closed circle of an automated process.

To build in new information in your patterns of behavior, you have to step back, leave the stage of unconscious competence and force yourself to the level of conscious inefficiency, back to the learning process.

To think:” arranging your doing”!

“Thinking is coming out of doing. Thinking starts, when the structure of doing is being threatened or has to be corrected!”

All of us are day by day caught by fully automated processes. Let`s think about the example of driving our car. Most of it became routine. Some of us are able to make phone calls or even write messages during the journey to work. We became driving professionals and the free capacity of attentiveness and concentration is used for other tasks.

Only when an unforeseen obstacle is blocking our way, we are in a flash back in reality. If we will have the time, thinking will for a short while dominate our action. We will desperately search for a solution to avoid the crash with the obstacle. Without time, our reaction will come as a reflex. The shortage of time triggered an immediate reaction to the different and unusual situation.

Theoretically we can differentiate between three stages of consciousness of action. Starting by the above mentioned reflex and followed by a bit slower executed automatisms. Intentional actions are the most time consuming between the three different forms of activities.

“To Think: Arranging your doing !”

“ Thinking is coming out of doing. Thinking starts, when the structure of doing is being threatened or has to be corrected !”

The consciousness of action

Reflex

Automatism

Intentional Actions

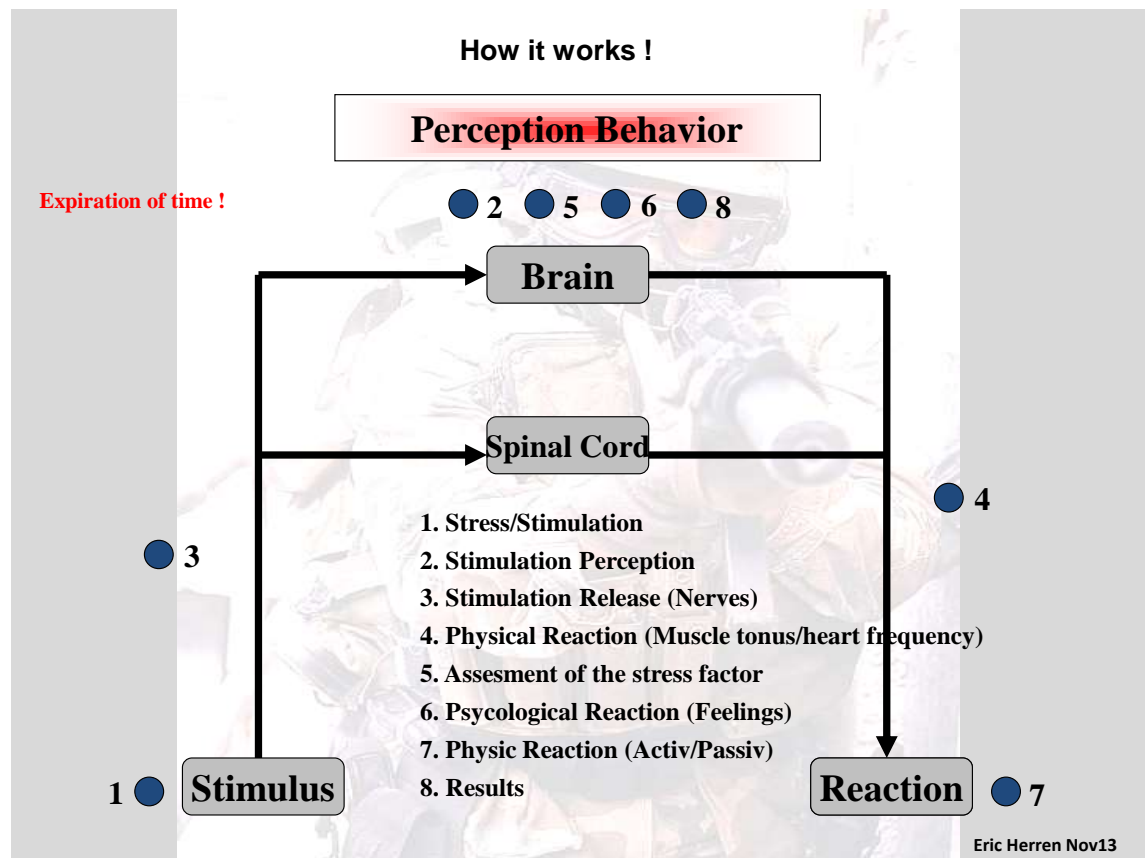
Decisive for the different kind of reaction- or action forms is the place of “switching” of the stimulation (or information) from the “lead in” to the “lead away” side of the peripheral nervous system !

Eric Herren Nov13

Decisive for the different kind of reaction- or action forms is the place of “switching” of the stimulation (or information) from the “lead in” to the “lead away” side of the peripheral nervous system!

Perception behavior

The multi faceted process of perception behavior is always starting with a stressor. This impulse is releasing a chain of different activities. The system is always the same, no matter if we talk about an special forces operator or an intelligence analyst.



Any kind of stressor that comes in to our focus of attention, is releasing a stimulus through the autonomous nervous system. The nervous pathway is preparing to forward impulses. Your brain will perceive this stimulation and will initiate and release the full stimulation of the nerves to act as a transportation system for the expected flow of impulses.

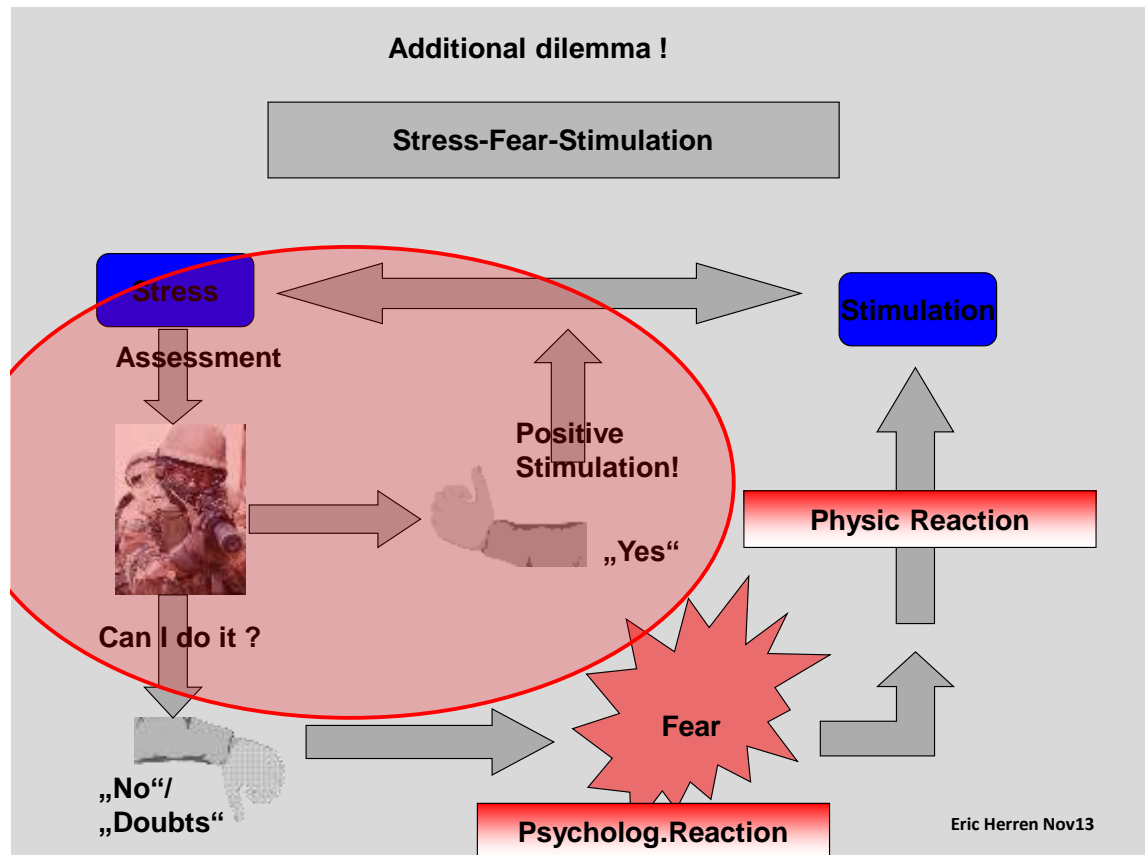
These activities will itself trigger a physical reaction. The heart frequency can rise and the tonus of the muscles increases. The system prepares itself for the following tasks. As we talked before about the reflex, here the impulse will be directly routed through the spinal cord and trigger an action. Almost all brain activities are skipped and therefore the action is much faster than a full intentional and conscious process.

But let`s come back to our stimulus that was responsible for the physical reaction. Only now the brain is assessing the stress factor. If we know what caused all this action, our brain will stimulate a psychological reaction. We will have feelings!

At the end of all this process will be finally activated the phycic reaction. This reaction can either be active or passive. The outcome of our intervention will now be registered and analyzed by our brain and influence the whole complexity of our further doing.

Stress-Fear stimulation

The assessment of the stressor by the brain is the critical process. The stressor or information can be assessed in either positive or negative way. A positive assessment will motivate our activities and positively stimulate our next assessment and therefore the whole behavior.



Negative assessments or doubts about the ability to handle the situation are immediately releasing psychological reactions. We have a feeling of fear or overstress. This will of course influence our physic situation by a strong stimulation of the heart beat for example. In such stress condition, further information processing will be difficult if not impossible.

From this one can learn that there are basically two methods to train people in high risk situation. One is based on reflexes, so the brain doesn't need to go through the whole assessment process and trainees are just acting like machines. They detect a familiar stressor and immediately the reaction is triggered. This kind of behavior could be accurate in war situations to avoid the overload of the soldiers system. Of course here one can support with medicaments and drugs.

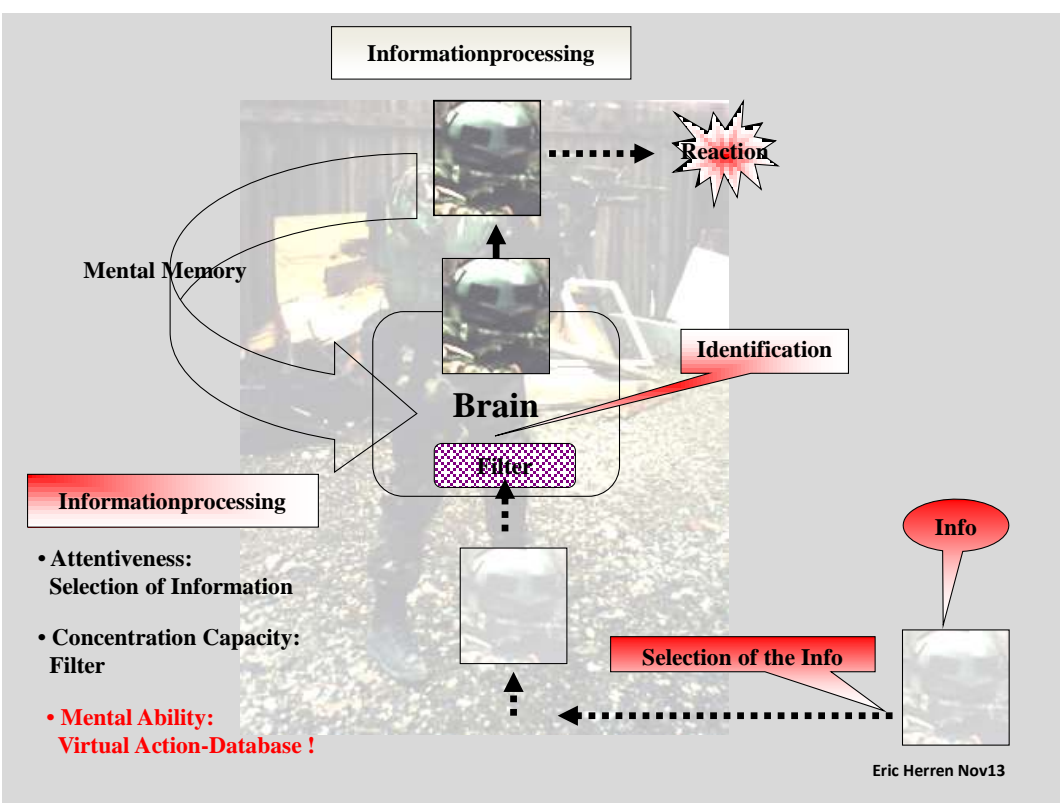
For counter terrorism and specifically pinpointed operations this reflex based behavior is not a good option. Successful operations cannot take the risk of a provoked overreaction. Terrorist

know how they can trigger a not controlled reaction by just creating a stressor strong enough to bypass proper assessment and release an overreaction that can be psychologically used to damage the whole operation. (Media war)

We have to do everything to support a positive assessment of the stressor and create a situation that our best prepared fighter can operate in a more or less controlled and intentional mode. Of course there will be moments and partial scenarios where absolute speed and efficiency is necessary. This phase of implemented automatic movements and reactions should never last for a whole chain of activities.

Information processing

After we basically learned about the way we act, we now can discuss how intelligence can support and influence this process. Perception behavior is based on information processing. Not every stressor has to influence our behavior. Special Police Forces use stun grenades to overload the perception behavior of their target. They protect themselves against the impact and prepare for detection and selection of necessary information to fulfill their task. Successful information processing starts with the detection of the accurate and relevant information. Especially in times of psyops and disinformation the selection of the important stressors and inputs is most valuable. Here training and experience has a most important role to play.



After detection and selection, the chosen information is filtered by our brain and processed for identification. We use our mental memory for alignment with stored information and data to match with the input we try to assess and identify. As soon as we match the info with existing data we then trigger a reaction.

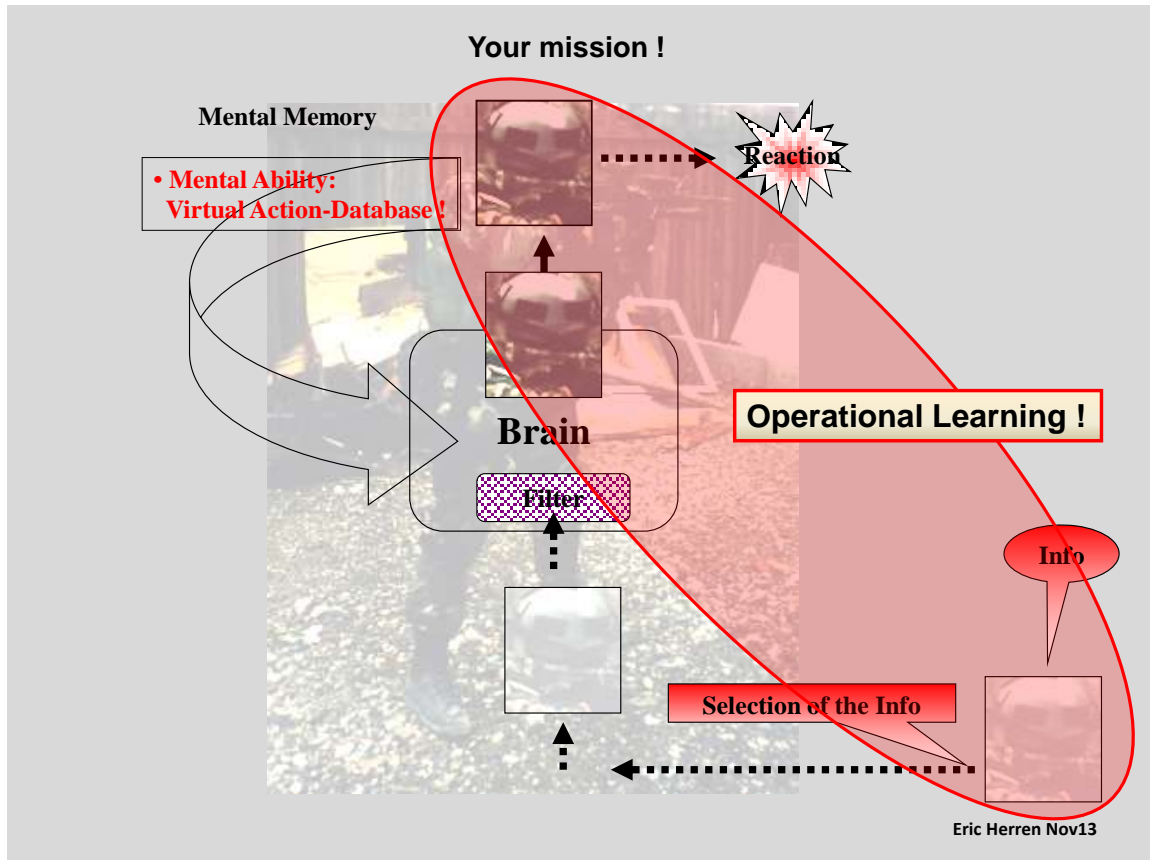
Successful information processing is depending on our ability to select the right information's over a certain period of time. For Special Forces operators, this time window might be smaller than for an intelligence analyst or somebody working on the strategic level. Nevertheless in any job, it needs attentiveness and knowledge about the range of targeted information sources. Also here the SF operator will have a more limited spectrum of sources than the intelligence officer at his desk or in the field.

The concentration capacity is crucial for filtering the ongoing flow of data and information. Once the acceptable limit is reached, nothing more will be or can be processed! This fact is more substantial due to the matter of fact that especially intelligence tend to act like a "dust machine" and suck in as much of information as possible. Let's bear in mind, that all this info has to be processed in order to create a useable output.

Most important is the mental ability! Operators need a "virtual action database". Identified inputs have to dock to limited variety possible reactions. This database serves as a virtual track for coming actions. It creates a feeling as if you've already been in this scenario. It guidelines your behavior and supports the stress assessment in a positive way. We will discuss after how intelligence can and must influence especially this process.

Operationalization of learning

With the knowledge of the above discussed issues, one has to identify the issue of information processing as a key for intelligence services to upgrade the operationalisation of intelligence. Here one can train and influence the ability to detect the relevant and mission oriented information. Especially in of the age of disinformation and psyops, intelligence has to affect and control the information selection process. What is useful and necessary and what can be neglected?

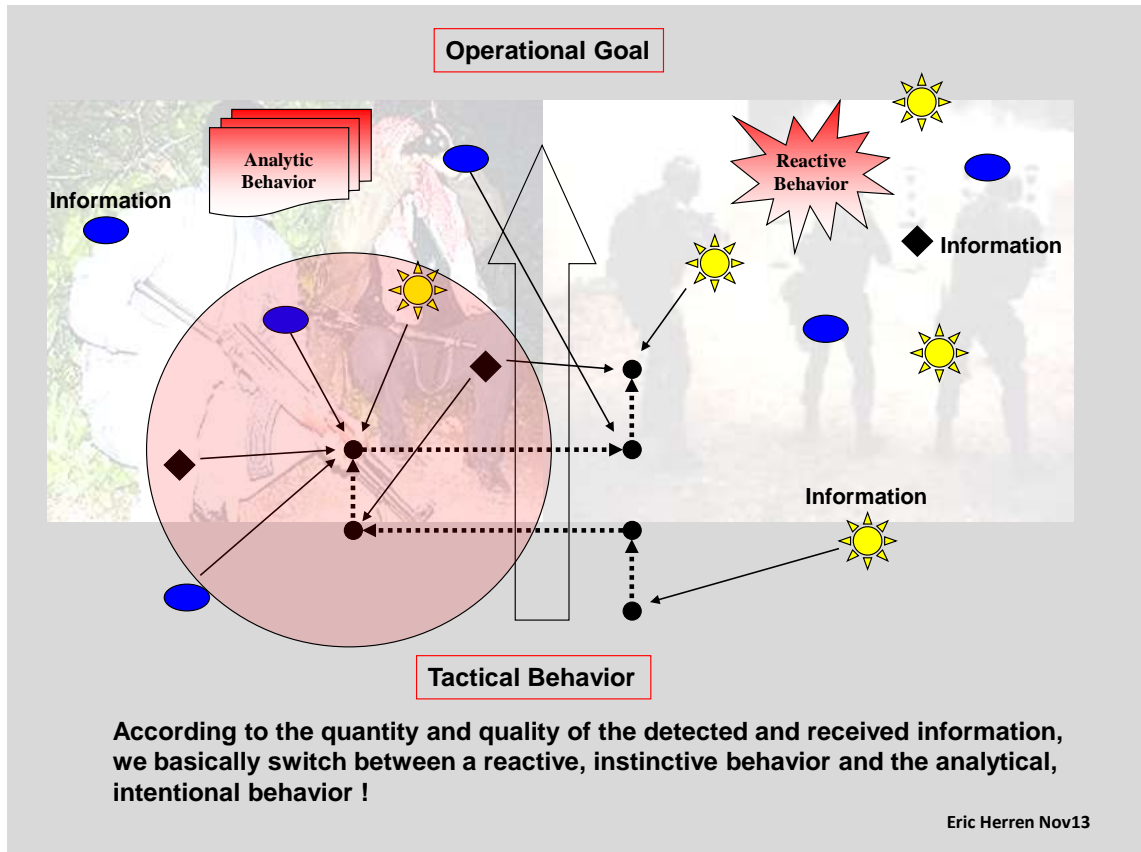


The identification process, the mental database is most valuable issues for effective and successful operational behavior. Intelligence has to be one of the master-builder of these abilities. Time after time this reservoir of knowledge has to be updated and the virtual action-database has to be refreshed, monitored and supervised.

Nobody wants an „intellectual fighter” but we need operators that can fight and act as “smart dogs“. They need the aggressiveness, instinct and determination of a fighter dog supplemented by the intellectual capability of an analyst!

Combat behavior

For each and every mission there is an operational goal. This is the guideline for tactical behavior. From the beginning to the fulfillment of the mission we are permanently exposed to a huge flow of all kind of information and stressors.



According to the quantity and quality of the detected and received information, we basically switch between a reactive, instinctive behavior and the analytical, intentional behavior!

This indicates that the pop up of a strong and dangerous stressor or information should automatically trigger an intentional, fast and accurate reaction. Our behavior is more instinctive driven and based upon speed and penetrating power.





After such a phase of psychological and physical peak one has to analyze and set the mode of action to a more anticipative level. This window of analytical behavior has to be used for operational learning. Only here one is ready to integrate new information and interrogate additional knowledge. The process of splitting a complex action into different partial actions and to allow analytical, intentional behavior is the art of new, complex training methods.

For example the tactical procedure of locking yourself into a shooting position, aiming and firing at the target is a complex exercise and action. But with the right training and technique, you can split up this procedure into part actions and build in one or two windows for selected information processing without losing time and efficiency.

The role of intelligence

In general one can say that intelligence has to support the process of information detection, - selection, identification and processing in order to allow the best possible (re)action. In this comprehensive and sensitive environment here some practical recommendations for tactical behavior based and supplemented by intelligence.

You have to :

	• detection	Teach operational forces about the tactical use of IED`s and other explosive charges ! (Expl. US Forces Iraq) Train them operational flexibility !
	• selection	Influence the training of selection processes in order minimize selection failures ! (Expl.US Forces explosive dogs) Change the training scenario into reality !
	• identification	Advise about the effect of psyops ! Not everybody with a weapon is a terrorist ! (Expl. Operation N.W. /S.Matkal Israel) Train the impact of strong stressors in order to control the reaction !
	• processing	Create the interface between intelligence and operational behavior ! Affect the virtual database and support the decision making process ! (Operational learning)

Eric Herren Nov13

Detection: Intelligence has to teach operational forces about the tactical use of IED`s by studying the forces combat behavior. Fake IED`s are place along the route of mobile reconnaissance patrols.

After successful detection, enemy watchers learn the procedures` of engagement. The target is to identify the command vehicle and its position in the convoy. The next patrol convoy will experience this form of operational learning in a hard way. The to be detected IED will stop the convoy; the deadly charge will be placed at the primary target position and remotely detonated as soon as the target is most vulnerable.

Selection: We all know the outstanding job of explosive sniffer dogs. Dogs act as repeaters. They learn a performance by imitating again and again the training scenario. If the trainer of the dog is repeatedly hiding the same amount of explosives, the dog has the following indications:

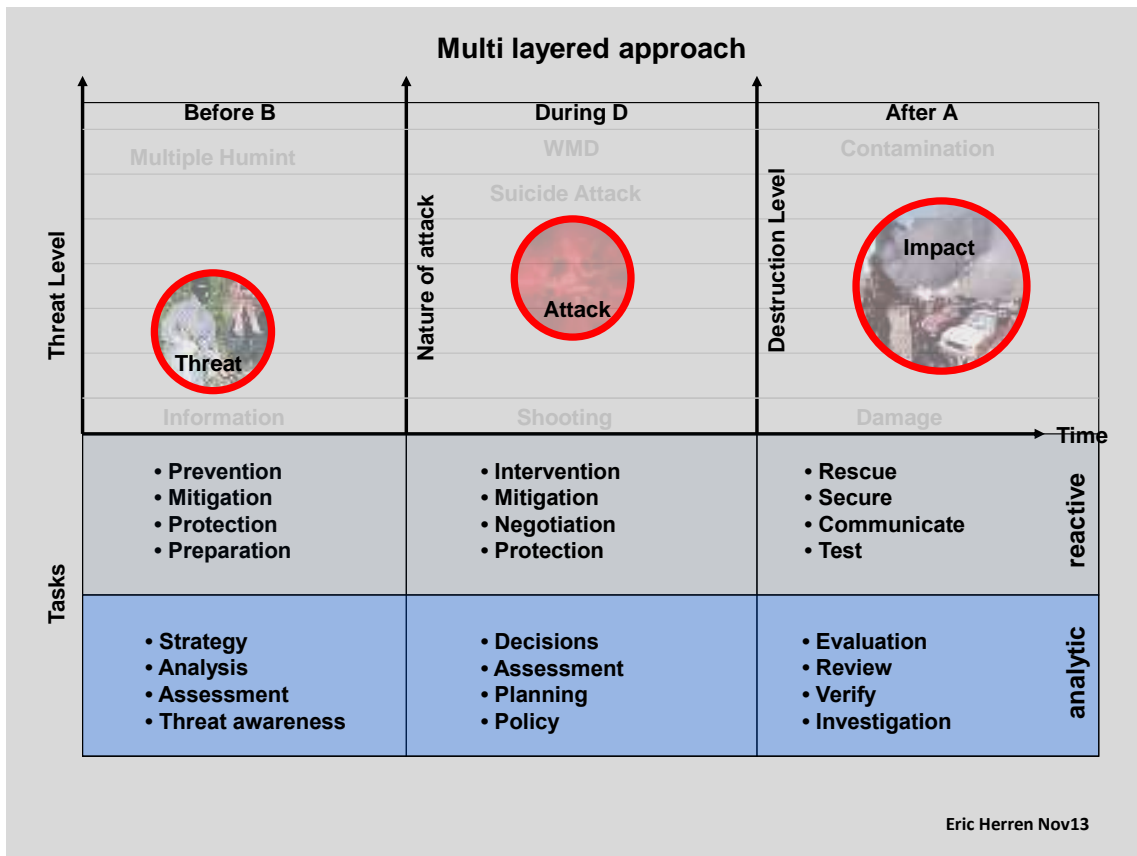
First the smell of the explosive according to the amount. Second: The dog assimilates additional the smell of the trainer. In real operation, the amount of explosives is usually much higher. More critical, the dog was used to two indicators; the smell of the explosives and the smell of the trainer. As deadly incidents proved, in reality it is not the trainer that places the explosives! Here intelligence has to allow knowledge management and keep the manuals of forces as flexible as possible to avoid routine and predictable behavior.

Identification: Not everybody with a weapon is a terrorist. Usually the stage of counter terrorist operations is carefully prepared by the enemy. For example in a hostage taking scenario the terrorist can influence the information processing devolution of the entering force by dress up the hostage and arming them with weapons without bullets. If the operator is not able to control his instinctive reaction to the stressor in form of the weapon, he will most probably kill the hostage. Intelligence must become a partner in the training process. Analytical windows have to become an indispensable part of combat drills.

Processing: Intelligence and operational force have together to create a successful interface. Operational learning must become an integral part of combat behavior. As we learned, the rucksack filled with self-confidence based upon a variety of mental abilities such as a extensive virtual action database and adequate mental footprints to guideline the appropriate (re)action basically decides about a positive assessment of the situation and minimizes panic reactions.

The conceptual, multilayered approach

In general one the stage of a terror attack can be partitioned into three phases: Before, during and after the attack. We can also draw a diagram about the development of a threat. Before an attack from a simple rumor up to multiple humint . During an attack its potential nature, from a shooting up to an attack involving WMD. After a successful attack its impact, ranging from simple damage to the contamination of a whole area.



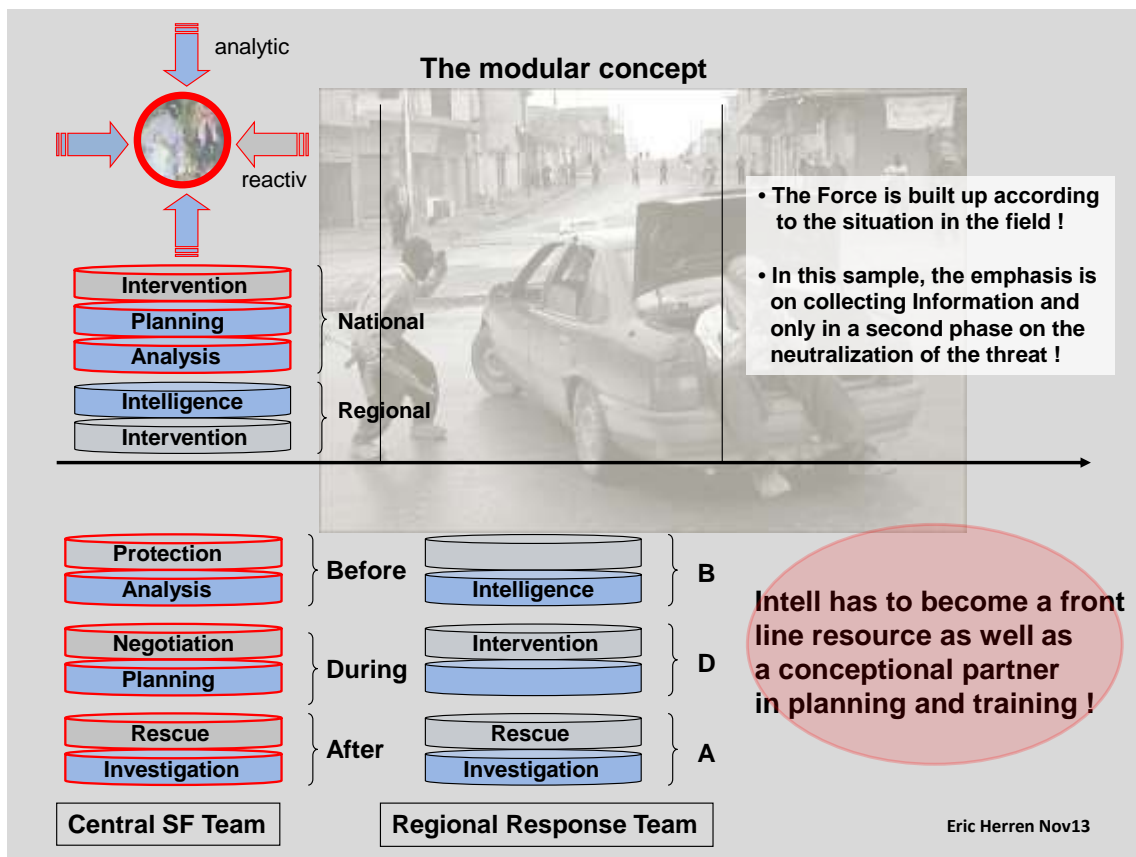
Each of these phases is demanding different tasks composed by reactive and analytical operations. Let's concentrate on the time window during an attack. Here every step is under pressure of time and there is no space for failures other than on the account of human lives. On the reactive, operational front the tasks are ranging from intervention to mitigation, negotiation and protection to name only few of possible actions. The analytical tasks include such as real time assessments, decision making and planning.

The analytical part is mainly intelligence driven whilst the reactive part belongs to the specialized forces.

If we look at whole picture, from the threat awareness until the after action review one has to come to the conclusion that the answer for such a developing, hardly predictable and diverse scenario has to be a modular, flexible concept.

The modular concept

In counter terrorism time is primary factor. If one can allow taking all the time necessary to detect, select, identify and process information there is no need for upgrading any interface between involved organizations. One can wait to get the full intelligence report about information picked up by some sensors out in the field. Special Forces can exercise and drill scenarios from the past until speed and accuracy are phenomenal. Even politicians and decision makers can manage problems instead of solving them.



But if the threat is real and developing, do we have the time to wait for analysis from some headquarter? Can we allow monitoring new developments and tactics without an immediate, accurate response? Does it make sense, to have exclusively military Special Forces as a front line organization to deal with terrorism in populated area?

History teaches us that most of the terrorist attacks have a more or less long lead time. The threat is not linear, there are times the opportunity to attack is perfect and the threat jumps from strategic planning to immediate execution. If the counter terrorist community claims to be

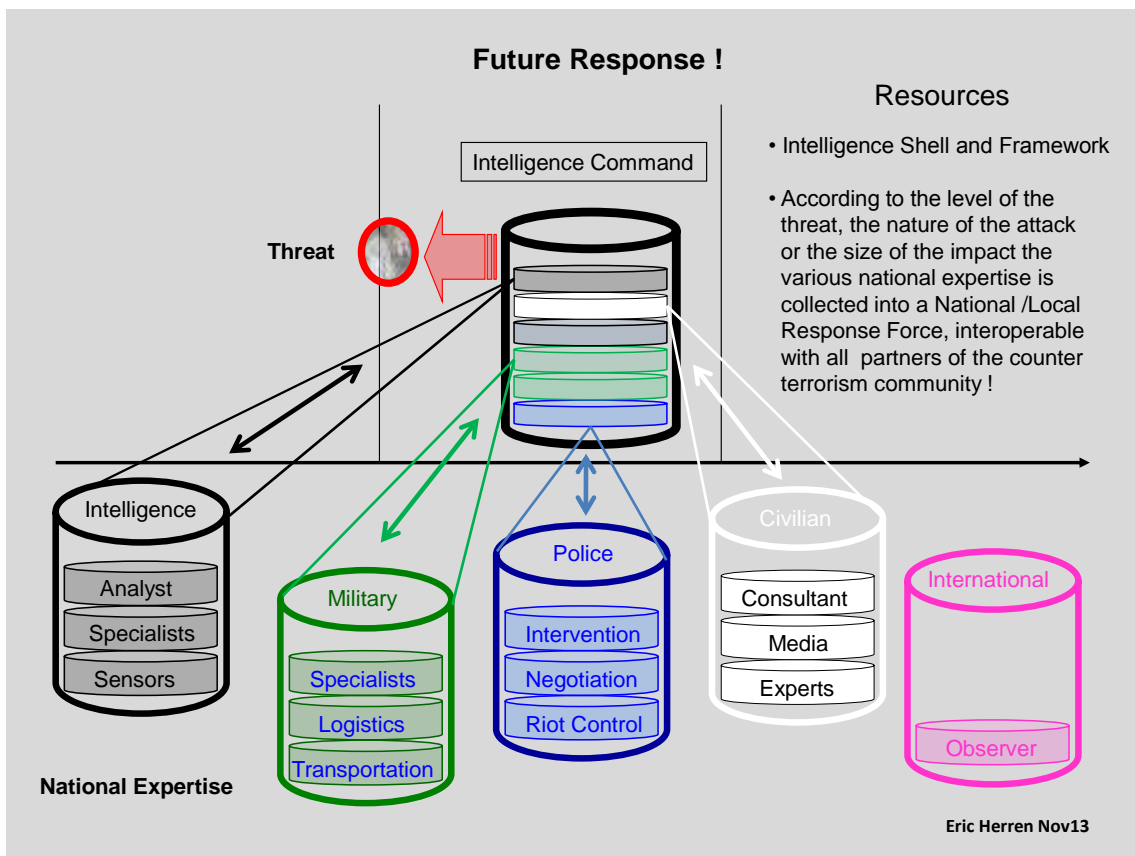
prepared for such scenario, the answer to the threat must be a modular force with all necessary tool, abilities and skills to handle the developing scenario.

If terrorists are in a recruiting phase, there is no need for military or even police intervention. This is a purely analytic task to learn about the structures and modus operandi of the group. The lead will be intelligence, even civilian academic one and the force can contain an intervention element, preferably police Special Forces, if something goes wrong. The benefit of such response is obvious. The counter terrorist community learns and collects information about equipment, training, planning and network of such a group. And still reactive forces should be an integral part of the response in order to assimilate and suit their tactics to the threat.

In this view the best response consist in a national or central and regional response teams. A serious, on multiple sources based threat, will trigger an immediate regional response, containing all necessary tools, from intelligence to intervention elements. According to their first assessment after stabilizing the situation, the central force will send additional selected forces to support, complement and intensify the best possible response.

The” future” counter terrorism force

In this concept one can integrate the whole experience and knowledge of different national and even international expertise. One organization, preferably the most politically acceptable, provides the framework and the umbrella for such unit or structure.



According to the level of the threat, the nature of the attack or the size of the impact the various national expertises is collected into a Central and Local Response Force, interoperable with all partners of the counter terrorism community!

To come back to the main thesis of this paper, the operationalisation of intelligence, such a modular force would be the best matrix for successful operational learning and knowledge management. The necessary transmissibility to become an interdisciplinary force, would allow to grow up together and influence each other in training and operation.

In the micro level, Special Forces group facing a change of enemy tactics or are exposed to kind of psychological warfare by the enemy using civilians, especially women and children as human shields, get an immediate analysis and interpretation by the embedded intelligence element with the full organizational back up of his institution. Of course one can argue that it is sufficient, if the intelligence cell sits in the same room with SF commanders analyzing the video transmissions of different sensors.

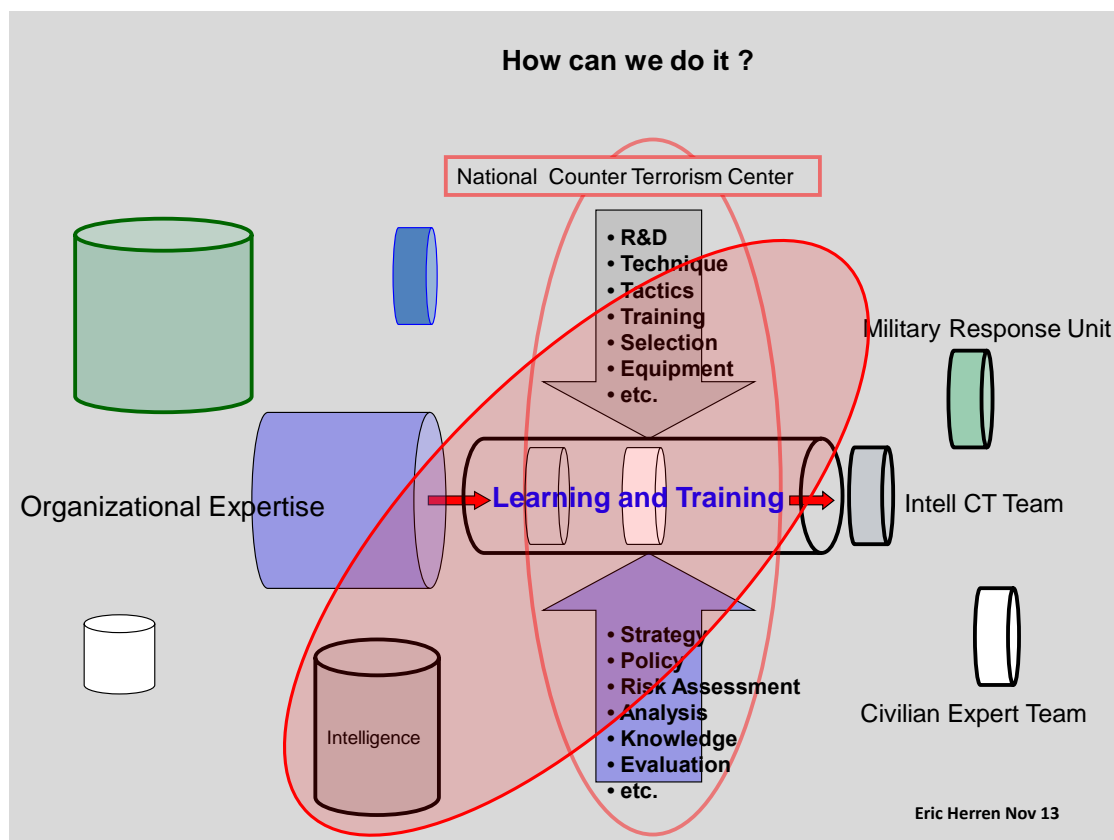
In counter terrorism we just have to bear in mind, that sometimes the pressure of time is immense and the frontline fighters have a different angle of view than intelligence based combat

operator. In such a setup, we could really talk about the immediate operationalisation of intelligence.

With or without direct combat involvement of such a unit, at least the concept of a modular headquarter, consisting all necessary elements is an absolute necessity. Modern technology allows a multi dimensional picture of an emerging situation. Without a central coordination and analysis, involved forces are tending to do what they know best. Military forces will engage too early or disproportional. Intelligence, in order to get the maximum of information is risking losing the best possible momentum for intervention. Even politicians have to become part of the process to experience the need of clear strategies and decisions.

How can we do it?

The answer must be the set up of a Central or National Center of Competence. Here the individual best resources from the armed forces, air force, intelligence, police, rescue and many other organizations come together to integrate their expertise into a comprehensive counter terrorism policy and strategy.



It is here, that at the micro level the intelligence officer teaches the Special Forces operator about the best division of complex activities into partial actions that allow operational learning and guidance.

In such center, the gaps between the strategic and operational level have to be located, discussed and solved. Here the individuals can grow to a community understanding the different mentalities and often different languages. This coherence can then be implemented back in to the individual organization. The transfer of knowhow and the readiness for unconditional cooperation could be the next step.

As a consequence of such development, states should build up National Operation Platforms to create the necessary playground to simulate multiagency cooperation as well as permeable information exchange within the relevant, national security organizations.

Such platforms will enhance and upgrade the ability of states to react on strategic threats and challenges using its full potential of available resources.

Sophisticated data fusion and data and sensor integrating capability should be the base for successful command and control competence. State of the art technology paired with effective, solution oriented processes together with the precious human factor, should empower modern states to cope with asymmetric threats such as terrorism and modern forms of proxy-warfare.

Reality

Reality shows us a different face. Organizations are fighting for power and individuals are imprisoned by their egos. As long as we produce homegrown “weak points” by missing cooperation, our operational and tactical response to terrorism will be questionable.

Every organization involved is looking at the problem from its very own perspective and focus. As soon as we are willing to integrate other frames of reference and expertise, we will enable ourselves to a constant learning process that is necessary to develop the most needed flexibility in accepting intelligence to lead our operational behavior.

We are not in charge of the global, political response to radicalization and terrorism, but what we are tasked, we should do best!