

SPECIFIC ASPECTS OF PRIVATE SECURITY IN HIGH-RISK ZONE

Srđan Srdanović
Edinburgh International, Basra, Iraq

Rapid commercialization of security services in high-risk zones and engaging security and private military companies has put private security in high-risk zones in the focus of interest.

As the tactics of attackers who act in high-risk zones is becoming more progressive and innovative, security experts and practitioners in the field of private security have to secure and improve the overall safety of the assigned zone, facility, individual, vehicle, aircraft or vessel by means of adequate organizational, intelligence-security and physical-technical measures.

It is believed that private security in high-risk zones will be of relevance in the near future as part of security system. This paper is an attempt of contributing to scientific material which describes the above stated security issues. The paper shall explain the concept, features and standards of private security operation in high-risk zones and offer some of the models for predicting the flow of suicide attacks, attacks on vehicles in movement by improvised explosive devices, attacks on road convoys, pirate attacks on commercial ships, as well as procedures of protection against such attacks in high-risk zones.

Key words: *private security, high-risk zone, private security companies, private military companies, suicide terrorist attack, static guards, securing individuals during vehicle movement, road convoy*

Introduction

Contemporary international social-political scene faces numerous security challenges and threats. Along with expansion of weapon for mass destruction, conflicts (especially interstate conflicts) and transnational organized crime, one of the most present challenges is terrorism in the so-called *high-risk zones*.¹ According to the western theory of security research, high-risk zones refer to warfare or low-intensity conflict areas. Current combat areas include the territories of Afghanistan, Iraq, Syria, Somalia, etc. Additionally, high-risk zones are present in socially-politically instable

¹ On terrorism and organized crime as global threats to security, see, *Organizovani kriminal i terorizam*, Academy of Criminalistics and Police Studies, Belgrade, 2012; Townshend, C., *Terrorism: A Very Short Introduction*, New York, Oxford University Press., 2002; Carr, M., *Unknown Soldiers: How Terrorism Has Transformed the Modern World*, London: Profile Books, 2006.

countries (Pakistan, Libya, Israel- Lebanon, Yemen, Mali, Algeria, Egypt, Sudan-South Sudan, Congo, etc.). Additionally, aggravated robberies, robberies and frequent pirate attacks on cargo ships in Somali sea area, Red sea, Gulf of Aden and waters around the Horn of Africa are present in high-risk areas, especially on the African continent.

Fundamental security system institutions of most countries are armed forces, intelligence-security agencies, police and anti-terrorist units. Rapid commercialization of security services has been present in high-risk zones, especially in the past two decades. Security-related tasks, which state security forces of the countries with armed conflicts or countries engaged in war conflict zones could not independently and efficiently handle, have become more and more present on security market and thus the above stated countries started relying on private security subjects.

As for high-risk zones, private security services are carried out by private security companies as new/modern security service "providers". However, there are numerous dilemmas regarding the foundation and operation of *private military companies* as important private security entities, and their active and key participation in security service providing in high-risk zones. As time goes by, private security entities take more part in accomplishing, preserving and improving integral (general) security, as well as all other security levels (individual, social, regional, international, economic, energy and corporative) in high-risk zones.

The increasing presence of private security actors in high-risk zones and the lack of material that deals with this topic have been sufficient justification for writing this professional paper.

Constant progress and innovations in attackers' tactics (methods of operation) create a changeable situation on the field and therefore the system of security measures is to be adjusted on regular basis in order to minimize attack risk and provide an efficient response to attacks in high-risk zones.

Necessity of researching the role of private security sector in high-risk zones derives from the fact that the basic actions of private security subjects are focused on fighting terrorism, which has become a global threat to security. Therefore, terrorism is to be eliminated by continuous, systematic, efficient and timely planned actions.

Scientific justification of this research comes from the fact that overall, objective and integrated overview of private security potential for fighting terrorism and other forms of jeopardizing safety in high-risk zones is impossible without actual insight into this area, including all facts and specificities on the field. Social justification of this research is in informing professional academic community about the necessity of timely and organized planning and conducting activities that make private security subjects more efficient in high-risk zones.

Innovations and changes of attackers' tactics require adequate measures of prevention and protection of clients, facilities, vehicles, vessels, aircraft, etc. by private security forces.

I believe that a special system of security measures, which are adjusted to field situation, is necessary for reducing risk to the minimum and responding to attacks on protected individuals, zones, facilities, vehicle, aircraft, vessels, etc. in efficient manner.

The subject of this research is emphasizing specificities of private security segment in high-risk zones.

Suicide terrorist attacks on facilities in high-risk zones

According to American politicologist *Robert A. Pappé's*² analysis of suicidal actions, a constant growth of suicide terrorist attacks has been recorded worldwide for the past thirty years. During 1980s, there were three suicide actions a year, during 1990s there were ten suicide actions, while there were around fifty terrorist suicide actions during the past decade.

My personal analysis of the information sold by the private companies that deal with collection and market distribution of data³ has shown that there are more than 80 suicide terrorist attacks on the territory of Afghanistan per year and that the number of attacks is constantly increasing.

Information from the same source show constant growth of light infantry armed attacks (using automatic rifles, guns, hand grenades, rocket launchers, mortars, etc.). However, as light infantry armed attacks are not characteristic for high-risk zones only, *suicide terrorist attacks are specific tasks that private security is facing in high-risk zones.*

Persons who are protected in high-risk zones move from accommodation facility to work facility (various private companies, banks, embassies, international organization offices, government and local institution facilities, military-police facilities, airports, construction sites, energy and industrial installations, etc.). As a rule, accommodation and work facilities are secured by professional military-police or private security companies. Additionally, attackers are interested in accommodation and work facilities, which are also the targets of suicide attacks.

A suicide attack on the selected facility is an individual act. However, the attacker is the last link in the chain of well-organized groups behind these suicide attacks. After making a decision on the attack, action organizers do the following:

1. select the target (facility, person, vehicle, etc.),
2. collect information about the target,
3. recruit the attacker,
4. carry out physical-mental preparation of the attacker,
5. prepare arms and explosive charge, and
6. organize the transportation of the attacker to the target.

Preparation of suicide attacks is different from the attack performed by military-police forces, as it does not imply attacker's rescue after the attack. This fact facilitates suicide attack organizers' job, but makes it harder for security services, both military-police and private security companies. *Specificity of private security in high-risk zones is a lack of plan for rescuing the attacker and lack of care for his personal safety in the final stage of the attack.*

Several people, sometimes more than ten, take part in organizing and carrying out suicide attacks. The number of direct attackers- suicide actors is the smallest, while the other members of the team, who will not perform self-detonation, are crucial for organizing and carrying out the attack.⁴ Such people select the target, collect information about the target, recruit the attacker, carry out training and psychological preparation of

² Pappé, Robert A., "The Strategic Logic of Suicide Terrorism", *American Political Science Review*, Vol. 97, No. 3 August 2003, pp. 20-32.

³ "Securo group", "Titan", companies which do business within "ACAS" group, etc.

⁴ Sprinzak, E., *Razumnifanatici*, vid. <http://www.bhdani.com/arhiva/223/122313.shtml>

the attacker, provide arms and necessary parts of explosive charge, and provide accommodation, supplies and safety of attacker during the attack preparation. They take part in both the above stated elements of attack preparation and in direct attacks as watchers, drivers, cameramen, landmark-positioned men, couriers- reporters from the location of the attack and other positions that are used for supporting the attacker.

Secrecy of preparation and initial attack stage is necessary for suicide attack success. In order to achieve the effect of surprise, suicide attack organizers are to make sure that preparations are secret. Simultaneously, they continue collecting information about the target. Information are obtained by watching the target- if the information are precise and thorough, the attack is planned to the smallest details. If the attack is well-planned the suicide attacker will not be noticed until the moment of the suicidal act. Having in mind that suicide attacks require large amount of information, attack organizers have the entire network of field agents who collect data. They watch the target facility, surrounding roads, record time and routes of target movement, time of guard service change and other characteristics of security service (security measures, procedures, equipment, vehicles, etc.).

International institutions(UN, EUPOL, UNDP, etc.), as well as private military and private security companies mainly hire local population of the area where they have been engaged, due to low cost of labour and the idea that local population should not see them as occupying forces. Suicide attack organizers collaborate with local workers who are located within the secured facility and who collect information about the target. Example of such collaboration is the attack on the largest military base on the planet, which includes *Camp Bastion and Camp Leatherneck*⁵ in Afghanistan province Helmandin 2012. A group of fifteen Taliban, organized by the growing Haqqani network, broke into the facility, killed two American marines, injured nine people and destroyed eight Harrier jets.

In order to prepare this attack, the organizers used information from the local workers who were engaged as construction site workers. These people made passages (holes in the fence) which were later used by suicide attackers. *Specificity of private security in high-risk zones is the presence of local workers inside the protected facilities.*

Local workers mainly come from tribal societies. One person (chief- tribe leader) is the leader of these ethnic-territorial groups. The chief is an authoritative leader and organizer of the life of tribe members. Tribe leaders are part of official local and state government organs. As for Afghanistan, tribe leaders constitute a specific legislature institution called Shura. Security managers of private military and security companies cannot hire new local workers without consulting the tribe chiefs. Security companies hire only the members of the local tribe who live on the territory of the secured facility. The exceptions are working positions that require specific education or skills which majority of the candidates does not possess (translators, drivers, technical equipment handlers, etc.). Strong sense of belonging to the tribe and tribe members' presence makes it hard for security management to deal with these people. Tribe members often collectively refuse to work, leave the workplace or collectively stop working.

In such cases, cooperation between security management and tribe chiefs is necessary for overcoming the above stated problems and enabling the work of security services. *Specificity of private security in high-risk zones is cooperation between security management and chiefs of the tribes that live on the territory of the protected facility.*

⁵ Compare: Camp Leatherneck, Internet 18/08/2014, <http://www.bbc.com/news/world-asia-19608561>.

High-quality selection (recruitment) of attacker is essential for the success of a suicide attack. During 1990s, selection of candidates for suicide attacks was exclusively connected with Islamic service and religious-terrorist organizations, such as “HAMAS”, “Islamic Jihad”, etc. which had their recruiting agents in mosques. Nowadays, modern suicide attacker recruitment is carried out in schools, workplaces and even families. Ideology-religious motives are not crucial for making a decision to take one’s life and kill other people. In order to attract new attackers, recruiting agents use blackmail, intimidation, financial compensation to the attacker’s family, etc. Attackers are chosen from various national, gender, social-intellectual and age structures, and include young men, experienced fighters, women with children, uneducated peasants and intellectuals. Taliban recruit young boys aged 12-15. Diversity of attacker selection could be supported by a famous example of suicide attack on the Chapman camp that took place in 2009 in Afghanistan province Khost when Jordanian doctor killed himself and 7 CIA agents and wounded six other people. This intellectual was a double agent. Both American CIA (*Central Intelligence Agency*)⁶ and Al-Qaeda used his services. On the date of the attack, the doctor arranged a meeting with several CIA operating agents within Chapman base⁷. Each agent wanted to find out the important information that the doctor wanted to reveal and thus all agents appeared on the meeting place together. At the moment when the agents approached to greet the doctor, he detonated himself.



Picture 1 – Suicide-bomber who will press electrical-switch and activate explosive charge

Selection of suicide attackers from various psychological and demographic structures is observed as specificity of private security in high-risk zones.

Vehicles that suicide attackers or their drivers use are often stolen or have stolen registration plates (usually, these are the vehicles or registration plates of UN which has

⁶ More about this intelligence agency: Bajagic Mladen, *Spijunaza u XXI veku – savremeniobaveštajno-bezbedonosisistemi*, MARSO, Blegrade, 2010.

⁷ (FOB Chapman/ Forward Operating Base Chapman)

the largest transportation fleet). Reason for stealing such vehicles or plates is the possibility of passing control military-police spots without problems, covering tracks and achieving the effect of surprise.

Suicide attackers' explosive charges are activated either personally or from a distance. Vehicle's forceful entrance into the facility usually happens before the suicide-bomber's attack. Most frequent time of the day for the attack is after one of five daily prayers, as Islamic fundamentalists are then very motivated for suicide attacks. Suicide bombers carry out the attacks by means of:

1. BBIED⁸
2. MBIED⁹ and
3. VBIED¹⁰.

Aside from the case where the attacker personally activates explosive charge¹¹ by pressing the switch fixed on his palm, the explosive charge can be activated from a distance by "the operator" who chooses the ideal moment for the detonation. In this case, explosive charge is activated electrically, usually by means of a cell phone or radio device.

The price of a suicide belt is approximately \$ 100 US and its construction is technically simple. Explosive, as well as other types of arms and ammunition are available on the black market. Trained men are always in charge of explosive charge construction¹².

Organization of facility security service in high-risk zones

Facilities in high-risk zones consist of accommodation facilities and work facilities (various private companies, banks, embassies, international organization offices, government institution facilities, local administration facilities, military-police facilities, construction sites, energy and industrial installations, etc.). These facilities are located in urban environment, as well as in city suburbs and rural areas.

⁸ BBIED- Body Born Improvised Explosive Device, Compare: Improvised explosive device, Internet 18/09/2014, http://en.wikipedia.org/wiki/Improvised_explosive_device, Alexander, Naomi et al., *Body-borne IED detection: NATO DAT#10 BELCOAST 09 demonstration results*, SPIE, Vol.7670, 76700G (2010).

⁹ MBIED-Motocycles Born Improvised Explosive Device, Compare: Briefing to the UN Convention on Certain Conventional Weapons: Diversion of Civilian Explosives and Commercial Products for use in IEDs, April 2014, Internet, 18/07/2014, [http://www.unog.ch/80256EDD006B8954/\(httpAssets\)/D4830D557AE1C3A0C1257CAE0045D4E0/\\$file/09+US+A-JIEDDO+\(Maj+O'Connell\)_APII+GX+2014.pdf](http://www.unog.ch/80256EDD006B8954/(httpAssets)/D4830D557AE1C3A0C1257CAE0045D4E0/$file/09+US+A-JIEDDO+(Maj+O'Connell)_APII+GX+2014.pdf).

¹⁰ VBIED- Vehicle Born Improvised Explosive Device, Compare: Vehicle Borne IEDs (VBIEDs), Internet 21/07/2014, <http://www.globalsecurity.org/military/intro/ied-vehicle.htm>.

¹¹ Explosive charge consists of high-blasting explosive bullets, electric detonator, cables, electrical battery, switch-trigger, mobile phone or radio device) packed into a vest which is adjusted to attacker's body

¹² YahyaAyyash, called "the Engineer" was the chief bombmaker and one of the leaders of Hamas wing "Al-Quassam". Ayyash was born 06.03.1966. inRafat near Nablus. He graduated from BeirZeit University, Department for Electrical Engineering in 1988. Yahya joined "Al-Quassam" in 1992. after which he specialized the process of making "homemade bombs" which were used for series of suicide attacks in Israel. Soon after that, he became one of most wanted terrorists in Israel. After a three-year search, he was killed by Israel security forces on January 5th 1996. by means of a bomb which was set in his mobile phone, ICT website <http://www.ict.org.il>.

Basic elements of security service formation in high-risk zone facilities are:

- Static guards¹³,
- ECP Enter Control Points,
- Patrol service, and
- Service for video and technical supervision of facility perimeter.

Each of the above stated services operates in accordance with its own standard procedures.

Static guards are mainly members of the local community or former members of military-police forces from „the countries of the third world“(Uganda, Philippines, Haiti, Nepal, etc.). Exception from this rule are facilities of special importance, such as embassies, facilities for accommodating commanding structures of coalition forces or facilities for security services. Former officers and sub-officers of local military-police forces are engaged on the position of lower management or have lower commanding duties. Former officers and sub-officers, members of military-police forces from Europe, USA, Australia and Republic of South Africa are on higher management level and are engaged as Shift Supervisors or Team Leaders. The Gurkha¹⁴ members are quite often the members of Static guard service in high-risk zones. Guard service is organized in two shifts (day shift and night shift). Guards are located on the towers which are at dominant height as compared to perimeter wall which is constructed from stone or prefabricated elements- combination of wire fence and impregnated canvas with sand between them, the so called “HESCO- Defensive Barriers”¹⁵.



Picture 2 – Guard towers with HESCO Defensive Barriers

¹³ Static Guards, Internet 29/06/2014, <http://www.consolidatedsecurity.com.au/static-guards/>.

¹⁴ Gurkhas are the people of Nepal. Having in mind the closeness of the Himalayan Mountain, male population traditionally works as escort to alpinists who climb Mount Everest. However, majority of Gurkhas work as soldiers. They are initially members of Nepalese army, but the best soldiers are recruited in Gurkha brigade which is a part of the British army. Due to their loyalty to superiors and employers, Gurkhas are present in private security guard service in high-risk zones. Additionally, an important reason of their massive presence is low cost of work and lower life standard of Nepalese population.

¹⁵ *Defensive Barriers*, Internet 21/06/2014, <http://www.hesco.com/products/defensive-barriers>; *HESCO Bastion - Protective Barriers, Accommodation Bunkers and Hostile Vehicle Mitigation Fences*, Internet 21/06/2014, <http://www.army-technology.com/contractors/infrastructure/hesco/>.

Guard shift is controlled by Shift Supervisor. Shift Supervisor manages the guards from the control room and visits guarding spots from time to time. He is in constant contact with facility Security Manager. The Supervisor coordinates activities with Patrol Supervisor on duty, Enter Control Point Commanders and Technical Supervision Shift Leader.

In case of an attack, Static Guards who are not on duty are to secure all individuals who are located within the facility. After they make sure that everyone has left the facility and that protected individuals have been sent to the closest bunker, members of Static Guard shift turn off electrical installations in the facility, use fire equipment in case of a fire, help the injured and, if necessary, support the Static Guards on duty in facility defence.

Enter Control Point Service consists of experienced guards who speak English and one of the local languages. Their duty is to control individual and vehicle entrance into the secured facility area. The presence of guides with dogs trained to detect explosive and gunpowder is mandatory. The important rule is that only one gate can be opened inside the barrier in order to direct the impact wave in case of explosion. Gate Commander manages the service and his direct superior is Shift Supervisor that is on duty.

Practice has proven that this team is most exposed to possible attacks. The members of the team are to recognize a suspicious person – a potential attacker in time by observing his body language, seeing if he is nervous, sweaty, looking at his eyes, checking if the potential attacker does not know what to do with his hands, if he frequently changes his body posture, monitoring the position of his mobile phone, checking if he is hiding something beneath his clothes, etc.



Picture 3 – Enter Control Point Team

In case of an attack, Gate Commander organizes locking of the gates at entrance and exit barrier, directs the fire towards the attackers and orders the position of manpower behind the shelter. He reports the details of the attack to Shift Supervisor, sends off manpower which is not part of security service and pays special attention to managing machinegun fire from the dominant point. Additionally, Gate Commander requires ammunition backup and other types of support (medical support, combat gear, etc.) from Shift Supervisor, sends wounded and the injured to the station for treating the wounded, and manages Static Guard fire in the gate area. In case of gate barrier penetration and attacker's infiltration into the protected facility area, Gate Commander organizes withdrawal of his team to the next defence position.

Patrol service consists of men with guarding experience. The patrol is carried out exclusively within the perimeter of the protected facility. Patrol Supervisor reports directly to Facility Security Manager and coordinates his work with Shift Supervisor on duty, Gate Commanders and Technical Supervision Shift Leader. Depending on the size of the area within the protected perimeter, patrol can be carried out simultaneously by several teams which have been assigned sectors. Vehicles are available to the patrol on duty. The patrol on duty is also the intervention group.

In case of an attack to the protected facility, Security Manager (or Shift Supervisor, in the absence of Security Manager) sends patrol to the place of attack. The patrol is expected to carry out rapid-fire manoeuvres and protect the attacked sector by closing the path of attackers' potential penetration deeper into the protected facility. In case the attackers have penetrated into the protected facility, patrol members cover the endangered area by shooting from reinforced-concrete shelters arranged inside the perimeter in accordance with previously defined fire system for each shelter in order to avoid jeopardizing the safety of protected individuals inside the facility. Members of patrol team are to be trained for *Close Quarters Battle – CQB*¹⁶ and for team "cleaning" of invaded facilities. Mandatory parts of their equipment are chemical means for temporary incapacitation (tear gas, shock, smoke grenades, chemical bombs, etc.).

Patrol's duty is to protect and control access to restaurants during meal times, since many people at the same location may also be targets. If the attackers have not penetrated inside the facility after the initial attack, patrol members secure the attack point until the damage recovery and help the group that looks after the injured.

Service for Video and Technical Supervision of the facility consists of Technical Supervision Shift Supervisor and the necessary number of operators of video and technical supervision (geophones, active "IC" motion detectors, lighting, etc.) of perimeter security. Their place of work is the control room. The most important task of this service is to provide timely detection of unauthorized access to protected facility perimeter and control remote alarm system.

Technical Supervision Shift Leader reports directly to Shift Supervisor on duty and coordinates his work with Patrol Supervisor on duty and Gate Commanders. The presence of *Closed-circuit television - CCTV*¹⁷ represents the minimum technical supervision in high-risk zone.

¹⁶ Close Quarter Battle

¹⁷ CCTV – Closed Circuit Television

Necessary level of protection and frequent technical systems for facility protection in high-risk zones

Possible adverse events in facilities which are secured in high-risk zones concern the life and health of individuals i.e. protected persons who are located inside the facility. *Specificity of private security in high-risk zones is high probability of suicide terrorist attacks which are usually followed by intruders' penetration into the facility.* Having in mind that the point of adverse event is intruders' "break-in" the protected facility area, security services frequently apply:

- measures for preventing and detecting unauthorized entrance into facility area, and
- measures for identifying individuals.

According to the principle of "golden number seven"¹⁸, the highest level of security in high-risk zones is achieved by maximum protection of the first line of defence, i.e. the line of perimeter with physical barriers. During the design of protection levels for facilities which are located in high-risk zones, items taken into consideration are values of lives of the secured individuals and economic justification of technical security of the border line. Protection level 4 – High level of protection¹⁸ is frequently applied with the aim of preventing unauthorized access into the protected facility area. This level of protection implies the use of alarm system which detects unauthorized access to border line (external perimeter wall), remote alarm system, CCTV, access control system and presence of physical security service – Static Guards. The role of such system for technical protection of facilities in high-risk zone is detecting the attack and discouraging the attackers. Practice shows examples when technical security has detected attack on the facility in timely manner, but has not immediately stopped the attack. There have been numerous records that show attack activity until the moment of the explosion. Due to strong explosive charge impact which aimed at demolishing entry barriers, CCTV system near the place of explosion was destroyed. However, recording devices kept on recording the area, even during the defence of the protected facilities. *Specificity of private security in high-risk zones is the use of CCTV pictures and records during the defence of the protected facility and their use for the analysis of security service work after the beginning of the attack, as well as for later use during trainings.*

In construction terms, perimeters of the facilities in high risk zones are fenced by means of stone walls or HESCO Defensive Barriers, width from 50 cm to 3 m and height which is not less than 4 m. Counter-sniper panels, i.e. high aluminium sheet fences are constructed on places which represent potential hazard from watching the inside area of the protected facility. Reinforced-concrete elements, usually in the form of tetrahedron, are constructed on the external side of the perimeter, i.e. along the roads. Barriers for vehicle direction and slowdown are places along the access to facility entrance gate. As a rule, facility gates are not located close to high-density roads. Dominant points (towers) are constructed for machineguns inside the facility area, as well as sufficient number of reinforced-concrete shelters for shooters. Bunkers made of reinforced-concrete or combination of HESCO Defensive Barriers and reinforced-concrete are secured inside

¹⁸ Radovanovic, Radovan V and Milan D. Blagojevic, *Sistemifizicko-tehnicke zastite*, Belgrade 2010.

the facility area for the purpose of securing individuals who are located within the protected facility. The bunkers are located near the facilities where protected individuals are accommodated and are planned for longer stay. They contain water and food supplies for at least a day, while many of them have electrical lighting, air conditioning, medical equipment, etc. *Specific aspects of private security in high-risk zones is the presence of comfortable reinforced-concrete bunkers within the area of protected facilities and security's obligation of training protected individuals how to use the bunkers in case of an attack.*

Most facilities in high-risk zones possess independent systems for electric power and water supply, sewerage network, internal telecommunication system, Internet and Intranet. Moreover, many facilities have catering, trade, bank, sports and many other elements. Such independency certainly increases security level.

When it comes to controlling the access to facilities in high-risk zone, all guests, protected individuals, local workers and security service workers are in obligation to carry visible ID cards. ID cards are of various colours and contain a photograph, work position, name of the company which employs them and card validity date. Guests of the camp-protected facility, as well as local workers are in obligation to go through metal detector door prior to entering the protected facility. Their personal items are examined by detectors with X-rays. Many security services use biometric authentication of cornea and fingerprint recognition during the process of employing new local workers in facilities in high-risk zones. The information is stored in database which is maintained by the members of military-police coalition on the field.

Observation balloons are used for the purpose of observation and supervision of high-risk zones. This aerostatic system is filled with helium and possesses day-night cameras, thermal imaging equipment, laser range unit, GPS, computer and screencorder. Balloon is fixed to the earth part of the system by means of metal rope and it can fly up to 500m. Balloon can record sharp and precise images which are tens of kilometres away. *Specificity of private security in high-risk zones is the use of aerostatic balloon system for territory observation and supervision.*



Picture 4 – Observation balloon

Securing individuals during vehicle movement in high-risk zones

“PSD¹⁹” tasks imply securing individuals during vehicle movement in high-risk zones. Such escort of protected individuals-clients is frequently performed by “PSD” team. Clients are usually: engineers of various fields, managers, officials and workers of private multinational companies, UN staff, EUPOL police forces and rarely members of military personnel. Leaders of “PSD” team – Team Leaders come from the Western states, Russia, Ukraine, the Balkans, Australia and the Republic of South Africa. Members of “PSD” teams are usually local workers with experience in securing individuals and driving experience.

The seriousness of such tasks requires highly trained professionals. “PSD” teams work independently on the field and therefore use modern means of communication (“VHF” radio devices and satellite phones for mutual communication, communication with the base and, which is most important, for communication with QRF²⁰ team. The use of “GPS” transponder²¹ is mandatory during the ride. Protected individuals are transported in armoured cars with B-6 level of protection.

Aside from other types of weapons, “PSD” teams use automatic rifles, usually AK-47 and M-4. *Specific aspect of private security in high-risk zone is mandatory use of automatic weapons.*

During the performance of their duties in high-risk zones, members of security „PSD“ team do not hide their weapons, combat or communication equipment, their armoured vehicles or equipment for observation. *Specific aspect of private security in high-risk zone is open type of security, without concealing battle equipment which security service members use for their work.*

Characteristics of Improvised Explosive Device (IED) attacks on vehicles in high-risk zones

According to analytical data of “Securo group” company, more than 66% of killed members of coalition forces in Afghanistan were killed by Improvised Explosive Devices (IED).¹⁷ Improvised explosive devices are hand-made and consist of explosive and

¹⁹ Personal Security Team, Compare: Army Regulation 190–58, Military Police

PersonalSecurity, Headquarters, Department of the Army, Washington, DC, 22 March 1989.

²⁰ QRF-Quick Reaction Force implies duty unit for intervention in case of attack on “PSD” team, attack on the facility, as well as attack on a vehicle or vehicle convoy, *Quick Reaction Force (QRF)*, Internet 29/06/2014, <http://www.globalsecurity.org/military/agency/army/qrf.htm>, Упореди: JFLCC, QRF/RRFPamphlet, Department of the Army FORSCOM Pamphlet 380-1, Headquarters, United States Army Forces Command, May 2003.

²¹ GPS (Global Positioning System) transponder is electronic device which tracks the current position based on longitude and latitude, gives user the information on current altitude and movement speed, and sends the same info to appropriate control room via satellite signal. GPS transponder can memorise several routes, send and receive messages in case of an attack by means of “panic” alarm. Most frequent model on the market is: “TRACK- 24”; Compare: *GPS-based tracking solution*, Internet 23/06/2014, http://www.track24.eu/static/GPS-based_tracking_solution.pdf.

chemical substances, the combination of which results in a chemical reaction. Basic characteristics of IED explosions are:

- strong impact,
- high temperature, and
- shrapnel effects.

Most frequent way of activating explosive charge is by electrical impulse. If the improvised explosive device- IED is fixed to the suicide bomber's body, it is called "BBIED"³, if IED is in a vehicle it is referred to as "VBIED"⁴ and if it is on the motorcycle, it is called "MBIED"⁵. *Specificity of private security in high-risk zone is a variety of use of improvised explosive devices.*

Improvised explosive devices (IED) are set up on the roads, next to the roads, in road beddings, on cross-sections, in parked vehicles, at places which are usually full of people (markets, bus stops, etc.), on places where a vehicle is to slow down due to a barrier, on road and street reductions, on road bends, at bridges, etc.

Safe distance from the place of explosion for improvised explosive device is:

- for explosive device the size of a shoebox – 200 meters,
- for explosive device set up in a vehicle – 300 meters, and
- for explosive device set up in a truck – from 600 to 1000 meters.

Humans who are present at the place of explosion may be injured or killed, and vehicles which are present may be damaged or completely destroyed. After the explosion, the attackers very often act by means of light infantry weapon. Such an attack is characterized as *ambush effect*.

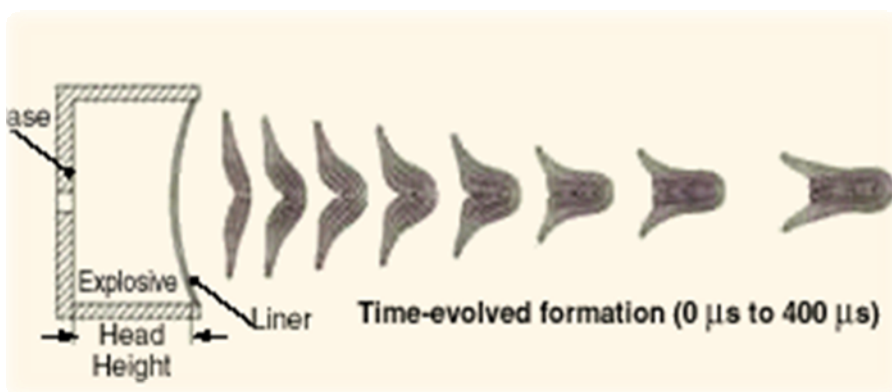


Picture 5 – Parts of improvised explosive device with initial part for stepping and explosive charge from rocket launcher gunpowder



Picture 6 – Ideal place for setting up “IED” – the driver will turn right, attempting to avoid water barrier

In the past few years, especially on the territory of Iraq, attackers use specialized improvised device called *Explosively Formed Penetrator – EFP*.²²



Picture 7 – Explosively Formed Penetrator – EFP²³

²² EFP- Explosively Formed Penetrator.

²³ Explosively formed penetrator – EFP, Internet 23/07/2014, http://en.wikipedia.org/wiki/Explosively_formed_penetrator.

This homemade explosively formed penetrator is a combination of formation and auxiliary means, and has become a weapon which cannot be fully defended against. Practice shows that this device has seriously damaged armoured military vehicles and tanks. Namely, professional knowledge of antitank production, dating from World War II, has been used for producing "EFP". Between the moment of firing and copper melting point, fragmented metal is moderately deformed into concave form of the missile. This enables enormous speed of incandescent metal mass which opens holes on the armour (or armoured vehicle protection) and has mechanical and heat effect on the cabin area.



Picture 8 – Armoured vehicle damaged by "EFP"

Organization of security service while protecting an individual in a moving vehicle in high-risk zone

Security service which protects an individual in a moving vehicle in high-risk zone is very complex. Its organization is based on fundamental principles of securing protected individuals. However, this type of organization is adjusted to security challenges which are always present in high-risk zones.

Unlike standard operative preparation of the area where the protected individual is transported, advanced guards are not used in high-risk zones. The risk that the members of advanced guard would be exposed to is not acceptable. Additionally, the presence of advanced guards would imply engaging new workers and vehicles, which would

significantly increase the cost of security organization, having in mind that movement of only one vehicle is avoided in high-risk zones. *Specificity of private security in high-risk zones is lack of security advanced guard during operative preparation of the area where the protected individual is travelling to.*

Unlike standard operative preparation of the area, preparation and accomplishment of the task-mission, security service members do not cooperate with local military-police forces of the area, from security reasons. Many times, the members of local military-police forces have been the actors of terrorist attacks. Even if there is cooperation with the members of local military and police, it is not completely open or professionally close. *Specific aspect of private security in high-risk zone is lack of close cooperation with local security forces.*

PSD teams use intelligence-security data and information that private security and military companies buy from other private companies specialized for intelligence-security work. Data and information are relevant for planning and carrying out activities on the field, as well as for assessing danger. These companies hire former members of intelligence-security services from military-police forces hired in the working zone. After the retirement or demobilization from secret services, these members continue their work, maintain their network of associates and use associates' services for collecting information, which is then sold on the market. Such specialized private companies (Titan, Securo group, ACAS Group, etc.)²⁴ offer intelligence bulletins (on daily, weekly and monthly basis). *Specific aspect of private security in high-risk zone is the use of intelligence-security data and information collected from specialized private companies-commercial intelligence work.*

PSD team for securing an individual who is transported by a vehicle in high-risk zone performs its tasks-missions based on daily agenda and, in very rare cases, based on weekly or monthly agenda. From safety reasons, information on the future mission is given to the team members as late as possible. Team Leader plans and carries out team training during the period without tasks-missions. Training is focused on practicing reactions to various types of attacks. Team Leader is to plan enough time for team preparation, personal preparation, preparation of "QRF"²⁵ team and vehicle preparation.

Right before the beginning of the mission, Team Leader carries out detailed preparation with the client (briefing). Client briefing contains information about "PSD" team, arrangement of vehicles in the convoy, radio, satellite and navigation equipment, indexes of participants in radio traffic, numbers of satellite and mobile phone of the base and "QRF" teams, vehicles used for the mission, details of the planned route (main and backup), medical equipment and person in charge of medical (MEDIC²⁵) and procedures for various types of attack. Team Leader and "MEDIC" should know blood type and medical conditions of each client, as well as of each member of the team.

Specific aspect of private security in high-risk zone is detailed client preparation (briefing) for the task-mission and the necessity of practicing various procedures, which is also the client's obligation.

²⁴ Sicuro group, Internet 23/06/2014, <http://www.sicurogroup.com/>.

²⁵ MEDIC- English translation, slang name for a person who is in charge of medical care of the injured and ill in PSD team. Individuals with experience in PSD are hired as MEDICs after completing appropriate courses for first aid, using oxygen equipment, using defibrillator and intravein administration of liquid.

Route observation is crucial during the transportation. The first vehicle in the convoy is usually “the observer”. The leader of the first vehicle informs the other vehicle leaders about all visible details on the road via radio connection. The leader pays special attention to:

- each unusual detail on the route,
- vehicles coming from the opposite direction, vehicles which are in front of the convoy, especially parked vehicles,
- lack of people, children, noise and crowd which is characteristic for the route,
- presence of cables, wires, rock piles, animal carcasses,
- lack of parked cars on the route,
- freshly dug holes or fresh soil on the road, waste, etc.

Based on the information from the first vehicle, other drivers react by moving away from the critical points. Team Leader makes the decision on the following manoeuvres.

All members of the team in the assigned zones observe:

- vehicles which make a sudden overtake,
- overloaded vehicles,
- vehicles which suddenly move from the parking,
- parked vehicles with drivers who sit inside and wait,
- several passengers in a vehicle, passenger structure,
- vehicles parked for a longer period of time, without a driver,
- vehicles which show clear intention of cutting the convoy route,
- motorists and cyclists, etc.

Depending on the side of the attack to the vehicle or vehicle convoy, there are standard operating procedures for reaction to:

- contact to the right,
- contact to the left,
- contact to the front, and
- contact to the back.

There are special standard operating procedures in case of vehicle incapacitation due to the attack or vehicle defect. *Specificity of private security in high-risk zone is the rule of destroying incapacitated vehicle with mandatory removal of radio, navigation and satellite telephone equipment, if the vehicle cannot be pulled out before leaving the attack zone.*

Conclusion

The evident increase of size and influence of private security in high-risk zones results in increased need for new analysis, discussions and innovative professional solutions in this area. Private armies and private security companies are positioning on the contemporary security service market, due to their efficiency, cost-effectiveness, flexibility and staff professionalism. Defence, security and armed forces are traditionally within state jurisdiction, and therefore a clear limit in security service privatization is necessary. Disputableness of the presence of this limit results in further research of private security issues, especially in combat zones.

The following specificities of private security in high-risk zones have come into focus during the research and writing of the paper:

- suicide terrorist attacks,

- lack of plan for rescuing the attacker and lack of care for his personal safety in the final stage of the attack,
- presence of local workers inside the protected facility area,
- cooperation between the management and tribal chiefs from the territory of the protected facility,
- selection of the attacker- suicide actor from various psychological and demographic structures,
- high probability of terrorist suicide attacks, which are often followed by attacker's further penetration into the facility,
- the use of CCTV pictures and records during the defence of the protected facility and their use for the analysis of security service work after the beginning of the attack, as well as for later use during trainings,
- the presence of comfortable reinforced-concrete bunkers within the area of protected facilities and security's obligation of training protected individuals how to use the bunkers in case of an attack,
- the use of aerostatic balloon system for territory observation and supervision,
- mandatory use of automatic weapons,
- application of open type of security, without concealing battle equipment which security service members use for their work,
- variety of use of improvised explosive devices,
- lack of security advanced guard during operative preparation of the area where the protected individual is travelling to,
- lack of close cooperation with local security forces,
- use of intelligence-security data and information bought from specialized private companies- commercial intelligence work,
- detailed client preparation (briefing) for the task-mission and the necessity of practicing various procedures, which is also the client's obligation,
- the rule of destroying incapacitated vehicle with mandatory removal of radio, navigation and satellite telephone equipment, if the vehicle cannot be pulled out before leaving the attack zone, and
- re-planning of working hours and organizing substitutes among the local members of security service during daily prayers and Islamic religious holiday Ramadan (as for the territory, high-risk zones are usually the zones in which the local population is Islamic).

When it comes to specificities of private security of vehicle convoy in high-risk zones, the most emphasized *specificity is the use of vehicles with machineguns*.

As for the specificities of anti-pirate private security of ships, most important specificities are *kidnaping ships, cargo and crew and demanding ransom, as well as armed attacks of pirates from small and instable skiff platforms*.

The aim of this paper is to show specificities of organizing individual, property and business protection in high-risk zones from professional and vocational aspect. Therefore, I have relied on my personal and official documents which have been available to me while performing this service. The fact that professional literature is not abundant with this topic motivates the experts who focus on security issues to study and enhance private security in high-risk zones.

Literature

- [1] Alexander, Naomi et al, „Body-borne IED detection: NATO DAT#10 BELCOAST 09 demonstration results“, *SPIE*, Vol.7670, 76700G (2010)
- [2] Bajagić, Mladen, *Špijunaža u XXI veku – savremeni obaveštajno-bezbednosn isistemi*, MARSO, Beograd, 2010
- [3] Greenberg, M., Chalk, P., Willis, H., (2006). *Maritime Terrorism*. RAND Corporation, Santa Monica, USA.
- [4] Eshel, D., (2005). *The Treat of Maritime Terrorism*. Defense Update.
- [5] Keković, Z., SavićS., KomazecN., Milošević M., JovanovićD., *Procena rizika u zaštiti lica i imovine*, Centar za analizu rizika i upravljanje krizama, Beograd, 2011
- [6] Kesić, Zoran, Specifični pojavni oblici privatnog obezbeđenja u svetu, *Bezbednost*, br. 1-2, 2009, str. 193-207
- [7] Mijalković, Saša, *Nacionalna bezbednost*, Kriminalističko-policijska akademija, Beograd, 2012
- [8] Mijalković Saša, Mladen Bajagić, *Organizovani kriminal i terorizam*, Kriminalističko-policijska akademija, Beograd, 2012
- [9] Army Regulation 190–58, Military Police
- [10] Radovanović, Radovan V. I Milan D. Blagojević, *Sistemi fizičko- tehničke zaštite*, Beograd 2010
- [11] Srdanović, S.: Specifičnosti privatnog obezbeđenja u zonama visokog rizika, Specijalistički rad, Kriminalističko- policijska akademija, Zemun, 2014
- [12] Standard Operating Procedures Private Security Company “Iron Hand Security”, 2013, Basra, Iraq.
- [13] Standard Operating Procedures Private Security Company “Al Salasel Al Fudhea Group”, 2012, Basra, Iraq.
- [14] *Vojna enciklopedija*, redakcija vojne enciklopedije, Grafički zavod Hrvatske Zagreb, Beograd, 1962.

Internet sources

- [1] GPS-based tracking solution, Internet 23/06/2014, http://www.track24.eu/static/GPS-based_tracking_solution.pdf.
- [2] Vehicle Borne IEDs (VBIEDs), Internet 21/07/2014, <http://www.globalsecurity.org/military/intro/ied-vehicle.htm>.
- [3] Defensive Barriers, Internet 21/06/2014, <http://www.hesco.com/products/defensive-barriers>;
- [4] HESCO Bastion - Protective Barriers, Accommodation Bunkers and Hostile Vehicle Mitigation Fences, Internet 21/06/2014, <http://www.army-technology.com/contractors/infrastructure/hesco/>.
- [5] www.globalsecurity.org
- [6] <http://www.defense-update.com/2005/12/threat-of-maritime-terrorism.html>
- [7] <http://www.bankarskaoprema.rs/vozila/daimler.htm>
- [8] <http://www.sicurogroup.com/>
- [9] <http://www.mschoa.org/docs/public-documents/yachting-piracy-bulletin-final-version.pdf?sfvrsn=2>
- [10] <http://www.shipping.nato.int/Pages/Piracystatistics.aspx>
- [11] E. Sprinzak: Razumni fanatici, <http://www.bhdani.com/arhiva/223/t22313.shtml>