Peter Álmos Kiss

DOI:10.33179/BSV.99.SVI.11.CMC.14.3.5

OBVEŠČEVALNA DEJAVNOST IN NOVA PARADIGMA VOJSKOVANJA

INTELLIGENCE AND THE NEW PARADIGM OF WARFARE

Povzetek Zaradi socialnega, gospodarskega in političnega razvoja po drugi svetovni vojni je prišlo do dveh vzporednih paradigem vojne: konvencionalnih meddržavnih vojn in asimetričnih spopadov med državo in nedržavnimi nasprotniki. Vzporedne paradigme obstajajo tudi na obveščevalnem področju in od obveščevalnih strokovnjakov zahtevajo nove načine razmišljanja ter nove postopke.

Ključne besede ***Asimetrično bojevanje, R2P, odgovornost zaščititi, obveščevalna dejavnost, nedržavni nasprotnik, uporništvo.***

Abstract The social, economic and political developments following WW II resulted in two parallel paradigms of warfare: that of conventional interstate wars, and that of asymmetric conflicts between the state and non-state belligerents. The parallel paradigms also exist in the intelligence field, and demand new ways of thinking and new procedures from intelligence professionals.

Key words ***Asymmetric warfare, R2P, responsibility to protect, intelligence, non-state belligerent, insurgency.***

A flaw in western asymmetric warfare doctrines

In the last decade or so, western (primarily European and North American) armed forces have come to grips with the challenges of asymmetric warfare. New doctrinal publications and scholarships have recognized the threat that non-state belligerents pose to their own governments and to other nations, and have outlined ways to meet the challenge. New regulations and field manuals have been issued and validated on the battlefield in Iraq, Afghanistan and elsewhere by various national forces. Yet they have one serious flaw (one they share with the national

and international security and defense strategies[1] and much of the professional literature): they discuss the challenge of non-state belligerents as an entirely foreign phenomenon, something that western forces would encounter only overseas, in the failed states of the third world.

This approach is not entirely unjustified. It is indeed in the unstable states of Asia and Africa where western troops have been deployed on counterinsurgency or stability operations. It is also an undisputable fact, that in the western world such conflicts have so far taken place only on Europe's periphery (Northern Ireland, Transnistria, the Balkans, the Caucasus). However, there are no guarantees that this happy state of affairs will endure. Domestic enemies may form alliances and acquire powerful foreign backers – a combination that may be beyond the capacity of law-enforcement agencies, thus making the deployment of the armed forces necessary. Even if no serious domestic challenges develop, this detachment limits the effectiveness of western forces deployed overseas on stability missions, because it encourages them to remain an aloof, alien presence and view the conflict only in the light of national or international command authority directives, and only through the prism of doctrine and past experience gained in other theaters. In order to be truly effective, western forces must have a more thorough understanding of the conflict than that provided by these authoritative sources of guidance. They must understand the point of view of the local political elite, which faces liquidation if the insurgents win; they must view it from the perspective of the commanders and men of the local security forces who do much of the fighting and dying, and they must see it with the eyes of the local citizens who are caught between the millstones of the insurgents and the security forces. Such understanding requires more than just ignoring references to "Host Nation" in Field Manuals and professional journals.

The following paper attempts to contribute to that understanding by focusing on a narrow (albeit crucial) aspect of counterinsurgency: intelligence and counterintelligence, ***from the perspective of the state and society under attack.*** The author does not pretend to know better than those who developed current western doctrines and validated them under hostile fire. His intention is not to contradict the doctrines, but rather to complement them by brushing in details that doctrinal publications – due to their more general nature – leave out, and to identify some areas where doctrine may have to be supplemented.

1 PARALLEL PARADIGMS IN WARFARE

As a result of six decades of changes in the international political and legal environment, conventional wars between nation states have become rare occurrences. Armed conflict within the borders of the nation state has become the dominant form of warfare. Asymmetry characterizes these internal wars: the goals, resources

[1] *See for example NATO's Strategic Concept, the European Union's Security Strategy and Internal Security Strategy, or the national security strategies of Great Britain and Hungary.*

and forces of the belligerents cannot be measured by the same yardstick. The state commands vastly superior resources, but partly due to the adversary's nature and tactics, and partly due to changes in the international political climate it is unable to exploit its superiority. The enemy is really more of an *adversary* or an *opponent* rather than an *enemy:* he is a non-state actor, usually a citizen of the state and a member of the society whose cohesion he is trying to disrupt. Maneuvering on the borderlines of parliamentary democracy, street politics, armed conflict and common crime, he claims the legal protections guaranteed to politicians, activists, combatants and criminals, but rejects all responsibility that is normally attached to these categories. Relying on propaganda, mass-mobilization techniques and intimidation, he creates a mass support base – or the appearance of one. He avoids confrontation with the armed forces and police and goes directly for the state's social foundations – the support of the civilian population. The battlefield is the society itself. Battles take place in the presence of civilians, against civilians or in the defense of civilians and civilian institutions, with the voluntary or forced participation of civilians. The civilian may be a target, a human shield, a source of information and resources, or a belligerent – and often it is difficult to decide which role he is playing at any given moment.

None of this is new – but, until recently, such challenges to the authority of the state were relatively easily handled internal problems. What is new is the dominant role insurgency has assumed: in the past 65 years, 80 to 85 percent of armed conflicts have been wars of national liberation, internal ethnic and religious conflicts, revolutions, counterrevolutions – or some combinations of these (Strachan, 2007). A new paradigm of warfare is emerging, in which modern war's conventional methods (the operations of mechanized brigades, divisions and corps) and weapons (tanks, artillery, high-performance aircraft) are generally useless, and the state's regular forces are often impotent. Rupert Smith calls the new paradigm ***"war amongst the people."*** (Smith, R. 2005, pp. 3-9)

In the right conditions, instigating or supporting such "wars amongst the people" can also serve state interests. By creating and sponsoring Hezbollah, Iran has acquired far more influence in the Eastern Mediterranean basin than it could have achieved through diplomacy or the deployment of its conventional forces. Pakistan has lost several wars against India, but what it has failed to gain by force of arms (integration of the state of Jammu and Kashmir into Pakistan), it has partially achieved by sponsoring non-state belligerents: it has acquired two thirds of the state and has prevented the remainder's integration into India.

The detailed analysis of the economic, social and political roots of this change is beyond the scope of this study, but the proximate cause is quite clear: the ***erosion of the nation state's sovereignty.*** By signing the UN Charter and by acceding to various international organizations the nation-state forfeits not only its right to advance its interests by force, but also its right to govern its own affairs as its people (or more accurately its political elite) see fit: monetary and trade policies, criminal justice,

labor relations, border security, family affairs – all are subject to intense and often hostile scrutiny by international organizations, non-governmental organizations, the media, and the governments of other states. In a relatively new development, the state has also lost its freedom to apply force within its own borders to defend itself against internal enemies. As Yugoslavia's government learned to its cost in 1999, the new international doctrine of "Responsibility to Protect" (R2P) allows even armed intervention in a state's internal conflicts, if a few influential powers convince the "international community" that the government's use of force against its internal enemies is excessive. And as the more recent example of Libya shows, once an international mandate is given, it can be gradually expanded to achieve just about any outcome the intervening powers desire.

The lesson of Yugoslavia and Libya is clear: the current international climate puts hardly any restraints on the rebels, but allows the government to apply only restrained, limited force in handling insurgencies.[2] To be effective, this limited force requires doctrines, tactics, training and equipment that differ radically from those of conventional war. But even more important, it demands a fundamentally different mindset from the elite that exercises political control, from the intellectuals that influence society's opinions, from the commanders of the security forces, and from the people.

But since the dangers of conventional war have not disappeared completely, a nation must retain sufficient capability to face them as well – therefore the state's asymmetric warfare capabilities must be additional to, rather than alternative to, its conventional military capabilities. Thus, ***two paradigms of warfare exist side by side,*** and they have very little in common. This may cause some severe headaches to those charged with developing national security strategies: only the largest states can afford to maintain separate armed forces to deal with an internal conflict.[3] In other states the security forces must be prepared to handle national security threats according to either paradigm - or even according to both at the same time, if necessary. Britain's experience in Northern Ireland is instructive. The usual tour of duty for a Regular Army battalion in Northern Ireland was four and a half months, but for nearly a year the battalion was not available for conventional operations: it required three months of counterinsurgency training before deployment, and on completion of its tour it required a nearly identical period for retraining to recover its conventional warfighting skills, as well as block leaves, schools and other administrative procedures. (*Operation Banner,* 2006. p. 7-2)

The ***parallel paradigms also exist in intelligence.*** Whatever the asymmetric challenge, traditional intelligence work must continue. The intentions and capabilities of potential enemies and (although this is seldom mentioned in polite company)

---

[2] *The successful suppression the Tamil Tiger insurgency in Sri Lanka by the full power of the armed forces between 2007 and 2009 is a rare outlier.*

[3] *Several successor states of the Soviet Union also maintain Internal Security Troops. Italy, France and some other nations maintain gendarmerie forces that can be deployed to handle an insurgency. India fields several hundred paramilitary battalions to maintain internal security – but occasionally even this large force must be augmented by regular army units and locally raised militias.*

those of friends and allies must be tracked. Counterintelligence must continue, in order to protect the nation' vital secrets. The intelligence capabilities that address the asymmetric threat must be additional to, not alternatives to, those earmarked for external intelligence and counterintelligence.

When tasked with counterinsurgency collection, the intelligence specialist must first determine who the ***target of collection*** is. In most cases the answer is politically so uncomfortable as to be difficult to acknowledge in public: the most likely adversaries are fellow citizens – voters and taxpayers, acquaintances, friends, brothers. This immediately raises legal obstacles. Observing a citizen's movements, tapping his telephone, listening to his conversations, reading his mail are limited by law in most countries. And they are illegal, if their foundation is a police profile consisting of ethnic or religious background, grooming habits and sartorial appearance, internet--surfing habits and choice of news sources – behaviors which suggest that sometime in the undeterminable future the citizen may perhaps pose a so far undefined threat to society.

Political correctness and excessive respect for civil liberties sometimes do pave the way for successful blows at the targeted society. The preparations for the terrorist attack on New York's World Trade Center attracted suspicion, but legal (and political) constraints prevented timely action. Many more examples can be cited for the opposite: when human and civil rights are seriously violated due to mere suspicion or malicious denunciation – or for being in the wrong place at the wrong time. Thus, the conditions of asymmetric warfare pose a serious dilemma not only for the political elite, but for all society: the ***correct balance*** between individual rights, citizens' responsibilities, national security, privacy and civil liberties must be found. The squaring of this circle is particularly important, because without such social consensus it is difficult to beat a non-state adversary.

2 CENTRAL VS. LOCAL INTELLIGENCE

Once some kind of social consensus is achieved (and it will only be "some kind of:" imperfect and full of contradictions), the next problem is that national-level intelligence organizations are not very useful against non-state adversaries. The legal foundation of their activities, their resources, tasks and doctrines, as well as the training of their personnel are all optimized to satisfy the information requirements of national level decision-makers, support the defense of the nation against external attack, and safeguard vital national security information. Consequently, hardly any of the intelligence services' resources will be useful in a "war amongst the people:" the adversary becomes part of the local community to remain hidden, obtain resources and information, and mount his operations.[4] If an internal intelligence network does exist, the insurgents usually destroy it at the beginning of an in-

[4] *As the Indian police discovered during the Khalistani insurgency in the Pujab (1980-1994), even the most important terrorists were operating with an 15 to 20 km radius of their hometowns – in area which were familiar to them in every detail. (Gill, 2001).*

surgency, and the security forces will be blind and deaf in the crucial, initial period of the conflict. In a worst case scenario the authorities may not even realize for a while that they no longer have an internal intelligence network.[5] A further serious problem is that intelligence cycle is too slow: the information is long out of date by the time the consumer receives it through the usual channels.

Intelligence targets, essential elements of information, collection methods, analysis methodology – they are also all different. "Order of battle" is not a useful category when the insurgents are part of a self-organizing network with a constantly changing structure. "Doctrine" is meaningless when tactics, techniques and procedures (TTPs)[6] – are copy-pasted from ideas downloaded from the internet, military manuals, action movies and propaganda videos. "Discipline" and "morale" are hard enough to evaluate in the context of regular forces; they are impossible to determine in the case of armed volunteer groups that form to execute a single operation and then disband. Logistics, supply, recruitment, training mean much the same thing for a 20 000-man regular force and for a mass army of two million, but they mean something entirely different for an urban guerrilla network consisting of a few dozen 10-man teams.

Since the adversary is hiding among the people, the security forces must make every effort to identify him *as an individual*, locate him and neutralize him without causing harm to civilians in the process. They needed every detail on the personal lives of the leaders and the membership of the various armed groups, the local informants, the liaison personnel between the groups, and the people operating the support networks. They must discover the insurgents' procedures for population control and identify the people exercising that control. They have to discover the arms smuggling routes, the relationships and communications channels between the clandestine armed groups and the legal political organizations, and a thousand other details. (Gill, 2001)

Only a ***locally focused intelligence organization*** can provide such extremely detailed information. It is best to base the organization on the local police service. Policemen are a permanent presence among the people; they are familiar with local conditions and customs; they maintain personal contacts in the local communities – not only with political leaders and bureaucrats, but also with the owners and staff of shops, restaurants, gas stations and garages, as well as with the local vagrants and petty criminals. These are elements of a local intelligence network which only needs focus, coordination – and funds. In addition to such ready-made networks,

[5] *This occurred in Rhodesia in 1970-71. The Zimbabwe African National Union (ZANU – one of the liberation movements) established an extensive underground infrastructure in Rhodesia's eastern provinces and at the same time systematically liquidated the informants of the government's intelligence services. The Rhodesian intelligence services failed to notice that their sources were going silent one after the other, and as there were no adverse (or any other) reports coming from the area, the government assumed that its security arrangements there were satisfactory – until ZANU commenced operations in 1972. (Cilliers, 1985, p. 220).*

[6] *TTPs is a useful abbreviation coined by the US uniformed services: "Principles alone are not enough to guide operations. Tactics, techniques, and procedures provide additional detail and more specific guidance, based on evolving knowledge and experience. (...)* ***Tactics*** *is the employment and ordered arrangement of forces in relation to each other. (...)****Techniques*** *are nonprescriptive ways or methods used to perform missions, functions, or tasks. (...)* ***Procedures*** *are standard, detailed steps that prescribe how to perform specific tasks." FM 3-0 Operations, pp. D-1-D-2.*

policemen have another advantage: they have both the authority and the skills to make deals with potential informants. They can promise protection and leniency in exchange for useful information, or they can threaten with the full majesty of the law if a source refuses to cooperate. Intelligence officers generally have neither such authority, nor such experience.

Without doubt, eventually military intelligence specialists can also learn these police techniques - and they may have to, if the police have to be supplemented by military forces. But at least in the early days of the conflict there is no choice but to rely on the police.

3 LINES OF INTELLIGENCE OPERATIONS

The Clausewitzian question of what is ***the nature of the conflict*** we are about to engage in must be answered in a counterinsurgency no less than in a conventional war. Insurgencies seldom develop without substantial (and well-founded) grievances, and a thorough – and unvarnished – understanding of its root causes and its social, political, economic and cultural and international dimensions is a must. Intelligence plays a crucial supporting role in acquiring this understanding. Even the directly affected national government can get this wrong, if intelligence is faulty – or if the decision makers find its conclusions unpalatable. For example the Rhodesian government persisted in treating the liberation movements as communist terrorists, and ignored their broad international and tribal appeal, until it was too late. As the Coalition's initial assessment of the insurgency in Iraq has shown, an expeditionary force is even more prone to make such mistakes.

It was a relatively easy task 40-60 years ago to ***determine the insurgents' real goals*** – the Hukbalahap in the Philippines, the Greek communists and Castro's bearded revolutionaries intended to seize the power of the state. Today insurgents may have less easily identifiable intentions. Some extreme Islamist organizations seem to have no interest in wielding the power of the state – they only want to force society to follow the path they consider righteous. For Latin-American drug cartels a weak state that enforces only the laws the cartels approve of is more advantageous than to seize and wield state power. Under the umbrella of a weak state they can produce and sell drugs without undertaking every burdensome detail of governance. Thus, one important intelligence task is identifying the enemy's true goals and tracking such changes as may occur in them.

Support of the population is the insurgent's source of legitimacy, his recruiting base, his main source of intelligence and one of his sources of funding; by mingling with the people he finds sanctuary from the state's oppressive military superiority. For the state, a key element of success is to isolate the insurgent from the population; therefore one of the fundamental tasks of intelligence is to ***identify the supporting structures and the key links between the insurgents and the people.*** These links are more than just interpersonal ties between relatives, friends, business associates or

ideological comrades, or channels to overt mass organizations that advocate the insurgents' cause in the political marketplace. Ideology and the meta-narrative that the non-state actor uses to persuade the people and the international audience, and the services he provides in return for the civilians' support also fall in this category – as do the acts and omissions of the political elite that may have caused the grievances at the root of the insurgency.

Modern non-state belligerents use the decentralized, self-organizing network as an organizational model. Networks are almost impossible to destroy, because they have no ideological, political or doctrinal center that could be attacked. Even after the greatest defeats and the greatest losses a few nodes will remain, which, given time, regenerate the network and reestablish insurgent control of the people. At best the security forces can disrupt the network to such an extent that it cannot function. To do that, ***the network must be mapped;*** its key nodes (individuals who provide ideological guidance, those with connections to sympathizers among the security forces and to foreign sponsors, others with such special skills as bomb-makers or computer experts, yet others who serve as liaison between two networks) must be identified.

The nature, goals and tactics of the adversary make it difficult, if not impossible, to reach the political compromises that are essential in ending armed conflicts. In most cases there is nobody to negotiate with: networks have no center, no leadership body or individual leader who could make a decision that is binding for every member of the organization. Even if a partner can be found, there is no guarantee that those who were not consulted would accept an agreement. On the contrary: an agreement may lead to die-hard elements doubling their anti-government efforts and turning on the "traitors of the people" at the same time. If the political elite cannot accept that there are no partners to negotiate with, then it becomes an intelligence task to ***identify decision makers in the adversary organization who may be turned into partners*** – and who may be made strong enough to enforce the conditions of an agreement within their organization.

For non-state actors – even though their operations are far less costly than those of conventional forces – ***money*** is a constant problem, because the sources of their funds are so uncertain. Their most generous donors may suddenly switch to a rival organization; the economic situation may change; banks may implement new security systems that cannot be circumvented. The insurgents' accounting may be no more certain than their sources: they can easily lose their funds to incompetence or embezzlement.[7]

Early insurgent movements levied "taxes" or "contributions" on the local peasants, laborers and merchants. Today the non-state actor takes advantage of cheap, fast and unobstructed travel to seek alternative sources of funding all over the world. This way he is not embarrassed, if the government finds a way to cut off one source. The

[7] *This is exactly what happened to the Malayan Communist Party: its secretary-general (Lai Tek) was a British agent; when his comrades begun to suspect him, he disappeared with the party's treasury. (Barber, 1971, p. 32)*

Irish Northern Aid Committee (Noraid) was one such alternative source of funding for the IRA; it collected donations in the United States, until the Justice Department (at the behest of the UK Government) began to pay closer attention to its activities. The Tamil Tigers invested in the business ventures of the Tamil diaspora. In 2002 their investments earned US$50-60 million in profits. (Glenn, 2002) Criminal activity, particularly the highly profitable drug trade is another alternative revenue source. Radical Muslim organizations often receive generous state subsidies (from Pakistani, Saudi or Iranian sources) and donations from wealthy private donors. A finance expert may be able to follow the state funds, but the private donations often move in cash-filled suitcases, or through the informal African and Asian money transfer system *(hawala),* instead of regular banking channels; to track them the skills of an intelligence specialist (or a reformed smuggler) are more useful.

A counterinsurgency effort is likely to fail without successful combat operations. However important a "political solution" may be, nothing compels insurgent organization to compromise as long as it can generate forces at a rate that exceeds losses. And nothing compels the individual insurgent to give up, unless he knows that hunter-killer teams are after him personally. Furthermore, to a certain extent, insurgency is a dangerous form of competitive theater, in which the belligerents perform to obtain the support of the domestic and international public. One convincing way for the state to obtain the audience's support is a steady stream of battlefield successes. The security forces must prove that they can provide security by regularly producing dead and captured insurgents, discovering weapons caches and bomb factories and disrupting insurgent operations. This requires detailed, reliable and up-to-date (preferably real-time) ***actionable intelligence.*** Battlefield success requires far greater detail than knowing the organization, plans, intentions, tactics and support structures of the adversary. Names, location, habits, virtues and vices of individuals; names and addresses of their relatives, friends, girlfriends and/or boyfriends; current location, numbers and armament of insurgent teams; their route, speed, destination and means of travel, if they are on the move – the information must be sufficiently detailed, accurate and current to allow strikes without collateral damage to civilian property, and above all without casualties among the civilian population.

External support is vital for non-state belligerents. (To the author's knowledge the only modern insurgency to succeed without significant external support was Castro's revolution in Cuba.) Obtaining weapons and training forces is much simpler with the active support, or at least the benevolent tolerance, of a neighboring state. Exhausted forces can be rested beyond the borders, out of reach of the security forces; funds can be collected without interference, and the leadership can confer in safety, and its members can posture as statesmen in exile. An important intelligence task is to ***uncover the external ties, identify the methods used to avoid border control measures,*** and identify the individuals (particularly the government employees) participating in them.

4 HUMAN INTELLIGENCE – THE KEY DISCIPLINE

The "war amongst the people" nature of insurgency requires "intelligence from the people". Human intelligence (HUMINT) is the most important intelligence discipline. The best, most reliable sources of information are long-term ***undercover intelligence officers,*** who infiltrate the target organization or its immediate support structures and social environment. Depending on the nature of the insurgent organization, this may be a difficult (or impossible) task. Language, ethnicity or religion may pose insurmountable obstacles. Radical Muslim organizations are notoriously difficult to penetrate: non-Muslim intelligence specialists rarely have the knowledge and behavioral patterns to pass themselves off as adherents, while Muslim officers often refuse to target their co-religionists – or worse, side with them in the course of an investigation.

Informants are an entirely different proposition. There are many reasons, from avarice through fear to the desire to avenge a personal insult, for a person to inform on his associates. The security officer just has to discover the right "buttons" to push in order to encourage an individual's cooperation. By applying the right combination of incentive and coercive measures they can reinforce the motivators for cooperation and suppress those for loyalty to the adversary. They have many incentives at their disposal: they can offer money or help with securing employment; they can help legalize an irregular immigrant's status; they can reduce charges or forego prosecution for minor offenses. They have just as many coercive measures available: they can threaten to break up a family by deporting those members who are in the country illegally; they can threaten vigorous prosecution for minor violations of the law; they can threaten to leak information to the insurgents about the source's valuable service.

Interrogating captured insurgents promises significant gains: they have the most authentic and most up-to-date information on their own organization, and if they can be made to talk shortly after capture, they may divulge immediately actionable information. However, in author's experience as a HUMINT specialist is that an unwilling source cannot be persuaded to divulge information, unless some form of pressure is applied. The challenge for the intelligence specialist is to apply coercive measures (as well as some incentives), and at the same time remain within the confines of the laws and service regulations. This requires highly skilled professionals. The omnipresent (and often hostile) media poses an additional problem. "Coercive measures" and "pressure" are not the same thing as "torture." Nevertheless, even if no physical pain or discomfort is inflicted, the media are quick to brand pressure techniques as such.

If the circumstances of capture allow it (e.g. the prisoner is the only survivor of an insurgent team), no effort must be spared to turn him and feed him back into his organization as a double agent. If that is not possible, Plan B is to recruit him to fight on the government's side. This is usually not as difficult as one would think. Commitment to the cause or to the ideology of the movement is a less important

factor in the motivation of most insurgents than it is generally assumed. (Molnar, 1965) The hardships and physical demands of a life on the run, the stress of constant readiness soon drain the enthusiasm of even the most ardent volunteer. A substantial monetary reward, care for the family, a reasonably secure future once the insurgency is over – these are powerful magnets. The most potent coercive factor that complements these incentives is the majesty of the law – certain prosecution and probable serious punishment if one refuses to cooperate – is enough for many captured insurgents. Others may guide security forces onto their erstwhile comrades in the hope of eliminating all witnesses to their involvement in the insurgency. This is very delicate work. Recruiting and running double agents and informants requires highly skilled, disciplined, patient case officers: the insurgents are not forgiving towards traitors, and the slightest mistake may lead to the loss of a valuable source.

A very valuable information source is the ***local civilian population****:* they know the area, they know the troublemakers and hotheads, and they can identify new faces. Furthermore, since the insurgents hide among the people, the civilians usually know them and know their habits and movements. However, they will divulge their information only if security forces gain their trust. The best – perhaps the only – way to achieve this is by isolating the civilian population from, and providing it long-term protection against, the insurgents. Once reliable protection is in place, and the locals are convinced that it will last, information will begin to pour in – especially if rewards are also offered. (Smith, N. and MacFarland, 2008, and Gill, 2001)

Patrols may obtain actionable intelligence as they interact with the civilians, but even if they do not, they are invaluable for getting the "feel" of a place and noting changes in the mood and behavior of the locals. ***Locally raised militias,*** once properly trained in patrolling and observation techniques, can be invaluable: they know their area intimately, and anything out of place will immediately catch their attention. The patrol's information is valuable only if it is obtained in a timely manner, preferably immediately after the patrol's return to base, when the impressions are still fresh, even before the patrol members had a chance to eat or clean up.

Checkpoints, if they are set up with an isolated and screened area where civilians who pass through are interviewed one by one (and without witnesses) can be a significant intelligence asset. It is a fairly safe and innocuous place for the intelligence specialist to meet his informants without arousing suspicion, to meet locals face to face and obtain such information as they may be willing to divulge, and to recruit new informants.

Another mass intelligence source, the ***interrogation of people arrested en mass in riots or in security sweeps*** is generally far less useful. The information thus obtained is often incorrect, or deliberately misleading, due to the detainees' resentment for their treatment or to their outright sympathy for the insurgents.

5 INFORMATION TECHNOLOGY – THE POTENTIAL FORCE MULTIPLIER

Human information sources are of primary importance in counterinsurgency, but ***technical means,*** especially the latest advances in information technology (IT), also play a role. Modern electronic systems can record face-to-face and telephone conversations; they can monitor e-mail streams and automatically flag messages with suspicious content; they allow surveillance from a great distance. Processing the scenes of earlier attacks (location, type of target, access and egress routes, assembly areas, hiding places) in a geo-information system may identify likely future attack locations. Network analysis programs can identify critical nodes, whose destruction would disrupt the network. Combining the firepower of military forces with IT (particularly if collateral damage is not a significant concern) can yield significant results – for example the Chechen president Djokhar Dudayev was killed by a Russian missile that homed in on the signal of his mobile telephone.

One of the pillars of the intelligence effort must be a data processing system that can access local and national private and government data bases and can supplement them with data obtained from the local informant networks. In Europe's highly developed bureaucratic states the databases already exist, they only have to be harnessed. In the less developed areas of Asia and Africa they have to be created and populated with data – a major undertaking, but well worth the effort, because a combination of IT and population control measures (ID card scheme, security patrols, checkpoints) can take the place of the physical control measures (curfews, protected villages and free fire zones) used in the past.

A well-designed data system can digest and compare data stored in widely differing formats, uncovers anomalies and helps in locating and apprehending insurgents and their supporters. It can flag suspicious behavior (frequent cash transactions in a generally cash-less society); it can identify unusually structured households (e.g. those with an unusually large number of young males); it can pick out names that appear in one list, but are absent from other, closely related lists (e.g. residential addresses and public utilities customers), or appear on mutually exclusive lists (e.g. a cell-phone conversation and a credit-card transaction at the same time by the same person, in widely distant locations); it can identify citizens who are long dead and buried, yet drive cars and visit dentists, etc.

In the counterinsurgency context such forensic data-mining is far more than just an intrusive investigative procedure of over-zealous law enforcement officials looking for suspects in a crime already committed. Its purpose is to identify potential insurgents, with a view to neutralizing them before they can strike. This is ***preemptive profiling*** based on racial, ethnic or religious stereotypes, personal habits and behavior patterns, therefore anathema to advocates of privacy and human rights.[8] However,

[8] *In 2003 Congress scuttled a very ambitious data-mining project of the United States government (Total Information Awareness), but similar projects are either in development, or are already functioning. The FBI has also been the target of criticism recently for its permissive domestic surveillance rules.*

the fact remains, that most insurgents do fit definable profiles. And, conversely, most citizens fit one of the "most likely not an insurgent" profiles (little old ladies in tennis shoes). A thorough inspection of the first category and a quick screening of the second makes life more difficult for insurgents and frees up resources that can then be focused on identifying the rare outliers – the attractive Belgian redhead with the suicide west, the university professor who doubles as ideological enabler and recruiter.

6 ACTIVE MEASURES AND SECURITY

Passive intelligence collection must be supplemented by ***active measures,*** directed against the insurgents' organization, support structures and cohesion. In "wars amongst the people" most actionable intelligence is extremely perishable: the non-state belligerent has nothing or very little by way of permanent structures and assets, and he can abandon whatever he has without seriously degrading his capabilities.[9] Creating an ***intelligence-action service*** that integrates intelligence specialists and small strike forces of police or light infantry can overcome this problem: the intelligence specialists collect the information, evaluate it immediately and pass it to the strike elements to act on it, well before the target realizes that he has been compromised. (Trinquier, p. 37.) Such forces have been used by the French in Algeria, especially in Algiers, with some success. (Aussaresses, pp. 117-121) However, there are two risks in employing intelligence-action teams. First, even with the best data--communications systems, the team's evaluation capabilities are likely to be limited. As a result, it may target the strike element on the basis of raw or only partially evaluated information. Second, such forces, unless they are very tightly controlled, often become rouge organizations and inflict far more damage to the government's cause than whatever benefits they can provide.

Strike teams organized from security forces personnel and masquerading as insurgents or their supporters can be particularly effective in sowing dissent, mistrust, suspicion and enmity among the insurgents' ranks, between insurgents and civilians, and insurgents and their international supporters. They can also eliminate the insurgency's emblematic figures who may feel safe among their own people – especially on the far side of an international border. In the English-speaking world these are generally called "pseudo-operations."[10] The key to the success of such operations is the participation of *captured and turned insurgents* both in training the teams and in the operations themselves. (Cline, 2005, Mahadevan, 2007 and Kiss, 2010)

The conditions of modern insurgency offer many opportunities for pseudo-operations: the meta-narrative at the core of the insurgency seldom provides sufficient

[9] *For example the Algerian independence movement fighting against French rule (FLN – Front de Libération Nationale) instructed its members to hold out for 24 hours under interrogation. After that they were free to divulge any information they had – by then their associates would disappear, weapons caches would be emptied, safe house would be vacated.*

[10] *A recent, spectacularly successful pseudo-operation was Operación Jaque (July 2, 2008). Colombian soldiers, masquerading as employees of a non-governmental organization rescued 15 hostages held by Colombian rebels.*

discipline and cohesion; an ambiguous rumor and a few suspicious incidents are enough for insurgent groups to start accusing each other of treachery and start fighting among themselves. Modern insurgencies, due to their heterogeneous ethnic composition and constantly changing, leaderless network organization, cannot develop effective counterintelligence screening measures that would identify such impostors and uncover their activities in a timely manner.

Effective intelligence must go hand in hand with ***effective counterintelligence.*** The insurgents will do everything in their power to penetrate the security forces, and their efforts are often successful. A disconcerting experience of western security forces is that loyalty to Islam overwrites other loyalties, even if they were undertaken voluntarily, and under oath: there have been a number of cases of Muslim personnel supplying the targeted organizations with information. Some other religions have a similar effect. During the Sikh insurgency in the Punjab many police officers sympathized with the insurgents and provided them with information. In this instance the police showed rare pragmatism: the suspicious officers were discreetly reassigned to positions where they had no access to sensitive information. Thus the insurgents not only lost valuable sources – they were also deprived of the propaganda value of the arrest and trial of policemen who had "answered the call of their conscience." (Gill, 2001) Compartmentalization, strict adherence to the principle of need-to-know (which can be detrimental to the quality of intelligence) and tight control and supervision may reduce this risk, but will never eliminate it completely.

7 HOW DOES IT ALL AFFECT WESTERN FORCES?

One conclusion we can draw from the preceding pages is that – at least in the area of asymmetric conflict – the customary division of intelligence work into collection areas (foreign-domestic; military-civilian, economic-technical-scientific, land-air--maritime, etc) has to be given up. This does not mean that every intelligence and counterintelligence organization must be amalgamated into a single unit - but it definitely does mean that the “intelligence community” must lower the dividing walls between disciplines, collection areas and collector agencies, and it must achieve a very high order of coordination. There must also be very close cooperation with the intelligence organizations of other nations.

The Punjab Police’s intelligence operations during the years of the Khalistani insurgency are particularly instructive. In the early years of the insurgency no systematic intelligence collection took place – even routine record-keeping was neglected. A dedicated, multisource counterinsurgency intelligence operation was set up only in 1984 – four years into the conflict. Officers from all the law-enforcement, paramilitary and military organizations were brought together, and given the task to carry out a detailed analysis of insurgent operations throughout the state. The most important sources of the intelligence "raw material" were:

– the periodic reports from the network of local police stations,
– the detailed documentation of every terrorist incident,

– the interrogation of captured insurgents and individuals who operated the insurgency's supporting infrastructure;
– technical means (voice intercept, remote surveillance),
– double agents in the insurgent organization,
– informants recruited among the population.

Gradually, patterns emerged from the apparent uniformity of terrorist operations across the state. The various insurgent organizations, their leadership and their main operatives were identified, their strength determined, their spheres of operation defined, their relationships of cooperation and hostility with other organizations documented. Detailed information was also gathered on sources and flows of weapon supplies, networks of safe-houses, shelter-providers and sympathizers, cross-border routes. Joint interrogation centers, a system of dissemination of information and liaison officers posted to operations centers and command posts solved the problem of intelligence sharing between the various organizations.

Rapid analysis of raw data and dissemination of the results meant actionable intelligence, planning based on near real-time information, and operations targeting specific organizations and individuals. The operations could be executed with surgical precision – which meant operations that affected only the insurgents, without "collateral damage." The key result was that the initiative passed to the security forces.

The insurgents retained the capacity to organise unpredictable and entirely random strikes against soft targets, but they lost the impunity of operations that they had previously enjoyed. Following each major strike, the responsible organization was targeted not only in the Punjab, but in their safe-houses all over the country. The detailed information available of their possible escape routes – including shelters with the extended families of each terrorist, extended families of terrorists who had been killed in the past, key sympathisers and harbourers – made it possible to mount surveillance and concerted pursuit operations that, even where they did not result in immediate arrest, paralysed individual terrorists and prominent groups, reducing their capacity to act in future.

There is no question that western military personnel can master the intelligence techniques and procedures most appropriate for a counterinsurgency campaign. They have proven this in many counterinsurgency campaigns, in several continents: the elimination of Saddam Hussein's sons, the capture of the dictator himself, the capture or liquidation of insurgent leaders in Colombia were no accidents. However, if we are serious about gaining and retaining the trust and support of the people, we must apply these principles not only to hunt down a limited number of high-value targets, but across the board. That requires familiarity with the social, political, economic and cultural environment and a thorough understanding of the conflict's root causes – and not only among intelligence specialists. Personnel with these qualifications are likely to be in short supply, especially when they would do most good – in the early phases of the insurgency. This is a serious challenge, because without such

understanding there is a risk of concentrating on those discrete parts of the conflict that we do understand well (e.g. finding, fixing and fighting the enemy), and neglecting other aspects that are equally important. (Flynn, Pottinger, and Batchelor, 2010) During the last three years or so the author conducted several command post exercises in Eastern Europe. When faced with the unfamiliar problem of a domestic insurgency scenario, the participants usually tried to fit the expeditionary experience they had gained in Iraq or Afghanistan to a domestic situation, and hoped that the umpire would not challenge them on rules of engagement or the provisions of the penal code. Those with no expeditionary experience usually fell back on the tactics, techniques and procedures (TTPs) of conventional war. Even senior police officers - supposedly trained in handling domestic disturbances – were not better prepared.
There is no reason to suppose that American, German or Danish officers would behave differently if – or when? – U.S., German or Danish forces have to be deployed within the United States, Germany or Denmark in support of civilian law enforcement agencies. This is no problem as long as the troops provide only logistics, communications or medical assistance. But if – or (again) when? – they have to take a more active role, they would have to face the reality of fighting fellow citizens, friends, brothers under rules of engagement that are far more restrictive than anything they have experienced overseas. Unless they are provided with appropriate doctrinal guidance (and appropriate training) ahead of time, they are also likely to fall back on TTPs that worked in conventional war or in the counterinsurgency campaigns in Iraq or Afghanistan, but are totally inappropriate for a conflict on their own soil. The time to develop and promulgate those doctrines is now – before they are needed, rather than the day after the troops are deployed.

8 ASYMMETRIC WARFARE IN EUROPE

It is a comfortable self-delusion (as well as political irresponsibility) to see the likelihood of asymmetric challenges only in the failed states of the third world, or in the remote, backward regions of the Balkan Peninsula. The factors that bring about the paradigm shift are present in Europe as well. The reduced authority of the nation states in the European Union, closed and corruption-prone political elites, the dominance of corrosive ideologies (moral and cultural relativism, multiculturalism, political correctness) have created a fertile soil for the growth of local asymmetric challengers. Kosovo's independence motivates other minorities to seek their own autonomy or independence. In several European states, we must take into consideration the aspirations of increasingly assertive and violent Muslim minorities.[11] Furthermore, as the solution to a long-running economic crisis seems more and more remote, old-fashioned class-struggle may appear again, especially in Eastern Europe. As a result of the coincidence of external and internal factors, asymmetric conflict is probable in the near future. In some states *de facto* autonomous zones have

[11] *The minorities in question naturally consider their aspirations for greater autonomy or full independence entirely justified and legitimate, and may even have the sympathy and support of the rest of the world. However, for the affected state they are usually a national security threat, which the government usually feels compelled to answer (by force, if necessary) in order to preserve the state's territorial integrity.*

developed: no-go zones not only for the majority population, but often also for public service employees, law enforcement officers, public transportation and ambulances. The zones are governed by local power centers that collect taxes, dispense justice according to their own code, and if necessary coerce the loyalty of the zone's residents.

Terrorism has proven to be one of the most effective instruments of the insurgents, consequently every intelligence organization in the world has been concentrating on identifying terrorist organizations and preventing their operations. Special units are standing by in every country to parry terrorist attacks or deal with their consequences. Police organizations – if they receive appropriate instructions from the political decision makers – are able to suppress street riots and possess every tool necessary for the destruction of alternative power centers. Extensive literature is available in most languages, and some armed forces have long institutional experience in this area. Minorities that are unable to (or refuse to) assimilate and obsessively insist on their traditions are routine tasks for the social infrastructure of most states. Thus, within the narrow limits of their own expertise, these institutions are able to handle particular aspects of asymmetric conflict.

However, if the interdependence and synergies between the various elements is not clear for the political decision makers, then they will not recognize the need for a state of emergency. If there is no state of emergency, then the organizations and institutions of the state machinery will work without coordination, in isolation from one another and, working at cross purposes, will neutralize each other's results (Kiss, 2006).

The most important task of the intelligence organizations is to support the political decision makers with up to date, accurate information. A hardly less important task is to monitor the actual political and security situation, identify potential threats, and call the decision makers' attention to them. When discharging the latter task they may have to accept the role of the mythological Cassandra. Whether the decision makers take the warnings seriously or not, the intelligence organizations must prepare for expected crises, at least with plans and capabilities. In the case of asymmetric threats this preparation is overdue today.

Bibliography

1. *Cabinet Office, 2010. A Strong Britain in an Age of Uncertainty: The National Security Strategy. London: HMSO.*
2. *Department of Defense, 2008. Operations (FM 3-0), Washington: US Army.*
3. *European Union, 2003. A Secure Europe in a Better World - the European Security Strategy. Brussels: EU.*
4. *European Union, 2010. Internal Security Strategy for The European Union "Towards a European Security Model". Brussels: EU.*
5. *Ministry of Defence, 2006. Operation Banner – An Analysis of Military Operations in Northern Ireland, London: HMSO.*
6. *Ministry of Foreign Affairs, 2012. Magyarország Nemzeti Biztonsági Stratégiája [National Security Strategy of Hungary]. Budapest: MFA.*
7. *NATO, 2010. Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation, Brussels: NATO.*

8. *Aussaresses, P. 2002. The Battle of the Casbah – Terrorism and Counter-Terrorism in Algeria 1955-1957, New York: Enigma Books.*
9. *Barber, N., 1971. The War of the Running Dogs: Malaya 1948-1960. Godalming: Fontana.*
10. *Cilliers, J. K., 1985. Counter-Insurgency in Rhodesia. Beckenham: Croom Helm Ltd.*
11. *Cline, L. E., 2005. Pseudo Operations and Counterinsurgency: Lessons from Other Countries. Carlisle: Strategic Studies Institute.*
12. *Flynn, M., Pottinger, M,, and Batchelor, P., 2010. Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan. Washington DC: Center for a New American Security.*
13. *Gill, K. P. S., 2001. Endgame in Punjab: 1988-1993. New Delhi: South Asia Terrorism Portal, http://www.satp.org/satporgtp/publication/faultlines/volume1/Fault1-kpstext.htm (last accessed: 09.26.2011.)*
14. *Glenn, R W., 2002. 'Cleansing Polluted Seas' – Non-State Threats and the Urban Environment. Small Wars and Insurgencies, 13 (2) pp. 109-120.*
15. *Kis-Benedek, J., 2009. Az Izrael–Hamasz háború biztonságpolitikai és katonai összefüggései, [The Security Policy and Military Aspects of the Israel-Hamas War]. Budapest: Felderítő Szemle, 8 (1). pp. 12-35.*
16. *Kiss, Á. P. 2006: Harc a terrorizmus ellen: A működő antiterrorista model [Fighting Terrorism – the Functioning Antiterrorist Model], Budapest: Új Honvédségi Szemle, 2006/12, pp. 14-26*
17. *Kiss, Á. P. 2010. Ál-gerillák – nélkülözhetetlen erők az aszimmetrikus hadviselésben [Pseudo-Guerrillas – Indispensable Forces in Asymmetric Warfare], Budapest: Hadtudomány, 2010. internet publication without page numbers, http://mhtt.eu/hadtudomany/2010_e_2.pdf.*
18. *Mahadevan, P. 2007. Counter Terrorism in the Indian Punjab: Assessing the 'Cat' System. New Delhi: Faultlines, Volume 18, http://www.satp.org/satporgtp/publication/faultlines/volume18/Article2.htm (last accessed: 06.26.2010.);*
19. *Molnar, A.R. et al 1965. Human Factors Considerations of Undergrounds in Insurgencies, Washington DC: Department of the Army Pamphlet No 550-104.*
20. *Smith, N., and MacFarland, S., 2008. Anbar Awakens – The Tipping Point. Military Review, 88 (2) pp. 65-76.*
21. *Smith, R. 2005. The Utility of Force – The Art of War in the Modern World. London. Penguin Books.*
22. *Strachan, H. 2007. British Counter-Insurgency from Malaya to Iraq. London: RUSI Journal. 152 (6) pp. 8-11.*
23. *Trinquier, Roger, 1964. Modern Warfare. London: Pall Mall Press.*