



Civil-Military
Co-operation
Centre of
Excellence

Counter Terrorism Seminar

15-16 November 2005



List of Speakers

Terrorist Threat in South East Asia – Mr. Kenneth Pereire, Institute of Defence and Strategic Studies/ Int. Centre for Political Violence and Terrorism Research, Singapore.

CIMIC and Counter-Terrorism from an Academic Perspective – Prof. Tom Mockaitis, DePaul University, Chicago, USA.

Military Contribution in a Civil Led Environment – Group Captain Robin W. Birtwistle, Ministry of Defence, United Kingdom.

Force Multipliers; CIMIC and Psychological Operations Combating Terrorism – Prof. Philip Taylor, Institute of Communications Studies, University of Leeds, United Kingdom.

CIMIC, Counter-Terrorism Operations and the NATO Response Force – Brigadier General Ton van Loon, Commander of NRF Brigade.

European Union CIMIC and Counter Terrorism – Mr. Lukas Holub, EU DG Justice, Freedom and Security.

Recent Experiences: The London Bombings – Chief Detective Inspector Hunter, Metropolitan Police, London, United Kingdom.

Civil Military Co-operation In the Campaign against Terrorism – An Interagency Issue. Mr. Paul Shemella, Centre for Civil-Military Relations, USA.

CIMIC and Counter Terrorism – Mr. Bart van Bussel, Counter Terrorism Unit, National Police of the Netherlands.

Editorial

Overall Responsible: Director CCOE Col. Jürgen Witzig

Action Official CT- Seminar: Capt. Mirjam Grandia (Grandia.M@cimicgroupnorth.org)

Seminar Moderator: Prof. Joseph Soeters, Royal Military Academy, Netherlands.

Report Official CT Seminar: LTC Jorgen Bech (Bech.j@cimicgroupnorth.org)

Civil-Military Co-operation Centre of Excellence

PO Box 982

6000 AZ Weert

The Netherlands

www.cimicgroupnorth.org

registry@cimicgroupnorth.org

Phone: +31 495 55 7030

Fax: +31 495 55 70 29

Press Requests:

Phone: +31 495 55 7263

E-mail: pio@cimicgroupnorth.org

Preface

The Director of the Civil-Military Co-operation Centre of Excellence

The second seminar “Counter- Terrorism and CIMIC” conducted by the Civil-Military Co-operation Centre of Excellence (CCOE) was a further milestone in becoming a NATO accredited Civil-Military Co-operation body for NATO, EU, UN and CIMIC players.

High profiled guest speakers and 40 participants from 13 different nations represented many institutions and professions varying from Vice Chairman of a Parliamentary Defence Committee to staff officers and experienced experts from non-governmental organisations, counter-terrorism staffs, academic institutes, NATO staffs and Ministries of Defence. All of them played a vital role in making the seminar successful.

The CCOE will continue to fullfill its role as a multinational contribution to NATO’s transformation efforts, and is offered for NATO accreditation by using its academic freedom in determining the subjects of its seminars, lectures and finding relevant speakers. By this CCOE will promote new ideas and findings among relevant institutions and individuals, and emphasise the value of mutual understanding through a continued debate.



**Col J. Witzig,
Director CCOE**





Content

List of Speakers	II
Editorial	II
Preface	III
Content	V
Abbreviations	VI
1 The problem of defining terrorism	1
2 Terrorism in South East Asia – an example	3
3 Counter- Terrorism in the UK – an example	7
4 Defining CIMIC and Counter- Terrorism	9
4.1 Mission of CIMIC	9
4.2 A new CIMIC definition?	10
5 Force Multipliers: CIMIC and PsyOps in combating terrorism	11
5.1 The problem of information management	11
5.2 A new role of media in war?.....	12
5.3 Media as asymmetric weapon	13
5.4 Recent changes in dealing with media	14
6 CIMIC, Counter- Terrorism Operations and the NRF	17
7 CIMIC and Counter- Terrorism – a European perspective	19
7.1 Differences in perspectives.....	19
7.2 Role of the military	19
7.3 Challenges for CIMIC	20
8 CIMIC in the campaign against terrorism	23
8.1 Dimensions of CIMIC.....	23
8.2 What can governments do to achieve this?	24
10 Role of CIMIC in Counter- Terrorism operations	27
The way ahead	VII
Complexity of future operations	VII
Strategic Anti-terrorism.....	VIII
Summary	IX



Abbreviations

ACT	Allied Command Transformation
CA	Civil Affairs
C2	Command and Control
CRO	Crisis Response Operations
CT	Counter- Terrorism
EBO	Effects Based Operations
EC	Enhanced CIMIC
EU	European Union
GO	Governmental Organizations
InfoOps	Information Operations
IO	International Organizations
JI	Jemaah Islamiyah
NGO	Non- Governmental Organizations
NRF	NATO Response Force
NSCS	National Security Coordination Secretariat
PD	Public Diplomacy
PI	Public Information
PsyOps	Psychological Operations
PSO	Peace Support Operations
PRT	Provincial Reconstruction Team
OSI	Office of Strategic Influence
UN	United Nations



1 The problem of defining terrorism

First, the different definitions of terrorism, counter-terror and anti-terror were discussed in the seminar including the terminology concerning “fight or campaign against terrorism” and “war on terrorism”. There are a number of different definitions on the market, but yet no conclusive international definition.

Counter-terrorism can be seen as offensive pre-emption whereas anti-terrorism includes security measures. The goal for all efforts is most likely to be defined as a reduction of the perceived risk of terrorism to a level, which can be accepted by societies. Contrary to the above, there is the perception of terrorism as a phenomenon that can be completely eradicated.

With regard to the issue of terrorism being a crime or war, the approaches varied from: “Terrorism is not a crime; criminals want to live, not blow themselves up” to “All terrorism acts are acts of crime and should be handled by the judicial system”. Basically, this characterises the splits causing the lack of an international definition.

There is a clear need for an international consensus on the terminology. However, it was also widely understood that the complexity of the subject and the variety of understandings, both in the United States of America and amongst European nations, are likely to prolong this process. For the time being, it therefore suffices to say: “We know it is terrorism when we see it”.





2 Terrorism in South East Asia – an example

In general, the threats from terrorism must be seen as regional threats and global threats. Al Qaeda is interested in South East Asia (SEA) as an arena for promoting international terrorism and spreading its ideology, mainly through use of their Afghans Veterans Network. It benefits from the Islamic resurgence in SEA, especially in Indonesia, from the Jemaah Islamiyah (JI) network – collectively, the resurgent target nations with weak state structures.

JI's regenerative potential has not been reduced, as there will be those who will continue to be misled by its ideology. Although it is difficult for the group to carry out high-profile, complex attacks, they are still able to prepare small-scale attacks.

Since around the time of 9/11, some authorities have made significant arrests, effectively crippling the JI network, especially in Singapore and Malaysia. However, JI is still active, particularly in Indonesia.

JI's leaders and experts are still at large. Also, its decentralisation has resulted in the group becoming more fragmented. This has left small, agile cells of the most radical and committed members presenting a serious threat.

The belief in Islam is the most unifying element – they share the same radical views; however, not necessarily the same goals. In a forecast for the region early this year, a meeting of Abu Sayyaf and JI chiefs in the area was reported. Intelligence shows movements between Indonesia and the Philippines. In Feb 2005, news about JI members being caught on suspicion of involvement in the Valentine's Day attacks emerged. This again reveals joint operations between Philippine and Indonesian groups. Moreover, many analysts agree on the fact that if the situation in Southern Thailand is not

handled appropriately, it may easily turn into another "jihad theatre" – perceived or real oppression of Muslims – as in case of the sectarian conflict in Maluku in which JI played a role.

The fight against terrorism requires the protection of critical infrastructure, enhanced security at high-profile events, increased international interagency coordination and inter-action. The latter starts from joint patrols and hot-pursuit authority for being able to continue a running chase crossing national borders and continues with joint education and training and international networking.


Why are well-educated individuals recruited to extremist organisations? This question cannot be answered easily, but comprises the perception of Islam being under siege. The extremist groups can therefore use religion as a tool for recruitment. There is a "fertile" recruitment ground – hopelessness in immigrant communities, lack of integration in the host societies (3rd generation but still not French, British etc.) – that entails recruitment of "home-grown" terrorists and recruitment to terrorist training camps.

Singapore used a multi-ministry networked approach. Combating terrorism includes:

- strong intelligence and coordination,
- effective border control,

but is definitely not only limited to these areas. Different strategic mindsets among the involved on how to address the issue of terrorism present a problem – which mainly presents crime versus socio-economic *raison d'être*. The answer probably lies in a comprehensive approach.

Singapore has been quite successful in dismantling terrorist groups by integrating Islamic clerics in their strategy. It aimed at explaining to Muslim communities the wrong interpretation of Islam by extremist groups and promoting Islam as a peaceful religion.



The Singapore government believes in the fact that reducing the threat at home does not only require strengthening of their own borders. It has to cooperate with its neighbours in the region when countering the threat of trans-national terrorism and its ideology. At the same time, its own intelligence infrastructure, public surveillance and interagency coordination is to be enhanced. An influential and autonomous centre must be established within the government to coordinate national security policy directions, where the operational coordination and responses are to be left up to other agencies. In addition:

- Structures and processes should be introduced to help maintain discipline and continuity.
- Where possible, structures should be based on existing ones in order to keep focus.
- Those that have proven to be robust should be allowed for continuous operation.
- Establish strategic forums to discuss critical issues and promote a common understanding of security concerns among all security policymakers and practitioners.
- Institutionalise a national security strategic planning and policy process.
- Develop a culture of cooperation.

In the Singapore example, the elements of Singapore's revised national security architecture comprise the following:

For effective policy coordination, the National Security Coordination Secretariat (NSCS) has been established.

The Coordinating Minister for Security and Defence presides this committee, which also comprises the Ministers of Defence, Home Affairs and Foreign Affairs. The committee meets regularly to elaborate national security strategies and formulate policies. It examines the country's most critical goals of national

security capability development, discusses critical issues and threats and reviews prevailing national security measures.


The national security coordination secretariat depends on two key agencies - the National Security Coordination Centre (NSCC) and the Joint Counter-terrorism Centre (JCTC) - to support its policy and intelligence functions. The NSCC comprises separate groups to undertake policy, planning, risk assessment and horizon-scanning responsibilities, including the operation of a Horizon Scanning Centre.

The JCTC provides intelligence and assessments on terrorist threats to facilitate policy-making and counter-terrorism efforts. It serves as a multi-agency centre of expertise on terrorism providing comprehensive and timely threat assessments relating to terrorists. The JCTC thus integrates the work of the various intelligence agencies and departments in Singapore.

The potential pitfalls are turf battles – fights for responsibilities, capacities and authorities – fundamental problems of joining disparate organisations with different cultures and modes of operation and the problems of a different strategic mindset. In summing up, terrorism will be a concern in the foreseeable future. It is important to note that the centre of gravity of terrorism has shifted beyond Al Qaeda to its associated groups posing various levels of threat in different regions.

There is no doubt that the current trend of terrorism is of strategic nature requiring the development of a sustainable national and international security strategy and a coherent security framework.

Problems of trans-national terrorism present scenarios that involve multiple authorities and varied expertise, i.e. one single agency will not have all resources or capabilities required for handling the range of threats on all levels. Accordingly, civil-military close co-operation is paramount in fighting international terrorism.



In addition, Singapore has introduced the so-called Ideological Response with the principal objective of providing an intellectual counterweight to terrorists' radical message. This can be achieved by developing a concerted method to identify, expose and counter the ideological threat posed by such groups. To this effect, the project outlines six strategic areas to be developed:

- Gather information on terrorists' ideology, propaganda methods and political apparatus.
- Analyse terrorists' radical worldview and map out its ideational content, dissemination and target audience.
- Expose terrorists' ideology.
- Develop policy recommendations for Southeast Asian governments on how to counter terrorists' ideological threat.
- Cooperate with academics, journalists, regional NGOs, civic groups and policy makers to expose and offset terrorists' indoctrination methods.
- Become the main academic repository for primary source materials and readings on radical Islam in Southeast Asia.

Scope:

- Academic research.
- Dissemination and public education.
- Training.
- Collation of materials.
- Policy recommendations.

Recommended tactical approaches:

- Response presentation must suit the targeted audiences. For example, response targeted at a Muslim community must be prepared in a way that it seems to be given by the Muslim communities themselves (the scholars) in order to avoid prejudices. While presentation to non-Muslims is to be done by non-Muslims to avoid the perception of bias and defensiveness.

- Response is to be focused on the ideas not on personal attack.
- Extensive collaboration with Muslim grass-root organizations is to be established to ensure better outreach and penetration.
- Though the primary focus of the response is on Muslim terrorists' ideology, minimum effort is to be made to study ideology of other terrorists' organization. This is to avoid the perception that the program only targets at Muslims. It is also in line with the understanding that terrorism is not only a particular phenomenon of Muslims. Proper projection of such work has to follow.



3 Counter- Terrorism in the UK – an example

The United Kingdom has faced a terrorism regime for the last 30 years. The characteristics have been mainly domestic and the terrorists have operated in tightly structured networks in order to avoid capture and ensure readiness. The terrorists limited the amount of victims of their bombs with warnings and showed a negotiable political agenda.

Currently, a new type of enemy is faced which is not operating under the law enforcement radars and not always on “home” ground. They are characterised by a relative overtness in their recce activities. This new threat presents a long-term problem. The terrorists’ only structure is their flexible network. They aim at mass civilian casualties and new methods of simultaneous attacks against several spectacular or iconic targets using improvised explosive devices. The attacks are deadly and determined.

In the United Kingdom, two relatively new joint institutions deal with threat assessment:

- Domestic Horizon Scanning Committee.
- Joint Terrorism Analysis Centre.

The direct involvement of the armed forces is based on the concept of military support of civil power in areas of specialist military expertise and unique capabilities. Recently, the involvement of armed forces was virtually nil.

With regard to the issue of threat levels to the public, there is a distinct balance between warning and not alarming the public in order not to achieve a counter-productive result. The United Kingdom strategic goal is to reduce the risk originating from international terrorism so that people can go about their business freely and confidently. The areas of mission are:

- Prevent - Tackle the underlying causes, resolve regional conflicts, promote mainstream Islam and make most of global action.
- Pursue - pre-emptive action, understand the foe, track, disrupt and bring him before the court and capacity building within government agencies.
- Protect: Target hardening (i.e. taking safety measures to make attacks difficult), both at home and abroad, protective security and communication.
- Prepare: Resilience and Consequence Management.

Crisis management is divided into three levels where the Cabinet Office Briefing Room (COBR) is established for ministerial control. COBR is a committee mechanism providing effective coordination and use of each agency without compromising its individual efficiency.



4 Defining CIMIC and Counter-Terrorism

4.1 Mission of CIMIC

The last years showed dramatic changes in the way CIMIC is performed on an operational basis. The differences in the doctrinal understanding of CIMIC have become evident. At the same time, the understanding of CIMIC's importance and therewith the term "Enhanced CIMIC" are gaining prominence.

Nations have different policies concerning CIMIC both inside their own territory and when participating in international operations. Terrorism does not know any geographical or organisational boundaries and lives on its opponent's lack of responsibilities and structures. Terrorists "love" these gaps, they hide in them, and there is a clear need for closing these gaps by working together. The doctrinal issue must be addressed, in particular the NATO doctrine which is obviously not as comprehensive as required, i.e. it should be made clear that "CIMIC is in support of the mission". In the fight against terrorism, civil-military co-operation is the mission. A good example on how not to organise interagency co-operation is a number of effective agencies being placed under the command of one body. This compromises the effectiveness of each body involved. The key is to integrate the involved agencies in a network. At the moment, CIMIC is a purely military concept. The problem is to change it into a practicable solution serving the fight against terrorism.

In its broader term, CIMIC includes co-operation between military and civilians at home and abroad. There are many different situations and participants so that the solution of the problems becomes even more complicated. Other terms for CIMIC may be

"influence operations" and "interagency co-operation".

The NATO definition on CIMIC is restricted to the co-operation in support of the military mission. When CIMIC was involved in international operations which include "nation building", many member states experienced this contribution as being hardly sufficient. This is also the reason why NATO operations are focusing on a wider and more efficient terminology, namely on Enhanced CIMIC and concerted action and planning initiatives.

The terms are not always as clear as wanted. One important note is that CIMIC does not present civ-mil operations – it is co-operation and not co-option. It should also be clear that the military aspect cannot solve political and social problems in a nation-building process.

It is rather a question of the type of functions than about whether CIMIC has a function or not. The possible functions are:

- Coordination of agencies of a "homeland" security.
- Coordination of crisis management.
- Coordination of international efforts to combat terrorism.

Furthermore, CIMIC plays an important mental role in being on the same level with the people and establishing a good and positive community, which in the end forms the basis of countering roots of terrorism. This is the primary value on which the CIMIC tasks should be based. It inspires people to have discussions. CIMIC, therefore, has a potential role to play in furthering the interagency coordination, which is absolutely needed in the fight against terrorism as everyone recognises. As regards the lack of a global strategy for counter-terrorism, the lines of action of the CIMIC policy and doctrine are a means to include the needed capabilities, i.e. in consequence management actions. Accordingly, CIMIC is not the capacity, but presents a concept of operations at the strategic, operational and tactical level.

4.2 A new CIMIC definition?

Current CIMIC definitions are too restricted. New structures and a transformation are required in order to extensively broaden the perception of its use in today's operations which are more complex than ever – Enhanced CIMIC might be the answer. It is first of all a strategic issue which is extremely complex in an international environment. How can it be realised? Often, a disaster has to take place until changes are put into action.

It is to be build from beneath. A consensus can probably be reached on the basis of the guidelines of Consequence Management, and afterwards this consensus can be extended. CIMIC mainly deals with strategic communication – linking responsibilities.

The NATO policy features three pillars: Counter-terrorism (offensive action, pre-emption), Anti-terrorism (Security measures) and Consequence Management mitigating the effects of an attack. They all involve CIMIC.

Counter-terrorism in coalition operations as in Afghanistan and Iraq makes use of Provincial Reconstruction Teams and Combined Action Platoons. Here, the value of CIMIC lies in force protection as a force multiplier and aid multiplier. The CIMIC effort is essential for rebuilding and restoring normalcy. The CIMIC tasks include coordinating the humanitarian effort, supporting the rebuilding of civil institutions and assuring uniform efforts.

Anti-terrorism amongst NATO allies is found in a standardized threat warning system, maritime security in Allied Endeavour, intelligence/information sharing and other measures to reinforce potential targets. Consequence Management comprises the responses to attacks and the apprehension of perpetrators. In context, all these measures, either in a "homeland" or "Coalition" scenario, require mechanisms for civil-military co-operation.

Does a global strategy for counter-terrorism already exist? Unfortunately, the answer is no. Currently, it does not exist. This is why ad hoc responses replace a strategy. A strategy requires co-operation rather than unilateralism and a mechanism to coordinate activities and encourage uniform efforts. CIMIC provides a good model for such co-operation.



A comprehensive approach

CIMIC is required for uniform efforts in a global campaign against terrorism. The military plays an important but limited role in the conflict. It must be noted that military force is of limited use in solving political or socio-economic problems. Training is the key effort. For this reason, it may be very helpful to resume the crisis management exercises NATO performed 15 years ago, provided they are adapted to the current new threat.



5 Force Multipliers: CIMIC and PsyOps in combating terrorism

5.1 The problem of information management

Global terrorism is indeed an asymmetric threat. Nation-building is the business, because there is a fundamental assumption that democracies do not fight democracies. If this is true, it indeed is the successful strategy. CIMIC and Public Information (PI) are in the human factor area, and hearts and minds are to be won. The means are info operations and nation-building. It is difficult to take command and control of the complex field of activity, such as the Internet where we operate on a perception level and which is absorbed by young people. This is a campaign or war fought not only with military means. The unconverted and unborn human beings must be addressed, as those converted to extremism are already lost.

The resistance of Public Affairs/ Public Information/ Media Operations to becoming one of the pillars of Information Operations, alongside Psychological Operations and deception in particular, has been evident in the Public Information community since the mid 1990s, embodied in the phrase “we are not in the influence business”.

It is indeed put into question whether the entire concept of “pillars” – a legacy of Cold War thinking as developed over a period of 40 years – is appropriate for a global info-sphere that has changed dramatically since the end of the Cold War and the arrival of the internet. People who take a look at the whole strategic context of Information Operations or Strategic Communications within this changed environment, consider the separation of Public Information from other attempts to shape the perceptual space within that environment as a disingenuous

argument. The idea that disclosing “factual information” to the media does not affect the way media report on events belies what everyone knows about modern journalism: Media are slaves to the information they are given, whether it is correct or not (Korans being flushed down the toilet at Guantanamo Bay or The Mirror’s faked photographs of British soldiers mistreating Iraqi prisoners).

In the global war on terror, the media are a major battleground and the effort to win hearts and minds may well depend on how effectively public information counters al Qaeda’s proven ability to exploit the increasingly complex global media “battleground”.

The anxiety can be understood. The debacle in Washington over the Office of Strategic Influence (OSI) in March 2002 was a microcosm of the wider issues. The fact that Victoria Clarke, the Pentagon’s spokeswoman, seems to have disclosed the existence of the OSI to the press shows just how much concern there is within the Public Information community about being commandeered into the business of defeating a terrorist enemy which regards the media as its best asymmetric weapon. But surely, the time for such turf wars is over?

The problem is how to do this without given information being considered as propaganda. In part, the solution for the Public Information community is to recognise that they are indeed part of the influence business, but it is also the responsibility of other components of the Information Operations/Strategic Communications business to recognise that there are certain “rules” to be followed in conducting their activities.

These rules are drawn mainly from the history of democratic propaganda. When the Allies first engaged in a modern propaganda battle, between 1914 – 1918, they failed to discourage atrocity propaganda about the “Beastly Hun’s” activities against “innocent




women and children” in Belgium and France. Worse still, they encouraged the peoples of Central and South Eastern Europe to rise up and overthrow their imperial overlords, the Dual Monarchy, in return for which they would be granted national sovereignty. This resulted in (arguably) unviable nation-states disputes (in particular Czechoslovakia and Poland) which would have resulted in the outbreak of a second world war within one generation. Britain and France declared war on Nazi Germany without the United States, partly because post-1918 revelations about the sheer extent of Britain’s secret propaganda war in the USA between 1914 and 1917 had led to great suspicion about Britain’s motives at that time. The Great War propaganda experiment had been handed over to the press barons, Lords Beaverbrook and Northcliffe. Their experience resulted in a different strategy the next time, especially when the US entered World War Two after Pearl Harbour. This was the “Strategy of Truth”. Thus the democratic propaganda tradition of telling as much of the truth as could be told without damaging civilian morale or operational security. It meant some censorship of news but rarely of views and was contrary to the approach of Josef Goebbels, Nazi Propaganda Minister, which is incorporated in the phrase “the Big Lie”.

Goebbels believed in the theory that by repeating any information often – whether it is true or not – people would eventually believe it. You are struck by the application of this totalitarian or authoritarian principle of propaganda in today’s war on terrorism. It probably explains why at one point 70% of the Americans believed that Iraq and 9/11 were connected or why so many politicians believed that Saddam still possessed his weapons of mass destruction. But the inclusion of such a principle in the democratic propaganda model to undermine the Strategy of Truth tradition that has been largely followed ever since World War Two has also

made the PI community more nervous than ever before of becoming one of the pillars of Information Operations. Would press conferences and statements by President George W. Bush and Donald Rumsfeld directly to the Iraqi people have been imaginable during the Iraq war of 2003? Had a press conference become a Psychological Operation? It certainly looked as though the introduction of Effects Based Operations, of “Shock and Awe”, was undermining the traditional rules of dealing with the media.

5.2 A new role of media in war?

Maybe the time for those traditional rules has passed and it is time to think no longer in terms of Cold War era pillars but to think about the use of the whole spectrum of Public Information, Psychological Operations and Information Operations. Full spectrum dominance is closest to this, but whether it is still possible to dominate the global info-sphere is where opinions diverge. Due to the arrival of the World Wide Web in the 1990s and the break of the Anglo-American global media monopoly upon the arrival in the mid 1990s of new regional players like Al Jazeera it is unlikely that western views on a given event will ever predominate in the future as they never had in the past. As an example, the media coverage of the Gulf war of 1991 and the Iraq war of 2003 can be mentioned. The arrival of “embedded” correspondents (not a new concept) equipped with portable satellite videophones enabled a global audience to watch the advance on Baghdad in real-time. In 1991, the 100-hour land war to liberate Kuwait was barely seen at all although pictures of its aftermath on the so-called “Highway of Death” are said to be one factor why the war was brought to a halt. But in 2003, not only Al Jazeera correspondents but also American forces were in Baghdad. And when Brent Sadler’s team of CNN was fired at by Iraqi insurgents, their bodyguards actually fired back – putting an end to the



idea of reporters being only observers of wars, not participants in it.

5.3 Media as asymmetric weapon

Clues that this thinking had entered military rules of engagement (though not stated explicitly anywhere) first surfaced during the 1999 Kosovo conflict when Radio-TV-Serbia had been briefly bombed off the air. NATO spokesmen justified it in terms of spreading false propaganda and it thus became a legitimate target; but the truth is that Serbia skilfully exploited coalition bombing mistakes by broadcasting images of convoys bombed out or trains full of civilian casualties to counter the NATO line that this was a humanitarian mission. The speed with which they did this often forced NATO Public Information on to the defensive – until perhaps the arrival of Alistair Campbell. But the Serbs illustrated how effective an asymmetric weapon television could be – and they also showed some skills on the Internet.


As a 17-year-old boy working in his bedroom in the Philippines demonstrated with the “I Love You” virus, one info-bomber can cause enormous damage world-wide. And as Al Qaeda also demonstrated, the Internet provides an alternative space for voicing views that may not be covered by traditional mass media outlets. This is not just about Bin Laden statements or “video-nasties” of hostages being beheaded. Only weeks ago, it was reported that Al Qaeda has begun casting news bulletins on the net on their belief that hurricane Katrina was God’s revenge against “the city of homosexuals”. The number of terrorist websites has increased considerably since 9/11.

You wonder if democracies have indeed forgotten the lessons of the past when dealing with this new environment, not least in the area of self-fulfilling prophecies. For if there was little or no connection between Iraq and 9/11 before, there is now. And Desert Storm blowback from black PSYOPS

broadcasts encouraging Iraqis to rise up against Saddam – even though “regime change” was not coalition policy in 1991 – helps to explain why most coalition forces were not greeted with enthusiasm and flower petals in 2003.

Hopefully, this rapid review will help illustrate how porous the global information space has become, how difficult it is to control or dominate and that tactical information does not exist anymore. Cameras are now literally everywhere, whether they are CCTV, the video-footage taken by the wife of a Spanish truck-driver of the Concorde crash or the images taken on mobile phone cameras of the bombed out London underground on 7/7. None of these images were taken by professional journalists, but by persons who can be designated “citizen journalists”. When the Israeli Defence Force entered Jenin, they took no journalists with them – a mistake, because they created an information vacuum that was quickly filled with media speculation that a “massacre” was taking place. Not just a mistake, but futile – as pictures of Israeli tanks destroying buildings were on the internet shortly after they had been taken by Palestinians armed with video cameras. And the photos they took reinforced the media speculation about who the victims in this operation were.

In addition to historical rules, there are legal constraints for dealing with these problems. For example, in the United States there is the 1948 Smith-Mundt act which clearly distinguishes between what US Government officials say to the American people through PA and what they say to foreigners through public diplomacy or psychological operations. Whether this distinction between the “national” and the “international” is possible in the age of the Internet must be doubted. And in operational terms, it is already nonsense because US politicians have revealed over the years that when they are speaking to foreign audiences, they are actually speaking



to domestic US audiences. If 9/11 was really a “wake-up call”, this will clearly need some attention. We have already seen how the Bush Doctrine of pre-emptive war undermines centuries of norms in the international state system, but we have yet to encounter much debate about the viability of the concept of pre-emptive Information Operations. But surely – provided the historical and legal rules of the Strategy of Truth are followed – this is a key component of waging a generational struggle for hearts and minds in the global war on terrorism.

In truth, Information Operations are somewhat limited in their application to the concept of a “war” on terror. It was a mistake to label it a “war”; “counter-terrorism” campaign would have been fine. Wars are historically and legally defined as armed conflicts between two or more nation-states but this “war” against an idea is a war without end. But it is the idea or set of ideas which has to be engaged if we are to “win”. We cannot be sure about how victory will be defined or how peace negotiations are to be conducted, but this new kind of war is to be considered in terms of Cold War + internet + citizen journalists. This requires more than just a military doctrine such as Information Operations. And this is where the emerging ideas about Strategic Communications come in. In a nutshell, it is about joining up all the pillars ensuring that turf wars do not break out between, for example, State and DoD in Washington (!) and ensuring co-ordination between elements of soft power alongside the needs of appropriate kinetic power so that the message is understood, shared, owned and spoken with one voice. But deception is still in there which creates problems (not in or of itself, but rather when it is linked to other influence operations) and it is suspected that too little attention is still given to CIMIC. Iraq’s 2003 aftermath was a warning regarding the dangers of not getting this one right.

5.4 Recent changes in dealing with media

As regards the traditional mass media, you have to recognise that the problem is both quantitative and qualitative. Almost 450 reporters covered the D-Day landings, while there were around 1500 in Riyadh in 1991. Nearly 4000 roamed the borders of Kosovo in 1999. In 2003, there were 600 embedded reporters and a yet unknown quantity of unembedded journalists. Such large numbers roaming around the battlefield require some form of “management”. Although, as a group, it is populated with a huge range of quality, the one thing they have in common is competitiveness. Journalism has changed enormously over the past 15 years including many changes in today’s understanding of the term “news”. Today’s war correspondent is next week’s cookery correspondent. Specialised journalism is being eroded by the advent of what Nik Gowing named the multi-skilled “robo-hack”. Experienced Public Information officers know that some of these journalists can be worked with and some can’t. But they all have to be dealt with in some way; ignoring them – as the Jenin example reveals – can render matters even worse.

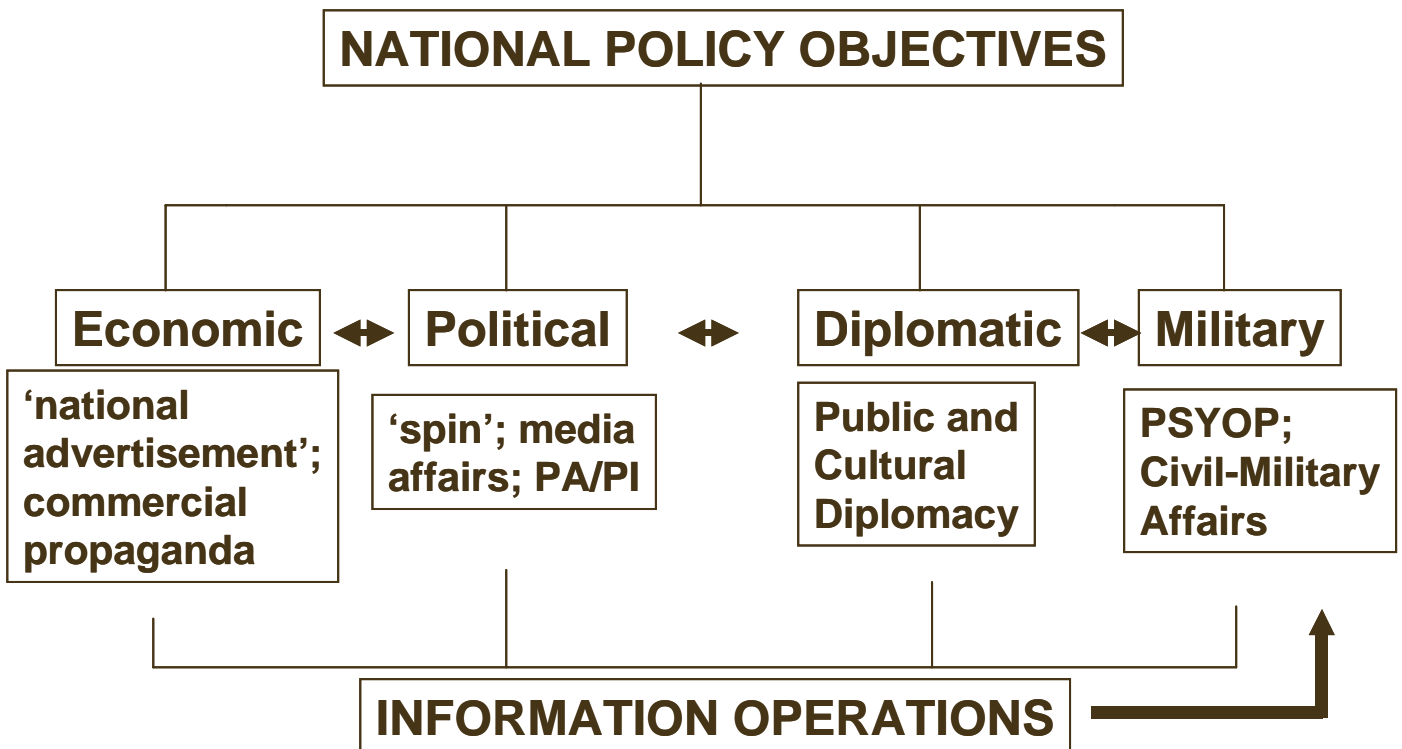
So where does Public Information fit in the Strategic Communications spectrum? Better minds than mine have wrestled therewith. The only solution: it should be as far away from deception as possible, but much closer to Psychological Operations, CIMIC and Public Diplomacy than in the past. One warning is that those other influence activities must adhere to the tradition that has served western democracies so well in previous wars against authoritarian ideologies. Democracies will perhaps always be on the defensive against ruthless enemies who exploit the very nature of democracy itself to achieve their goals. They will latch on to normal democratic self-reflection and self-criticism or to negative comments made in the course of free debate

to prove their point about our hypocrisy, selectivity and aggressive intentions. We are sensitive to counter-themes, such as NATO's help for the Muslims in Bosnia and Kosovo. And we certainly do not think of claiming that the recent earthquake along the Afghan border was God's revenge on Al Qaeda! But, if huge parts of the world are to be convinced that we are not the infidels or crusaders that our enemies claim we are and if part of that conviction is to export democracy in the hope that this is the true way forward for all of us, we have to ensure that our Strategic Communication messages are real and credible and that they can benefit others. Dealing with the media – old and new – requires constant, speedy, honest attention to a tricky and truculent target audience, but most of all we have to ensure that in the process of “selling” democracy, we do not sell it out.

CIMIC can be referred to as the “forgotten” element of Information Operations. There are numerous examples from Bosnia, Kosovo and Iraq. Media are not interested in “Peace”

and “Smile Operations”. Some commanders are not interested in non-kinetic deployment. It is a fact that CIMIC is just as much a part of “shaping the information space” as other elements. The overall relationship between Public Information, Psychological Operations etc. can be seen in the context of Strategic Communications.

Information Operations are about humans and human factors are about people, not just networks. This part of Information Operations consists of “Public Affairs”, Civil Affairs, Media Relations and Public Diplomacy – all aiming at influencing the leadership's decision making process. In the Information Operations sphere, CIMIC has its place in Influence Operations together with Psychological Operations and Public Information.





6 CIMIC, Counter-Terrorism Operations and the NRF

As a response to the challenges of the 21st century, NATO designed the NATO Response Force – in order to have a force which is able to operate across the entire range of conflicts and to be able to apply the force rapidly, selectively and decisively. The NATO Response Force is a high-readiness joint combined force capable of performing certain missions on its own as well as participating in an operation as part of a larger force or serving as an initial entry force in preparation of a follow-on-force. The possible missions of the NATO Response Force include operations like Non-combatant Evacuation, support of Consequence Management, Crisis Response Operations and support of Counter-Terrorism. The force is a complex toolbox for NATO integrating many different capabilities. The capabilities must also focus on the non-kinetic effects such as CIMIC and Psychological Operations. For the first time, NATO earnestly tries to truly integrate forces by no longer using the concept of having the core force from one single nation. In this way, NATO Response Force becomes a means of transformation.

There are certain trends in future operations. First of all, operations will (always) be conducted in coalitions. This emphasises burden-sharing and the political will to operate. In general, multinationality increases capabilities and broadens views. On the other hand, it also causes frictions and requires intensive preparations, and the more nations involved, the more time is needed for preparations. Accordingly, operation of the force is more complex.

Another trend is that operations seem to become more complex. The nature of operations is no longer either article V “War fighting” or “Peace Support Operations” merging humanitarian, peace support and

combat operations. They are characterised by asymmetric (the opponent chooses), irregular opponents operating in difficult urban terrain. In other words: Today’s adversary is a dynamic, adaptive foe who operates within a complex, interconnected operational environment. The challenge is the conceptual leap from two-dimensional awareness to multi-dimensional understanding.

There is a need for constant escalation dominance and quick changes in force posture. The operation can no longer be divided into front and rear operations which requires rethinking about logistics and also tactical CIMIC. The situational awareness becomes crucial and the behaviour of each individual soldier is very important for the operation.

All modern operations will have to be considered as peace support, humanitarian and combat missions and can never be conducted by a single service and with combat power only. The trend is therefore thinking in Effects Based Operations with emphasis on the three-dimensional use of force capabilities, non-lethal attacks and synchronisation. Many of the required effects are often achievable through effective CIMIC. Thinking in effects offers a more comprehensive approach and growing emphasis on non-kinetic ideas. It also means that measuring effects becomes much more difficult and the decision-making process even more complex.

So where does that lead CIMIC and counter-terrorism? First of all, we have seen that Effects Based Operations require an integrated approach in which the desired effect is to reduce the support of terrorists. In this connection, a delicate balance between traditional CIMIC and direct action will always be required. Secondly, the force protection can never be considered as being separate from force posture. Full spectrum operations will always involve CIMIC. As defined, NATO



Response Force operations include initial entry in which substantial support from civilian authorities must be either provided or substituted. At the same time, the role of NATO Response Force in counter-terrorism emerges.

This also means that CIMIC is changing. It must no longer be seen as a side show activity, but requires the entire attention of the commander. In this respect, the military term CIMIC is misleading, since the field of application is almost unlimited. CIMIC is no longer a rear area operation. It must be regarded as important aspect in influencing the population during counter-terrorism operations. Just look at Provincial Reconstruction Teams in Afghanistan. They are most of the time in the frontline, and CIMIC personnel are a target, too.

Military operations become becoming ever more complex. Effects based thinking is the key to success. CIMIC and other non-kinetic approaches are crucial and no operation can be successful without a full-spectrum approach.



7 CIMIC and Counter-Terrorism – a European perspective

7.1 Differences in perspectives

In general, CIMIC and Counter-Terrorism personnel work in a non-permissible environment in which the opponent decides when and where to attack. CIMIC personnel and also civilian people engaged in the nation-building sphere are high-value targets for terrorism.

A clear distinction was indicated between the use of military forces for CT purposes inside and outside our own nations. The approaches varied from: “Terrorism is not a crime; criminals want to live, not blow themselves up” to “All terrorism acts are acts of crime and should be handled by the judicial system”. For example, within the European Union, terrorism is generally considered a crime and not war, as the fight against terrorism is regarded in the United States. This mainly characterises the split caused by the lack of an international definition, even though it should be recognised that the American perception is also based on domestic political reasons. If it was not called a war, it would have been difficult to get public backing for a US engagement outside own territory.

In the EU, there are two views with regard to CIMIC and terrorism:

- Use of military in support of actions outside the Union. This clearly presents implications for internal security (i.e. crisis management, restoring order, preventing local conflicts, etc. depending on the mission).
- Use of military within the territory of one’s own state or the Union.

As a basic premise, the use of military force must be really the last resort or a resort in situations when the civil component is overwhelmed or does not have any capabilities to respond adequately. In other words, military is complementing the civilian component with its specialised capabilities (such as disposal of explosives, chemical, biological or other dangerous substances, field hospitals, transportation capabilities, etc.). In this case, the population approves the use of military forces.


In European nations, the impression given by the picture of military out in the streets of the cities is: Something is really wrong or a military parade is held.

On the issue of communicating terror issues (warnings etc.) to the public, the military should be used only in a way that it does not give the impression to its own citizens that they are under siege, as such an impression is certainly in nobody’s interest. In turn, this will require a better communication about what the military can provide and cannot provide with regard to internal security. It is therefore necessary to clearly draw the lines and enhance the general understanding of what the military is capable of and how it can help in difficult situations within the European Union member states.

In some countries, the picture is more complicated because they have a conscript service which could have certain social functions within the society. This is changing considerably today due to the specialisation within the military.

7.2 Role of the military

The EU approach in fighting terrorism consists of: Prevention, protection, prosecution and response. The possible role of the military in specific circumstances can be imagined in protection and response (citizens, infrastructures, borders, CBRN). Only under very extreme circumstances when



military is involved in policing of own territory, specific parts of military forces can be involved in prosecution (or pursuing terrorists). It must be noted that in some nations, the military has no jurisdiction within its own territory or it can even be forbidden to use military force within the own territory.

One aspect of the use of military force is the avoidance of power vacuums in crises situations in affected areas. This appears to be crucial even in the territory of own states. The latest disasters in the US also showed the above. Here, the role of military forces is to be considered. In all circumstances, the aspect of interoperability or interaction between the military and civilian capabilities in the fight against terrorism and the work on generic scenarios need to be included.

Thus, military forces must be capable of cooperating effectively with civilian authorities as well as coordinating with police forces and rescuing forces directly on the ground.

This issue must also be discussed in relation to a cross border crises when multinational civilian and military forces have to conduct combined activities in a timely and coordinated fashion. These issues are discussed between the 25 member states of the European Union.

The discussion about and answering of these questions does not only concern conceptual thinking about CIMIC, but also exercising. This is absolutely crucial in discovering weaknesses and blank spots which require attention and improvement in order to prepare for crisis situations effectively. Under the Community Civil Protection Mechanism – the EU Commission funds several exercises each year, and for 2006 an exercise with terrorism-specific scenario is planned.

It is necessary to integrate military capabilities in civilian consequence management operations. In this context, the EU has implemented the modalities, procedures and criteria for establishing a database of various

military capabilities available to the Civil Protection Mechanism. These capabilities are relevant to the protection of the civilian population against the effects of terrorist attacks, including chemical, biological, radiological and nuclear attacks.

7.3 Challenges for CIMIC

One of the concerns is found in the area of procedure and standards. Common procedural manuals and minimum standards may be very helpful to assure effective co-operation and coordination of versatile forces including civilian and military components. It is necessary to teach not only the military but also the civilian divisions and to raise the awareness of what the military can do for the civilian sector, including their availability and readiness.

In this context, it is important to train soldiers on how to deal with civilian populations, including how to deal with legal issues in the area in which they have to operate, e.g. teach and exercise proper ways of policing and detaining civilians, if necessary, under extreme circumstances. The EU is a community based on law. In this context, it is necessary to take a look at the legal and political obstacles of such joint civil-military co-operation in internal security matters, for example concerning the cross border police co-operation (e.g., legislation on internal EU cross border hot-pursuit or legislation on joint investigation teams). At this stage, it is premature to have legislation for the European level cross border civil-military co-operation, but it would certainly be beneficial to know the existing legal situation within the Union.

Another issue is the role of the military in the protection of the population and self-protection (Force Protection) as well as in the protection of essential civilian staff which needs to be identified and trained accordingly.

The important issue of avoiding local power vacuums after evacuations (avoiding looting etc.) is also an area in which the use of military forces can be helpful.

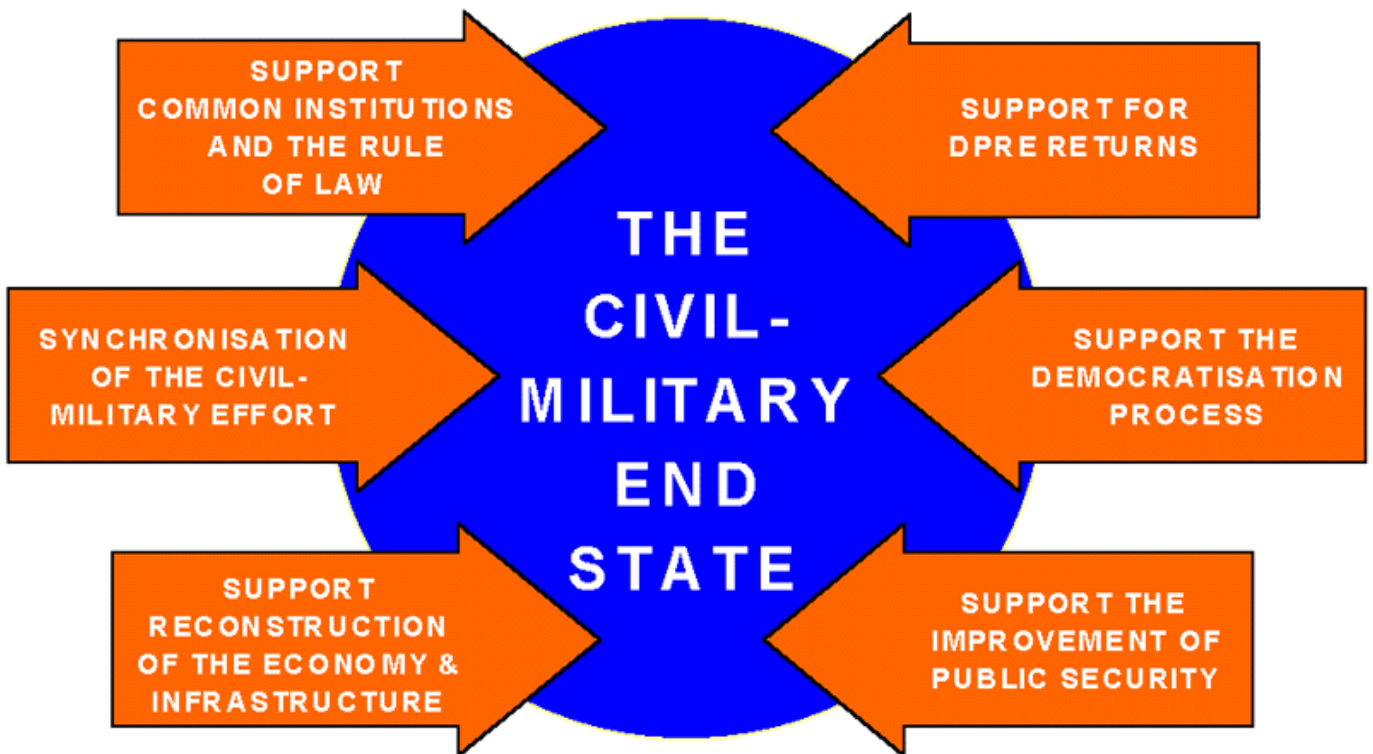
The issue of language skills is often ignored. In the EU and in co-operation with civilian authorities, language is of paramount importance.

Another question to be handled is how to deal with neighbours who are not members neither of the Union nor the NATO. In fact, our quick response can prevent damages to territories and threats to populations.

The civil military co-operation and relations are not only found on the security level, but

also in the economic-technical sphere. The trend of changing the security business is a new element in civil military relations to be faced in a changing security environment with threats coming from the inside of our societies. This is highlighted by the fact that the military is scaled down and specialised.

From the EU point of view, the long-term purpose of CIMIC is to create and sustain conditions supporting the achievement of a lasting solution of the crises as shown in the following figure:





8 CIMIC in the campaign against terrorism

8.1 Dimensions of CIMIC

First of all, CIMIC is much more than just an acronym. It is a concept that applies to all levels. CIMIC must be seen as the operational extension of civil-military co-operation on the political level. "Macro-CIMIC" is based on the same principles as NATO CIMIC and must be regarded in the light of the principles of Enhanced CIMIC:

- Coordination,
- Collaboration,
- Complementarity.

The desired "Final State" in the campaign is a world free of terrorism as a legitimate means of social change. For this purpose, a wide range of national and international mechanisms to defeat terrorism is needed to reduce terrorism to a level at which it becomes an isolated and sporadic criminal activity without any international connections. Basically, there are three types of overlapping strategic approaches:

- Core Strategy: Attack the root causes of terror – Long-term effect.
- Offensive Strategy: Attack the threat.
- Defensive Strategy: Consequence management.

The players are at the national level of interagency decision-making. On the regional level, there are various collective security organizations such as the EU including cross-border alignment of policy and strategy, and last but not least, there are the UN and global coalitions on the global level.

On the spot, you will also find the civilians in the political and humanitarian ministries and agencies, including Non-Governmental Organisations and International Organisations which all apply "Soft Power". The military with

its vast resource reservoir can be considered as "Hard Power".

In the campaign, two different communities can obviously be found: On the one hand, there is the civilian/political community with a process-oriented approach. These people strive for change, act in an independent manner and manage their "just-in-time planning". On the other hand, there is the military with its typically apolitical and action-oriented mentality. It presents organisations hating change, having a team mentality, clear structures and leadership and making use of deliberate planning.

This of course causes interagency conflicts entailing disagreements on what the real problem is and thus disagreements on the possible response. There are also different measures of effectiveness and overlapping responsibilities which at least cause waste of resources. It is also apparent that many agencies believe that they are equally capable of competition as a consequence. In many situations, one agency will have the authority, but another has the resources.

Fighting terrorism requires co-operation, but the problems are multi-dimensional and interdependent. There is a clear need for different actors providing different expertise. National governments therefore need to ensure:

- Effectiveness and efficiency,
- capability and capacity,
- redundancy where needed,
- no "gaps" between agencies.

Improving the coordination requires extensive interaction at both senior and working levels. The well-proven concept of liaison must be widely used. Other issues are networked education, joint training and teamwork ethics. When resolving conflicts, the principle of negotiations is to be introduced.

Here, it is very important to mention that the opponents, the terrorists, benefit from "gaps".

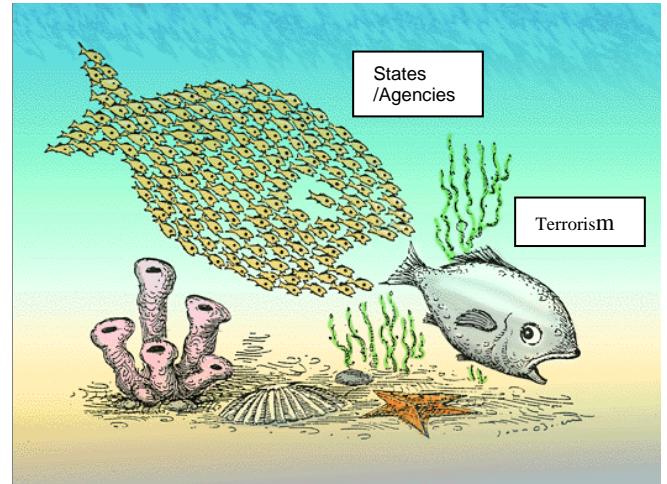
This is the un-governed space of command & control, inter-agency responsibilities, geographical boundaries etc. It is in these spaces where weaknesses are to be identified.

In the attempt to reduce the interagency conflict, the political leadership position assigns functions and responsibilities and has to ensure the settlement of disputes at an early stage. It should be noted that political or any other higher-level interference at the operational level is destructive to any operation. All of the above has to be provided before the crisis arises. A way of dealing with it is to identify “comparative advantages” of each agency and then establish an interagency hierarchy so that each agency understands its role and is provided with the necessary resources. However, interagency coordination requires a lot of practice through training, exercises and conferences in which the details (logistics, technical) as well as the operating procedures are elaborated. It is important to promote a habit of co-operation and to construct formal and informal channels of communication. In the processes of dealing with interagency coordination:

- confidence is to be provided,
- interagency response teams are to be established,
- liaison personnel is to be assigned.

Another issue can be simplified in the phrase: it takes networks to defeat networks. It is characteristic for the structures of our societies to have “vertically” organized governments or organisations. In the campaign against terrorism, these agencies face “horizontally” organized threats. Therefore, governments must “flatten” their decision-making processes which again means increasing decentralisation and requires increasing coordination. This is Networked Operations and we need to work in a network to use information more effectively and to benefit from the ultimate

product of networks – “Creativity at the edge of chaos”.




This is called scale-free networks (like the www) in which a complex system forms nodes. In this way, CIMIC gets a series of super-connected nodes (meetings, capacities, relations, information sharing etc.). A characteristic of the scale-free networks is the resilience against random attacks. In these networks, the social networks and relations become extremely important when countering terrorism, both in operations at home and abroad. To understand the networks, you have to speak to people.

8.2 What can governments do to achieve this?

- Train in networked operations,
- promote action-oriented people,
- reverse the bureaucratic development,
- devolve decision-making authority down the chain,
- set policy and procedural guidelines - and let individuals operate freely,
- cultivate imagination,
- forgive mistakes.

The role of the military as a facilitator in this process is to share information on the basis of: not “who needs to know”, but “who does not need to know”. Additionally, in the field of arranging interagency meetings, planning workshops and taking initiatives for



organising interagency exercises, the military systems will have an important role. The Centre for Civil-Military Relations in the US is an example of such an organisation. It is guided by a common vision – small, flat, and agile with decentralised planning and execution. It works in a self-reinforcing networked way. Establishing organizations like this requires an out-of-the-box mentality. Another example is the US Marine Corps Chemical, Biological Incident Response Force.

When adapting to the new situation, it is vital to use a bottom-up versus top-down approach. The complex situation requires field-level solutions even though their nature is often unpredictable. However, it is crucial that governments promote policy and resources.

Multinational operations require both regional and international coordination. Here, the same principles as mentioned above should be implemented. It must be realised that there are more variables and that different national doctrines result in different interpretations of mission. In addition, there are the challenges posed by local and international NGOs – language and cultural issues, intelligence sensitivities and diplomatic and political constraints from differences in national versus coalition control, misaligned strategies and different measures of effectiveness.

Coalitions are defined as a temporary combination of parties that retain distinctive principles. Coalitions for CT operations need to be established on a broad basis (countries and agencies) and capable of operating on many fronts. A coalition must be capable of integrating civilians and able to assume risks. Another characteristic of the coalition is the ability to involve unprecedented levels of co-operation.

As terrorism is declared to be a threat to “International Peace and Security”, UN’s efforts must be regarded as a global coalition

against terrorism. 162 nations supported the UN resolution on terrorism, and 35 or more nations participated militarily in the operations in Afghanistan. More than 48 countries provided indirect support to operations such as intelligence, over-flight rights and basing.

A coalition is first of all based on a consensus to reconcile the national interests of all participants. This co-operation must benefit all participants (but not equal benefit) and the benefits of acting in a coalition must exceed the perceived benefits of acting alone. Actual guidelines for Coalition Operations must further contain effective command arrangements on all levels and formal as well as informal exchange of information. Here the liaison mechanisms must be strong. The coalition must be open for meetings between all military and civilian entities involving CIMIC capabilities and personnel trained specifically for civil-military co-operation.

It is obvious that the idea of civil-military co-operation plays an important role in the campaign against terrorism. The main issue is to develop the synergy of the civilian and military capacities through:

- Interagency coordination,
- networks,
- diminishing gaps,
- bridging the military and civilian society.





9 Role of CIMIC in Counter-Terrorism operations

In the interagency co-operation, CIMIC must be seen in the perspective of:

- Nation-building,
- military support of law enforcement on an national and international basis,
- Governmental Organisations and International Organisations, including Non-Governmental Organisations.

In other words, the role of CIMIC in counter-terrorism operations will be a matter of which actions can be taken at which level. On the strategic level, nation-building efforts must be made at the earliest possible stage in order to achieve a consensus amongst all agencies and partners, including governmental agencies and organisations, International Organisations and primary Non-Governmental Organisations. On the operational and tactical level, CIMIC must be an integral part of both planning and operations to include Information Operations and Psychological Operations. In detail, CIMIC humanitarian, economic, societal, infrastructural etc. assessments should be used as a reality check of the military intelligence and force protection assessments.





The way ahead

Complexity of future operations

All modern operations have to be considered as peace support, humanitarian and combat missions and can never be conducted by a single service and never with combat power only. The trend is therefore thinking in Effects Based Operations with emphasis on the three-dimensional use of force capabilities, non-lethal attacks and synchronisation. Many of the required effects can be achieved by effective CIMIC. Thinking in effects gives a more comprehensive approach and growing emphasis on non-kinetic ideas. It also means that measuring effects becomes much more difficult and the decision-making process even more complex. Also future operations will be conducted in coalitions. This emphasises burden sharing and the political will to operate. In general, multinationality increases capabilities and broadens views. On the other hand, it also causes frictions and requires intensive preparation, and the more nations involved, the more time is needed for preparation. Accordingly, the operation of forces seems to be more complex and will require high levels of co-operation skills among all involved, including skills and the will to co-operate with civilian/political components and organisations.


CIMIC is therefore much more than just an acronym. It is a concept applying to all levels and must be seen as the operational extension of civil-military co-operation at the political level. This “Macro-CIMIC” is based on the same principles as NATO CIMIC and must be viewed in connection with the guidelines of Enhanced CIMIC which include the overall concept of coordination, collaboration and complementarity.

The terms are not always as clear as wanted. The NATO definition on CIMIC is limited to the co-operation in support of the military

mission. This is also the reason why NATO focuses on a wider and more efficient terminology, namely Enhanced CIMIC and other initiatives. Concerning the terrorism terminology, there is a clear need for an international consensus and understanding. However, it must be understood that the complexity of the subject and the variety of understandings are likely to prolong this process.

Civil-Military Co-operation has a potential role in furthering the interagency coordination which is needed in the fight against terrorism. Accordingly, the idea of civil-military co-operation in its broader framework plays an important role in the campaign against terrorism. The main issue is to develop the synergy of the civilian and military capacities by promoting interagency co-operation and coordination and training in networked operations in order to reduce the gaps used by terrorists. The military role as a facilitator in this process is to share information on the basis of: not “who needs to know”, but “who does not need to know”. Additionally, in the field of arranging interagency meetings, planning workshops and taking initiatives for organising interagency exercises, the military systems will play an important role.

These ideas are more pertinent to the political-military strategic level than to the operational and tactical level operations. At these levels, the role and focus of CIMIC in counter-terrorism operations must be seen in the operational context of Effects Based Operations and Information and Psychological Operations. Information Operations are about humans and human factors are about people not just networks. This part of Information Operations consists of Public Affairs, Civil Affairs, Media Relations and Public Diplomacy – all aiming at influencing the leadership’s decision-making process. In the Information Operations sphere, CIMIC has its place in Influence



Operations together with Psychological Operations and Public Information.

Strategic Anti-terrorism

There is no doubt that the current trend of terrorism is of strategic nature requiring the development of a sustainable international and national security strategy and a coherent security framework. The problems of trans-national terrorism present scenarios involving multiple authorities and varied expertise. This means that one single agency will not have all the resources or capabilities required for handling the range of threats at all levels. It also means that civil-military close co-operation is paramount in fighting international terrorism. In other words: It takes networks to defeat networks.

Fighting the root causes of terrorism must include a governmental intention to use the idea of civil-military co-operation to create and sustain conditions supporting the achievements of a lasting solution.

The trend of robust military interventions with subsequent “nation-building” is of great strategic importance for world politics. Both for power and development politics, the ambitions are growing in terms of reconstruction and military intervention. If “nation-building” replaces stabilisation as aim, long-term efforts are comprised, while early conflict intervention means wartime-like operations with civilian purposes. The basic challenge is the transition from a military dominated process to a civilian dominated process and the capacities include all military and civilian instruments. The aim is to establish a legitimate, local political process. In general, civilian and military actors have difficulties in harmonising this with their professional view on transition operations.

But as these subjects are becoming focal points of the foreign policy (security and development) of many nations, both parties have to learn how to include the transition

operations. Governments have to upgrade their capacities and capabilities with regard to this aim.

The idea of stabilisation versus imposing democracies must be preferred as effect of “nation-building”, since democracy is an evolving process. Finally, the more synergy of the civil-military capacities can be developed and the more competition is reduced between capabilities, the more effective the strategy of reducing terrorism will be.



Summary

Since the end of the cold war, the United Nations, NATO, and more recently the European Union have all employed armed forces in post-conflict environments with the objective of supporting a political transformation. These missions have all been different to this point. However, nation-building, peace-building or stabilisation operations have become dominant terms in the use of armed forces.

Furthermore, the growing concern of all governments towards the increasing threats caused by regional and global terrorism in its different forms of appearance is of increased significance. Whether or how to involve military forces as only one arm of the state executive power in the prevention of and “fight” against terrorism is being discussed. Defence against terrorism has thus become an integral part of the missions of the military forces.

Defence and response to terrorist attacks on national ground also involve new combinations of regular military, paramilitary, law-enforcement and emergency-response forces. Here, civilian capabilities will be at least as important as military ones, and the priority for interaction between governmental agencies and increased resources requires “transformation” in a far broader sense of the term. Furthermore, the approach towards the public requires coordinated “Strategic Communication” and a clear view of the advantages and disadvantages of each course of action in order to avoid unwanted images and perceptions.

Military planners have recognised the necessity of broadening the view on the civil-military aspects by introducing the term “Enhanced CIMIC”. Allied Command Transformation is thus providing a conduit through which American and European ideas


on civil-military interaction in a transformed operational environment can be exchanged and synthesised.

To understand what enhanced future CIMIC may include, discussions need to be continued in order to identify the role and the level of involvement in the fight against terrorism. This is emphasised by the fact that counter-terrorism is one of the possible tasks of the NATO Response Force (NRF). This was the overall background why CIMIC Group North – in its new role as a Centre of Excellence for civil military co-operation – decided to participate in this discussion to support NATO’s transformation efforts.

The debate centred on various understandings and definitions of terrorism, counter-terrorism, anti-terrorism, war on terrorism and their connections to CIMIC in its broad context (Enhanced CIMIC) and furthermore its relations to Information Operations, Psychological Operations and Intelligence. All of the above aspects should be seen in the context of operations either “at home” or deployed in international missions. It is vital that Information Operations, Psychological Operations and CIMIC become prominent in a more comprehensive approach to Effects Based Operations and that field commanders avoid the tendency of emphasising kinetic effects only.

With regard to the issue of counter-terrorism being regarded as either a “crime” or “war”, the understandings varied from: “Terrorism is not a crime; criminals want to live, not blow themselves up” to “All terrorism acts are acts of crime and should be handled by the judicial system”. These statements mainly characterise the spectrum of splits. This also causes the difficulties in achieving an international consensus on a clear definition.

It was clear to all participants that precise and commonly accepted international definitions on terrorism and its related terms are needed. Otherwise, it will be difficult to reach a



consensus for a collective strategic approach on the fight against terrorism. However, it was commonly agreed that in the operational world - when actually dealing with the issue - terrorism is “something you recognise when you see it”!

It was concluded that the idea behind CIMIC in its broader modern definition indeed has a very important function in the fight against terrorism: At home in the sense of combining and communicating effectively the efforts of both civilian and military agencies; in nation-building abroad as the concept and the tool to integrate civilian and military means in a common strategic goal. It should be noted that in the actual fight against terrorism in their own territory, in most nations the police is in charge and the military only plays a role in adding unique or supplementary capabilities on request.

CIMIC has a supporting function in counter-terrorism. This may include:

- Coordination of agencies of “homeland” security,
- coordination of crisis management,
- coordination of international efforts to combat terrorism.

In particular, in the field of interagency coordination it must be realised that the problems of trans-national terrorism present scenarios that involve multiple authorities and varied expertise. It means that one single agency will not have all the resources or capabilities needed to handle the complete range of threats at all levels. The main challenges addressed in the discussion are:

Building coordination mechanisms between the existing structures and preferably not establishing new command and control elements. In this respect, effective networks seem to provide the answers,

establishing strategic forums to discuss critical issues and promoting a common understanding of security concerns among all


security policymakers and practitioners, avoiding “turf battles” fights for responsibilities, capacities and authorities by promoting a culture of co-operation.

In modern operations, CIMIC plays an important mental role in being on the same level with the local population and authorities and in establishing robust and positive community connections. In the end, these are the basics of societies in any nation. The CIMIC tasks should be based on this primary value. Additionally, CIMIC provides for mechanisms to get people discussing and therefore has a potential role in furthering the interagency coordination.

If we have to convince the public that our societies do not consist of the infidels or crusaders our enemies claim we are, and if part of that conviction is to export democracy in the hope that this is the true way forward, we have to ensure that the Strategic Communication messages are real and credible. When engaged in counter-terrorism operations during international missions, CIMIC plays a vital role as part of the Information Operations on the operational and tactical level and by adding crucial information about the society and the human factor to the military intelligence. From the Western point of view, the cultural differences are often forgotten and CIMIC is the tool to avoid this.

Lacking a global strategy for counter-terrorism, the guidelines in the CIMIC policy and doctrine can provide a way of integrating the needed capabilities i.e. to handle Consequence Management actions. Accordingly, CIMIC might not be the capacity but may smooth the path on the strategic, operational and tactical level.

At the same time, a CIMIC approach in the military way of thinking (the military command and control levels, and strategic, operational and tactical levels) is to be promoted when dealing with international terrorism. The key



word here is “networks” in order to match the way terrorists are working. At the minimum, stove piping must be avoided, i.e. a series of independent actions which are not concerted.

In the fight against terrorism, there is a clear risk of enhancing the underlying ideological struggle behind terrorism. This is to be avoided. In the Singapore example, the families of detainees are supported in order to minimise the next generation of terrorists. It is clear that the CIMIC-related idea of emphasising “cultural awareness and sensitivity” is also important for the success of the fight against terrorism.

The trend of robust military interventions with subsequent “nation-building” is of great strategic importance for world politics. Both in foreign and development politics, the ambitions are growing in terms of reconstruction and military intervention. If “nation-building” replaces stabilisation, long-

term efforts are comprised, while early conflict intervention means wartime-like operations with political intentions. The basic challenge is the transition from a military-dominated to a civilian-dominated process. The required capacities include both military and civilian instruments. The aim is to establish a legitimate, local political process. Military and civilian actors have to learn how to include the transition operations, and governments have to upgrade their capacities and capabilities with regard to this aim.

The idea of stabilising versus imposing democracies is to be preferred as effect of “nation-building”, since democracy is an evolving process. Finally, the more synergy of the civil-military capacities can be developed and the more competition is reduced between capabilities, the more effective the strategy of reducing terrorism to the fringes of human behaviour will be.