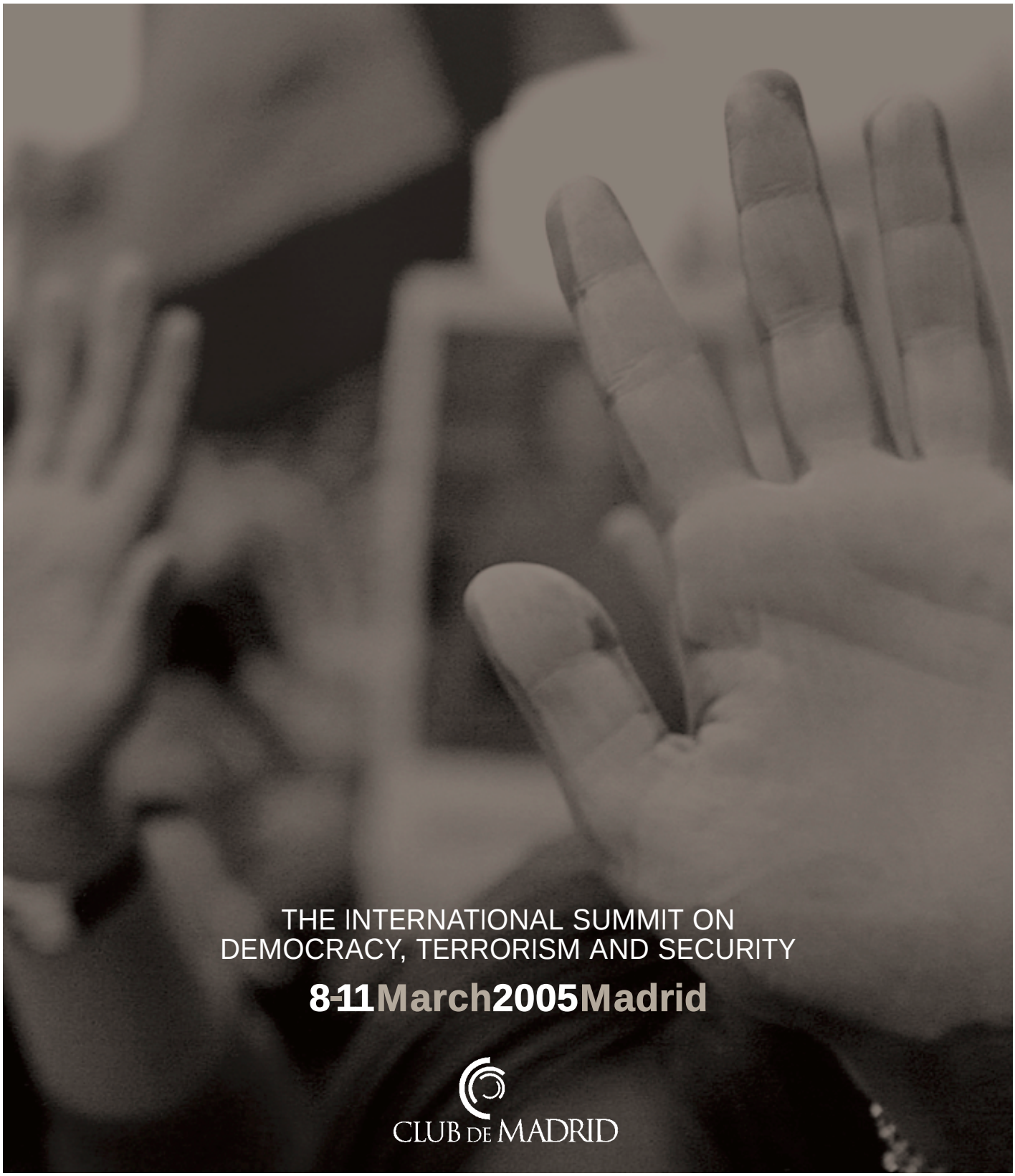
Confronting Terrorism

The Club de Madrid Series on Democracy and Terrorism

Volume II



THE INTERNATIONAL SUMMIT ON
DEMOCRACY, TERRORISM AND SECURITY

8-11 March 2005 Madrid

CLUB DE MADRID

THE INTERNATIONAL SUMMIT ON
DEMOCRACY, TERRORISM AND SECURITY

8-11 March 2005 Madrid

Confronting Terrorism

The Club de Madrid Series on Democracy and Terrorism

Volume II

CLUB DE MADRID

The opinions expressed in individual papers are based on the discussions of the working groups at the International Summit on Democracy, Terrorism and Security. They reflect the views of their authors, but not necessarily those of the Club de Madrid or any of its members.

The *Club de Madrid Series on Democracy and Terrorism* is available in Spanish and English. To order additional copies, please write to:

Club de Madrid
Felipe IV, 9 – 3º izqda.
28014 Madrid
Spain

Tel: +34 91 523 72 16
Fax: +34 91 532 00 88
Email: clubmadrid@clubmadrid.org

Series editor: Peter R. Neumann
Editorial Assistance: Henrik A. Lund and Milburn Line
Production: ESC/Scholz & Friends

Contents

Introduction

to the Club de Madrid Series on Democracy and Terrorism

Dear friend,

I am delighted to introduce the *Club de Madrid Series on Democracy and Terrorism.* The policy papers that can be found in this volume are the result of an unparalleled process of debate which culminated at the International Summit on Democracy, Terrorism and Security in Madrid in March 2005.

The Madrid Summit – held on the first anniversary of the Madrid train bombings on March 11, 2004 – was the largest gathering of terrorism and security experts that has ever taken place. It was our intention to be as comprehensive as possible, that is, to launch a strategic dialogue between scholars, practitioners and policymakers, but also to come up with practical suggestions that may help to resolve some of the dilemmas we have encountered since September 11, 2001.

The two hundred experts that participated in our working groups took up the challenge with great enthusiasm and dedication. In the months leading up to the conference, thousands of messages and hundreds of papers were exchanged. At the event itself, a whole day was spent on concluding the (sometimes heated) debates. The policy papers which resulted from this process will, I believe, be of enduring significance:

- With the input of two hundred of the world's leading scholars and expert practitioners, they represent the most informed judgement on the issue of democracy and terrorism to date.

- In being explicit about areas of consensus and disagreement, they provide an honest picture of the 'state of the debate'.

- They outline a number of fresh, practical ideas, which will be of great interest to policymakers and practitioners across the globe.

Taken together, the three volumes of the *Club de Madrid Series on Democracy and Terrorism* outline the elements of a comprehensive response to the challenge from terrorism. The first volume examines the roots and underlying risk factors of terrorism and details concrete measures on how these could be addressed. The second looks at the security side, including creative proposals for improving the effectiveness of the law enforcement effort. In the third, we explore how the foundations of democratic governance (human rights, civil society, the rule of law, etc.) can be turned into assets rather than obstacles in the struggle against terrorism.

The emphasis on democratic values is no accident. The members of the Club de Madrid are all former heads of state and government committed to strengthening democracy around the world. The Madrid Summit was not our first initiative, nor is terrorism the only challenge to democratic governance we have addressed. In fact, we are currently running programmes and projects in four different continents. If you want to learn more about the Club de Madrid, please contact us or visit our web site at www.clubmadrid.org.

For the moment, though, I hope you enjoy reading the policy papers in this volume of the *Club de Madrid Series on Democracy and Terrorism.*

Yours truly,

Kim Campbell
Secretary-General of the Club de Madrid
Former Prime Minister of Canada

Policing

By Jürgen Storbeck

Terrorism is not an isolated phenomenon. Terrorist movements originate in political and military conflicts, chronic ethnic and religious tensions, as well as bad governance. The police services and other law enforcement agencies should therefore view terrorism as a complex problem which requires a multi-faceted response. Our working group agreed on the following principles:

- The police's counter-terrorist approach must be comprehensive. Measures of policing have to be co-ordinated with all the other instruments that are used in the fight against terrorism. This includes political, economic, diplomatic, legal, social and – as a last resort – military means.

- Our counter-terrorist approach needs to reflect the fact that terrorism has 'gone global'. Many terrorist movements maintain a worldwide presence in order to raise and transfer funds, create false identities, procure weaponry, and set up operational sanctuaries. Consequently, the response of states, governments, societies and – especially – law enforcement agencies must be global as well as national.

- Furthermore, the fight against terrorism must be carried out with full respect for the purposes and principles of the United Nations Charter and general norms of international law, including human rights and humanitarian law. Necessarily, this applies to police forces and all other law enforcement agencies.

Within this framework, our discussions produced a number of outcomes which are summarised in the following.

Areas of Discussion

Availability of information and intelligence

Information and intelligence are the raw material of all police work. Only the complete and timely availability of terrorism related data enables police and other law enforcement agencies to monitor suspects, the movement of goods and financial transactions. In practice, however, the exchange of data between national and international law enforcement agencies continues to be reactive rather than pro-active. Indeed, in most cases, terrorism-related information is transmitted only following a specific request.

The exchange of terrorism related data should be governed by the principle of availability, meaning that a police agency which holds information and intelligence will make it available for the purposes of preventing and combating terrorism in another state, and that police officials can obtain the necessary data from other states without further ado. Needless to say, the implementation of this principle should be guided by a number of principles, such as the requirement that the exchange of information may only take place for the purpose of performing legitimate police tasks; the strict observation of established standards of data protection; the appropriate protection of sources; and the development of shared professional standards for access to the data.

Whereas such methods for exchanging terrorist related data and providing direct access to other states' national databases are already practiced among some states (for example, in the European Union), there are deficiencies at the global level. Making full use of new technologies, states should allow for mutual access to national law enforcement data bases, or – even better – create direct (online) access to regional and global data bases. Furthermore, police and other law enforcement agencies should be encouraged to store information and intelligence on terrorists and terrorist organisations in these international data bases.

Prevention, preparedness and crisis management

Prevention is an indispensable part of fighting terrorism. The scope of prevention, however, is very wide, and responsibilities are shared by a large number of public and private institutions. It is essential for the police, therefore, to focus on measures in which the police possess capacity and experience.

The unique strength of the police lies in its permanent contact with the population and different social groups. In order to detect radicalisation processes and the gradual change towards a more hostile attitude, it is necessary for the police to develop a good 'antenna function'. In this respect, only community policing and the establishment of a permanent dialogue with minorities make effective prevention and early intervention possible. In addition, national and international instruments for collecting, analysing and comparing information on terrorist ideologies and their supporters should be created in order to support these efforts.

Major terrorist events usually have significant international ramifications and any international counter-terrorism strategy should therefore include a 'preparedness programme'. National preparedness programmes – which exist in some countries, but not in others – need to be linked to an international concept of preparedness. Being the first at the scene of the attack, the police have a key role in this respect.

The dangers resulting from the proliferation of weapons of mass destruction and the knowledge to build and use lethal weapons pose a particular challenge. Given its limited human and technical resources, the police should enter into national and international partnerships with both private and public institutions in order to provide the best possible protection. Emergency measures as well as internationally agreed plans for co-ordinated response need to be worked out in cases where more than one state is affected. In particular, police forces and other competent authorities should set up an international rapid alert system for nuclear, radioactive, biological or chemical attacks to allow for the prompt notification of alerts and consultations on counter-measures.

The effective management of major terrorist events requires international arrangements for mutual assistance, which should include an assessment of capabilities (availability of expertise and technology in the police and other public services), the stockpiling of equipment and material, joint training, joint exercises and operational plans for crisis management by the police and other law enforcement agencies.

Strengthening operational police co-operation

The international co-ordination of operational counter-terrorist activities by the police and other law enforcement agencies must be strengthened. This is of particular relevance when it comes to the crucial task of denying the terrorists particular regions or states as sanctuaries in which to prepare attacks in other countries. Consequently, border security is one of the most important tools with which to prevent

the terrorists from entering into (or transiting through) particular states:

- The quality of travel and transport documents has to be improved in order to prevent and detect counterfeiting. These documents need to be standardised and allow for computer supported control.

- Border police must be trained more thoroughly.

- Data on terrorists, their travel routes and travel documents needs to be made available to all police forces concerned (see above).

- Internationally agreed procedures and methods should be established for the appropriate handling in cases of suspicious entry and transit.

Another major issue is the investigation of terrorist activities and crimes. In most states, the police are not yet sufficiently trained, equipped and adapted for the difficult, long-lasting and far reaching investigations conducted against international terrorists. In order to help address these deficiencies, best law enforcement and police practices in prevention and investigation need to be shared. In addition, an international peer review system could be established.

Since terrorism has 'gone global' (see above), the investigation of terrorist acts and activities of terrorist organisations has acquired an international dimension, which should be systematically developed:

- International intelligence and investigation efforts need to focus on specific target groups of terrorists. International law enforcement organisations and offices (such as Interpol or Europol) could be involved in these investigations in order to maximise the use of available data, expertise and facilities. Indeed, while the implementation of coercive measures would remain with national police forces, international organisations may be invited to co-ordinate these investigations.

- It may be useful to establish international investigation teams that will focus on the most threatening activities of international terrorist organisations. Models for such international task forces are the 'joint investigation teams' in the European Union. The mandate of these teams is politically and legally defined by the European Union, and Member States have already had initially positive experiences with this modality.

- Special international investigation programmes should concentrate on specific subjects, such as the recruitment and training terrorists, the financing of terrorism, the communication between members of terrorist groups, travel and transport, as well as the use of weapons and explosives.

Strategic analysis, threat assessment and risk analysis

Law enforcement agencies require a counter-terrorist strategy that is embedded within a comprehensive, balanced and multi-disciplinary approach – an approach which connects prevention, preparedness and investigation. A new way of establishing such a holistic strategy is the concept of 'intelligence-led policing' which links the collection of data with strategic analysis, resulting in threat assessments and, in its final consequence, the application of law enforcement measures:

- The strategic analysis of terrorism enables states and their law enforcement agencies to be better prepared for the challenge of modern terrorism, which depends on a thorough and timely definition of the specific risks for states, societies, economies as well as for individual citizens.

- The strategic analysis of terrorism will result in political decisions, action plans, legal measures, and also in concrete recommendations for police activities to make best use of resources and to improve the international co-operation between law enforcement agencies.

- The strategic analysis of terrorism is based not only on information and intelligence from the police and other law enforcement agencies, but also on data from the security services. In fact, the potential success of strategic analysis – that is, the effectiveness of threat assessments and risk analysis – depends heavily on the availability of terrorist related data from a wide variety of sources.

In our view, a network should be created which integrates national analysis centres, cross-border intelligence and law enforcement cells, regional offices and international centres. This network should be tasked to establish a 24/7 system for terrorist warnings. It should also prepare a directory of the existing institutions of co-operation in the area of fighting terrorism, making use of the directories at the UN, Interpol and the European Union.

Policy Recommendations

Roles and responsibilities of the police

As mentioned above, the counter-terrorist activities of the police need to be comprehensive, pro-active, and occur simultaneously at the local, national and international levels. In particular, it is the responsibility of the police to:

- Prevent terrorist activities.

- Ensure preparedness.

- Respond effectively to terrorist attacks, so that it becomes possible to limit the damage, reduce further risks, and re-establish public order.

- Investigate all forms of terrorist crimes in order to identify, trace and arrest terrorists and prosecute them before the courts.

However, it should be noted that the police do not operate in a vacuum and will fail in their responsibilities unless adequately supported. In this respect, the provision of political and public support, appropriate legal instruments and sufficient resources are pre-conditions for the police's effectiveness in fighting terrorism.

Improving co-operation

- The global threat from terrorism requires international solidarity, mutual trust and the willingness for cooperative support. As a matter of principle, therefore, police forces should take into account the security interests of other states, thus helping to prevent and combat terrorist attacks against other states and their citizens in addition to attacks against their own.

- Existing channels and instruments for international co-operation should be improved before new institutions and instruments are created. Officials and law enforcement agencies should be made aware of the capabilities offered by established regional and international institutions and agencies.

- In order to avoid 'security gaps', states should enter into agreements to allow for mutual assistance in emergencies and the co-operation of their police forces, including the secondment of experts, stockpiling, joint training and exercises. In addition, it is necessary to foster partnerships among different police services as well as between the police and judicial agencies, security services, the financial sector and private business.

- Police services across the world need to engage in capacity-building. Distinguished units should be invited to assist smaller countries, for example in the standardisation of travel and transport documents, or the creation of joint investigation teams.

- Legal standards need to be improved by harmonising penal and police laws, as well as by ratifying and implementing the relevant United Nations Conventions and Protocols and similar regional agreements.

- In order to facilitate intelligence-led counter-terrorist policing, there should be agreed standards and methods of analysis in a network of national analysis centres and international intelligence cells supported by a 24/7 system for terrorist warnings and related intelligence.

Exchanging information and intelligence

- There is an urgent need for law-enforcement agencies and the intelligence services to share information at the operational level and to co-ordinate the resulting activities. This could be accomplished, for example, by establishing regular, informal forums between these services both at the national and the international levels.

- Exchange of data should be governed by the principle of availability with full respect for legality, integrity, source protection, confidentiality and data protection. This means facilitating the timely sharing of information and intelligence, enabling the compatibility of law enforcement and intelligence data bases, allowing direct access to regional data bases, and creating global data bases.

- Co-operation with non-democratic countries should not be discouraged. However, the relationship needs to be more restrictive than the collaboration with other democracies, especially when it involves the exchange of personal data. The decision to co-operate should be made on a case to case basis, including criteria such as (1) possible obligations to co-operate due to the existence of binding agreements, (2) the specificity of the threat, (3) the credibility of the threat, (4) and the gravity of the possible damage.

Preparedness

- The police needs to develop its 'antenna function' in society by intensifying its role in community oriented policing. It needs to establish a permanent dialogue with minorities which may serve the purposes of detecting radicalisation and terrorism recruitment, as well as isolating radical groups and calming down tensions in situations of crisis.

- It needs to be involved in the creation of early warning systems, institutions and specialised units for CBRN (chemical, biological, radioactive, nuclear) attacks. The police should also be encouraged to develop strategies and concepts that enable co-ordinated emergency measures.

Members of the Working Group

- Jürgen Storbeck, Federal Ministry of the Interior, Germany (co-ordinator)

- E.S. Akerboom, Police for Brabant-Noord, The Netherlands
- Willy Bruggeman, Benelux University Centre
- Randolph P. Eddy, Center for Tactical Counter-Terrorism, USA
- Christer Ekberg, Swedish Criminal Intelligence Service
- Juan Hidalgo, Senior Advisor to the Spanish National Security Advisor
- Gary Lafree, University of Maryland, USA
- Gilles Leclair, Anti-Terrorism Co-ordination Unit, France
- Antero Lopes, United Nations Department for Peacekeeping Operations
- Denise Sorasio, European Commission

Intelligence

By Brian Michael Jenkins

Our discussions took place in the shadow of perceived intelligence failures, dramatically revealed in the 9/11 and Madrid attacks, but also in the erroneous intelligence connected with the Iraq War – the failure to find weapons of mass destruction or to anticipate the ferocity of the Iraqi resistance. These perceived failures have led to intense examination of the intelligence services by various government commissions, legislative committees, and internal boards. Official inquiries have been augmented by a broad public discussion of how to 'fix' intelligence.

Although it could be expected that the impressive roster of experienced intelligence professionals and analysts represented in the working group had strongly-held views on the right lessons to be learned from past failures, and that these may differ from what has appeared in the public discourse, our focus was on how we might significantly improve intelligence in the future. Our objective was to offer observations and recommendations that are more specific than mere exhortations to share more information, think more creatively, be smarter analysts, respect civil liberties, yet are above the level of craft. What was remarkable, given the diversity of the group, was the degree of consensus among participants. The following is a summary of our discussions and some of the key recommendations that emerged.

Areas of Discussion

Despite the inherent difficulty of collecting and analysing intelligence about terrorists, significant progress has been made in reducing the operational capabilities of the global jihadist movement responsible for 9/11 and 3/11 and a continuing terrorist campaign across the globe. Terrorist leaders have been apprehended, numerous operatives detained, finances squeezed, training disrupted, preparations for future attacks uncovered, plans thwarted. There are lessons from success as well as from failure.

The role of intelligence

We defined the task of intelligence broadly, perhaps more broadly than its consumers. Policymakers often look to the intelligence services to solve their policy problems: if all attacks can be thwarted, if all terrorists can be eliminated, difficult policy choices may be avoided. This can lead to asking the wrong questions.

While intelligence plays a critical role in assisting policymakers to understand and frame the challenges they face, and in reducing the adversaries' capability to carry out attacks, good intelligence cannot by itself solve political problems. Intelligence managers must contribute to a fuller understanding of policy problems, but they also must assist in shaping policy considerations. Intelligence-tasking should reflect a very wide perspective, even broader than policymakers might prefer, identifying and illuminating issues which are being overlooked, or which are inconvenient and, for political reasons, are being ignored. In addition to getting the right answers, intelligence must make sure their customers are asking the right questions.

Adapting to new threats

Part of the 'failure' of intelligence before 9/11 was a failure during the previous decade to fully comprehend and adapt intelligence to a changing threat environment populated by a growing and increasingly dangerous jihadist movement, extremists who were increasingly willing to engage in large-scale indiscriminate violence and increasingly fascinated with weapons of mass destruction, the first tendrils of a nuclear black market, new combinations of corruption, organized crime and political extremism, and the emergence of new technologies that would create new vulnerabilities as well as facilitate criminal and terrorist activity. It is the strategic dimension of the threat characterised by destructive ideologies, global enterprises mobilizing significant resources, and with a capacity for long-term planning that requires new approaches to security and intelligence.

This threat is dynamic and diverse. While it is the jihadists who currently command our attention, and are likely to do so for years, ten years ago, an odd religious sect in Japan, not considered a terrorist organization, carried out the first large-scale chemical attack on a civilian population in Tokyo. We cannot confidently forecast what the terrorist threat will be ten years from now, where its center will lie, or how it will manifest itself.

Old models of intelligence collection and analysis will not work. We no longer confront hierarchical, highly-structured foes, mirrors of our own institutions but rather shifting networks, constantly mutating configurations and constellations. Our intelligence services must be agile, capable of rapidly creating their own new networks for the collection, analysis, and exchange of intelligence, self-initiating ad hoc assemblies that transcend institutional and national boundaries. Intelligence services will have to learn how to get smart fast, exploiting a variety of closed and open sources, both old-fashioned espionage and collection systems employing the newest technology, in-house and external consultants, current and perhaps retired staff.

Oversight

The scale of destruction in the hands of today's terrorists – or possibly greater destructive power that might be possessed by future gangs whose grievances, real or imaginary it may not always be possible to satisfy – push us from reliance on protection and prosecution to prevention and pre-emption. This places a greater burden on intelligence, which will require, in some circumstances, greater latitude.

That, in turn, increases the requirements for strict oversight. If intelligence collection must necessarily be more aggressive and cannot be hobbled by rigid rules that try to anticipate every conceivable circumstance, then sound judgement must be exercised by intelligence managers who are monitored by elected authorities. New technologies that allow more intrusive covert surveillance (nanotechnology, for example) or the exploitation of vast electronic databases will increase the demands on oversight.

Organization

Current threats, not surprisingly, do not match how we have organized national security and law enforcement activities over the past half-century. The old boundaries between law enforcement and counter-intelligence, between domestic and foreign intelligence already have begun to blur. We are operating in a new domain where intelligence, law enforcement, and military operations come together. New rules will be required, but without creating unwarranted obstacles to intelligence operations.

Intelligence activities are organized differently in each country, reflecting unique historical circumstances. Most countries have multiple intelligence-gathering agencies with divided responsibilities. These protect the state and citizens against a too-powerful monolithic intelligence service and they ensure 'multi-perceptivity', although they may complicate intelligence sharing and international co-operation.

There are some overall trends in organization. Without touching the collecting agencies themselves, scaffolds have been erected – new centres staffed from multiple agencies – to encourage and facilitate sharing and combine analysis. These centres also are appearing at the international level, such as in Europe. Saudi-Arabia has ambitiously proposed the creation of a worldwide center to share intelligence on terrorism.

To improve co-ordination, several countries have established new national-level coordinators to oversee the activities of the various entities involved in intelligence collection. It is not clear whether these co-ordinators are to be managers of intelligence enterprises or directors of intelligence. Gains in co-ordination may be offset by creating additional layers of demands and diversions of talent and expertise.

International co-operation and sharing

While some terrorist groups can be dealt with locally, within the confines of a single state, perhaps with the co-operation of its immediate neighbours, the most dangerous terrorist enterprises and the global phenomenon of terrorism – in particular the escalation of terrorist violence itself – will require a sustainable global counter-terrorist strategy. International co-operation is not a desirable end – it is an absolute prerequisite to success, as demonstrated in the successes against the jihadist enterprise since 9/11, which reflect unprecedented unanimity of focus. This co-operation can be further institutionalized.

There are many paths. These include adding terrorism to the agenda of existing alliances and international organizations, which to a large extent already has been done; expanding bilateral and multilateral arrangements for the exchange of intelligence; and creating new multilateral entities. But this raises an unresolved question of whether the creation of multilateral centres will facilitate or impede international co-operation with countries beyond their membership. Will the creation of a new European intelligence centre complicate existing trans-Atlantic bilateral and current multilateral exchanges, which ultimately rest upon confidence and trust, not formalities?

While collection will remain in the hands of individual national intelligence services for the foreseeable future, despite some suggestions to create a single European intelligence service, greater fusion of analysis does seem possible. This has worked at the national level. The old style of sharing only the processed, analysed, and scrubbed finished product (on the presumption, probably correct, that everyone else's service was penetrated) can no longer be the operational code. We need to re-examine the classification and clearance process to see if barriers to sharing can be removed or new categories can be created to allow the more rapid sharing of counter-terrorist intelligence.

Reorganization by itself is not a solution. There is no single organizational model that guarantees good intelligence, and the process of reorganization itself may get in the way of improving intelligence. Incremental adjustments may be better than radical overhaul or entirely new structures. Above all, more than rearrangements of their organizational diagrams, cultural revolutions are required inside the intelligence services.

Police

We agree on the need to improve intelligence capabilities at the local level. This means creating intelligence collection and analysis capabilities within national and local police departments. Police know their territory, are likely to be more ethnically diverse, closer to the communities they serve, more sensitive to local changes, more acceptable to local community leaders, younger and more willing to change. They need support, training, and rules, and they will need to be better connected with the national intelligence services and with each other.

The creation of direct police-to-police networks nationally and internationally is not always readily accepted by national-level investigative or intelligence services. To those accustomed to compartmentalised worlds, flat networks seem chaotic, even dangerous. But there have been a growing number of direct liaisons among some of the major police departments in cities where the terrorist threat is obvious. This should be encouraged.

Connecting the cops can also take the form of counter-terrorism workshops and best practices sessions that bring together major metropolitan police departments, starting with a few participants and gradually expanding membership, but avoiding becoming large unwieldy conferences.

The role of analysis

While there is some debate on how or how much analysis can be improved, there are again some areas of consensus, which have important implications for the organization of intelligence and personnel management. Analysts should be brought closer to those in charge of collection, not isolated in separate worlds. The separation was possible when targets and tasks could be clearly delineated, but it does not work well where collectors are less certain what to look for and analysts often need to know subtleties not always conveyed in written reports.

Analysts must also be broadly educated, encouraged to think imaginatively and critically, not driven into narrow corridors by too narrow questions or too narrow delineations of the need to know. And they must be able to autonomously organise and reorganise themselves around leads and potential new threats, calling on reinforcements, from the outside when needed.

Civil liberties

As a final comment, while we recognize that rules will be changed to meet new security challenges, that intelligence by its nature cannot be too rigidly controlled, although oversight is absolutely essential, we are highly sceptical of the rhetoric of war, of secret arrests, secret detentions, of the denial of any legal process or judicial review, of dismissal of international conventions as they apply to treatment during interrogation – which often is excused as necessary to collect intelligence.

We question the utility of the measures, the quality of the information thus obtained, and the heavy cost paid when patent abuses are revealed, as inevitably they will be. Good intelligence does not require the suspension of civil liberties or of human dignity.

Policy Recommendations

The world's democracies must recognize that preventing catastrophic violence by terrorists has become one of the most important tasks for governments and their intelligence services

True, small arms still kill more people than the sum of all terrorist attacks thus far, but the attacks of 9/11 and 3/11, which caused significant casualties and destruction, also had a profound effect on the economy, society, even how people view their government. The scale of death and destruction, if terrorists were to engage in catastrophic attacks involving chemical, biological, radiological devices or worse, if they were to acquire and use nuclear weapons, could imperil democracy itself. Intelligence is democracy's first line of defence.

Democratic governments must provide a stronger legal basis for early intervention to prevent terrorist attacks of great magnitude

The increasing determination by terrorists to engage in large-scale indiscriminate violence, and their growing fascination with weapons of mass destruction, propels society from relying exclusively on physical protection of targets and prosecution of offenders after a terrorist attack, to prevention by means of early intervention, for which most current legal regimes are weak and ill-suited, and which also is contrary to the culture of law enforcement-oriented, case-driven investigative services. Intervention now may take the form of investigation prior to the presumption of criminal activity, arrest for violation of conspiracy or illegal association laws, deportation, or temporary preventive detentions. However, the intelligence working group categorically rejects extra-judicial detention, declaring that such measures do not help the intelligence community.

Led by the democracies, all nations must co-operate in combating terrorism by ensuring that information about terrorist organizations and their supporting criminal infrastructures is shared within and among nations

It is the duty of all nations to maintain their own national security, but it is also their duty to actively assist in the security of all other nations – terrorism threatens everyone's security, which we regard as a fundamental human right. However, mere exhortations to share information seldom work in institutions that must, of necessity, protect sensitive sources and methods. Information-sharing must be not only encouraged but facilitated. New multi-agency staffed structures erected to facilitate exchange across institutional lines within countries seem to be working, but need continued support. Exchanges between national services will always be on the basis of trust – the most sensitive unprocessed information may be exchanged though bilateral and informal procedures. The creation of ambitious multilateral structures seldom works. Networks must grow organically. However, regional centres for analysis stand more chance of success.

Clearance and classification regimes, while necessary, must be reviewed

The regimes developed during the decades of the cold war may no longer apply to today's asymmetric, fast-moving, terrorist threat. Instead of avoiding all risks, we must accept trade-offs to ensure the timely dissemination and exploitation of information.

The intelligence culture must be transformed

While it is true that today's threats do not match yesterday's intelligence structures, re-organization, which political leadership sometimes mistakes for progress, cannot by itself solve the problem, and may become a distraction. Meeting a dynamic and constantly mutating threat will require agile and adaptive institutions, capable of autonomously organizing and re-organizing themselves around new challenges as they arise. In some cases, it may mean less organization rather than more organization, less hierarchical, flatter structures, staffed by quick-footed intelligence managers.

Public education about the purpose and role of the intelligence services must be made a vital component of national security

At the same time, policy makers must learn the capabilities and limitations of intelligence in dealing with difficult terrorist foes. If, in order to meet the threat of possibly devastating terrorist attacks, the intelligence services must adopt more assertive actions, it is essential that they have continued public support. There is a natural tendency in open democracies to mistrust intelligence services, which engage in secret activities. Suspicion is exacerbated by fictional depictions of omnipotent secret organizations operating outside of the law. Frequent resort by political leaders to what may come to be seen as scare tactics, add to distrust. Moreover, while intelligence successes are difficult to count and seldom recorded, 'failures' are obvious. Credibility and trust are necessary corollaries to competence.

Democratic governments must ensure adequate and appropriate control, review and oversight of intelligence operations, even in heightened threat environments

These take many forms from executive control to judicial authorization, to parliamentary review, to internal inspection. Oversight does not mean the formulation of volumes of rigid rules intended to cover every contingency, which can become obstacles to effective operations. It does require proper lines of authority and responsibility, and education of those involved in oversight. The intelligence services see these relationships as a means of protection and support against ill-founded and ideologically-motivated attacks.

Combating terrorism requires the orchestration of both suppression and political strategies

Those who employ terrorist tactics diminish their own legitimacy--all terrorist campaigns are, by definition, outside the law. The need to suppress terrorism makes no judgement about causes. Political leaders must accept that intelligence can reduce the operational capabilities of terrorists, it can contribute to the containment of the terrorist threat, it can buy time, but it cannot eliminate or resolve fundamental political conflicts or relieve political leadership from the need to address the underlying issues that contribute to terrorist proselytization, recruitment and, in some cases, popular support.

Members of the Working Group

- Brian Michael Jenkins, RAND Corporation, USA (co-ordinator)

- Richard Chua, Internal Security Department, Singapore
- David Cohen, New York Police Department and CIA (rtd.), USA
- Barbara Haering, Swiss Parliament and OSCE Parliamentary Assembly
- Michael Hurley, CIA and 9/11 Commission, USA
- Ephraim Kam, Jaffee Center for Strategic Studies and Israel Defense Force (rtd.)
- Alexandr Kostin, Ministry of Interior, Russia
- Christina Landaburu, National Intelligence Center, Spain
- Alfredo Mantici, Servizio Informazioni Generali e Sicurezza, Italy
- Francois Mermet, Direction Generale de la Securité Exterieure (rtd.), France
- Takashi Minami, Advisor to the Prime Minister, Cabinet Intelligence and Research Office, Japan
- Michael Oatley, MI6 (rtd.), United Kingdom
- Jean-Jacques Pascal, Direction Centrale de Renseignements Generaux (rtd.), France.
- Wolbert Smidt, German Forum for the Discussion of Intelligence and Bundesnachrichtendienst (rtd.), Germany
- Greg Treverton, International Security and Defense Policy Center, RAND Corporation, and National Intelligence Council (USA), USA
- David Veness, United Nations and Scotland Yard (rtd.), United Kingdom

In addition, the Working Group benefited from its external reviewers and members, including:

- Richard Barrett, Al-Qaida/Taliban Monitoring Team, United Nations
- Rolf Ekeus, UNSCOM Weapons Inspection Mission to Iraq
- Ward Elcock, Deputy Minister of Defence and Canadian Security Intelligence Service (rtd.)
- Michael Goodman, King's College London, United Kingdom
- Raymond Kendall, former Secretary General of INTERPOL
- Peter Neumann, King’s College London, United Kingdom
- David Wright-Neville, Monash University, Australia

Military Responses

By Sir Lawrence Freedman

The difficulty for the group considering military responses to terrorism is that the issue touches on the most fundamental questions of how the phenomenon of terrorism is best understood and how the challenge it poses is best addressed. As a strategy, terrorism is designed to use actual or threatened violence to cause psychological effects which can be turned into political gains. There are many permutations, depending on the forms of violence used and its regularity, the impact on the victim population, the sources of resilience, the nature of their political demands, and whether or not a government could respond to them.

The challenge is to find forms of response to terrorism that are both efficient and conform to liberal democratic principles. It would be nice to believe, and better to prove, that such responses are inherently superior, as they establish legitimacy and assert a better way of life, just as the terrorists' methods are not just tactics but reflect their malign philosophy. No doubt, these normative implications of the counter-terrorist methodology adopted influenced our group's discussions.

Resort to military means poses in the starkest form the problem of the compatibility of liberal democratic principles with a counter-terrorist campaign. The problem is aggravated by both the operational requirements of armed forces and the particular problems posed by terrorist methods. We therefore started from the proposition that the preferable measures are civil rather than military, drawing on established legal frameworks, conducted by the police and supported by intelligence agencies. The challenge was to identify when it is appropriate to go beyond this preference and accept the need to define the contest as an effective war, which – to a significant degree – might be decided by military means.

Areas of Discussion

Two models of terrorism

To keep terrorism as a police matter within the confines of civil society, it would be best if it could be considered as a form of criminality, which means that the most appropriate responses are found through the methods of law enforcement, involving domestic intelligence, the police and the judiciary. For this model to work, the terrorists must act as criminals. This may be literally true in the use of robbery and extortion and even kidnapping to obtain finance. Some groups that start off as political zealots may decide over time that criminality is more profitable; some groups, such as those dealing in drugs, may develop political interests. The main point, however, about treating terrorists as criminals is that they should be denied political status, instead making their activities an issue for the courts and unfit for any dialogue with government. The criminal definition, therefore, has important implications in terms of propaganda as well as the choice of counter-measures. It is normative as well as descriptive.

The criminal treatment is also likely to be appropriate as long as the terrorists adopt the standard Leninist organisation of small cells of militants, aiming to hide within the host population and emerging

to undertake occasional operations against available targets. The intelligence job is to pick out the terrorists before they do much damage. To prevent damage, key targets must be protected. The most basic counter-terrorist work in the West therefore involves intelligence gathering and isolating people believed to be engaging in terrorist acts (even before there is good evidence).

The terrorist preference is normally to be considered as warriors. This is why even with a small number of militants they may have a political wing and adopt military-style structures. Their campaigns are presented as a form of insurgency, directed against the sources of state power. In a true insurgency, the terrorists would be linked to a broader-based movement probably involving a number of forms of activity. To the extent that this is the case, the most appropriate response must be found through the methods of counter-insurgency, involving armed forces. Thus, once it becomes necessary to rely on military means, it can be said that the terrorists have already been granted a propaganda victory.

Degrees of support

While it may be preferable to cut the terrorists down to size rhetorically by branding them as common criminals or, at most, political extremists with violent tendencies, at some point such language may be contradicted by events. At the start of the US occupation of Iraq, those engaged in violence were denounced as criminals, disgruntled *Ba'athists* and opportunistic *Jihadists,* but eventually the violence became too regular and sustained, and with too much support, for it to be described as anything other than an insurgency. Again, a key test of the nature of the threat lies in the degree and nature of public support.

Under the criminality model, the local population can be assumed to be hostile to the terrorists, while under the counter-insurgency model the local population is potentially supportive. The circumstances in which a local population may be supportive of terrorists will be where the state has lost authority and legitimacy, or is facing limits, for example as a result of a secessionist movement or one that is divisive (that is, based on ethnicity/class/religion/ideology), or when the terrorists are using the territory of another state as a sanctuary. The distinction may be less than clear-cut: *Al Qaeda* presented itself in a criminal form while mounting offensive operations in western countries, while as a relatively organised army (albeit on the defensive) in protecting their Afghan base. In practice, the more these groups can operate as an insurgency the less they need to rely on terrorist tactics. That is, they can use attacks on the armed forces/police to undermine the authority of the state and do not need to terrify the civilian population.

In terms of traditional guerrilla warfare, the objective of the insurgents is to play for time while they build up their own strength and sap that of their enemy. This will be done through ambushes combined with defensive measures to avoid capture, tempting the enemy forces into repression on the assumption that this will turn the people in their direction.

Counter-insurgency theory defines the role for the military, which is normally described in terms of 'hearts and minds' versus 'search and destroy'. A 'hearts and minds' approach requires that the military gain the trust of the local people by promoting good works in order to leave the militants isolated, bereft of recruits and practical support. The alternative, as defined in Vietnam, has been a tougher doctrine, known as 'search and destroy'. This has tended to be more successful at destroying than searching, but so lacking in discrimination that as many recruits were generated for the enemy as eliminated. The relationship with the local population therefore defines the character of the terrorism and the most appropriate form of counter-terrorism.

Managing counter-insurgency

At some point, a failure to contain terrorists as criminals will allow them to appear as insurgents. Should a counter-insurgency approach become necessary the hearts and minds approach (as described above) is closer to liberal democratic norms. It carries less risk of 'collateral damage' and a greater possibility of separating the militants from their possible sources of popular support, and so impeding their recruitment and financing.

It is, however, important to note that while poor tactics and doctrine can feed rather than starve an insurgency, the political measures necessary to make a hearts and minds strategy work can not in themselves come from good doctrine and tactics. The political context is crucial. The sort of light touch associated with hearts and minds operations will not work in support of a government that is perceived to be antagonistic, and it can put forces in danger if undertaken against a hostile population. It is not enough to take off helmets and walk with a smile down the main streets.

The British Army, for example, is normally assumed to have learned lessons from dealing with the IRA in Northern Ireland based on a hearts and minds approach that it has sought to apply in wider peacekeeping operations and latterly in Afghanistan and Iraq. In none of these cases has it provided a means of defeating an enemy: what it has done is help contain a potentially dangerous situation and create the conditions for more focused political measures to be applied. These parallel political processes, designed to build trust between the authorities and civil society are essential complements to any counter-insurgency campaign.

Even if we accept that a democratic approach to counter-terrorism can be identified – and that it is generally more effective as well as more principled – many states facing serious challenges are likely to feel that the choices they are confronted with are not so simple. This leads to a potentially significant proposition. By and large military methods are not that important when countering terrorism within liberal democracies. Elsewhere, however, terrorism may well emerge as a consequence of a violent conflict. In practice, it has been the failure of counter-insurgency in a number of non-western countries – Kashmir, Chechnya, Indonesia as well as Afghanistan, Iraq and Palestine – that has created the conditions under which *Jihadism* has prospered. As an asymmetrical strategy, terrorism has long offered a means not only of hitting back against the immediate enemy but also of internationalising a conflict and drawing attention to a particular plight. This, after all, was the purpose behind the start of modern Middle Eastern terrorism that was used effectively by the PLO after the 1967 war. This is one reason why democracies can develop stakes in the management of apparently parochial local conflicts.

The conclusion must be that, in certain cases, the military instrument can be helpful in responding to terrorism, but for most of the time these are likely to take the form of contributions from specialist services provided by the armed forces. When Western forces find themselves engaged directly in counter-insurgency it is best that they opt for a hearts and minds approach. It is important, however, to be realistic about what this can achieve when there is good reason to suppose that the hearts and minds of at least sections of the local population have been lost some time before. At any rate, whether a 'hearts and minds' or 'search and destroy' philosophy is followed, the most important accompanying measure is to establish political processes that address underlying grievances even while avoiding direct negotiation with terrorist groups.

The military instrument is most likely to be used, however, in conflicts in which western countries have yet to be involved and where conditions are altogether harsher. As the wider community has a stake in the conduct and outcome of these conflicts, external actors may well decide that they must get involved. If they do so, then the choices they face may be difficult – between a harsh regime and

a vicious opposition. To avoid such choices, it is necessary to not only to develop early warning of emerging conflicts, but to encourage the spread of best practice on handling political violence so that over-reaction does not turn a dangerous situation in something worse.

Key Principles and Recommendations

Tackling popular support

All successful strategies for dealing with terrorism require that the terrorists be isolated – from their potential sources of recruits, supplies, finance and targets. They therefore also depend on the attitudes of the populations within which they plan and conduct their operations. The challenge is to ensure that measures designed to increase the physical isolation of terrorists and limit their operational capacity do not have the contrary effect of increasing their popular support, thereby making the process of isolation harder to achieve. In the short-term drastic measures may on occasion be needed to prevent a great tragedy: over the long-term the objective must be to create the conditions where terrorism can not flourish.

As a multi-faceted problem, terrorism requires a range of responses, some of which will be forceful. Even when forceful measures are involved, the preference must always be to treat terrorism as a form of criminality to be handled through the established system of law enforcement. Casting terrorists as criminals helps in their delegitimisation. Conversely, the need to resort to armed force by itself may raise their status.

Roles for the military

There are certain circumstances where military responses will be appropriate. These will always be complementary to other responses and will never be sufficient by themselves. Even when counter-terrorism leads to a large-scale military campaign, parallel political processes will always be essential as a means of addressing the sources of conflict.

The military have a role when:

- Police forces cannot cope with the threat because it risks being overwhelmed by either its quality or quantity.
- Police forces are deemed to be corrupt, incompetent or sectarian in nature, and distrusted by the target population.
- The threat has acquired a cross-border dimension, and may involve a wider interaction with the region or the international system as a whole.
- There are particular needs or capabilities which only armed forces can meet, relating to intelligence-gathering and analysis, communications, logistics, the provision of a sizable, disciplined, and trained force.
- Counter-terrorist operations require unique skills and capabilities, for example special force units prepared to deal with hostage or hijacking crises, or naval forces interdicting attempts to smuggle weapons into areas of conflict.

These responses will take on distinctive forms at different stages of the development of threat. Broadly speaking these are:

- *Anti-terrorism measures*, which are essentially defensive and are geared to reducing the vulnerability of individuals, property and critical infrastructure (including military assets) from possible attacks. Here, intelligence as well as guard duties may be of crucial importance.

- *Consequence management*, supporting the civil authorities in mitigating the effects of a terrorist act. Military resources, including communications and logistics, are likely to be called upon in the event of any major civil emergency, but they may have a special role if unconventional weapons have been used. These might include decontamination or the evacuation of civilians.

- *Counter-terrorist measures*, acting to undermine, disrupt and – if possible – eliminate terrorist groups.

Of these, the first two categories are relatively unproblematic, although they still require detailed preparation and planning. The third category, which may well see armed combat, is the most controversial.

Military force in democratic societies

In democratic societies, any military use in the counter-terrorist role must meet demanding standards:

- It must be accountable to government, with reliable forms of oversight and monitoring. If operating within national borders, it must clearly be seen to be acting in support of the civil power and not as a semi-autonomous actor.

- This will best be achieved through co-ordination with civil agencies and international bodies. A cross-regional dialogue should reduce the possibilities of terrorists using the territory of another state as a sanctuary. The problems of intelligence sharing must be addressed as a necessary condition for all responses to terrorism, including ensuring that military operations are successful and do not lead to misplaced and counter-productive activities.

- This requires a clear national and international legal framework. While the emerging international framework can be developed through the UN, as well as bilateral discussions, it must be responsive to the realities of military operations and their changing character. Otherwise it might be discredited. An example of an anticipatory framework would be protocols to facilitate hot pursuit across borders.

- The ability to act within legal frameworks and with a sense of restraint, including sensitivity to the local political environment, places great demands on training and doctrine.

Transformation of the armed forces

We do not see a need for dedicated counter-terrorist forces as special branches of the military establishment. Rather we would see this role, as well as the anti-terrorist and consequence management roles, as fitting in with what might be considered to be the emerging model for Western armed forces. These are moving away, on the one hand, from models geared to conventional warfare between major powers (with large units, organic and heavy firepower, geared to defeating a comparable force in battle) and, on the other hand, models geared to peace-keeping (with only a limited capacity for self-defence and dependent upon local consent).

The experiences of the humanitarian interventions as well as the counter-terrorist operations of recent years point to a need for lighter, more agile forces, drawing on modern technologies (for example in combining the ability to track targets and attack them with precision) while understanding the difficulties when it becomes necessary to mingle with civil society and the overall political context within which operations are conducted.

By the same token, we would note that even many policing tasks have to be conducted at a higher intensity than hitherto, and that these are often those which touch on the interaction between terrorist groups and related forms of criminal activity, in particular drug, arms and people trafficking. Just as drug cartels can seek to sustain themselves through terrorism, so can terrorist groups seek to sustain themselves through drug trafficking.

Accompanying measures

In a number of parts of the world, the military are often used in what are claimed to be counter-terrorist operations without the appropriate forms of accountability, legal, normative and international frameworks, doctrines and training. Such operations may well aggravate rather than mitigate the problem by alienating the local populations and undermining the credibility of the military, so that they come to be seen as being more threatening than the military. These are often the conflicts that give rise to terrorist groups that seek to internationalise their cause though activities in other countries.

Because the wider international community has a stake in the successful management of these conflicts it should seek to disseminate best practice in counter-military operations. It should also seek to ensure that the military provide elements of the solution rather than the problem through the activities associated with security sector reform and disarmament, demobilisation and reconstruction.

Members of the Working Group

- Sir Lawrence Freedman, King's College London (co-ordinator)

- Miguel Angeles Ballesteros, Senior Staff College of the Spanish Army
- Virginia Gamba, Safer Africa, South Africa
- Louis Gautier, former military adviser to the French Prime Minister
- Roger Karlsson, Swedish National Defence College
- Gustav Lindstrom, European Union Institute for Security Studies, France
- Satish Nambiar, United Services Institution of India
- Funmi Olonisakin, Centre for Democracy and Development, England
- Rahul Roy-Chaudhury, International Institute for Strategic Studies, England
- Andreas Vogt, Norwegian Institute for International Affairs
- David Wright-Neville, Monash University, Australia

Terrorist Finance

By Loretta Napoleoni and Rico Carisch

More than three years after the attacks of September 11, 2001, terrorist funding mechanisms and their networks remain obscure, the flow of money poorly understood, and no credible and effective strategy to prevent future attacks has emerged.

Most members of the working group attribute this failure to the inability of the international community to apply universally acceptable principles of governance that are solidly based upon democratic principles. Some members of the working group believe that a specialized ad-hoc organization within the United Nations – a forum for informed discussions about counter-terrorism financing strategies and international policies – may have produced better results than the current approach. Instead of pursuing a unified strategy under the United Nations umbrella, however, national efforts have fractured the UN Security Council's leading role and resulted in paralysis.

The following is a summary of our discussion as well as a brief overview of the principles and key recommendations which we hope will contribute to overcoming the harmful dissent that continues to prevent the implementation of an effective strategy at curbing terrorist financing.

Areas of Agreement

Obstacles to combating jihadist funding networks

The existing studies of terrorist financing provide no coherent or comprehensive understanding of the origins of *Jihadist* funding networks. Resting mostly on anecdotal accounts, there has been no effort yet to go beyond the analysis of isolated factors. At the same time, it has become clear that funding networks cannot be fully understood without exploring the linkages between their sources and the political factors that underpin them, including regional grievances, anti-Western sentiments and pan-Islamist aspirations:

- In its efforts to counter Western influence on Muslim countries, global terrorist organizations, such as *Al Qaeda* or the *Abu Nidal Organization,* have obtained funding from Libya, Syria and Iran, and are now believed to receive funds from a widely diversified group of constituencies and supporters.

- Palestinian groups (for example, the *Al Aqsa Martyr Brigades,* the Palestine Liberation Front, the Popular Front for the Liberation of Palestine, etc.) – sometimes in combination with Islamist organisations (such as *Hamas*) – are sponsored by expatriate Palestinians, private donors in Saudi-Arabia and the Gulf States, as well as Iranian and Muslim charities.

- Shiite militants opposed to Western influence in Lebanon, such as *Hezbollah,* obtain funding from Syria and Iran.

- Visions of a united Malayan archipelago – the so-called *Nusantara* – are spurred by South-East Asian terrorist groups, such as *Jemaah Islamiyah* and the *Abu Sayyaf Group*. They obtain funding through charities, ransom payments and the promotion of a regional Islamist economy. These efforts are bolstered by the regimes in Malaysia and Indonesia, which express similar pan-Islamic aspirations.

An analysis of global and regional terrorist funding shows that *Jihadist* funding networks have little or no formal structures in the Western sense, and that informal, personal initiatives are the bloodlines of terrorist funding. For this and other reasons, confronting terrorist financing in the Muslim world has been an uphill struggle. Only a quarter of the total amount of terrorist funds frozen since September 11, 2001, has been seized in the Muslim world. The working group believes that this constitutes a major failure, as *Jihadist* groups appear to continue their funding efforts through the Islamic economic system, that is, by using financial entities based in the Muslim world.

Indeed, in addition to the ideological motives discussed above, economic and institutional weaknesses in the Muslim world seem to have been at the root of the phenomenon. These include:

- The absence of technical and institutional capacities, especially in failed or nearly-failed states whose financial systems continue to operate in a regulatory vacuum. This has not yet been sufficiently addressed through international aid and assistance programmes.

- The lack of independence and transparency in judicial and political entities, as well as in the financial structures more specifically, which are a hindrance to the monitoring and enforcement of good governance and compliance.

- The non-existence of accepted financial standards in the Muslim world.

The 'war against terror funding'

Needless to say, efforts to combat terrorism predate the attacks of September 11, 2001. Over several decades, the United Nations has passed twelve conventions which cover a number of terrorist threats, ranging from civilian passenger aircraft to funding issues. The latter was addressed in the 1999 UN Convention for the Suppression of the Financing of Terrorism. The patchwork of multilateral agreements, however, has failed to generate a coherent strategy that would be capable of countering the informal nature of *Jihadist* funding mechanisms. Also, opportunities were missed to assist weak governments in enhancing their capacities to respond to terrorism.

September 11, 2001, did not prompt a new strategy to confront terror financing. The UN Security Council Resolution 1373 (2001), adopted under Chapter VII of the UN Charter, contained no new sanctions, but strengthened Resolution 1267 from October 1999 with which some of the financial assets of the *Taliban* and *Al Qaeda* had been frozen through a policy of 'smart sanctions'. The September 11 attacks accelerated the activation of the Monitoring Group, whose principal mandate was to report on member states' compliance with UN Security Council resolutions. In response, some UN member states submitted the names of a significant number of terrorist suspects and terrorist funding networks for inclusion in the UN's consolidated lists of *Taliban* and *Al Qaeda* associates.

This mechanism was soon believed to be flawed. Lack of evidentiary standards allowed for the highly problematic blacklisting of financial entities such as *Al Barakat* or *Al Taqwa*. Even after more than three years, the standards that were applied in these cases have not successfully passed the courts of law. The pre-mature blacklisting of financial institutions pre-empted potentially critical intelligence

gains that might have resulted from more systematic investigative efforts. In addition, the lack of due process provided some UN member states with an excuse for not complying with Security Council Resolutions. This, in turn, undermined the credibility of the UN Security Council and its role in confronting terrorism financing, and it left states with no other choice than to pursue their own – unilateralist - initiatives at confronting terrorist financing.

Areas of Discussion

Following intense debates, the working group has not come to a unanimous consensus on the question whether the 'war on terrorism' has succeeded in combating *Jihadist* funding networks. There were vigorous disagreements about whether there is a credible and effective interdiction policy or not, and if the absence of such a policy resulted from a lack of democratic principles applied by individual states and the international community. In some cases, however, the disagreements over matters of interpretation were resolved, for example, vis-à-vis the functions of a proposed Anti-Terrorism Financing Center (see below).

The proposed repositioning of counter-terrorism assets for the purpose of enhancing prevention efforts met with equally strong – and well reasoned –rejections. While the importance of the enhanced sharing of sensitive information relating to individuals was underscored by all members of the working group, some warned about the security and privacy risks when involving the private sector. In particular, serious doubts were raised about forging partnerships with an industry that stands accused of disregarding its compliance obligations.

The most substantial disagreement, however, occurred when discussing the general strategy that was embarked upon in the wake of the September 11 attacks. Both supporters and opponents of the current approach in the 'war on terrorism' appeared to be unwilling to accept opposing views. This observation is significant, because it reflects the controversies observed in the UN Security Council and the consequent problems in advancing counter-terrorism funding efforts. As a consequence, we believe that the most urgent issue facing not only this particular working group, but the international community in general, to be the ongoing need to build consensus and a shared agenda.

Key Principles

Democratic principles and multilateral efforts

The working group believes that, while fighting terrorism will remain the primary responsibility of individual states, multilateral efforts should be undertaken and continuously supported. Further, to sustain the expected long-term confrontation with terror financing, new initiatives must be based on sound democratic principles in order to guarantee their stability and cohesion.

Even if differences in their exact interpretation exist, the group is united in proposing two initiatives:

- The first aims at the establishment of a centre that will have overall responsibility in multilateral counter-terrorism activities.

- The second proposes a judicial review process, which grounds the international fight against terror funding firmly in democratic principles.

The democratic principles guiding the fight against terror financing should include the following:

- All multilateral efforts against terrorism funding networks should be undertaken under the direct supervision of the UN Security Council.

- All multilaterally sanctioned punitive actions against terror funding networks should be based on verifiable evidence that stands up to internationally established prima-facie evidentiary standards, and which can be challenged in a specially designated judicial review process.

- Evidentiary standards that allow for punitive actions, the procedures under which a court reviews accusations and other internationally compatible standards of due process, all need to be defined by a panel of globally respected legal experts, taking into account not only Western but other legal philosophical strands such as Sharia law.

Enhancing compliance methods as part of a preventive strategy

If confronting terrorists has challenged even the most sophisticated defences of modern nations, then confronting terrorism funding networks and preventing funds from reaching terrorists has proven to be an almost impossible task. The fact that terrorist attacks continue at a nearly unabated pace, and that most intelligence indicates growth in terrorist recruiting, supports the view of many experts that terrorism funding can not be stopped altogether, but at best be curtailed. Only the removal of the root causes of terrorism – in combination with the removal of the disorder in preventive counter-terrorism strategies – will end terror financing.

Improved provisions against counter-terrorism funding need to address the use of legitimate funds and legitimate financial institutions for terrorist attacks. The terrorists carrying out the September 11 attacks operated with seemingly legitimate money. They opened accounts at over a dozen reputable international banks; and they transferred, deposited and withdrew funds without triggering any alarm in the compliance and security centres of these financial institutions.

That these gaps must be closed should be self-evident. While the members of our working group accept that most Western nations have adopted adequate regulations to confront terror funding networks, the greatest challenge is the effective implementation of these rules. Is the 'know your customer' rule adequately complied with if a prospective terrorist can open an account and transfer funds? How can services ever be denied to clients if the true intention of the client is not known to the financial institution?

While these questions present impossible challenges, the working group believes that our responses can be optimised within the existing regulatory and legal framework if the information gap between the private sector (banks, fiduciaries, incorporation services, etc.) and government entities is reduced. In other words, it is no longer sufficient for governments to accumulate vast, secret intelligence files without carefully determining where, how and when to utilize this information in partnership with the private sector. In an improved information sharing scheme with those who have a demonstrable need to know, the established network of Financial Intelligence Units (as defined under the so-called Egmont Group) could take responsibility for disseminating critical information to private sector compliance officers.

Summary of Recommendations

In summary, the working group understands that, while the fight against terrorism will always be the primary responsibility of states, critical responsibilities should be delegated to appropriately structured multilateral bodies and the private sector. While the precise nature of these political initiatives still gives rise to disagreements, there is a broad consensus that the grave and urgent character of global terrorist financing needs to be met by a bold and comprehensive agenda that breaks with outdated conventions.

Recognizing limitations imposed by time constraints and analytical means, the members of the working group recommend that three panels of individuals with significant technical and practical experiences are appointed to further develop the following initiatives:

- The creation of an independent International Anti-terrorism Financing Centre with a mandate to lead and coordinate all multilateral anti-terrorism funding activities. This body would be supervised by the UN Security Council.

- The creation of an International Judicial Review Process that will firmly ground the fight against terrorism funding networks in sound democratic principles. Mandated by the UN Security Council, a judicial body will serve as the ultimate review instance to which cases may be referred to by states, or to which suspects may appeal for a final review of evidence against them. The court may also serve as an alternative process in the freezing of alleged terrorist assets and the administration and distribution of confiscated terrorist funds.

- The definition and integration of preventive Forward Looking Compliance methods involving carefully maximized information sharing schemes that are suitable for adaptation into the West's and the Muslim world's fight against terrorist financing.

The complexities of these three initiatives are commensurate with the nature of the present global threat. The international community should follow the example of other specialized agencies that have been created to further the fight against drugs, AIDS, or hunger. As these have demonstrated, global solutions to global threats require adjustments in the way nations relate to each other, and these adjustments should not be avoided merely because of potentially far reaching ramifications. Conscious of the difficulty of this challenge, the working group does not recommend a one-step path, but encourages further explorations by panels of individuals with the appropriate expertise.

Members of the Working Group

- Loretta Napoleoni, independent economic consultant, Italy (co-ordinator)

- Brian Bruh, Senior Advisor to the US Treasury and Department of Defense (advisory)
- Rico Carisch, journalist and member of the UN panel of experts
- Carlos Castresana, University of San Francisco, USA
- Daryl Champion, Daily Star, Lebanon
- Michael Chandler, former chairman of the UN Monitoring Group
- Nick Fielding, Sunday Times, England
- George Magnus, UBS Investment Bank, Switzerland
- Ganesh Sahathevan, journalist, Australia

Science and Technology

By David Ucko

The working group on Science and Technology sought to explore how terrorists exploit technology, and how we can use technology to combat this threat. The working group agreed on three broad principles:

- Armed with the required knowledge and equipment, a terrorist can use technology to cause large-scale death, destruction or disruption. This threat must not be underestimated.

- The likelihood and consequences of a high-tech terrorist attack demand a drastic reworking of our current counter-terrorism policies.

- Technology can help us combat the threat of terrorism in several ways but it is no panacea. The process of selecting which technology to develop and how it will be used requires shrewd investment of finite resources, creative thinking and good knowledge of ourselves and our enemy.

Areas of Discussion

What is high-tech terrorism?

'High-tech terrorism' is predicated on the use or exploitation of high-technological equipment, structures or networks to maximise the effect of a terrorist attack. The most evident use of technology relates to the weapon itself or the means of its delivery. Nonetheless, the technological component of an attack can also lie in the use of technology during the recruitment phase, in the terrorist group's communications or in its training. Finally, rather than integral to the attack itself, the technological component can also be its target, should the terrorist identify and strike the technological nodes that hold our society together (Brian Jenkins, Steve Lukasik).

There is no one purpose for a high-tech attack. As with a conventional terrorist attack, the aim can be to cause physical damage to persons or property, to attract attention or to cause disruption in the targeted society (Lukasik). Following the events of September 11, 2001, the counter-terrorism community has also had to confront the likelihood of mass-casualty terrorism, where entire populations are targeted. In each of these scenarios, the intelligent use of technological means or a good knowledge of society's technological vulnerabilities greatly enhances the effect of the attack.

What are the possible scenarios of a high-technological terrorist attack?

The outcome of a high-technological attack varies with the effect desired by the terrorist. Clearly, the type of attack that will kill in large numbers will differ from one geared towards mass-disruption. It is, however, possible to draw up a number of scenarios, ranging from the near apocalyptic to the

tactical use of technology for limited ends. Importantly, every high-tech terrorist attack – even a hoax, if credible – will tend to produce high levels of fear, alarm and disruption.

Peter Zimmerman raised the issue of nuclear terrorism – the most lethal and destructive high-technological attack by far. More than chemical or biological arms, the nuclear bomb is the quintessential weapon of mass destruction. For this very reason, the nuclear option is particularly attractive to a group such as *Al Qaeda*, which openly subscribes to mass-casualty terrorism on an almost apocalyptic level.

The detonation of a nuclear weapon in a major city would be likely to kill as many as half a million people. The terrorist group could also use the nuclear option to disrupt society, rather than destroy it. Zimmerman offered the possible scenario of Caesium-137, which could be stolen from cancer-therapy clinics or bought openly via an application process. If this radioactive element were spread or somehow disseminated, it would effectively shut down large areas of society and cause significant disruption and panic. The necessary evacuation, decontamination and monitoring would be both physically and psychologically testing, yet the terrorist group would not have killed a substantial number of people.

There are other forms of high-technological attacks, some of which are currently being refined by insurgents in Iraq. Declan Ganley pointed to the use of cellular-telecommunications infrastructure in the Madrid bombings of March 2004. This same type of remote detonation is now seen regularly in Iraq, where cellular-telephone communications are being employed to trigger improvised explosives devices (IED). To Ganley, the trend towards remote detonation is part of a natural learning curve for terrorist organisations. With the adequate technology, it would even be possible for a terrorist group to trigger an IED from a different country. If this method were perfected and several devices in different countries were detonated near-simultaneously or in a timed sequence, the range and lethality of the attacks would clearly be significant and the psychological message of such an attack would be a veritable force multiplier.

From the terrorists' perspective, remote detonation has the added benefit of triggering the attack through 'our' communication infrastructure. This scenario presents the policy-maker with a difficult choice, as it may be necessary to shut down a network in order to prevent it being co-opted for terrorist purposes. This, Ganley added, was a chief lesson of the 11 September 2001 attacks, which effectively shut down the air-transportation infrastructure.

Furthermore, Lukasik emphasised that a terrorist attack could exploit our society's technological vulnerabilities and effectively shut down the technological infrastructure or network on which our society depends. He explained that much of the technology that we use is based around software, which allows for a high level of technological integration into society, but also generates new vulnerabilities, particularly because – as Lukasik put it – 'we don't understand software'. The complexity of software programming means that a malicious code or instruction could be inserted and remain undetected or even undetectable for a substantial period of time. The use of hardware brings its own vulnerabilities: if destroyed, it will require replacement, yet a lack of planning, resources and 'spares' makes this process highly time-consuming and therefore costly, not only in financial terms. As an example, Lukasik pointed to the transformers for the electric power-grid: these devices are only manufactured by a handful of companies globally and replacement would come with an estimated fourteen-month lead-time. At the same time, building and stockpiling spares would probably be far too costly. Indeed, an attack on the power-grid would be a highly attractive option for a terrorist group, as it would strike a large area, be difficult to reverse and cause financial and psychological damage (Zimmerman).

How likely is high-tech terrorism?

Mark Lampert alerted the working group to a critical admonition in the discussion of the likelihood of a high-tech terrorist attack: do not confuse the unfamiliar with the improbable. Lampert warned of a prevailing state of denial regarding the probability of a high-tech attack and cautioned against letting the past determine our understanding of the future. It is tempting – but unproductive and potentially dangerous – to mould one's expectations of future attacks on what has already occurred. Thus, Lampert urged the counter-terrorism community to beware of its own assumptions and acknowledge the high and constant degree of uncertainty. A rush to make speedy conclusions based solely on empirical evidence can obscure more than it explains and lead to policies that expose more vulnerabilities than they protect.

Jenkins drew up a graph to illustrate the likelihood of a mass-casualty high-tech terrorist attack. By correlating a group's willingness to launch a deadly high-tech attack with its capability to do so, Jenkins argued that, as the capability increases, the willingness could reasonably be expected to decline. A group with the required capability would normally be a large organisation, which implies a constituency, a sizeable pool of members and a more sophisticated agenda. For a group of this size, operational failure would also be very damaging and one can expect that the group would for these reasons be conservative and risk-averse in its decision-making. Conversely, a mentally or emotionally disturbed individual with millenarian intent would find few checks and disincentives other than his or her lacking capability. So, whereas a large organisation probably could but wouldn't, a lone terrorist or small group might want to, but can't. However, as Jenkins emphasised, the optimism of this formula is undermined by four important caveats:

- There is inevitably an intersection between the declining willingness and the increasing capability – this is where a group is radical enough *and* sufficiently technologically advanced to launch a high-tech terrorist attack.

- This intersection is migrating as technology becomes increasingly available and advanced. The proliferation and rapid evolution of technology empowers the individual to do more with less. As Jenkins put it, 'smaller and smaller groups are acquiring the capacity for large scale violence once possessed only by armies'.

- With the emergence of mass-casualty terrorism, as typified by *Al Qaeda*, it is no longer safe to assume that larger organisations will be more conservative. Indeed, following the attacks of September 11, 2001, the inverse relation between willingness and capability might not hold.

- The 9/11 attacks have revolutionised the operative assumptions of security planners and forced us to consider new scenarios for attacks, new weapons as well as our own societal vulnerabilities. What used to be the stuff of fiction has now become a distinct possibility and, in the process, the plausibility of an attack has been redefined.

Ganley identified a further factor pointing towards the likelihood of a high-tech attack: a terrorist group is a learning organisation. The learning curve can be discerned both in relation to the Irish Republican Army (IRA) and the insurgents currently causing havoc in Iraq. In both instances, 'smart terrorists' learn to channel the assets at their disposal, including technology. Furthermore, much like a venture capitalist, a terrorist group bent on large-scale destruction will increase its chances by spreading its investments of time and energy into many different schemes, and, as these projects become more or less promising through subsequent iterations, commit itself to those with the highest pay-off. This iterative process greatly enhances the possibility of success and forces us to put up strong defences across the board.

Policy Recommendations

The working group agreed on the general principle that a terrorist attack be viewed not as an isolated event, but as the apex of a cycle of processes and phenomena that originates with root causes, radicalisation, recruitment, planning and training, culminates in the attack itself, and concludes with its immediate consequences and long-term ramifications (Anja Dalgaard-Nielsen). This cycle must be grasped in its entirety and appropriate technologies must be developed and/or mobilised to deal with the threat in each phase. The further upstream the intervention, the better. At the same time, there is and should be considerable overlap between the recommendations, as the effectiveness of counter-terrorism depends on what Zimmerman referred to as the 'stacking' of various measures in order to gain a more integrated and holistic defence mechanism.

Against this backdrop, the working group arrived at a number of policy recommendations, ranging from the very general to the quite specific. Going through the aforementioned cycle of the attack, the recommendations could be listed as follows:

Effective counter-terrorism requires wise investment of finite resources

It is critical that counter-terrorism does not lose out in the political and bureaucratic competition for limited resources and funds. However, even when financing has been secured, it is unlikely that it will be sufficient to pursue every desired counter-terrorism policy and programme. There is, therefore, a need for prioritising, and the process of selecting what to do requires wisdom and a thorough understanding of the threat as well as of the particular vulnerabilities of modern society. Ultimately, however, uncertainty and complexity can only be minimised, not eliminated.

Lampert suggested one approach to prioritisation based on the venture capitalist's approach to uncertainty in the market. He recommended placing small investments in many counter-terrorism policies or programmes across the board. From this starting-point, the counter-terrorism community can observe the performance of the various projects and reward those that indicate a high pay-off. This type of 'adaptive learning', Lampert stressed, can drive the resource allocation. He added that this process would work best with the solid support and input of the commercial sector. When mobilised, the nimbleness, cleverness and creativity of the entrepreneurial class can be a powerful weapon against terrorists and generate quick results employing advanced technology.

Enhancing usability of existing counter-terrorism technologies by adapting them to avoid civil-liberty violations

Our technological capability to intercept and gather intelligence is a powerful tool in the fight against terrorism. However, the usability of this instrument is reduced when the methods of investigation also violate civil liberties. For this reason, both Lukasik and Dalgaard-Nielsen urged the counter-terrorism community to depersonalise the intelligence and datasets relevant to investigations. If the analysis of signal intelligence can be done anonymously – without reference to the personal identifiers – this would circumvent some of the civil-liberty issues currently stifling the employability of information technology. Dalgaard-Nielsen and Lukasik both recommended pattern recognition in depersonalised datasets, with the authorisation for action provided through the legal system when probable cause can be discerned.

Developing and harnessing our technological advantage to identify and infiltrate terrorist recruitment grounds

One means of undercutting terrorist recruitment might involve infiltrating European prisons – an established recruitment ground for Islamist extremists. Here, better monitoring and innovative initiatives would do much to sap the sway and spread of radicalism. For example, Dalgaard-Nielsen recommended connecting prisons with virtual libraries holding Islamic texts as a means of limiting the influence of radical preachers.

Investing in border-control technologies to intercept and check terrorist smuggling and movement

Further downstream, the planning phase of an attack might be most effectively disrupted by developing and consolidating technologies that help intercept and stop terrorist smuggling operations. Combating smuggling is demanding both in terms of time and resources, yet it remains indispensable. Border-control technologies can, in this instance, play a key role. Pattern recognition and pattern-based searches would complement this effort and narrow the search.

Biometrical identification technology is often raised as a potential technological asset in countering terrorist smuggling and movement. Biometrical identification systems will increasingly be used in travel documents as well as in other transactions. Nonetheless, this technological system has its own drawbacks: there are already means of changing the biometric, and these will develop in synch with the technology itself. Secondly, a biometric system will link the individual with his or her documents, yet is blind to whether that person has been created or fabricated in the first place.

Developing effective 'red-teaming' procedures to pre-empt terrorist targeting and recruitment

'Red teaming' is essentially a role-playing exercise in which a network of experts from different professional backgrounds review how they would attack a Western society, as if they were the terrorist. It is a brainstorming exercise placing a high premium on inter-disciplinary interaction, open communications and innovative thinking. Ideally, the system works to pre-empt the thought process of our opponent and leads to more effective and more precisely targeted counter-measures. Lukasik argued that a red-teaming group composed of engineers, financial experts, scientists and transportation experts would be able to identify and devise means of minimising the vulnerabilities in our technology, our buildings, infrastructure and networks. Similarly, a 'red team' with a different structure could shed light on how to deter or undercut the terrorists' recruitment drive, either by identifying with the potential recruit or with the recruiter.

Preparing and developing a roster of first responders

Should an attack occur – or fail to be prevented – it is essential that first responders are trained and ready to intervene. Zimmerman urged the counter-terrorism community to systematise the training and preparation of first responders, particularly in relation to chemical, biological, radiological and nuclear (CBRN) attacks. Clearly, responding to these types of attacks requires an in-depth understanding of the effect of each. For example, depending on radiation or contamination levels, it can sometimes be highly inappropriate to launch a search-and-rescue operation. To be effective, first responders need to be able to identify a situation and be trained to respond accordingly. This requires familiarity with the CBRN technologies and effects, achieved through contingency planning and training.

One means of improving and systematising the performance of first responders is to focus on good communications. Just as 'jointness' has been identified as an invaluable asset in the modern battlefield, it is critical that the first responders can share their situational awareness up and across the command chain. Ganley reminded the working group that the communications technology that would allow this level of jointness is both commercially available and inexpensive.

Members of the Working Group

- Brian Jenkins, RAND Corporation, USA
- eter Zimmerman, King's College London, England
- Steve Lukasik, entrepreneur, USA
- Declan Ganley, Rivada Communications, Ireland
- Anja Dalgaard-Nielsen, The Danish International Studies Institute
- Mark Lampert, entrepreneur, USA

David Ucko is a research fellow at the International Policy Institute and a PhD candidate at the Department of War Studies, both King's College London.

The Club de Madrid

Mission

The Club de Madrid is an independent organisation dedicated to strengthening democracy around the world. It launches global initiatives, conducts projects, and acts as a consultative body for governments, democratic leaders and institutions involved in processes of democratic transition. The personal practical experience of its members – fifty-seven former heads of state and government – in processes of democratic transition and consolidation is the Club de Madrid's unique resource. Along with the experience and co-operation of other high level political practitioners and governance experts, this resource is a working tool to convert ideas into practical recommendations.

Programmes and Activities

The Club de Madrid brings three major resources to its work:

- A unique mix of former heads of state and government.
- A committed focus on democratic transition and consolidation.
- Programmes with a practical approach and measurable results.

The Club de Madrid undertakes projects related to its core mission of promoting and defending democracy. One of the Club de Madrid's major assets is the ability of its members to offer strategic advice and peer-to-peer counsel to current leaders striving to build or consolidate democracy. The organisation also plays an advocacy role in promoting democratic principles in certain country, regional or thematic cases, such as with the International Summit on Democracy, Terrorism and Security.

To learn more about the Club de Madrid's mission and activities, please go to our web site – www.clubmadrid.org – or contact us directly:

Club de Madrid
Felipe IV, 9 – 3º izqda.
28014 Madrid
Spain

Tel: +34 91 523 72 16
Fax: +34 91 532 00 88
Email:clubmadrid@clubmadrid.org

List of Members

Fernando Henrique Cardoso,* President. Former President of Brazil.
Mary Robinson,* Vice President. Former President of Ireland.
William J. Clinton, Honorary Co-Chairman.
Former President of the United States of America.
Kim Campbell,* Secretary General. Former Prime Minister of Canada.

Valdas Adamkus (on leave), President of Lithuania.
Martti Ahtisaari, Former President of Finland.
Raúl Alfonsín, Former President of Argentina.
Sadig Al-Mahdi, Former Prime Minister of Sudan.
Alvaro Arzú, Former President of Guatemala.
Patricio Aylwin, Former President of Chile.
José María Aznar, Former Prime Minister of Spain.
Belisario Betancur, Former President of Colombia.
Carl Bildt, Former Prime Minister of Sweden.
Gro Harlem Brundtland, Former Prime Minister of Norway.
Leopoldo Calvo-Sotelo, Former Prime Minister of Spain.
Jimmy Carter,** Former President of the United States.
Aníbal Cavaco Silva, Former Prime Minister of Portugal.
Joaquim Chissano, Former President of Mozambique.
Jacques Delors, Former President of the European Commission.
Philip Dimitrov, Former Prime Minister of Bulgaria.
Leonel Fernández (on leave), President of the Dominican Republic.
José María Figueres,* Former President of Costa Rica.
Eduardo Frei Ruiz-Tagle,* Former President of Chile.
César Gaviria,* Former President of Colombia.
Felipe González Márquez, Former Prime Minister of Spain.
Mikhail Gorbachev, Former President of the Soviet Union.
Inder Kumar Gujral, Former Prime Minister of India.
Antonio Oliveira Guterres, Former Prime Minister of Portugal.
Václav Havel, Former President of Czechoslovakia and the Czech Republic.
Osvaldo Hurtado, Former President of Ecuador.
Lionel Jospin, Former Prime Minister of France.
Helmut Kohl, Former Chancellor of Germany.
Alpha Oumar Konaré, Former President of Mali.
Chairperson of the Commission of the African Union.
Milan Kučan, Former President of Slovenia.
Hong-Koo Lee,* Former Prime Minister of Korea.
John Major, Former Prime Minister of the United Kingdom.
Antonio Mascarenhas Monteiro, Former President of Cape Verde.
Ketumile Masire, Former President of Botswana.
Tadeusz Mazowiecki, Former Prime Minister of Poland.
Rexhep Meidani,* Former President of Albania.

Lennart Meri, Former President of Estonia.
Valentín Paniagua,* Former President of Peru.
Anand Panyarachun, Former Prime Minister of Thailand.
Andrés Pastrana, Former President of Colombia.
Javier Pérez de Cuellar, Former Secretary-General of the United Nations.
Former Prime Minister of Peru.
Romano Prodi, Former President of the European Commission. Former Prime Minister of Italy.
Jorge Fernando Quiroga, Former President of Bolivia.
Fidel Valdes Ramos, Former President of the Republic of the Philippines.
Poul Nyrup Rasmussen, Former Prime Minister of Denmark.
Petre Roman, Former Prime Minister of Romania.
Gonzalo Sánchez de Lozada, Former President of Bolivia.
Julio María Sanguinetti,* Former President of Uruguay.
Jennifer Mary Shipley, Former Prime Minister of New Zealand.
Mário Soares, Former President of Portugal.
Adolfo Suárez, Former Prime Minister of Spain.
Hanna Suchocka,* Former Prime Minister of Poland.
Ernesto Zedillo,* Former President of Mexico.

(*) Member of the Executive Committee
(**) Honorary Member

Other Members of the Executive Committee

Diego Hidalgo, President of the Fundación para las Relaciones Internacionales
y el Diálogo Exterior (FRIDE).
George Matthews, President of the Gorbachev Foundation of North America (GFNA)
T. Anthony Jones, Vice-President and Executive Manager of GFNA.
José Manuel Romero, Trustee of FRIDE.

Other Honorary Members

José Luis Rodríguez Zapatero, Prime Minister of Spain.
Esperanza Aguirre, President of the Regional Government of Madrid.
Alberto Ruíz-Gallardón, Mayor of Madrid.

The International Summit on Democracy, Terrorism and Security

March 11, 2004

Ten bombs exploded on four trains during rush hour in Madrid. More than 190 people died, almost 2,000 were injured. It was one of the most devastating terrorist attacks in Europe in recent history. As in the United States of America on September 11, 2001, it was an attack on freedom and democracy by an international network of terrorists.

One year on, Madrid was the setting for a unique conference, the International Summit on Democracy, Terrorism and Security. Its purpose was to build a common agenda on how the community of democratic nations can most effectively confront terrorism, in memory of its victims from across the world.

Objectives

The Madrid Summit aimed to promote a vision of a world founded on democratic values and committed to effective co-operation in the fight against terrorism. It brought together the world's leading scholars, practitioners and most influential policymakers. It was the largest gathering of security and terrorism experts that has ever taken place:

- 23 Heads of State and Government
- 34 former Heads of State and Government.
- Official Delegations from than 60 countries.
- Heads of inter-governmental and international organisations including the United Nations, the European Parliament, Council and Commission, NATO, Interpol, the League of Arab States, and many others.
- 200 experts on terrorism and security.
- 500 representatives from non-governmental organisations and civil society.

The Working Groups

In the months leading up to the Madrid Summit, more than two hundred of the world's leading scholars and expert practitioners explored the issues of democracy, terrorism and security in an unparalleled process of scholarly debate. The discussions were conducted through a system of password-protected web-logs. On the first day of the summit, the groups met in closed sessions to conclude their work.

Each working group issued a final paper of recommendations on which the individual contributions in the Club de Madrid Series on Democracy and Terrorism are based.

Results

The principal legacy of the Madrid Summit is an innovative plan of action: The Madrid Agenda.

It draws on the various contributions made at the summit, in particular the speeches given by the leaders of official delegations, the discussions that took place during more than twenty panel sessions, and – most importantly – the conclusions of the working groups.

The document was adopted by an Extraordinary General Assembly of the Club de Madrid on March 11, 2005.

The Madrid Agenda

To remember and honour the victims of the terrorist attacks of March 11, 2004, the strength and courage of the citizens of Madrid, and through them, all victims of terrorism and those who confront its threat.

We, the members of the Club de Madrid, former Presidents and Prime Ministers of democratic countries dedicated to the promotion of democracy, have brought together political leaders, experts and citizens from across the world.

We listened to many voices. We acknowledged the widespread fear and uncertainty generated by terrorism. Our principles and policy recommendations address these fundamental concerns.

Ours is a call to action for leaders everywhere. An agenda for action for governments, institutions, civil society, the media and individuals. A global democratic response to the global threat of terrorism.

The Madrid Principles

Terrorism is a crime against all humanity. It endangers the lives of innocent people. It creates a climate of hate and fear. It fuels global divisions along ethnic and religious lines. Terrorism constitutes one of the most serious violations of peace, international law and the values of human dignity.

Terrorism is an attack on democracy and human rights. No cause justifies the targeting of civilians and non-combatants through intimidation and deadly acts of violence.

We firmly reject any ideology that guides the actions of terrorists. We decisively condemn their methods. Our vision is based on a common set of universal values and principles. Freedom and human dignity. Protection and empowerment of citizens. Building and strengthening of democracy at all levels. Promotion of peace and justice.

A Comprehensive Response

We owe it to the victims to bring the terrorists to justice. Law enforcement agencies need the powers required, yet they must never sacrifice the principles they are meant to defend. Measures to counter terrorism should fully respect international standards of human rights and the rule of law.

In the fight against terrorism, forceful measures are necessary. Military action, when needed, must always be co-ordinated with law enforcement and judicial measures, as well as political, diplomatic, economic and social responses.

We call upon every state to exercise its right and fulfil its duty to protect its citizens. Governments, individually and collectively, should prevent and combat terrorist acts. International institutions, governments and civil society should also address the underlying risk factors that provide terrorists with support and recruits.

International Co-operation

Terrorism is now a global threat. We saw it not only in Madrid, New York and Washington, but also in Dar-es-Salaam, Nairobi, Tel Aviv, Bali, Riyadh, Casablanca, Baghdad, Bombay, and Beslan. It calls for a global response. Governments and civil society must reignite their efforts at promoting international engagement, co-operation and dialogue.

International legitimacy is a moral and practical imperative. A multilateral approach is indispensable. International institutions, especially the United Nations, must be strengthened. We must renew our efforts to make these institutions more transparent, democratic and effective in combating the threat.

Narrow national mindsets are counterproductive. Legal institutions, law enforcement and intelligence agencies must co-operate and exchange pertinent information across national boundaries.

Citizens and Democracy

Only freedom and democracy can ultimately defeat terrorism. No other system of government can claim more legitimacy, and through no other system can political grievances be addressed more effectively.

Citizens promote and defend democracy. We must support the growth of democratic movements in every nation, and reaffirm our commitment to solidarity, inclusiveness and respect for cultural diversity.

Citizens are actors, not spectators. They embody the principles and values of democracy. A vibrant civil society plays a strategic role in protecting local communities, countering extremist ideologies and dealing with political violence.

A Call to Action

An aggression on any nation is an aggression on all nations. An injury to one human being is an injury to all humanity. Indifference cannot be countenanced. We call on each and everyone. On all States, all organizations – national and international. On all citizens.

Drawing on the deliberations of political leaders, experts and citizens, we have identified the following recommendations for action, which we believe should be extended, reviewed, and implemented as part of an ongoing, dynamic process.

The Madrid Recommendations

Political and philosophical differences about the nature of terrorism must not be used as an excuse for inaction. We support the Global Strategy for Fighting Terrorism announced by the Secretary General of the United Nations at the Madrid Summit on March 10. We urgently call for:

- the adoption of the definition proposed by the United Nations High-Level Panel on Threats, Challenges and Change.
- the ratification and implementation of all terrorism-related conventions by those states which have not yet done so.
- the speedy conclusion of the Comprehensive Convention on International Terrorism.

And we believe it is a moral and practical necessity to address the needs of terrorist victims. We therefore recommend:

- the exploration of the possibility of creating high commissioners for victims both at the international and the national level, who will represent the victims' right to know the truth, as well as obtain justice, adequate redress and integral reparation.

International Co-operation

The basis for effective co-operation across national borders is trust and respect for the rule of law. Trust is built through shared norms, reciprocity and the practical experience of effective collaboration. To encourage this sense of mutual confidence, we propose:

- the establishment of regular, informal forums for law enforcement and intelligence officials, which may grow from bilateral consultations into a formalised structure for multilateral co-operation.
- the strengthening of regional organisations, so that measures to combat terrorism are tailored to local needs and benefit from local knowledge and networks.
- the effective co-ordination of these mechanisms at the global level.

International collaboration in the fight against terrorism is also a question of human and financial capital. We call for:

- the establishment of an international mechanism – including states, non-governmental organisations and the private sector – to help link states that are in need of resources with those that can provide assistance.
- the creation of a trust fund for the purpose of assisting governments that lack the financial resources to implement their obligations, as proposed by the United Nations High-Level Panel.

Underlying Risk Factors

Terrorism thrives on intimidation, fear and hatred. While authorities have a responsibility to ensure freedom, including religious freedom, leaders, including religious leaders, have a responsibility not to abuse that freedom by encouraging or justifying hatred, fanaticism or religious war. We propose:

- the systematic promotion of cultural and religious dialogue through local encounters, round tables and international exchange programmes.

- the continuous review by authorities and the mass media of their use of language, to ensure it does not unwittingly or disproportionately reinforce the terrorist objective of intimidation, fear and hatred.
- the creation of programmes, national and international, to monitor the expression of racism, ethnic confrontation and religious extremism and their impact in the media, as well as to review school textbooks for their stance on cultural and religious tolerance.

While poverty is not a direct cause of terrorism, economic and social policy can help mitigate exclusion and the impact of rapid socioeconomic change, which give rise to grievances that are often exploited by terrorists. We recommend:

- the adoption of long-term trade, aid and investment policies that help empower marginalised groups and promote participation.
- new efforts to reduce structural inequalities within societies by eliminating group discrimination.
- the launch of programmes aimed at promoting women's education, employment and empowerment.
- the implementation of the Millennium Development Goals by 2015.

Terrorists prosper in societies where there are unresolved conflicts and few accountable mechanisms for addressing political grievances. We call for:

- new initiatives at mediation and peace-making for societies which are marked by conflict and division, because democracy and peace go hand in hand.
- a redoubling of efforts to promote and strengthen democratic institutions and transparency within countries and at the global level. Initiatives such as the Community of Democracies may contribute to this goal.

Confronting Terrorism

Democratic principles and values are essential tools in the fight against terrorism. Any successful strategy for dealing with terrorism requires terrorists to be isolated. Consequently, the preference must be to treat terrorism as criminal acts to be handled through existing systems of law enforcement and with full respect for human rights and the rule of law. We recommend:

- taking effective measures to make impunity impossible either for acts of terrorism or for the abuse of human rights in counter-terrorism measures.
- the incorporation of human rights laws in all anti-terrorism programmes and policies of national governments as well as international bodies.
- the implementation of the proposal to create a special rapporteur who would report to the United Nations Commission on Human Rights on the compatibility of counter-terrorism measures with human rights law, as endorsed by the United Nations Secretary General in Madrid.
- the inclusion and integration of minority and diaspora communities in our societies.
- the building of democratic political institutions across the world embodying these same principles.

In the fight against terrorism, any information about attacks on another state must be treated like information relating to attacks on one's own state. In order to facilitate the sharing of intelligence across borders, we propose:

- the overhaul of classification rules that hinder the rapid exchange of information.
- the clarification of conditions under which information will be shared with other states on the basis of availability.
- the use of state of the art technology to create regional and global anti-terrorism data bases.

The principle of international solidarity and co-operation must also apply to defensive measures. We recommend:

- the creation of cross-border preparedness programmes in which governments and private business participate in building shared stockpiles of pharmaceuticals and vaccines, as well as the seamless co-operation of emergency services.

Solidarity must be enhanced by new efforts at co-ordinating the existing instruments of anti-terrorist collaboration. We propose:

- the streamlining and harmonisation of national and international tools in the fight against terrorism.
- the creation of clear guidelines on the role of the armed forces in relation to other agencies of law enforcement at the national level.
- the drawing up of national plans to co-ordinate responsibilities in the fight against terrorism, allowing for agencies or organisations with special skills to contribute to a comprehensive effort.

The threat from terrorism has made efforts to limit the proliferation of weapons of mass destruction even more urgent. We call for:

- the United Nations Security Council to initiate on-site investigations where it is believed that a state is supporting terrorist networks, and if necessary to use the full range of measures under Chapter VII of the United Nations Charter.
- the conclusion of the International Convention for the Suppression of Acts of Nuclear Terrorism, and the strengthening and implementation of the biological weapons convention.
- the continuation of innovative global efforts to reduce the threat from weapons of mass destruction, such as the Global Threat Reduction Initiative and the Global Partnerships.

Terrorists must be deprived of the financial resources necessary to conduct their campaigns. To curb terrorist funding networks, we recommend:

- increased and co-ordinated law enforcement and political and civic education campaigns aimed at reducing the trafficking of illegal narcotics, revenues from which are used to finance terrorism.
- the creation of an international anti-terrorist finance centre, which furthers research, trains national enforcement officials, and serves as a source of co-ordination and mutual assistance.
- the development of tools to increase the transparency of fundraising in the private and charitable sectors through the exchange of best practices.
- the expansion of ‘financial intelligence units’, which facilitate the effective corporation between government agencies and financial institutions.

Civil Society

The process of building democracy as an antidote to terrorism and violence needs to be supported by the international community and its citizens. We propose:

- the creation of a global citizens network, linking the leaders of civil society at the forefront of the fight for democracy from across the world, taking full advantage of web-based technologies and other innovative forms of communication.
- an 'early warning system' as part of this network, helping to defuse local conflicts before they escalate, as well as providing a channel for moral and material support to civil society groups facing repression.

Taking The Madrid Agenda Forward

The Club de Madrid will present the Madrid Agenda to the United Nations, the forthcoming Community of Democracies ministerial meeting in Chile, as well as other institutions and governments. The Club de Madrid will engage with universities, specialised research institutes and think-tanks to elaborate the proposals made by the Summit's working groups and panels.

The space for dialogue and exchange of ideas opened by this Summit, drawing on the work of the numerous experts, practitioners and policymakers involved, must continue. The papers prepared provide a powerful tool for all those who wish to understand the challenge from terrorism and seek effective solutions.

Keeping in our hearts the memory of the victims of terrorism in different continents, and in particular the terrible attacks in the United States in 2001, we believe it would have both symbolic and practical value to hold a further global conference on September 11, 2006, to take stock of the progress made in realising the Madrid Agenda.

Madrid, March 11, 2005

CLUB DE MADRID

The Club de Madrid Series on Democracy and Terrorism consists of three volumes:

• **Volume I**
Addressing the Causes of Terrorism
includes contributions on the psychological roots of terrorism, political explanations, economic factors, religion, and culture.

• **Volume II**
Confronting Terrorism
deals with policing, intelligence, military responses, terrorist finance, and science and technology.

• **Volume III**
Towards a Democratic Response
addresses the role of international institutions, legal responses, democracy promotion, human rights and civil society.

CLUB DE MADRID