

Chapter 9

Challenges of Intelligence Sharing in Combating Terrorism: An Academic Point of View

Anton Dengg¹

Introduction

Global challenges require global answers. This is especially the case with the current threat of transnational terrorism. Undoubtedly, there is an increasing need for states to cooperate in the sphere of counter terrorism. Information, even sensitive information, has to be shared because of two compelling reasons:

- to prevent attacks, or
- to investigate after an attack, as fast as possible and to ensure that attackers get appropriate punishment, and to nip further attacks in the bud.

But what should such cooperation actually look like? Especially after the 9/11 attacks, state institutions have tried to share information – about knowledge of terror organizations and to interlink them. Similarly, after the attacks in Madrid (2004) and London (2005), the European Union (hereafter EU) has intensified the coordination and interlinking of security organizations.

EU Information Sharing

The EU has decided upon many new regulations and cited some requirements that have to be undertaken to counter the new threats. Here are some relevant examples:

- The exchange of information between intelligence services² of the Member States of the European Union will be required and a joint investigation team has to be set up (September 2001);

¹ Colonel Anton Dengg, Austrian Army, has been a longtime member of the CTWG. He has been serving at the OSCE and working as a research fellow at the Institute for Peace Support and Conflict Management of the Austrian National Defense Academy since 2004.

² Extraordinary European Council Meeting on 21st September 2001, Conclusion and Plan of Action, SN 140/01, p.2.

- The close cooperation between Europol and the relevant US authorities (September 2001);³
- The commitment to establish operational links and improve existing cooperation between relevant bodies to facilitate enhanced exchange of information on terrorist financing (March 2004);⁴
- The establishing of a “specific intelligence capacity in relation to terrorist financing within SitCen to inform the work of relevant bodies” (June 2004);⁵
- The statement that Member States use the power of their intelligence and security services not only to counter threats to their own security, but also, as the case may be, to protect the internal security of the other Member States (December 2004);⁶
- The statement that from 1 January 2005, SitCen (Joint Situation Centre) will provide the Council with strategic analysis of the terrorist threat. This analysis is based on intelligence from Member States’ intelligence and security services and, where appropriate, on information provided by Europol (December 2004).⁷ Thereupon, this is taken into account in the European Security Strategy (ESS, 12 December 2003) in which terrorism is cited as one of the five key threats to the European Union.

In 2005 the EU arranged in “The Hague Programme”⁸ to identify the goal of setting up and implementing a methodology for intelligence-led law enforcement at the EU level. Another fundamental regulation exists in the EU for cooperation between intelligence authorities: A Member State which organizes a major event with an international dimension should be facilitated with collection, analysis and exchange of relevant information on the event. “The information could, inter alia, include:

- Information and intelligence obtained prior to the event that can potentially affect the course of the event or the maintenance of law and order and security in general,
- Persons involved in terrorist organizations, terrorist actions or other major criminal activities, which might be indirectly related to terror-

³ Ibid.

⁴ European Council, *Declaration on Combating Terrorism*, 7906/04 (Brussels, 29 March 2004).

⁵ Council of the European Union, *EU Plan of Action on Combating Terrorism*, 10010/3/04 (Brussels, 11 June 2004), p.17.

⁶ Council of the European Union, *The Hague Programme: Strengthening Freedom, Security and Justice in the European Union*, 16054/04 (Brussels, 13 December 2004), p.19.

⁷ Ibid., p.20.

⁸ Ibid., p.22.

ism.”⁹ But for the prevention of terrorist attacks, information and intelligence about terrorist groups and organizations is essential for sharing information and intelligence in general and as appropriate to the incident.¹⁰ Therefore the organizing Member State may request the deployment of police or intelligence officers for operational support from another Member State.¹¹

In addition to these developments, there are large numbers of close partnerships to strengthen intelligence cooperation in the field of counter terrorism between individual European Member States and the USA.¹² Albania, for example, has adopted a number of legislative acts calling for stronger cooperation in “counterterrorism efforts of its police, military, intelligence service, and Ministries of Finance and Foreign Affairs.”¹³ Also, Brussels is “timely and proactive in sharing information with the United States regarding terrorist threats to US citizens or facilities”¹⁴ and the Belgium “General Intelligence and Security Services also cooperated closely with US authorities.”¹⁵ “Intelligence and security agencies” of the United Kingdom have deepened their bilateral measures on counter terrorism and increasingly work together in solving acts linked to terrorism with countries such as Australia, Greece, Indonesia and the United States.

It should be noted that practitioners from the field of intelligence often state that they have an excellent international cooperation. But if that is true why is there always a demand for better cooperation?

Foiled Attacks

An increase in intelligence cooperation is also apparent from the long list of foiled terrorist attacks. These successes of international cooperation between and among security agencies—especially from the legal perspective—can be seen in various disrupted plots and in the rapid investigations of the perpetrators. Some notable examples are:

- London, August 2006: attempted attacks on several airplanes with binary liquid explosives at the Heathrow airport in London;
- Dortmund and Koblenz, July 2006: attempted attacks on two high-speed ‘ICE’ German trains with bombs hidden in luggage;

⁹ Council of the European Union: Handbook for police and security authorities concerning cooperation at major events with an international dimension, 10589/1/07, p.9.

¹⁰ *Ibid.*, p.16.

¹¹ *Ibid.*, p.17.

¹² U.S. Department of State, *Patterns of Global Terrorism (2002)*, 2003/0430, www.state.gov/j/ct/rls/crt/2002/.

¹³ *Ibid.*

¹⁴ *Ibid.*

¹⁵ *Ibid.*

- London, June 2007: the attempted attack with a car bomb in front of a nightclub in London.

The rapid investigation work after the attacks in Germany demonstrated the good cooperation between the intelligence services. Following a tip-off from the Lebanese intelligence service, one of the so-called “suitcase bombers” was arrested at the railway station in the North German city of Kiel.¹⁶

Similarly, a good approach for professional intelligence information sharing was the news of the arrest of 14 terrorist suspects at the beginning of 2008 in Spain. As an outcome of their investigation, the Spanish Intelligence Agency was able to warn France, Great Britain and Portugal of new attacks being planned by terrorist cells.¹⁷

Success versus Failure

From another vantage point, the attempted attacks in Dortmund (2006) and London (2007) could also be seen, in a sense, as failures of the intelligence services. Only good luck prevented the terrorists from carrying out these attacks successfully. The bombs did not explode because of a mistake in their construction. Upon reviewing these foiled attacks, how can one accuse the intelligence agencies of having failed, because they could not gather information at an earlier stage? Or is prior detection by intelligence services made more difficult because of the decreasing size of the terrorist groups involved who carry out their attacks with simple and easily produced means? Or is the possibility of intelligence failure made more likely because of the “home grown” terrorists who remain quiet, as in sleeper cells? The recent foiled attacks show that a new organizational structure exists. As Mark Sageman has indicated, “the world’s most dangerous jihadists no longer answer to al Qaeda. The terrorists we should fear most are self-recruited wannabes who find purpose in terror and comrades on the Web. This new generation is even more frightening and unpredictable than its predecessors ...”¹⁸

Another highly relevant question to consider is whether it is becoming more difficult to fight against terrorists using purely conventional means? Is traditional international cooperation and information sharing between intelligence agencies sufficient to confront the current threat? Or is there a need to entirely rethink counter terrorism measures? Still further, do we need a total restructuring in the field of intelligence? It should be noted that at the beginning of 2008, two underwater cables were destroyed on the Egyptian Mediterranean coast. The result was an immense restriction of nearly the whole of internet traffic in the Middle East, Saudi Arabia, Kuwait, Qatar and

¹⁶ http://orf.at/060824-3138/?href=http%3A%2F%2Forf.at%2F060824-3138%2F3140txt_story.html.

¹⁷ “Spain arrests 14 terror suspects,” *BBC News online*, 19 January 2008, <http://news.bbc.co.uk/go/pr/fr/-/2/hi/europe/7197562.stm>.

¹⁸ Mark Sageman, “The Next Generation of Terror,” *Foreign Policy* 165 (March/April 2008), p.37.

even India. The Egyptian Ministry of Telecommunication stated that fully 70% of the Internet failed.¹⁹ The two very extremely stable cables ten kilometers away from each other had been destroyed nearly at the same time²⁰ but there were no visible hints of an attack. However, it should be noted that there were some appeals in the internet to attack this kind of infrastructure.²¹ If this incident really was an attack, the ability of intelligence agencies to stop it would be still very much in question.

Do we need quantitatively more or qualitatively better international cooperation for effective counter terrorism? Why does the United States—as well as the EU—demand increased efforts to achieve better cooperation? At the end of January 2008 President Bush demanded in Las Vegas, that the fight against terrorism “requires all assets of the United States, and requires coalitions working together. I mean, we need to be sharing intelligence.”²²

Does this mean that all of the decisions which have been made up until now, accordingly, were only empty words? Have all the efforts of the past years been in vain? One might well ask where precisely are the current problems in counterterrorism cooperation and collaboration. What should this cooperation ideally look like? At what level should these cooperative efforts be managed?

Additionally, we might inquire what should counterterrorism intelligence cooperation look like between agencies? The first challenge is to find out in which area useful cooperation is actually possible. Intelligence agencies have different ways of acquiring data²³:

- Human Intelligence (commonly called Humint)
- Technical Intelligence
- Material intelligence, and
- Open source intelligence.

The question is, then, in which area is useful cooperation possible? In the new information age, there is a huge amount of information available and it is nearly impossible to analyze all of it. There can certainly be useful cooperation between intelligence services in the field of “Open Source Intelligence” through more division of labor and burden sharing on particular subjects for the sake of efficiency and cost effectiveness. This would be similar to what has transpired regarding “technical intelligence.” Because of the technical

¹⁹ “Kabelschaden legt Nahost-Verbindung lahm,” <http://www.manager-magazin.de/it/artikel/0,2828,532310,00.html>, 31 January 2008.

²⁰ “Arabische Länder und Indien ohne Internet,” *Der Tagesspiegel*, 31 January 2008, <http://www.tagesspiegel.de/weltspiegel/Internet-Asien;art1117,2467361>.

²¹ <http://alekhlaas.net/forum/showthread.php?t=121738>.

²² <http://www.whitehouse.gov/news/releases/2008/01/20080131-2>.

²³ Boaz Ganor, *The Counter-Terrorism Puzzle: A Guide for Decision Makers* (New Brunswick and London: Transaction Publishers, 2005), p. 50.

and resource restrictions of some states, a division of labor can bring a real additive benefit.

Fixing the Society

If you demand cooperation in the intelligence field you must not forget to fix intelligence organizations. The more convinced the public of a state is that there is a security need for intelligence, the more the society can be convinced to support better domestic and international cooperation in this field. This situation is reflected in the willingness to give more rights to the intelligence authorities of some countries, notably the United States, in order to fight terrorism. To be sure, more authorities for intelligence and law enforcement agencies also introduce the potential danger of increased abuse of power. Therefore the society will need to maintain a special critical focus on the observance of basic rights. Thus, the winning public trust (to acquire and handle information in a proper manner within a democratic framework) is the highest precept in the field of intelligence. The more important human and basic rights for a society are, the less that society will forgive violation of these rights. This is applicable to domestic intelligence as well as for partners.

Accordingly, we might ask whether we need international agreement about common rules of conduct. That the legal prerequisites to prosecute terror suspects and cooperation between agencies of states are heading in the right direction can be seen in the example of the arresting of terror suspects in Sweden and Norway in late February 2008. The arrested Swedish and Norwegian citizens with Somali background are accused of financing terror attacks in Somalia.²⁴

Double Standards

Society will criticize what it perceives as the application of double standards in basic rights. There is no way to punish one traffic offender, so to speak, while tolerating exceeding the speed limit by another one. Opponents always use things like that for their propaganda.

As an example, there are slides from Iraq on which you can see torture described as a device to instill humiliation and to force confessions. At the end of January 2008, US Deputy Secretary of State and former Director of National Intelligence admitted in the press that the US Intelligence employed methods of torture.²⁵ One method is the “waterboarding” – a simulated inundation. Double standards in counter terrorism play a special role in moral questions. In modern states, there is generally the principle of not using information that is obtained by torture, and not permitting such information to be admissible as evidence in a court of law. But would a government decline any information if

²⁴ Mehrere Terrorverdächtige in Skandinavien verhaftet, NZZ, 29 February 2008, p. 3.

²⁵ Die Presse: Negroponte gibt Folter zu, 30 January 2008.

such information prevents attacks in their country and saves human lives? This is a real, not theoretical, dilemma.

Intelligence Sharing

Intelligence Service is often a very complex activity, and requires a large amount of money in order to work effectively. But how is it possible to share high quality information gathered with expensive means when the cooperation partner is not ready to spend (in relation) as much money as another Intelligence Service? Or do you cooperate nevertheless with “free riders” to achieve a unit conflict scenario? As a general principle, trust is the only way to achieve a better degree of cooperation, in particular for “extraterritorial” cooperation. The building of trust can only be successful through the reduction of prejudice. Common workshops and seminars should accordingly enjoy a special status. This also includes, ideally, a mutual exchange of intelligence employees from disparate organizations. This, in turn, involves another problem, namely the strained relationship between trust and control. Proponents of purely unilateral intelligence will cite “loss of control” and even sovereignty issues as a reason to oppose more collaborative counterterrorism arrangements with other services. But the cooperation between the intelligence services of the European Member States is a good example, that, in principle, a deepened level of cooperation is in fact possible.

The USA has with their NCTC (National Counter Terrorism Center) access to dozens of networks and information systems from across the intelligence, law enforcement, military, and homeland security communities, containing many hundreds of data repositories. These systems contain foreign and domestic information pertaining to international terrorism as well as sensitive operational and law enforcement activities. And the NCTC Online (NOL) serves as a counterterrorism community library of terrorism information with over 6,000 users and 6 million documents.²⁶

Common Problems in Cooperation

At times, problems can occur when a state or intelligence organization does not agree to a cooperative effort, or reduces its willingness to cooperate with others. In this case how would the intelligence services of other states react? Would they respect the decision of the sovereign state? Or would they conduct unilateral activities and conduct their own operations and try to get the information in a different way? Will pressure be applied to the non-cooperative state? Furthermore, if such a situation occurs, does it automatically imply the loss of trust in the work of security forces and intelligence? The more “intelligence failures” which are made public, the more difficult it is for politicians to defend intelligence activity in the future.

²⁶ *NCTC and Information Sharing. Five Years since 9/11: A Progress Report* (September 2006).

Internal Conflicts

A frequently underestimated problem in international cooperation is arguably the problem between competing domestic security services. There are always hints of authority problems and rivalry between security forces in states. The chairman of the German detectives Klaus Jansen commented on the reporting of the defensive information policy of the German Intelligence regarding the search for the Islamist attacker in the Sauerland: The intelligence service sucked out the information from the Common Terrorism Center (GTAZ = Berliner Gemeinsames Terrorabwehr Zentrum) in Berlin, the provincial police only taking part in the GTAZ with a very half-hearted approach.²⁷ Jansen complained that the intelligence services do not want or are not allowed to cooperate with the responsible police organs in countering Islamist terrorism.

Similarly, Robert Baer, a former CIA clandestine operations officer, also quoted in his book some inconsistencies in US domestic security agencies.²⁸ Perhaps with the help of the NCTC Online with their classified repository some inconsistencies between the agencies can be solved. When problems in cooperation in the domestic intelligence field are discovered, how is it possible to engender a better relationship between external intelligence authorities?

At any rate, it is broadly agreed that there is good international cooperation between intelligence, and the level of intelligence-law enforcement cooperation has clearly enlarged.²⁹ The wish to cooperate has especially increased after the attacks of 9/11 and the following attacks in Europe (Madrid 2004 and London 2005). We might say that terrorism has served as the primary driving force for cooperation.

Propaganda

Where can terror organizations be most easily hurt? Where are their strengths? This can only be explained with reference to their mode of operation. Terror organizations live from their propaganda. The media broadcast their strategies, goals and methods. The most important media that terrorists employ for their actions is the internet. One of the reasons for the triumphant progress of current terrorism is the internet. With the internet, terrorists are able to spread their information in a very cheap and easy way and have an enormous worldwide affect.

Perhaps we can find an effective counterterrorism strategy precisely here. If the terrorists can be successful in their propaganda campaigns, why shouldn't counter terrorism forces succeed with their own counter terror propaganda? The challenge for intelligence agencies is to identify and employ effective

²⁷ www.cop2cop.de.

²⁸ Robert Baer, *Der Niedergang der CIA* (München: Goldmann Verlag, December 2003).

²⁹ Wolfgang Braumandl und Desbalmes Christian, *Nachrichtendienstliche Kooperation der EU im Kampf gegen Terrorismus* (Schriftenreihe der Landesverteidigungskademie, 2007), p.15.

counter propaganda. But does the field of a counter narrative also lend itself to a cooperative effort? Research in this area is critical. It is highly important to analyze under which conditions and with which arguments young Muslims can be lured away from the Jihad. But such an effort can only work with the help of moderate Imams who can provide resonant counter arguments to the jihadist hate campaigns. Is it possible to accept an Imam as a special adviser on counter terrorism issues? Is there a need to employ more Muslim specialists in Western intelligence services? Is there an additional need to cooperate and to share more information and analyses with intelligence services from Muslim countries?

Privatization of Intelligence

There is too little attention paid to the “privatization of security” where intelligence obtaining measures are concerned. This also provokes the “competence solving measures” of intelligence agencies and can also be a public rivalry.³⁰ The private sector (catchphrase “Intelligence Commercialization”) is constantly increasing. So the question is: can also private intelligence play a special role in counter terrorism? There is a need to address whether there is a logical requirement for cooperation between state intelligence organs and private intelligence organizations.

Conclusion

Intensive cooperation in the field of Intelligence creates trust which, at the same time, is a contributing factor for a better relationship between states and therefore can also be a peace-building measure. Trust is a critical building block for intelligence sharing. Common training measures are important steps in the right direction. Organizations have to undergo a steady change to establish their stability, efficiency and identity. Therefore changes are always needed. The so called status quo is a “dynamic condition.”³¹

Homeland security and intelligence sharing in combating terrorism is also an “ongoing project.” Available examples show that good results have been obtained from cooperative intelligence efforts. Nevertheless, it is also important to understand that intelligence capabilities must be improved at the local level. Subsidizing the construction of intelligence fusion centers may be valuable in this regard, but does not create intelligence capability by itself. That requires manpower and training, which also require continued support, and, equally important, a “less bureaucratic approach to the ownership of intelligence information.”³²

³⁰ Ibid., p. 46.

³¹ Ralph Grossmann, *Kooperationen im Public Management* (Weinheim und München: Juventa Verlag, 2007), p. 63.

³² Brian Michael Jenkins, *Basic Principles for Homeland Security* (RAND Corporation, 30 January 2007), p. 2.

The relevance of intelligence agencies and their important and excellent work must be brought home to people. Especially, the success achieved through robust intelligence sharing must be demonstrated – with the understanding that more public relations is needed. A splitting of responsibility in the field of “Open Source Intelligence” can lead to the timely and financially prudent saving of resources. The data base of NCTC could be a good example for transnational cooperation. But, in terms of international cooperation, what authority should give the right of access to such a transnational data base? Who should receive which information and when? The former German Minister of the Interior Dr. Wolfgang Schäuble remarked in a speech in November 2007 at a BND Symposium in Berlin: “The most important instrument in counter terrorism is intelligence.”³³

Therefore, intelligence sharing must be seen as an activity of paramount importance. To fight terror with terror³⁴ is the same as an eye for an eye, a tooth for a tooth, and in the long term is not linked to ultimate success.

³³ http://www.bmi.bund.de/cln_012/nn_165104/Internet/Content/Nachrichten/Reden/2007/11/BM_BND_Symposium.html.

³⁴ Kontraproduktive US-Strategie: “Terror mit Terror bekämpfen,” APA 0071, 11 October 2001.