

**MAX PLANCK INSTITUTE
FOR FOREIGN AND INTERNATIONAL
CRIMINAL LAW**

COUNTERTERRORISM POLICIES IN GERMANY*

HANS-JÖRG ALBRECHT

Contents:

1. Introduction into Experiences with Terrorism and the Development of Counterterrorism Strategies in Germany	2
1.1 Terrorist Phenomena in Germany	2
1.2 Responses to Terrorist Activities and Organizations between 1970 and 2000	5
2. After 9/11 Counterterrorism Strategies	44
2.1 Introduction.....	44
2.2 Counterterrorism Policy after 9/11	49
2.3 The Flow of Legislation after 9/11	50
2.4 Dangerousness and incapacitation	58
3. Summary	61
3.1 Legislation issues.....	61
3.2 Policies.....	61
Literature	62

* Originally published as: Country Report on Germany, in: Rudie Neve, Lisette Vervoorn, Frans Leeuw, Stefan Bogae (eds.), Een eerste inventarisatie van contraterrorebeleid: 'Policy and research in progress' in Duitsland, Frankrijk, Italië, Spanje, het Verenigd Koninkrijk en de Verenigde Staten [A first inventory of counterterrorism policy: policy and research in progress in Germany, France, Italy, Spain, the UK and the US], The Hague 2006 (WODC).

1. Introduction into Experiences with Terrorism and the Development of Counterterrorism Strategies in Germany

1.1 Terrorist Phenomena in Germany

Experiences with terrorism in Germany date back to the end of the 1960s and the beginning of the 1970s when the RAF or “Baader-Meinhof” group emerged as a terrorist organization. The RAF fell into the subcategory of social-revolutionary (left wing) terrorism, guided by an explicit political programme and political goals as well as an explicit appeal to international coordination and cooperation among (national) terrorist groups (Laqueur 1998). Terrorist violence was directed against individuals representing political parties, the government, the capitalist economy or the US military (Peters 1991). Links between the RAF and Palestinian terror groups were established in the early 1970s. Such links resulted in the use of Palestinian training camps by several members of the RAF group and the launching of joint terrorist attacks (Entebbe, Vienna). RAF strategies also included acts of transnational terrorism (Stockholm embassy 1975; Wittke 1983). Beside the RAF, which after the arrest of its leading figures in the first half of the 1970s was succeeded by second and third generation terrorist groups (closely related to groups supporting detained RAF members and active in rallying support during ongoing criminal trials against RAF members), other groups developed out of the youth and student movement (and the rallying impact of the Vietnam war). Although these latter movements never gained much momentum, they nevertheless engaged in several spectacular acts of violence (Wittke 1983). The RAF disbanded – according to statements of then members of the group – shortly after German re-unification in the early 1990s. Disclosure of documents of the former GDR revealed that the RAF was supported by the former GDR Ministry of State Security and the state security secret police. Such information also uncovered a number of former members of the RAF living in the territory of the former GDR who, since their retirement in the late 1970s and early 1980s, had settled down (evidently with the permission of the GDR government) and led ordinary lives.

Right wing terrorism surfaced in the second half of the 1970s with small militant groups aggressively furthering Nazi ideology. These groups were detached from right wing political parties. Such groups attempted to establish military style training camps in the 1970s – on a rather small scale – but never managed to instigate effective terrorist campaigns. However, a bomb explosion at the Munich “Oktober Fest” in 1980, that could be linked to right wing extremism, claimed some 13 lives (among them the terrorist himself) and clearly signaled the existence of right wing extremist violent groups and individuals ready to commit terrorist acts. Except in this case, right wing extremism and, in particular, right wing violence, are presently confined to acts of hate violence carried out in small groups and directed against immigrants and visible minorities. In particular in the East of Germany (however, not entirely restricted to the East) over the last decade locally organized right wing extremist groups emerged which – according to assessments of intelligence services and police – recruit members among violence prone young men and engage in violent acts that occasionally amount to terrorist activities. Besides visible minorities and the Jewish minority other groups (left wing activists, the disabled and homeless) are also targeted by hate violence. For example, a group of right wing activists was dismantled in 2003 by Bavarian police. The group allegedly conspired to carry out a large scale bomb attack in Munich directed against Jewish targets. The subsequent trial (2004) revealed that the group was loosely organized, poorly trained and evidently not in a position to carry out well planned and effective terrorist acts. Nevertheless, the Federal General Prosecutor decided to prosecute the case before the Bavarian High Court which has jurisdiction over selected political offences (offences affecting security of Germany) and to indict the group members on the basis of having formed and/or being a member of a terrorist group (§129a German Criminal Code). The leading figure of the group, Martin Wiese, was sentenced to seven years imprisonment; other group members received suspended and unsuspended prison sentences of up to 5 years. Evidently, the borderline between organized right wing hate groups on the one hand and organized crime, soccer hooliganism and ordinary violence on the other is blurred and there seems to exist considerable overlap.

Another line in the development of terrorism on German soil concerned foreign terrorist groups active in Germany. The Kurdish PKK (re-named in

1999 into KADEK and today named KONGRA-GEL) – as a result of substantial numbers of Kurdish immigrants in Germany – was involved in raising funds (“taxes”) from the Kurdish immigrant community for the violent struggle of the PKK in Turkey and resorted to violence and threats in extorting money from the Kurdish community. The PKK was also involved in terrorist attacks on Turkish businesses and embassies as well as violence exerted to keep in line with PKK interests, Kurdish communities, and members of the group (Verfassungsschutzbericht 2002, pp. 202). The PKK was banned by order of the Federal Minister of the Interior in 1993. Law enforcement activities resulted in several large trials against PKK members carried out during the 1990s. Subsequent to the arrest and conviction of the head of the PKK, Öczalan, PKK activities in Germany dried up. The PKK was re-founded as KADEK in 1999 and finally was re-organized as Kurdish People’s Congress (KONGRA-GEL). However, it is assumed that despite claims to change from an organization geared towards establishing a Kurdish state by violent means into a political party using political means in achieving the aim of independence, there still remains a large potential for violence.

A singular act of terrorism committed by a Palestinian terror group targeted the Olympic games held 1972 in Munich, and in particular the Israeli Olympic team. The bloodshed following the botched attempt to free Israeli hostages led to heavy criticism of police and certainly disclosed that German security forces were not well prepared to effectively counter well organized terrorist attacks. Responses included the foundation of the GSG9 – commandos specialized in counterterrorism – on the federal level (GSG9 was part of the former Federal Border Police) as well as the creation of police task forces and SWAT teams on the level of the states.

Debates in the 1990s that emerged around the sensitive issue of asylum and immigration pointed to a risk that Germany may be used as a safe haven by foreign terrorist groups. Discussed were Islamist radical groups from Algeria involved in the civil war there, the PKK, Chechen groups, Chinese Uigur and radical Palestinian groups. The events of 9/11 resulted in a large scale revision of the terrorist landscape as described in official documents and political and police accounts and placed transnational (religious or cultural) terrorism at the center of political and police attention.

1.2 Responses to Terrorist Activities and Organizations between 1970 and 2000

1.2.1 An Overview of the Institutional/Organizational and Legislative Structure of Counter-Terrorism in Germany

1.2.1.1 Constitutional Arrangements

Germany is a federal state which has entrusted fields of “internal security” (and with that police and policing) almost completely to the states. According to Art. 72 of the German Federal Constitution, the states have exclusive power of legislation in all those areas where the Constitution does not explicitly assign legislative powers to the Federal Parliament. Legislation on security related matters (police etc.) are mentioned in Art. 73 (No. 10) which restricts federal legislation to issues of cooperation between the federal and state levels in the fields of criminal police, the protection of the democratic order of the Federal Republic of Germany, the maintenance of the security of the Federal Republic and the single states, and the protection from attempts to endanger the foreign affairs related interests of Germany by exertion of violence or conspiracies to exert violence. Furthermore, Art. 73 No. 10 empowers the federal level to legislation on establishing a Bundeskriminalamt (Federal Criminal Office) and on the international control of crime (internationale Verbrechensbekämpfung).

The German Federal Constitution (Art. 21) then particularly protects political parties and foresees that the prohibition and dissolution of political parties are possible only after an indictment and trial before the Federal Constitutional Court on the basis of evidence that a political party attempted to destroy or harm the democratic and rule of law based order of the Federal Republic of Germany or attempted to eliminate the Federal Republic of Germany.

The Constitution restricts in Art. 87a the deployment of military forces (Bundeswehr) to war or pre-war situations and allows deployment on the territory of the Federal Republic of Germany (and for reasons of internal security) only if grave risks for the existence of the Federal Republic of Germany cannot be prevented otherwise. With that, a strict separation of external (military) and internal security (police) has been introduced.

1.2.1.2 Counter-terrorism Legislation

1.2.1.2.1 Introduction

Counter-terrorist strategies unfold within the framework of existing legislation. Anti-terrorism legislation is enacted in parallel and as a response to the development of terrorist phenomena described in the introductory remarks. Counter-terrorism legislation represents cross sectional legislative activities made up of amendments to immigration laws, police laws, laws on secret services, telecommunication laws, general criminal and procedural laws, economic laws, general order laws as well as legislation establishing particular powers in monitoring professional activities in sensitive areas. Out of this cross sectional nature follows the basic problem associated with anti-terrorist legislation. This type of legislation interferes in civil society in a way which understands freedom and uncontrolled spaces as potential risks that are then put under a general suspicion. Immigrants and asylum seekers, religious organisations and political movements, ethnic minorities, foreign nationals and transnational communities, workforce participants that are associated with security risks are made targets of supervision.

1.2.1.2.2 Federal and state police laws

Legislation addressing issues of counter-terrorism impacts upon state legislation on police (*Landespolizeigesetze*) which regulate the powers of uniformed and criminal police. Police, according to police laws, have the function of maintaining order and security on the territory of the states (a second function refers to crime investigation which is regulated in the federal criminal procedural law).

The Law on the Federal Police Office (*BKA Gesetz*) outlines tasks and powers of those Federal Police working within the *Bundeskriminalamt*. The Law on Federal Police (*Bundespolizeigesetz*) addresses issues of police control and monitoring of the federal border as well as particular places on the federal territory such as airports and railway stations.

With respect to state police laws, significant changes took place in the last few decades. Of particular importance are the legal amendments that inserted so called proactive investigative techniques (also available in the German criminal procedural law) into police laws. While such investigative

techniques within the framework of criminal procedural law should serve primarily repressive functions, the very same investigative methods under the goals of police laws must be justified with preventative reasons. Such methods may be applied in order to enable police to prevent risks from turning into harmful situations. Here, we find undercover police, informants, telecommunication surveillance, the use of technological devices (audio/video equipment) and (in some state police laws) also surveillance of communications at private premises/homes falling under the particular protection of Art. 10 German Federal Constitution (Grundgesetz).

1.2.1.2.3 Laws on intelligence services

Legislation on internal intelligence services is found in the state laws on “Verfassungsschutz” (literal translation: Offices for the protection of the constitution) and federal legislation has been enacted on the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz).

Federal Office for the Protection of the Constitution was established in order to protect the constitutional order (or the very substance of the democratic order as laid down in the Federal Constitutional Law/ Grundgesetz) of the Federal Republic of Germany (§1 Federal Law on Internal Intelligence (Bundesverfassungsschutzgesetz). It has the task to collect information relevant to the prevention of dangers arising out of attempts to destroy this order, out of activities of foreign intelligence services active on the territory of the FRG, out of activities directed against the peace of nations etc. (§3). According to §8 the Federal Office for the Protection of the Constitution is authorized to use various methods to secretly collect information. Such methods concern the deployment of informants, the use of audio and video technology and undercover operations. But, the office has no enforcement powers (and may not demand executive powers (police) for (substitute) enforcement). In individual cases the office may retrieve data from financial institutions and banks, postal services, airlines and telecommunication providers (traffic data). Retrieval of data from airlines, financial institutions and telecommunication providers requires an application in writing and with grounds for justification provided; moreover, actual evidence must speak for serious dangers for selected protected values.

Intelligence services which have the task of collecting information about risks and threats coming from outside the territory of the Federal Republic of Germany fall under the exclusive authority of the federal level. Here, we find the Law on the Federal Intelligence Service (Bundesnachrichtendienst) as well as the Law on Military Intelligence Services (Militärischer Abschirmdienst).

Powers to intercept telecommunication are regulated for all intelligence services in a separate law (G 10 Law, see below).

1.2.1.2.4 Substantive and procedural criminal law

Criminal procedure law and substantial criminal law are federal laws, however, the administration of justice (courts and public prosecution services) is assigned to the state with the exception of the Office of the Federal Public Prosecutor which has jurisdiction over political (and with that terrorist) crimes that aim at endangering or destroying the democratic order of Germany. Furthermore a range of other political criminal offences fall, according to the Law on the Constitution of Courts, under the jurisdiction of the Federal Prosecutor General (Generalbundesanwalt). In particular, terrorist organization offences (§129a, b) are prosecuted by the Federal Prosecutor General.

1.2.1.2.4.1 Criminal offence statutes and counterterrorism

German substantive criminal law (Strafgesetzbuch) contains a range of criminal offence statutes that are of relevance in responding to terrorism and activities concerning terrorist acts. However, criminal offence statutes are also annexed to administrative laws that can be of relevance in investigating terrorism.

A first group of criminal offence statutes are linked to activities around *banned political parties and groups and propaganda* activities. The rationale behind such offence statutes has been to counter communist and Neo-Nazi political movements – perceived to be particularly dangerous in light of the processes leading up to the fascist rule from 1933 to 1945.

Section 84 threatens criminal penalties (up to 5 years imprisonment) for anybody who continues to organize a political party or be a member of such a party which has been declared unconstitutional by the Federal Con-

stitutional Court or an organization which has been banned by order of ministries of the interior (federal or state). Section 85 addresses the creation and maintenance of substitutes for prohibited organizations or parties. Dissemination of propaganda for prohibited organizations and parties is also criminalized (Section 86). Dissemination of propaganda is prohibited, too, if such propaganda comes from a government organization or institution based outside the territory of the Federal Republic of Germany and pursues the same objectives as the ones pursued by prohibited organizations or parties. Dissemination of propaganda which is intended to further the aims of former National Socialist organizations is also punishable (imprisonment of up to three years or a fine). Section 86 II restricts the meaning of propaganda to such written material which is directed against a free and democratic order (as protected by the constitution) or against the peace of nations. Section 86a penalizes the (domestic) distribution or public use/display of symbols of prohibited organizations or parties, their production, import or export.

Sabotage of sensitive infrastructure intending to damage interests of the Federal Republic of Germany

Sections 87 and 88 criminalize acts of sabotage against facilities of national defence, the economy or sensitive infrastructure (telecommunication, water, energy etc.) carried out by groups or individuals in pursuit of goals directed against the Federal Republic of Germany or its constitutional principles.

Breaching the peace and incitement to crime

Public incitement (successful and unsuccessful) to a criminal act is punishable according to Section 111. Conventional “breaching public peace” offences as well as the offence of forming an armed group are found in section 125, 126 and 127.

Criminal and terrorist organizations

Forming and running a criminal group/organization is penalized by section 129. §129a specifically addresses terrorist organizations (without defining explicitly a terrorist group). Other than the criminal organization/-group which is defined through the objective of committing any criminal offences, a terrorist organization is defined through the goal of committing

crimes listed in a catalogue of criminal offence statutes (for example murder, genocide, taking hostages etc.). Moreover, §129a upgrades support of or recruitment for a terrorist group to a separate criminal offence (§129a III). §129 VI contains a clause that, in the case of voluntary and serious efforts to prevent continuation of the criminal organization or in the case of disclosure of information that can be used in preventing crimes to be committed by the criminal organization, provides for mitigated punishment or complete exemption from punishment (at the discretion of the court). If the continuation of the criminal organization is successfully prevented, then punishment (because of breaching Section 129) may not be imposed. §129 VI is also to be applied in cases of terrorist organizations and thus contains a limited crown witness rule. In the wake of 9/11 §129b has been introduced. §129b extends the reach of §§129 and 129a to organizations and groups based outside the territory of the Federal Republic of Germany. Organizations and groups outside the territory of the European Union fall under sections 129, 129a only if an act (establishing the criminal offence of §§129 or 129a) has been committed on the territory of the Federal Republic of Germany or if offender or victim is a German national or resident of Germany. In the latter cases prosecution requires the consent of the Federal Ministry of Justice. Consent can be given for individual cases or generally. When making decisions on consent, the Ministry shall consider whether the aims of the organization/group run counter to the basic values of state order based on human dignity or against the peace of nations and whether – all circumstances considered – such goals are assessed to be of a low character.

Denial of the holocaust, incitement to hatred, dissemination of instructions on how to commit crimes and dissemination of graphic descriptions of violence/glorification of violence

Some criminal offence statutes deal with incitement and propaganda activities. Denial of the holocaust has been penalized (§130) in order to respond to right wing extremism and Neo-Nazi groups/parties. In 2005, the offence of denial of the holocaust has been expanded. Glorification, legitimating or approving the national-socialist (Nazi) terror regime when done in public and in a way which disrupts the public peace and infringes on the dignity of victims (of the Nazi regime) is punishable with imprisonment for up to three years or a fine.

According to §130 a criminal offence is established if somebody publicly incites hatred or calls for violence against social groups/segments of the population or assaults human dignity through insulting or defamatory statements if such acts may disrupt the public peace. Dissemination, displaying etc., of written material that pursues incitement of hatred, calls for violence or assault human dignity establish a criminal offence (§130 II). Dissemination, publicly displaying etc. of instructions how to commit certain crimes when intended to encourage others to commit such crimes is penalized by Section 130a. Finally, dissemination, publicly displaying graphic descriptions of cruel or inhuman acts against humans in a way which glorifies such violence, or downplays the harm of such violence or emphasizes the cruel and inhuman aspects of such violence provided that the way of presentation infringes on human dignity establishes a criminal offence (carrying a maximum of one year imprisonment). Journalist accounts on historical or current acts of violence are exempted from section 131 (§ 131 III).

Taking hostages

Taking hostages in order to commit extortion (§239a) or to coerce the hostage or another person (§239b) carries a minimum of five years and a maximum of 15 years imprisonment.

Sabotage of sensitive infrastructure and interference with air and maritime transportation

§§ 316b, 316c, 317, 318 penalize (partially as a consequence of the ratification of several anti-terrorism conventions) sabotage of sensitive public infrastructure (transportation, water and energy supply, telecommunication etc.) and the interference with air and maritime transportation. Maximum penalties range between 5 and 15 years.

Criminal Offences related to nuclear materials

Unlawful possession, trafficking, import, export etc. of nuclear material is penalized through §328 criminal code. §328 represents an endangering offence statute which does not require the establishment of a concrete danger arising out of dealing unlawfully with nuclear material. It is sufficient that the material is generally suited to result in death or serious bodily harm to other persons. Criminal penalties also apply to a violation of duties es-

tablished by the Law on Nuclear Substances (Atomgesetz), the procurement of nuclear material by persons who have no authority to possess such substances lawfully and the causing of a nuclear explosion. Handling other dangerous substances in the context of an enterprise – as listed in the Law on Chemicals – or handling dangerous substances in general in violation of administrative duties is punishable according to §328 III.

Bombings, use of explosives and conspiracy

With §307 causing a nuclear explosion has been penalized. In §308 causing an explosion by conventional means is also criminalized. §310 provides for a separate offence of conspiracy with the aim to cause nuclear or other explosions (bombing).

Crimes against Internationally Protected Persons

§102 provides for a maximum of five years imprisonment or a fine for carrying out an attack on a foreign head of state, a member of a foreign government or the head of a diplomatic institution when such person sojourns on the territory of the Federal Republic of Germany.

1.2.1.2.4.2 Criminal procedural law

German criminal procedural law has been amended on various occasions as a response to terrorism.

Holding prisoners incommunicado

When the then head of German Associations of Employers, Schleyer, was held hostage by members of the RAF in 1978 with the release of detained members of the group being demanded by the hostage takers, it was suspected that the offence was orchestrated by leading figures of the RAF from within prisons and with the support of lawyers communicating with the hostage takers. The government therefore decided to keep those leading figures incommunicado for the time of the hostage case carried on (Wächtler 1979). Withholding access in particular to lawyers was justified with necessity (and preponderance of interests of the hostage). However, a Supreme Court ruling clearly addressed the problem by pointing out that acceptance of “necessity” as a sufficient basis for executive powers would amount to a catch all authorization and would undermine the rule of law principle. But,

in the specific case justification of withholding communication between lawyers and detained prisoners and suspected terrorists with necessity was accepted in terms of assuming a unique case as the legislature evidently had not foreseen (when creating criminal procedural law) that lawyers would collude with prisoners in carrying out serious crimes. The legislative response then was the introduction of rules to permit the imposition of a period of being held incommunicado by court order. According to §31 Introductory Law to the Law on Constitution of Courts (Einführungsgesetz zum Gerichtsverfassungsgesetz), a prisoner convicted or suspected of being a member of a terrorist organization may be subject to restrictions of communicating with lawyers (and other persons), provided that there exists an immediate danger to the life of another person, for a period of up to 30 days (for a discussion of restrictions of access to lawyers and Art. 6 of the European Convention on Human rights see Safferling 2001).

Trial in the absence of an accused

§§231a and b were introduced in the Criminal Procedure Code in order to be able to continue a criminal trial if the accused has put him-/herself in a state of being unfit for trial or if the accused has provoked his/her exclusion from the trial because of misconduct.

Pretrial detention and terrorism

When §129a (terrorist organization) was introduced rules on pretrial detention were amended too. §112 III Criminal Procedure Code which allows for pretrial detention alone on the ground that strong suspicion of murder (or genocide) can be established has been expanded to include allegations of being the founder or a member of a terrorist group.

Jurisdiction over cases of §129a, b

The Counter Terrorist Law of 1976 established jurisdiction of High courts (Oberlandesgerichte) over cases of §129a (74a Law on the Constitution of Courts, Gerichtsverfassungsgesetz) and assigned the power of prosecution of such cases to the Federal Prosecutor General. This, in fact, had the consequence of centralizing prosecution and investigation of terrorist cases as investigating judges (deciding on arrest warrants etc.) now come from a small group of federal Supreme Court judges.

Defence councils and terrorist trials

Experiences with the first trials carried out against alleged terrorists of the RAF in the 1970s showed that the accused were represented by a multitude of defence councils who themselves were representing sometimes more than one of those tried in the same proceedings and that trial procedures were, as a result, heavily delayed. Furthermore, in the wake of the suicides of the remaining leading figures of the RAF after the failed attempt to free them in 1978, it became known that several defence councils had conspired with prisoners and in particular had smuggled guns and other items into the prison. The answer of the legislature was to limit the number of defence councils to three per suspect or accused (§137 Criminal Procedural Code) and to prohibit a defence council from representing more than one accused in the same criminal proceeding. In the case of trials that include allegations of §§129a, b German Criminal Code the possibility of excluding lawyers from representing an accused was expanded (§138a German Criminal Procedural Code). Furthermore, in terrorist cases a judge may order that communications between defence council and prisoner be subject to control. Subsequent to such an order, mail may be refused to be delivered (to the defence council or to the prisoner) if the sending party does not agree with the control of mail by an investigative judge. If an order is in place, meetings between the defence council and the prisoner have to take place in a way that precludes letters or other items from being exchanged (§148 II German Criminal Procedural Code).

The anonymous witness

Another amendment of criminal procedural law concerns protection of vulnerable witnesses, in particular witnesses that are at risk of falling prey to retaliatory acts (§68). Such vulnerable witnesses may remain anonymous.

Proactive investigative techniques

From the 1980s on in addition to terrorism the topic of organized crime started to play a significant role in pushing German criminal law reform, in particular reform of criminal procedural law (Albrecht 1998). Organized crime became especially important in justifying the introduction of new or covert (or proactive) methods of criminal investigation. This was due to the

apparent need to extend investigative methods beyond those techniques of investigation which rely primarily upon information provided by victims of crime. Victimless crime and transactions crimes, essentially informal economies and black markets where conventional triggers of criminal investigation are not available, demand for an active role for police and prosecution services in generating initial information on criminal cases.

In 1993, the law on Control of Drug Trafficking and Other Forms of Organized Crime (Gesetz zur Bekämpfung der Betäubungsmittelkriminalität und anderer Formen organisierter Kriminalität) came into force. This law touched both basic criminal law as well as criminal procedural law. In basic criminal law, new sanctions were introduced and aggravating circumstances for certain types of crimes were re-organized – giving particular attention to property, violent and drug offences committed in the context of gangs and criminal networks/criminal organizations. Here, it was especially the new penalty of confiscation which added a new line in the system of criminal sanctions. Then, a whole range of new procedural devices were introduced which change the character of the criminal procedure tremendously. These changes concerned first of all the introduction of new and the extension of old investigative techniques, among them the undercover agent, computerized information screening, telephone tapping and other electronic surveillance measures, long term observation and the crown witness. Furthermore, the emergency powers of police and public prosecution were expanded. The Crime Control Law 1994 (Verbrechensbekämpfungsgesetz) must also be mentioned, as, through this law, the exchange of information between intelligence services and police was authorized (Köhler 1994).

As regards new criminal investigative techniques, first, a dragnet procedure based upon electronic information reduction techniques has to be addressed (Rasterfahndung, §§98a-c Criminal Procedural Code). This investigative method had already been implemented (without a statutory basis) in the 1970s as an instrument to identify apartments and other locations used or frequented by suspected terrorists of the RAF. The creation of a statutory basis, however, was necessary as the Federal Constitutional Court in a decision of 1983 (BVerfGE 65, pp. 1) had ruled that collection, use etc., of personal data infringes upon the right to privacy (right to self-determination of personal data (Recht auf informationelle Selbstbestimmung) Art. 2 Grundgesetz).

Modern societies produce enormous amounts of information on individuals in various public or private sectors. Credit card companies, telephone companies, social service administration, housing agencies and many other institutions collect data from their clients. §§98a-c Criminal Procedural Code empower police and public prosecutors to search these information systems by using certain matching techniques in order to filter out smaller groups of individuals who, in principle, fit into profiles established for certain groups of offenders (e.g., terrorists or drug traffickers). Critics argue that the principle of proportionality might be violated as with such techniques privacy of a large number of innocent citizens is infringed upon and large numbers of actually innocent citizens fall under the scope of police investigations and public prosecution.

Wire tapping had been authorized in Germany by a legal amendment of 1968. The introduction of wiretapping in the second half of the 1960s was justified with needs of intelligence services and subsequently by needs of effective law enforcement in the field of illicit drugs. Surveillance of telecommunication in order to be legal and to generate evidence that can be introduced in a trial has to comply with requirements set out in §100a German Criminal Procedural Code. According to these requirements an order of telecommunication surveillance has to be issued by a judge. However, in emergency situations a public prosecutor may order surveillance (a judicial confirmation has to be sought as soon as possible and the order becomes ineffective automatically if it is not confirmed by a judge within 3 days). Telecommunication surveillance may be ordered in case of (simple) suspicion of a criminal offence listed in a catalogue attached to §100a Criminal Procedural Code. An order is to be issued only if telecommunication surveillance is assessed to be the “last resort” in investigating a catalogued crime or in locating the suspect. A “last resort” situation may be assumed only if other investigative methods would be unsuccessful. The order may only be made against the suspect or against third persons who either receive messages for the suspect or transmit messages from the suspect or whose telephone lines are used by the suspect. The order must be given in writing. It must indicate the name and address of the person against whom it is directed as well as the telephone number or other identification of the person’s telecommunication connection. The type, extent and time of the measures shall be specified in the order. The order is to be limited to a maximum of 3 months. An extension of not more than 3 months is admissible if requirements as set out under §100a continue to

exist. If the conditions spelled out in §100a no longer prevail, the measures resulting from the order must be terminated immediately. Information obtained by a wire tap may be used as evidence in other criminal proceedings only insofar as such information relates to a criminal offence listed in the catalogue of §100a. Conversations between the suspect and individuals entitled to a professional duty to remain silent (lawyers, priests, physicians) may not be intercepted nor may their content be used as evidence. Those affected by a wire tap must be informed after completion of the criminal investigation at a time when such information would not obstruct the course of justice (§101 German Criminal Procedural Code). Another problem related to the use of deceptive and covert investigative techniques concerns the use of information found by chance. Wiretaps may, for example, generate information on other crimes not related to the offence which is investigated or on suspects until then not known to police. Using covert surveillance technologies, information may be produced which is not relevant to the case being investigated but could prove to be useful in launching further criminal investigations and proceedings because of other offences detected during the course of observation and surveillance. In order to restrict the use of so-called “random hits” (Zufallsfunde) the German legislature has opted for a compromise. If new investigative techniques produce information which was not intended to be produced but in principle could lead to criminal procedures then only such information may be used which establishes the suspicion of criminal offences for which the respective surveillance techniques legally could have been applied.

While the content of telecommunication may be intercepted on the basis of §100a German Criminal Procedural Code, seizure of traffic data collected by telecommunication providers had been regulated (with imposing essentially the same conditions as applicable for content data) by §100g Criminal Procedural Code.

Eavesdropping (on private premises), according to §100c Criminal Procedural Code, may be authorized – as is the case for wiretaps – in the case of serious crimes listed in a catalogue annexed to §100c and under those conditions required for wiretapping. However, other than for wiretaps judicial authorization requires a decision made by the criminal chamber of the district court (and not by an individual investigative judge). Authorization of eavesdropping is limited to a period of 4 weeks (which can be extended to further periods of 4 weeks on the basis of separate judicial decisions). As

is the case with wiretaps professional secrecy is protected by way of introducing a prohibition to listen to conversations between members of certain professions and their clients. In addition, the use of information stemming from conversations between relatives (who are entitled to refuse testimony against each other) is limited insofar as a balancing of interests (of the right to remain silent and of law enforcement) must lead to the priority of the interest in law enforcement.

The Federal Constitutional Court, in a recent decision (Federal Constitutional Court, decision as of March 3 2004, 1 BvR 2378/98; 1 BvR 1084/99), held that the statutory authorization of eavesdropping on private premises complies, in principle, with constitutional requirements, but that statutory requirements must enable the absolute protection of the core of private communication (in intimate relationships) which may not be subject to a balancing of interests and foresee procedural safeguards that under all conditions allow for protecting this core of intimate communication. Insofar, the Federal Constitutional Court ruled that the current statutory framework of wiretaps and eavesdropping in Germany does not comply fully with proper protection of the fundamental right to privacy as it does not provide regulation which prevents information being collected and used when such information belongs to the core area of privacy.

Other surveillance technologies have been introduced through the 1993 legal amendment with §§ 100c, d that allow for the electronic and video based surveillance of suspects. Police may follow up suspects supported by video cameras as well as other electronic equipment in order to visually and acoustically tape the communication and behaviour of suspects. Another investigative technique has been introduced with “undercover policing” (§§110a-e CPC). With undercover policing a series of legal problems come up that can be summarized under the heads of “deception” and “secrecy”. An undercover agent, according to German criminal procedural law, is a police officer who has adopted a “legend” and thus has changed his or her identity. False documents and false names should - according to the official reasoning - enable an undercover agent to penetrate gangs and organized criminal networks in order to procure evidence that otherwise (and with traditional methods) would not be obtainable. The undercover agent is empowered to approach other people as well as to enter private premises under disguise and to deceive others as to his or her true identity. The basic reason to introduce such methods of investigation lies in the con-

ception of organized crime which is seen to create heavy obstacles for traditional methods of criminal investigation. Nevertheless, such investigative procedures bring about several legal problems such as the circumvention or neutralization of basic rights of suspects – among which the right to remain silent as well as the right not to be obliged to support investigative authorities in producing evidence against him or herself are included. Furthermore, the right to remain silent also applies to certain categories of relatives who are not obliged to give testimony. The legislature therefore has restricted the use of undercover agents to cases of serious crimes and tried to limit such investigative techniques to cases where traditional investigative techniques presumably would not be successful. What can also be observed is a dislocation of powers from the judiciary to the investigation authorities. Pre or post facto control of the use of undercover policing through the judiciary is reduced to exceptional cases (§110b CPC). What we find here is also clear evidence that this type of pre-pre-trial investigation is seen to be a merely executive task. Insofar, the investigative strategies allowed through undercover policing set further limits to the implementation of the principle of legality. Undercover policing and covert investigative methods are based on discretion and it is up to the investigative authorities to choose among the crimes and groups of potential suspects which should be subject to undercover policing.

What was not regulated in the amendments to the criminal procedural law during the nineties is the role and deployment of so-called “whistleblowers” or private informants during pre-trial investigations as well as provocation of criminal offences by law enforcement officers. Such informants have been heavily used since the seventies, essentially out of the very same reasons which triggered legislation on undercover policing. There are two techniques applied with private informants. First, private informants usually are used to provoke crimes. So, for example, a regular method is buy and bust techniques in drug markets: a private informant approaches another person and asks him or her to sell illegal drugs. When drugs and money are passed over police, having observed the transaction, interfere and arrest the trafficker. Second, private informants are used to trigger information out of suspects (or other people likely to refuse to cooperate with police) in terms of confessions or other information leading to evidence. However, the statutes regulating undercover policing may not be applied to private informants. But, the Supreme Court has ruled several times that private informants and the provocation of criminal offences can

be used legitimately under certain conditions. These conditions stipulate that offences investigated by means of private informants must be crimes of a very serious nature and that those individuals approached by private informants can be assumed to be already involved in the types of crimes they should be provoked into. If such conditions are not complied with the trial court may mitigate punishment. Heavy criticism was and still is raised in respect of the Supreme Courts decisions that authorize these types of investigative activities which are said to create conflicts with basic procedural and other rights among them the right to remain silent. The European Court of Human Rights – contrary to the decisions of the German Supreme Court – has ruled that provoking crimes under certain conditions violates the European Convention on Human Rights and therefore precludes that criminal proceedings be carried through (EGMR (European Court of Human Rights) *Strafverteidiger* 1999, pp. 127).

Finally, another newly introduced technique of criminal investigation concerns “police observation”. With police observation, information on suspects or persons assumed to have contacts with a suspect can be collected routinely during police controls in order to facilitate the location of a suspect. This type of investigation may run for a period of up to 12 months.

Police laws and introduction of proactive investigative techniques for the purpose of preventing dangers and crime

While surveillance of telecommunications (and other proactive investigative techniques) within the context of criminal proceedings may be applied only for repressive purposes, in police laws they serve preventive aims. In 2003, the parliament of Lower Saxony enacted a new police law that in §33 authorized the police to intercept telecommunications (1) in order to prevent an immediate danger to life, limb or freedom of a person, (2) in order prevent serious crimes or to facilitate prosecution of such crimes if facts justify the assumption that individuals will commit serious crimes and if prevention is not possible by other means, and (3) in order to monitor persons close to individuals mentioned under (2) if this is absolutely necessary in order to prevent serious crimes or to provide for prosecution of such crimes.

The Federal Constitutional Court has held in 2005 that §33 a (2) and (3) are unconstitutional (because of vagueness and lack of formal competence of state legislature, BVerfG, 1 BvR 668/04 as of July, 27, 2005).

Crown witness rules

Until 1999 a crown witness law was in force which allowed dismissal of cases by the public prosecutor or mitigation of punishment respectively immunity from punishment in case of criminal or terrorist organizations (§§129, 129a) and any criminal offences carried out by criminal/terrorist organizations. A sunset clause had been attached to the crown witness law and in 1999 the Federal Parliament did not opt for further extension. Evaluation of the crown witness law demonstrated – according to the assessment of the then coalition government - that the crown witness regulations have not been of particular value for prosecution and trial purposes. In particular, it was criticized that the crown witness status could be granted only for selected criminal offences. However, crown witness rules have been criticized also from the viewpoint of the principle of the rule of law. The debate on crown witnesses has – since its origins in the 1970s – oscillated between the positions of rule of law and effectiveness of law enforcement. While police and ministries of interior emphasized the need for flexible and effective incentives for accomplices, defence councils and parts of academia spoke out fervently against strategies that reward the contributions of accomplices in law enforcement and criminal investigations.

Since 1999 therefore, only offence specific rules on crown witnesses apply. Such offence specific crown witness rules have been attached to the offence statutes of criminal or terrorist organizations, money laundering and drug trafficking.

Recently however and due to continuing lobbying for the introduction once more of a general crown witness regulation, the Minister of Justice presented a draft crown witness law (www.bmj.bund.de). According to this draft, a new crown witness rule shall be embedded in the sentencing statutes (§46 criminal code) and allow for mitigation or the refraining completely from imposing punishment. Conditions for the status as a crown witness concern information by an offender that is suited to contribute to prevent the commission of a serious crime intended by another person, or to clear up a serious criminal offence committed by another person, or to clear up a criminal offence committed by the crown witness him- or herself beyond the activities of the crown witness. The consequence of cooperation with law enforcement authorities will be mitigation or complete exemption from punishment. Restrictions shall apply insofar as in the case of a crimi-

nal offence statute threatening exclusively life imprisonment mitigation may not lead to a lesser punishment than 5 years imprisonment and that exemption from punishment requires that the offence statute does not carry life imprisonment as penalty and the possible concrete penalty to be imposed would not amount to more than 5 years imprisonment. The status of a crown witness will also require that information has been disclosed before a court has decided on opening a criminal trial against the cooperative offender. In contrast to former crown witnesses statutes the draft crown witness law is not restricted to a selection of criminal offences and the offence that has been committed by the crown witness as well as the criminal offence that is prevented or cleared up by information provided by the crown witness must not belong to the same class of criminal offences. Furthermore, information provided by the crown witness must be only suited to contribute to prevent a crime or to clear up a crime instead of actually contributing to the clearing up of a criminal offence.

1.2.1.2.4.3 International conventions and European framework decisions and directives

Anti-terrorism legislation has also been influenced by the ratification of international treaties against terrorism. Thus far, Germany has signed and ratified all United Nations Conventions aimed at preventing and suppressing terrorism.

United Nations Initiatives

The Convention for the Suppression of Unlawful Seizure of Aircraft ("Hague Convention", 1970 - aircraft hijackings) has been signed and ratified. Hijacking of aircraft has been made a criminal offence with the enactment of §316c which threatens a minimum of 5 years and a maximum of 15 years imprisonment.

The Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation ("Montreal Convention", 1971, which applies to acts of aviation sabotage such as bombings aboard aircraft in flight) has also been signed and ratified. Obligations as to the creation of criminal offence statutes coming with this convention have been implemented through the enactment of §316c.

The Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons (1973) which outlaws attacks on senior

government officials and diplomats has been signed 15 August 1974 and ratified 25 January 1977. The convention has been implemented through the creation of §102 (see above).

Taking hostages according to the International Convention Against the Taking of Hostages ("Hostages Convention", 1979) has been signed 18 December 1979 and ratified 15 December 1980. Implementation took place with the insertion of §§239a, b into the Criminal Code.

The Convention on the Physical Protection of Nuclear Material ("Nuclear Materials Convention", 1980--combats unlawful taking and use of nuclear material) has been ratified. Unlawful possession of nuclear substances, trafficking and the like have been penalized.

The Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, (1988 – which applies to terrorist activities on ships) has been ratified. Penal provisions have been introduced that criminalize interference with maritime transportation (see above).

The Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf (1988--applies to terrorist activities on fixed offshore platforms) has been ratified. A legal regime has been established that provides for criminal sanctions against interference comparable to that of maritime transportation and installations.

The Convention on the Marking of Plastic Explosives for the Purpose of Detection (1991--provides for chemical marking to facilitate detection of plastic explosives, e.g., to combat aircraft sabotage) has been ratified and implemented with the Law on the Convention of 1991 Referring to the Chemical Marking of Plastic Explosives (as of 9 September 1998 (Gesetz zu dem Übereinkommen vom 1. März 1991 über die Markierung von Plastiksprengstoffen, BGBl II 1998, 2301).

The International Convention for the Suppression of Terrorist Bombing (1997): (UN General Assembly Resolution) was signed 26 January 1998 and ratified 23 April 2003. Universal jurisdiction applies to acts of bombing (§§307, 308, 310) according to §6 Criminal Code.

The International Convention for the Suppression of the Financing of Terrorism (1999) was signed 20 July 2000 and ratified 17 June 2004. Legislation implementing the Convention had already partially been in place or was enacted subsequent to the ratification of the Convention.

Finally, the International Convention for the Suppression of Acts of Nuclear Terrorism 13 April 2005 was signed 15 September 2005.

European Union initiatives

The European Union framework decision on the European Arrest Warrant (13 June 2002) had been implemented by a law that was subsequently declared unconstitutional by decision of the Federal Constitutional Court (18 July 2005). The Federal Constitutional Court argued that the law did not respect the particular protection of German citizens as regards their legitimate and constitutionally protected trust in being prosecuted and tried in Germany and not delivered to foreign jurisdictions when having committed a crime which has significant links to Germany. Moreover, the German Constitution demands for the possibility of appeal before a court of law. In the meantime, the Federal Government has drafted a new version of a law implementing the European Arrest Warrant which – according to a statement of the Minister of Justice will respect constitutionally protected rights of defendants. Extradition of a German citizen (and foreign nationals with a status comparable to that of a German citizen) may only be granted if – after a trial has been completed and a criminal sanction imposed – it is ascertained that the convicted person will be re-delivered to Germany in order to execute the penalty in Germany, and if the offence does not have a significant relation to Germany and if the offence has a significant relation to another European Union member state or if mutual punishability is established and trust of being not delivered to a foreign state worth of being protected is not present.

Anti terrorism framework decision (see below).

Money laundering directives. All money laundering directives have been implemented.

Reports to the Security Council (Counterterrorism Committee)

Until now three reports have been submitted to the Security Council's Counterterrorism Committee: S/2002/11, S/2002/1193, S/2003/671.

Bi- and multi-lateral Agreements, Conventions etc.

The basis of international cooperation consists of a multitude of bi- and multi lateral agreements and conventions which also extend to international

export control regimes, in particular in order to effectively counteract the danger of proliferation of weapons of mass destruction.

In principle, the Federal Republic of Germany participates in international judicial cooperation with all the countries of this world, either on a treaty or non-treaty basis. The Federal Republic has signed all relevant agreements on the rendering of judicial assistance within the European framework. The Federal Government has implemented all international conventions on terrorism, incorporating them into national law. Agreements have been concluded with a large number of Central and Eastern European countries on the prevention of organized crime and terrorism.

Among the mechanism used to exchange operational information we find Interpol. The BKA performs this task in its capacity as a central agency. This ensures that information can be forwarded swiftly. The BKA also employs liaison officers to facilitate the swift and reliable exchange of operative information. To this end, 56 liaison officers of the Federal Criminal Police Office are currently deployed in 44 locations in 40 countries. Intensive use is made of the possibilities available to police forces of exchanging information with Europol. Cooperation with a body that has been set up at Europol to analyse the international financial structure of Islamic groups can be given as an example. In addition and in terms of police practice, the "Police Working Group on Terrorism" provides a well-established forum for the exchange of information between 17 Member States (Austria, Belgium, Denmark, Finland, France, Greece, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, the United Kingdom, Germany). As a direct consequence of the attacks of 11 September 2001, the Customs Criminal Investigation Office (Zollkriminalamt) has set up a special unit (named BAO INFO). Its tasks include the coordination of the flow of information in support of counter-terrorism action within Customs and ensuring that relevant information gathered is forwarded to other competent national and international law enforcement authorities. To this end the Customs Criminological Office has also intensified cooperation with foreign Customs Attachés/Customs Liaison Officers in the Federal Republic of Germany. Relevant information will be passed on in full detail. It has also been agreed that regular meetings with the Customs Attachés/Customs Liaison Officers will be held on specified topics.

The intelligence services of the European Union have always worked closely together at different levels. In international terms, there are a large

number of well-established contacts at bilateral and multilateral level that ensure there is efficient cooperation and that the relevant information is actually exchanged. Due to decisions taken by the Special Council of Justice and Home Affairs Ministers of the European Union on 20 September 2001, two meetings have already been held by the heads of services. The decision was taken at these meetings to intensify cooperation between the services as well as cooperation with Europol and the authorities of the United States. Furthermore, meetings are held on a regular basis between the heads of the relevant departments of the services responsible for the prevention of international terrorism. Germany helps to prevent terrorism by participating constructively in the EU Task Force of Heads of Anti-Terror Units.

A statutory basis on Joint Investigation Teams was established in 2005 with implementing the 2000 European Union Convention on Mutual Assistance in Criminal Matters.

Agreements on Cooperation against Terrorism, Organized Crime

Bilateral:

Agreement between the Government of the Federal Republic of Germany and the Government of the Republic of Belarus concerning Cooperation in the Fight against Organized Crime, Terrorism and other Significant Offences, Bonn, 4 April 1995

Agreement between the Government of the Federal Republic of Germany and the Government of the Kingdom of Belgium concerning Cooperation between Police Authorities and Customs Administrations in Border Areas, Brussels, 27 March 2000

Agreement between the Government of the Federal Republic of Germany and the Government of the Republic of Bulgaria concerning Cooperation in the Fight against Organized Crime and Drugs-related Crime, Sofia, 14 September 1992

Agreement between the Ministry of the Interior of the Federal Republic of Germany and the Ministry for Public Security of the People's Republic of China concerning Cooperation in the Fight against Crime, Beijing, 14 November 2000

Agreement between the Government of the Federal Republic of Germany and the Government of the Czech and Slovak Federal Republic con-

cerning Cooperation in the Fight against Organized Crime, Prague, 13 September 1993

Treaty between the Federal Republic of Germany and the Czech Republic concerning Cooperation between Police Authorities and Border Police Authorities in Border Areas, Berlin, 19 September 2000

Agreement between the Government of the Federal Republic of Germany and the Government of the Kingdom of Denmark concerning Police Cooperation in Border Areas, Berlin, 21 February 2001

Agreement between the Government of the Federal Republic of Germany and the Government of the Republic of Estonia concerning Cooperation in the Fight against Organized Crime and Terrorism and other Significant Offences, Bonn, 7 March 1994

Agreement between the Government of the Federal Republic of Germany and the Government of the French Republic concerning Cooperation between Police and Customs Authorities in Border Areas, Mondorf (Luxembourg), 9 October 1997

Agreement between the Government of the Federal Republic of Germany and the Government of the Republic of Hungary concerning Cooperation in the Fight against Organized Crime, Bonn, 22 March 1991

Agreement between the Government of the Federal Republic of Germany and the Government of the Republic of Kazakhstan concerning Cooperation in the Fight against Organized Crime, Terrorism and other Significant Offences, Almaty, 10 April 1995

Agreement between the Government of the Federal Republic of Germany and the Government of the Kyrgyz Republic concerning Cooperation in the Fight against Organized Crime and Terrorism and other Significant Offences, Bishkek, 2 February 1998

Agreement between the Government of the Federal Republic of Germany and the Government of the Republic of Latvia concerning Cooperation in the Fight against Organized Crime, Terrorism and other Significant Offences, Bonn, 30 March 1995

Agreement between the Government of the Federal Republic of Germany and the Government of the Republic of Lithuania concerning Cooperation in the Fight against Organized Crime, Terrorism and other Significant Offences, Vilnius, 23 February 2001

Arrangement between the Minister of the Interior of the Federal Republic of Germany and the Minister of Justice and the Minister for the Public Force of the Grand Duchy of Luxembourg concerning Police Cooperation in the Border Area between the Federal Republic of Germany and the Grand Duchy of Luxembourg, Bonn, 24 October 1995

Arrangement between the Ministry of the Interior of the Federal Republic of Germany and the Minister of Home Affairs and the Minister of Justice of the Netherlands concerning Police Cooperation in the Border Area between the Federal Republic of Germany and the Netherlands, The Hague, 17 April 1996

Agreement between the Government of the Federal Republic of Germany and the Government of the Republic of Poland concerning Cooperation in the Fight against Organized Crime, Bonn, 6 November 1991

Agreement between the Government of the Federal Republic of Germany and the Government of the Republic of Poland concerning Cooperation between Police Authorities and Border Police Authorities in Border Areas, Bonn, 5 April 1995

Agreement between the Government of the Federal Republic of Germany and the Government of Romania concerning Cooperation in the Fight against Organized Crime and Terrorism and other Significant Offences, Bucharest, 15 October 1996

Agreement between the Government of the Federal Republic of Germany and the Government of the Russian Federation concerning Cooperation in the Fight against Significant Offences, Moscow, 3 May 1999

Agreement between the Government of the Federal Republic of Germany and the Government of the Republic of Slovenia concerning Cooperation in the Fight against Significant Offences, Ljubljana, 2 March 2001

Treaty between the Government of the Federal Republic of Germany and the Swiss Confederation concerning Cross-border Police and Judicial Cooperation, Berne, 27 April 1999

Agreement between the Government of the Federal Republic of Germany and the Government of Ukraine concerning Cooperation in the Fight against Organized Crime and Terrorism and other Significant Offences, Bonn, 6 February 1995

Agreement between the Government of the Federal Republic of Germany and the Government of the Republic of Uzbekistan concerning Cooperation in the Fight against Organized Crime, Terrorism and other Significant Offences, Bonn, 16 November 1995

Protocol on Cooperation between the Ministry of the Interior of the Federal Republic of Germany and the Ministry of the Interior of the Socialist Republic of Vietnam on Preventing and Combating Crime, Hanoi, 28 February 1996

Multilateral:

European Convention on the Suppression of Terrorism, Strasbourg, 27 January 1977

United Nations Convention against Transnational Organized Crime, New York, 15 November 2000

Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, New York, 15 November 2000
Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime, New York, 15 November 2000

Council of Europe Convention on Cyber Crime, Budapest, 23 November 2001

Agreements on Mutual Assistance and Extradition

Bilateral:

Treaty of 14 April 1987 between the Federal Republic of Germany and Australia concerning Extradition

Supplementary Treaty of 31 January 1972 to the European Convention on Extradition between the Federal Republic of Germany and the Republic of Austria

Supplementary Treaty of 31 January 1972 to the European Convention on Mutual Assistance between the Federal Republic of Germany and the Republic of Austria

Treaty of 11 July 1977 between the Federal Republic of Germany and Canada concerning extradition

Supplementary Treaty of 2 February 2000 to the European Convention on Extradition between the Federal Republic of Germany and the Czech Republic

Supplementary Treaty of 2 February 2000 to the European Convention on Mutual Assistance between the Federal Republic of Germany and Czech Republic

Supplementary Treaty of 20 July 1977 to the European Convention on Mutual Assistance between the Federal Republic of Germany and the State of Israel

Supplementary Treaty of 24 October 1979 to the European Convention on Extradition between the Federal Republic of Germany and Italy

Supplementary Treaty of 24 October 1979 to the European Convention on Mutual Assistance between the Federal Republic of Germany and Italy

Supplementary Treaty of 30 August 1979 to the European Convention on Extradition between the Federal Republic of Germany and the Kingdom of the Netherlands

Supplementary Treaty of 30 August 1979 to the European Convention on Mutual Assistance between the Federal Republic of Germany and the Kingdom of the Netherlands

Supplementary Treaty of 13 November 1969 to the European Convention on Extradition between the Federal Republic of Germany and the Swiss Confederation

Supplementary Treaty of 13 November 1969 to the European Convention on Mutual Assistance between the Federal Republic of Germany and the Swiss Confederation

Treaty of 20 June 1978 between the Federal Republic of Germany and the United States of America Concerning Extradition, in the version of 21 October 1986

Multilateral:

European Convention on Extradition of 13 December 1957

First Additional Protocol of 15 October 1975 to the European Convention on Extradition

Second Additional Protocol of 17 March 1978 to the European Convention on Extradition

European Convention of 20 April 1959 on Mutual Assistance in Criminal Matters

Additional Protocol of 17 March 1978 to the European Convention on Mutual Assistance in Criminal Matters

Convention of 8 November 1990 on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime.

Convention of 10 March 1995 on simplified extradition procedure between the Member States of the European Union

Convention of 27 September 1996 relating to extradition between the Member States of the European Union

The Council of Europe in May 2005 has opened the Convention on the Prevention of Terrorism (ETS 196) as well as the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (ETS 198) for signature. These conventions have not yet been ratified.

Agreements against Proliferation, Chemical and Biological Weapons etc.

Protocol for the Prohibition of the Use in War of asphyxiating, poisonous or other Gases and of bacteriological Methods of Warfare, Geneva, 17 June 1925

Treaty on the Non-Proliferation of Nuclear Weapons, 1 July 1968

Convention on the Prohibition of the Development, Production and Stockpiling of bacteriological and toxin Weapons and on their Destruction, 10 April 1972

Convention on the Prohibition of the Development, Production, Stockpiling and Use of chemical Weapons and on their Destruction, Geneva, 3 September 1992

Comprehensive Nuclear Test Ban Treaty, New York, 10 September 1996

OSCE Document on Small Arms and Light Weapons, Vienna, 24 November 2000

UN Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects, New York, 20 July 2001

1.2.1.2.4.4 Special terrorist offence statutes

Special terrorist criminal offences have not been enacted until now – beside §§129a, 129b - although the European Union Framework Decision of June 13, 2002 on Combating Terrorism requires member states to introduce the category of terrorist offences (Troosters 2004). A terrorist criminal offence – according to the Framework Decision – is established by subjective elements such as the purpose of seriously intimidating a population, unduly compelling a government or international organisation to perform or abstain from performing an act or seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization. The creation of separate anti-terrorism offence statutes strengthens an international trend towards creating and implementing hate crime legislation, which means that increased penalties are established for such motives that are perceived to be particularly dangerous or particularly low. This, however, is criticized as leading to a concept of criminal law that is directed towards the criminal mind and sidelines the criminal offence itself. International and national terrorism alike may also be conceived as “crimes against democracy” thus highlighting a particular aspect of, in particular, international terrorism that hits so called soft targets in an attempt to undermine the very basis of a democratic society (see Saul 2003, pp. 330-333, who also points to the possibility to conceive terrorist offences as crimes against international relations).

§129a covers a broad range of terrorist activities and expands criminal law to acts that precede conventional (terrorist) crimes. It is modelled along §129 which penalizes the formation of a criminal group (which has its roots in the 19th century). But, §129a goes beyond conventional criminal legislation on criminal groups (or conspiracy to commit crimes). Four types of activities have been criminalized: founding a terrorist organization, being a member of a terrorist organization, supporting a terrorist organization and campaigning for a terrorist organization. The latter two concern typical “aiding and abetting” activities that have been upgraded to separate criminal offences. §129a was part of a law package against terrorism which came into force in 1976. It was a law that was focussed on the RAF (and German or local terrorism) and the offence elements of “supporting” and

“campaigning” addressed the particulars of the terrorist groups of the 1970s which had been embedded in a network of supporters.

With a criminal law amendment that came into force in 2005, Germany adjusted §129a in order to comply with the European Union Framework Decision on Terrorism 2002. §129a is now applicable if a group (association/Vereinigung) is founded that pursues the commission of murder (Mord, Totschlag), genocide, war crimes or crimes against humanity (as defined through the German International Criminal Code (Völkerstrafgesetzbuch)) or particular acts of racketeering and hostage taking. The penalties range from a minimum of 1 year imprisonment to 10 years. The same penalties apply if a group (association) is founded which pursues the commission of selected criminal offences (listed in §129a) – among them aggravated assault, arson, trafficking of explosives and nuclear material, certain environmental criminal offences, arms trafficking, sabotage of sensitive infrastructure. In addition to pursuing to commit a criminal offence of the second group of criminal offences the statute requires as offence elements that such offences must be intended to significantly intimidate the public or to compel a national or international administration/organization by force or the threat of force or to destroy the political, constitutional, economic or social basic structure of a state or an international organization and that the way the crime is committed or the results of the crime can in fact do significant damage to a state or to an international organization. While the range of penalties of 1 to 10 years imprisonment applies to acts of founding or participating (being a member) in a terrorist group, lesser minimum and maximum penalties apply to the threat of the offences listed in §129a I, II (§129a III, 6 months to five years). Providing for support/aid (Unterstützung) for a terrorist group results in a penalty range of a minimum of 6 months and a maximum of 10 years (§129a V). Recruitment of members or supporters of a terrorist group also establishes a criminal offence with a penalty range of between 6 months and 5 years.

The 2005 amendment of the terrorist group offence (§129a) according to statements of law makers responded on the one hand to requirements set out in the 2002 EU framework decision and on the other hand to the ongoing criticism of the wide and vague penalization of “campaigning” for a terrorist group as established by the old version of §129a. Now, campaigning (werben) is reduced to recruitment of members for a terrorist group.

1.2.1.2.5 Law on private associations

The law on private (legal) associations (Vereinsgesetz) contains rules that allow the prohibition of associations on three grounds. Associations may be prohibited (and as a legal consequence be dissolved) if their activities run counter to the criminal law, if their activities are directed against the democratic order or if their activities threaten the “peace of nations” (Völkerverständigung). In the case of associations founded and run by foreign nationals (Ausländervereine), other grounds have been added (§ 14 Vereinsgesetz). Foreign national associations may be prohibited if their aims or actions threaten or harm the process of democratic decision-making (politische Willensbildung), peaceful co-existence of German and foreign nationals or of different groups of foreign nationals, public safety and order or other significant interests of the Federal Republic of Germany. Associations may be prohibited if their goals and actions are opposed to the obligations of Germany as established through the law of nations. Furthermore, prohibition may result from activities that support processes abroad which run counter to state order that respects human dignity. Finally, associations fall under the threat of prohibition if they support or instigate violence as an instrument to achieve political, religious or other goals or support groups abroad which threaten, approve or carry out violent attacks against persons or property. The consequences of a formal prohibition (imposed either by state or federal ministries of the interior) concern dissolution of the association (as a legal entity), forfeiture of assets, and the applicability of criminal offence statutes that carry criminal penalties for activities that support such associations (including being a member of a prohibited association).

1.2.1.2.6 G 10 Law (Interception of telecommunication by intelligence services)

The Law on Restrictions of the secret of telecommunication, telephone communication and mailed communication (G 10 Gesetz) allows infringements on communications through telephone lines, telecommunication or ordinary mail through federal and state intelligence services (Bundesnachrichtendienst, Verfassungsschutzämter, Militärischer Abschirmdienst).

According to §1 of the G 10 Law intelligence services (internal and external) may intercept telecommunications or other communications (by mail) in order to fulfill the tasks assigned to them in the respective laws.

The G 10 law establishes two sets of conditions for interceptions that can be collapsed into individual case interceptions and “strategic” interceptions. According to §3 of the said law, communications may be intercepted in individual cases if factual evidence exists that somebody plans or has committed crimes that are listed in a catalogue (among them being a member of a terrorist organization). Interception in such cases is further subject to the requirement that other, equally effective, means of investigation are not available (principle of subsidiarity). The Bundesnachrichtendienst may carry out strategic interceptions after authorization from the government and with consent of the parliamentary control group (responsible for monitoring intelligence services) according to §5 G 10 Law). This means that packages of information transmitted through telecommunication providers may be monitored on the basis of search terms in order to filter out communications relevant for identifying and preventing strategic threats. Conditions concern the search for information on selected types of criminal offences (drug trafficking or international terrorism affecting the Federal Republic of Germany, international arms trafficking, unauthorized transactions in controlled goods, technologies and software, international and organized money laundering etc.). Search terms furthermore may not be used that can lead to the targeted interception of individual telecommunication lines. This does not apply to foreign telecommunication lines, if it can be excluded that German nationals use such lines. Under conditions set out in §7 G 10 Law, data retrieved through strategic interception may be transmitted to internal intelligence services and to the MAD.

Information concerning §129a Criminal Code (terrorist organization) and other selected criminal offences catalogued in §7 G 10 Law may also be transmitted to police and public prosecution services under conditions specified in §7.

1.2.1.2.7 Immigration law

Immigration laws have been amended in particular as a response to European Union initiatives and then as a response to UN Security Council resolutions. Changes in immigration (and asylum) laws concern:

The collection of personal data which allows for identification of foreign nationals

Information systems that contain identification data

Access to such data for the purposes of threat assessment, investigation and law enforcement.

In order to enable early identification of individuals who are suspected to have links to the terrorist milieu, intelligence services are involved early in the procedure to issue visas.

Stricter provisions in respect of granting residence permits and grounds for which a person can be expelled from the country have been introduced.

Protection against deportation has been restricted. Foreign nationals who are suspected on serious grounds of being involved in serious crime will no longer be granted legal status under the Geneva Refugee Convention

1.2.1.2.8 Telecommunication law

Amendments to telecommunication laws have been set into force (1995, 2002, 2005) with the Telecommunication Surveillance Ordinance which regulates technical and organizational conditions to be complied with by telecommunication providers in order to be able to implement surveillance orders. Telecommunication providers have to bear the costs arising with keeping the systems in line with conditions set in the Ordinance. The Ordinance does not regulate the retention of telecommunication and traffic data.

The debates in Germany around the question of whether and to what extent periods of data retention regarding telecommunication traffic data should be introduced revealed that the German position was more restrictive than that of many of the other EU member countries. The EU directive on retention of telecommunication data that sets the period of retention at a minimum of 6 months and a maximum of 24 months now finds support in the Federal Parliament (see Drucksache 16/545, as of 7 February 2006: *Speicherung mit Augenmaß – Effektive Strafverfolgung und Grundrechtswahrung*). Particular attention is paid to the question of weighing interests in basic rights (right to telecommunication privacy Art. 10 Federal Constitution) and – as regards telecommunication providers – the right of “occupational freedom” (*Berufsfreiheit*, Art. 12 Federal Constitution). Furthermore, it is pointed out that retention of telecommunication data may infringe on the fundamental right of a free press (and other media), as enshrined in Art. 5 I, 2 Federal Constitution. It is recognized that a general rule that demands for mandatory retention of all sorts of telecommunication data will infringe upon fundamental rights of a vast group of individuals

who have not established any ground to assume that they might be involved in criminal acts. Insofar, the principle of proportionality requires particular scrutiny when weighing interests of effective law enforcement against interests concerning the fundamental rights of individuals affected by data retention. The Federal Government has been urged by a group of members of parliament (representing the coalition parties) to draft a telecommunication law amendment that does not go beyond the minimum retention period that is required by the EU directive (6 months), which restricts the use of such data to the investigation of serious crimes (and crimes committed through telecommunication) and which prohibits the retention of content data. Furthermore, the Federal Government has been called on to elaborate a law that regulates financial compensation of telecommunication providers for costs arising out of providing support to law enforcement authorities (BT-Drs. 16/690, 16 February 2006).

1.2.1.2.9 Money laundering, Financing terrorism and freezing accounts

Through the enactment of §261 (money laundering) Criminal Code and the Money Laundering Prevention Act (Geldwäschegesetz) Germany has implemented various UN, Council of Europe and European Union as well as OECD demands. Financing of terrorism establishes a criminal offence according to §129a (supporting a terrorist organization) since its enactment in the 1970s.

In Germany it is possible to take preliminary national measures to restrict capital and payment transactions involving the persons or organizations targeted as terrorists. These measures are based on §§2 and 7 of the Foreign Trade and Payments Act (Außenwirtschaftsgesetz). The provisions enable the German Federal Government to restrict legal transactions or activities concerning foreign trade and payments in order to protect against specific risks to the values referred to in §7, 1 of the Foreign Trade and Payments Act (security of the Federal Republic of Germany; the peaceful co-existence of peoples; the external relations of the Federal Republic of Germany). Insofar, the restrictions of transactions and freezing of bank accounts can go beyond the measures demanded for by the European Union and the UN. There are, however, no lists of individuals, groups or legal entities, other than those established by the UN or the EU.

The Federal Financial Supervisory Office (Bundesanstalt für Finanzdienstleistungsaufsicht - BaFin) and the Financial Intelligence Unit – FIU

(Zentralstelle für Verdachtsanzeigen), which is part of the Federal Office for Criminal Investigations (BKA), are responsible for the suppression of the financing of terrorism in terms of investigating suspicious (money laundering and financing) cases, reported also by banks and other financial institutions as well as persons and institutions which have a duty to report particular transactions or suspicious cases on the basis of the Money Laundering Prevention Act.

The Fourth Financial Market Promotion Act (Viertes Finanzmarktförderungsgesetz) came into force on 1 July 2002, followed by an amendment to the Money Laundering Prevention Act (Geldwäschebekämpfungsgesetz, 15 August 2002). These legal amendments particularly address the financing of terrorism. Under the new Section 24c of the Banking Act (Kreditwesengesetz, KWG), a data retrieval system has been introduced that gives the Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin) electronic access to all key account data held by banks (name and account number of the account holder, names of further persons having the right of disposal and the name of the economic beneficiary). This new system also allows for the immediate freezing of the financial assets of persons and organisations according to the respective regulations. Section 25a (4) of the Banking Act - implementing core principle No. 15 of the Basle Committee "Customer due diligence for banks" of 4 October 2001 - requires financial institutions to deploy an internal data based system to monitor customers, accounts and transactions for irregularities or deviations from a predefined standard pattern of behaviour. If need be, the matter is referred to the Compliance Officer for further processing and inspection. It also requires institutions to conduct investigations on a risk based approach.

The Federal Financial Supervisory Authority is empowered:

1. to issue instructions to the institution's directors;
2. to prohibit the institution from disposing of an account or deposit held at the institution;
3. to prohibit the institution from carrying out further financial transactions.

This is applicable especially to cases where the name of an account holder has been included in the list of terrorists issued by the European Union

for the purpose of implementing UN Security Council Resolution 1373 (2001).

Intelligence services, police, prosecutors and tax authorities now have, under conditions specified in the respective laws, access to account data.

1.2.1.2.10 Money laundering control and bank secrecy

A statutory form of bank secrecy never existed in Germany. However, restrictions applied that are backed up by the constitutionally protected right to self determination as regards personal data and the principle of proportionality. The automatic data retrieval system mentioned above was introduced especially to control terrorism and transnational organized crime. However, the system has now been generalized and also allows in principle access to account data in order to investigate tax cases and social security fraud. According to the Law on Promoting Honesty in Declaring Taxes (Gesetz zur Förderung der Steuerehrlichkeit) which went into force 1 April 2005, tax authorities will have access to approximately 500 million accounts administrated through the data retrieval system of BAFIN. In several cases brought before the Federal Constitutional Court complainants have argued that the legal amendments allowing general access to account holder's data would infringe disproportionately on the right to self determination of personal data. The court, however, declared that in face of eminent threats access to personal account data of the kind allowed by the amendments does not result in an unconstitutional interference with personal data (Decision as of 22.03.2005, Az. 1 BvR 2357/04; 1 BvQ 2/05).

1.2.1.2.11 Protection of Sensitive Infrastructure

After 9/11 the issue of protecting sensitive infrastructure was placed on the counter terrorist agenda. According to the official concept (on the federal level) the Bundeskriminalamt has the task to serve as an agency that advises infrastructure related organizations and institutions with respect to information on threat assessments and protective arrangements.

The Federal Office for the Security of Information Technology (Bundesamt für Sicherheit in der Informationstechnik, BSI) was established 1998 in order to provide services for IT security.

Since May 1st 2004 the Federal Office for the Protection of the Public and Disaster Relief (Bundesamt für Bevölkerungsschutz und Katastrophen-

hilfe, BBK) is responsible for developing emergency plans and the deployment of rapid support in all sorts of disasters.

The Federal Office for Technical Support (Bundesanstalt Technisches Hilfswerk, THW) may be deployed in all cases of problems arising out of failures of sensitive infrastructure.

1.2.1.3 Institutional Arrangements

1.2.1.3.1 Cooperation and coordination

The federal system of policing and intelligence services has always been criticized because of the problems arising out of different and independent systems of policing, including the operation of different information systems etc. Insofar, it is not surprising that efforts to improve control of terrorism (and organized crime etc.) emphasize the need for proper cooperation and coordination of policing and intelligence services. Over the last decades a multitude of initiatives have been implemented. However, the fundamental constitutional principle of federalism and the assignment of powers of policing (and internal security) to the states have not been subject to changes.

Joint Counterterrorism Centre

The establishment of this office lies in the assumption, that the elaborated competence distribution in the field of security in Germany produces confusion, obstructs efficient preventive police work and could lead, in the worst case, to not being able to prevent a terrorist attack on German soil. It is also common knowledge that police and intelligence services, state and federal agencies, often do not cooperate, due to traditional “professional egoism”.

The Joint Counterterrorism Centre (Gemeinsames Terrorismusabwehrzentrum - GTAZ) was founded on December 14th 2004 in Berlin. Specialists from the Federal Criminal Office (Bundeskriminalamt – BKA) and the Federal Office for the Protection of the Constitution (Bundesverfassungsschutz – BVerfSch) work together in this centre. The GTAZ is capable of exchanging information quickly. The analysts working there can supply fast, goal-oriented interpretations about present danger scenarios, which help form a consensus on what operative measures should be taken against them.

The Federal Secret Services, the State criminal offices and State offices for the protection of the Constitution, the Federal Police, the Customs Office, the Federal Attorney General, the Federal Office for Migration and Refugees and the Military Counter Intelligence work together with GTAZ and are involved in its routine.

The GTAZ's tasks are:

- Daily briefings which are used to exchange information about the present situation from the point of view of police and secret services, to achieve preliminary conclusions and to decide on proper measures. Approximately 50 representatives of all agencies involved participate in these meetings.
- Threat assessments: incoming warnings and information as well as newly collected intelligence are rapidly analysed and jointly evaluated. Threat assessments should provide valid and reliable answers to questions such as “Is there a concrete demand for action?”, “Should the scenario for particular fields, or generally, be re-assessed?”
- Operative information exchange: here, the goal is to achieve a structured exchange and to thereby accelerate agreement on operative measures.
- Case evaluation: under this task fall interpretation of terrorism related issues such as the acquisition of false IDs, weapons or explosives.
- Structural analysis: Subjects like Arabic Jihadist training camps or the analysis of potential terrorist travel movements.
- Investigation of the Islamic terrorist potential: information about potential terrorists and their supporters are collected and analysed.
- Achieving synergy effects in strategic information collection and investigation.
- Analysis of immigration related issues: it will be for example examined, based on the new Immigration Act (ZuwG), if foreign nationals supporting terrorist organizations, can be deported.

The main objectives can thus be found in the collection and exchange of information and threat assessments as well as advising other bodies. Operational powers are not available to the office. Criticism has been voiced as

regards possible infringements on privacy (self determination of personal data).

Recently, however, the president of the Bundeskriminalamt argued that under the umbrella of the GTAZ information systems of police and intelligence services should be merged in order to allow for more effective use of available data on terrorism. This, of course, would provoke the question of whether such merging of information systems would not amount to a complete removal of the wall between operational police and intelligence collecting services.

1.2.1.3.2 Data Exchange between law enforcement, police and intelligence services

Another field of cooperation concerns data exchange between police and intelligence services. As has been outlined above, intelligence services are now empowered to transmit data to police and law enforcement agencies in the field of terrorist crimes. This process of opening the borders between police and intelligence services was initiated by allowing intelligence services collection of data in the field of transnational and organized crime as well as in the case of crimes that affect the “peace of nations”. Data transfer in cases of transnational and organized crime as well as terrorism now may take place.

1.2.1.3.3 Data exchange between police, intelligence services, immigration authorities, banks etc

Another field where data exchange has rapidly developed concerns exchange between administrative agencies (like immigration authorities) on the one hand and police on the other hand as well as data exchange between the private sector (banks etc.) and police/intelligence services. The latter also points to an accelerated pace in placing statutory duties to cooperate and support law enforcement in the private sector and civil society.

1.2.2 Experiences with Counterterrorism strategies and tactics

The development of terrorism and radicalism in Germany is documented fairly well in the annual reports of state and federal Internal Intelligence agencies (Verfassungsschutzämter, see for example Verfassungsschutzbericht 2003, 2004). The Internal Intelligence agencies have a statutory basis in the Bundes- and Landesverfassungsschutzgesetze) and have been es-

tablished in post Second World War Germany to monitor extremist and radical individuals, groups and political parties. The annual reports demonstrate that the emphasis was on leftist radicalism (and the German Communist Party as well as communist parties succeeding the GCP after it was dissolved by a decision of the Federal Constitutional Court in 1954) in the 1950s, 1960s and 1970s, and later right wing extremism was added as well as radical groups among immigrants. From the 1990s on hate violence and hate speech received attention and 9/11 was evidently the signal to place the focus on Islamic groups.

1.2.3 A Framework of Analysis

Responses to terrorism can be roughly broken down into three areas: legislation, institutional developments, (re-) arrangement of institutional configurations (in terms of coordination and cooperation between agencies) and the programming or development of (national and local) counter-terrorism policies.

The most remarkable institutional development concerns the Bundeskriminalamt and its expansion in terms of resources and powers since the late 1960s. From a small and merely noticeable federal police force, the BKA developed into a powerful federal agency which deals today with all those phenomenon that are high on the political agenda (transnational organized crime, terrorism, drug trafficking). The point of departure was the federal system of police and policing which concentrated police powers in the Bundesländer and at the beginning of post war Germany restricted federal police to border police (back then Bundesgrenzschutz, now: Bundespolizei, custom police and the Bundeskriminalamt which served as a national point for international cooperation through Interpol).

What can be seen here is a move towards the centralization of police and policing as the BKA adopted powers in particular based on the perceived need to create a central agency that could effectively manage transnational and international safety threats.

The overall picture thus reflects an institutional and organizational patchwork which is caused by federalism (in particular effective in the fields of internal security).

German Counterterrorism strategies emphasized from the 1970s on a strategy of criminal law based prevention. The emphasis was on criminal

investigation and prosecution. Counterterrorism strategies that went beyond dealing with what establishes “sympathy” with terrorists did not develop. The conflicts around the issue of “sympathizers” of terrorism became in particular visible when the late Heinrich Böll was drawn into the disputes on the basis of allegations of expressing sympathy with leading figures of the RAF. The novel and film “Die verlorene Ehre der Katharina Blum” is a significant expression of these debates unfolding in the 1970s and 1980s.

Legislative responses to German terrorism, also known as anti-terrorism legislation (Berlit/Dreier 1984) can be characterized as swift reactions to terrorist acts, they signalled the state’s activity and readiness to act; these responses have also been characterized as expressions of a loss of distance between the legislative and executive branches of the state (Berlit/Dreier 1984, pp. 258). What could also be observed in German anti-terrorism legislation of the 1970s concerns a politicisation of criminal legislation which included fundamental debates on questions of terrorism, in particular as regards the question of how supporters of terrorism should be separated from legitimate criticism of the state’s response to terrorism. It is back then that the label of “sympathizers” of terrorism was created and made operative in political debates on terrorism. However, the political debates following September 11th have been less spectacular than those of the 1970s.

2. After 9/11 Counterterrorism Strategies

2.1 Introduction

German legislation that came in the wake of 9/11 emerged along several lines that, in principle, are not new but were rather initiated around the mid 1980s. These lines are drawn by various United Nations conventions, regional conventions, moreover in treaties and decisions within the framework of the European Union and the OECD. These lines deal with the control of transnational organised crime, money laundering as well as illegal immigration. Anti-terrorist legislation is then clearly an expression of those Security Council resolutions that have been set into force after September 11 (in particular Resolution 1373). However, besides these international and supranational developments it should be noted that specific trends emerged in national systems. German national anti-terrorism legislation was enacted in due course.

The continuation of political and legislative lines after 9/11 therefore takes as a point of departure those anti-terrorism laws that have been a consequence of joint international anti-terrorist conventions, however, it is also the result of national legislation which has been set up since the 1960s in order to respond to various phenomena of national (and international) terrorism.

Legislation, pre-designed for the control of transnational crime, money laundering and illegal immigration as mentioned above, represents the core of anti-terrorist legislation after September 11 (Militello/Arnold/Paoli 2001; Albrecht/Fijnaut 2002; Albrecht 2002; Huber 2002). This also means that the label of anti-terrorism legislation can be assigned to laws without any basic changes after 9/11. This type of legislation goes into the creation of “precursor” criminal law as, for example, with offence statutes that criminalize participation or support of criminal or terrorist groups and money laundering, offence statutes which have been designed through the Vienna Convention of 1988 as well as in the UN Convention to control transnational organised crime of 2000. We find expressions of such developments in the attempt to get hold of information collected by private telecommunication providers, in the creation of obligations on the private sector (individuals or companies/organisations) to actively support criminal law based strategies of prevention and repression. These developments become visible in the further deployment and extension of new investigative methods that have been initiated since the 1980s within the context of control of organised crime or transaction crime as well as in the systematic and wide spread use of conventional precarious investigative methods such as use of private informants or crown witnesses (see for Germany e.g., Stern 2002; Maurer 2002; Albrecht/Dorsch/Krüpe 2003). The trends extend to building up networks of preventive and repressive strategies and also become visible in laws on associations or/and political parties, laws on religion and religious groups, laws facilitating the prohibition of certain associations and organisations and laws threatening criminal penalties if activities justifying prohibition are not put on hold.

Anti-terrorism legislation thus becomes part of general security legislation (Parent 2002, p. 51) which from the viewpoint of industrial countries, in particular Europe and North America, represents the response to configurations of problems made up of immigration, transnational and cross-border crime, transaction crime, money laundering and shadow economies.

Such legislation and programming also represents a move towards a unified security concept joining together internal and external concepts of safety and security. This becomes for example visible in a recent threat assessment made by the European Union which sees the key threats in terrorism, proliferation of weapons of mass destruction, organized crime, regional (violent) conflicts and failed states (European Council 2003). It seems then clear that such threats are interrelated and require a “mixture of instruments” which combines intelligence, police, judiciary, military and economic means (European Council 2003, p. 7). Furthermore, anti-terrorism legislation represents cross-sectional legislative activities that are made up of amendments of immigration laws, police laws, laws on secret services, telecommunication laws, general criminal and procedural laws, economic laws, general order laws as well as legislation establishing particular powers in monitoring professional activities in sensitive areas.

Legislation that followed on from September 11 took on developments, the substance of which, were already in place during the last 20 years (Paeffgen 2002, p. 338) and which were also part of a globalization of criminal law allegedly following an aggressive policy of “legal imperialism” (Schünemann 2003) which was again fuelled by neutralization of conflicts and the elimination of controversial discourses from law making and policy programming in the field of terrorism. Within the framework of the European Union past changes in immigration policies today turn out to be relevant for terrorism control. Here, we find, for example, the directive to establish Eurodac (in force since 15 December, 2000). This directive implements a system which should prevent asylum shopping in the Schengen space by way of systematically collecting personal data and in particular fingerprints (or in the future biometric information; Albrecht 2002). However, the system can easily be adjusted to control terrorist or extremist individuals or groups.

Anti-terrorism legislation draws attention in particular to the so-called money trail and with that to the control of financial and money markets by way of introducing elaborate money laundering control systems (United Nations Office on Drugs and Crime 2004; FATF 2003; Jahn 2002). The money trail has been highlighted as an important issue since the end of the 1980s, back then the focus was on the control of drug markets; however, the approach since then has been generalised and made available for control of organised and transaction crime at large (Albrecht 1998). As is the

case with goals pursued in the control of conventional forms of organised crime, control of international terrorism should be made more efficient through adjusting money laundering control rules and forfeiture legislation (FATF 2002). In this context the extension of duties to identify clients and to forward information to prosecution services or police has to be mentioned. The Second Money Laundering Guideline of the European Union (Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001) extends such duties to professions such as lawyers, accountants and notaries (besides other professions) as does the Third Money Laundering Guideline of the European Union.

Furthermore, besides general money laundering activities it is now also the financing of terrorist groups or terrorist activities that has become relevant in establishing duties of identification and reporting. With that, money laundering control enters a new dimension - it is now not only a precursor in terms of predicate crimes that provoke these duties but is now also concerned with the specific purpose of money or asset transfers that establish an obligation to report.

Within the framework of the European Union, the Common Council Directive as of December 21, 1998 should be noted which demands harmonisation of a criminal offence statute of participation at a criminal organisation as well as the recommendation of the Council as of December 9, 1999 which concerns co-operation in controlling money laundering with the purpose of funding terrorist activities. Immediately after September 11 the European Council presented an action plan which highlighted those points in the control of international terrorism which were deemed to be particularly relevant. Here, acceleration and intensification of police and judicial co-operation (in particular by way of introducing a European arrest warrant), establishing an anti-terrorist department within Europol and an intensification of information exchange between the European Union and North America were all made priority issues. Also noted in this recommendation was the control of the financial basis of international terrorism (which lead the Council to indicate that such countries should be blacklisted and subject to coercive measures that are assessed to be uncooperative by the Financial Action Task Force of the OECD). An update of the anti-terrorism strategy of the European Union can then be found in the European Council Declaration on Combating Terrorism (25 March 2004); following the Madrid

bombing. The update stresses among other points the need to effectively assist victims of terrorist attacks (see also Council Framework Decision of 15 March 2001 on the standing of victims in criminal proceedings (Official Journal L 82, 22 March 2001) and the Council Directive on compensation to crime victims, 2003/C 45, E 08; Albrecht/Kilchling 2005).

A series of framework decisions of the European Union implement parts of the action programme. A framework decision on Combating Terrorism of June 13, 2002 requires member states to introduce a new offence category of terrorist offences. This evidently expresses the view that terrorist motivations make a profound difference and justify separate elaboration in terms of criminal offence statutes (Saul 2003, p. 328). Another framework decision as of June 13, 2002 concerns the European arrest warrant which has been made mandatory for European Union members and was to be implemented in national law as of January 31, 2004 at the latest (German legislation implementing the European Arrest Warrant, however, has been declared to be unconstitutional by the Federal Constitutional Court, decision of July 18 2005). A framework decision of the European Union deals with the harmonization of the substantive law of terrorist crimes, in particular statutes on terrorist organisations as well as participation in terrorist organisations and penalties foreseen for such activities. This framework decision should be implemented as of December 31, 2003. The Council Framework Decision of 13 June 2002 obliges the member states of the European Union to implement a concept of Joint Investigation Teams that are seen to be a priority issue in the control of terrorism. The focus here is on information sharing and the facilitation of criminal investigation in cases affecting several national systems of law enforcement.

Then, the European Union has issued rules which demand the member states to freeze financial means and assets of such organisations that are listed as an annex to such rules. The Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence provides for the basic guidelines along which cooperation in this area shall take place. Specific measures are dealt with in the Council Regulation No 2580/2001 of 27 December 2001 where specific restrictive measures (for example freezing of bank accounts) are outlined. These can be imposed on individuals and entities listed as terrorists, accomplices to terrorism or supporters of terrorism (see also Council

Regulation 881/2002 dealing specifically with the Taliban, Usama Bin Laden and Al Qaeda). Such lists are, by unanimous decision, set up, amended and updated by the Council (see also the updated list in Council Decision of 22 December 2003, 2003/902/EC or Council Regulation No 391/2004 of 1 March 2004). With that, not only are the financial bases of international terrorism dealt with but with the list annexed there is also a definition implemented that, besides the question of who is an international terrorist, determines which organisation must be treated as an international terrorist group (a technique well known from the creation of drug laws).

Finally, the Financial Action Task Force (established by the OECD) plays a significant role in implementing money laundering controls. Its role does not concern only the development of standards of money laundering control, but also the evaluation and supervision of international money laundering legislation and its implementation. The Financial Action Task Force has on the occasion of its meeting on 29 and 30 October 2001 issued special recommendations for the control of international terrorism which focus in particular on the expansion of powers of freezing accounts and forfeiture of assets, on harmonization of criminal offence statutes that deal with financing international terrorism as well as on the creation and implementation of anti-money laundering standards in alternative money transfer systems (e.g., Habalah). In the future, evaluation activities of the Financial Action Task Force should include also reviews of compliance with standards established in the field of controlling the funding of terrorist acts as well as their implementation. This includes recommendations concerning which sanctions should be imposed on such countries that do not comply with standards as issued by the FATF (Financial Action Task Force 2001).

2.2 Counterterrorism Policy after 9/11

According to official statements, German anti terrorism policy is characterized by 5 goals:

To destroy terrorist structures through exerting strong pressure on terrorist and terrorist groups by way of criminal investigation.

To prevent terrorism from developing by way of controlling extremism through administrative instruments (banning radical organizations and tightening border and immigration controls).

To strengthen international cooperation and data exchange on suspicious immigrants and terrorists.

To protect the public and sensitive infrastructure through permanent monitoring and risk assessment and through providing intensive security checks in risk prone areas (airports etc).

To eliminate causes of terrorism through contributing to international peace and order building and maintenance missions.

2.3 The Flow of Legislation after 9/11

The flow of legislation is characterized through language that announces the creation of counter-terrorism packages including not only legal amendments but also resource allocations and a re-configuration of organizations and institutions.

“First Counterterrorism Package”

On October 11 2001, exactly one month after the terrorist attacks on the World Trade Center and the Pentagon in the USA, the German Parliament expressed its solidarity towards the United States of America and promised military and other support.

The German government introduced the so-called “first counterterrorism package” shortly after the attacks in New York and Washington. It was passed by the Federal Parliament within a short time. The core of this first package concerns:

- Strengthening the military in order to enable armed forces to cope with new types of wars (against what is called small or private wars waged by terrorist groups). New communication equipment and new weaponry were dominant issues.
- Introduction of §129b Criminal Code (see above): it complements §§129 and 129a, which prohibit the formation or support of an association whose objectives are directed towards committing murder, genocide, or certain other criminal acts against personal liberty or endangering the public. Convicted persons can be barred from holding public office and acquiring rights from public elections. §129b now outlaws associations, which are established exclusively abroad. The Parliament approved the change in legisla-

tion on April 26 2002, and the Federal Council the following day. It came into force on September 1 2002.

- Airport security: airports and airline staff will be more intensively monitored. Information from the Military Counterintelligence (Militärisches Abschirmdienst – MAD), the Federal Secret Services (Bundesnachrichtendienst – BND), the Aliens Central Record (Ausländerzentralregister) or the former GDR’s State Security Office (StaSi-Unterlagen Behörde) can be used for monitoring and security checks, especially when new employees are hired.
- Abolition of the so called “religious privilege” (§2, section 2, No. 3 Law on Associations): extremist groups can be banned, even if they appear on the surface as merely religious associations. The amendment came into force on December 8 2001.
- Drying up of terrorist groups financial sources: a programme for the implementation of controls relating to financing terrorism activities was put in place that implements UN and other (e.g., FATF) guidelines.
- Investigations based on data mining (fishing net expeditions) as regulated in the Criminal Procedure Act, paragraph 98a, b and c were highlighted. The former Hamburg Home Secretary, Olaf Scholz (SPD) demanded a wider approach to this type of investigation. Subsequent legislation amending police laws resulted in Lower-Saxony in legislation that was declared to be unconstitutional by the Federal Constitutional Court (see above).
- Fingerprints when issuing visas: foreign nationals may be fingerprinted in the process of issuing a visa.
- Foreign nationals entering the territory of the Federal Republic of Germany shall be subject to investigation on the basis of information systems of the Federal Office for the Protection of the Constitution in order to identify individuals having contact to extremist groups.

In the wake of 9/11 attempts were made to identify so called “sleeper cells”. All state police forces carried out large scale fishing net expeditions on the basis of police laws (partially amended immediately after 9/11 to include data mining investigation) and on the basis of various data sources (including university information systems). Police laws allow for “data

mining” or launching “fishing net expeditions” when grave risk for the Federal Republic of Germany or a state or immediate dangers for life and limb of individuals require such investigative techniques in order to counter such risks. Systematic evaluation of the fishing net expeditions launched after 9/11 was not carried out. However, scattered information that can be derived from parliamentary debates allow for the conclusion that this approach did not generate relevant information (Niedersächsischer Landtag 14. Wahlperiode Drucksache 14/3339; Hesse, Drucksache 16/2042, 16. Wahlperiode 18. 05. 2004: “Sleeper cells” have not been identified. Information on Islamic extremism has been collected; Bavaria 14. Wahlperiode Drucksache 14/9221 06. 05. 2002: suspicious sleepers could not be identified (search criteria applied in Bavaria concerned: male, 18 to 40 years old, Islamic religion, student or former student, legal immigration status, not dependent on social security and coming from selected (Islamic) countries); Brandenburg Landtag Brandenburg Drucksache 3/4023: suspicious cases have not been identified). The Berlin Ombudsman for data protection summarized in 2002 the experiences with data mining and concluded that out of 58032 data sets some 114 individuals had initially been selected for further (conventional) investigation. None of these cases ultimately resulted in administrative or criminal proceedings (Berliner Beauftragter für Datenschutz und Informationsfreiheit 2002).

The then minister of finances Hans Eichel (SPD) earmarked 3 billion marks for this Counterterrorism package. The funds were collected by a two-step increase – on January 1, 2002 and 2003 - on the tobacco tax.

“Second Counterterrorism Package”

Changes in Aliens and Asylum Law represent a substantial part of the second Counterterrorism package. The reforms belong, on the one hand, to a wide-ranging catalogue of measures issued by the EU Ministers of Justice and Home Affairs on September 20, 2001. On the other hand, they turned the UN Security Council resolution 1373 into national law. The latter demanded, among other things:

- To prevent the movement of terrorists or terrorist groups by effective border controls;
- To prevent counterfeiting, forgery or fraudulent use of identity papers and travel documents;

- To find ways of intensifying and accelerating the exchange of operational information, especially regarding actions or movements of terrorists persons or networks, forged or falsified travel documents and weapons;
- To ensure, in conformity with international law, that refugee status is not abused by the perpetrators, organizers or facilitators of terrorist acts, and that claims of political motivation are not recognized as ground for refusing requests for the extradition of alleged terrorists.

Nevertheless, not all reforms contained in this package in the field of Aliens and Asylum Law were a product of 9/11. Some of them implement previous EU standards about harmonisation in this respect (for instance, the European EURODAC-regulation). These were also implemented in the Immigration Act draft presented by the Federal Government on November 6, 2001.

The second Counterterrorism package is also known as the “International Counterterrorism Act” (Gesetz zur Bekämpfung des internationalen Terrorismus) and contains 23 paragraphs amending 17 laws and 6 decrees. The Act passed the Federal Parliament rapidly in November 2001 and came into force on January 1, 2002. All in all, it widens cooperation between police and intelligence services and gives more powers to the Federal Police, the Federal Criminal Office and the Intelligence Services.

- Changes in Intelligence Services Laws

The fields of competence of the Federal Office for the Protection of the Constitution (Bundesverfassungsschutz), of the Military Counter Intelligence (Militärisches Abschirmdienst) and of the Intelligence Services (Bundesnachrichtendienst) were enlarged. The Federal Office for the Protection of the Constitution now also has the power to collect information on activities against the peace of nations (§3 par. 1 Nr.3 BVerfSchG). With that, the powers have been enlarged beyond the domestic field.

The Federal Office for the Protection of the Constitution is authorized to retrieve data from banks, postal offices, telephone companies, and airlines. Although the legal requirements to request such information concern a qualified risk, typical police powers have been granted to intelligence services going beyond strategic information collection. The Military Counter Intelligence (MAD) and the Intelligence Service (Bundesnachrichtendienst) received similar powers to retrieve information from the aforementioned

institutions. The use of the IMSI-Catcher (International Mobile Subscriber Identity) would be ruled by decree of the Federal Office for the Protection of the Constitution, included the mere stand-by function. This should allow investigators to know a person's position and the card and telephone number of his/her cell-phone.

- Modification of the Security Inspection Act

The Federal Security Inspection Act (Sicherheitsüberprüfungsgesetz) was widened, in order to cover sensitive security fields and to prevent acts of sabotage.

- Amendment of the Federal Criminal Office Act (Bundeskriminalamtsgesetz)

The amendment enlarged the possibilities of the Federal Police to act as a Central Office. The Federal Police are empowered to request any governmental or non-governmental office for information to fill in eventual gaps in investigations or for evaluation purposes, no matter whether this data might be already available for the local or State Police. This amendment strengthens the role of the Federal Police.

- Amendment of the Social Security Code's 10th Book

Data on social security will no longer be protected from data mining investigations after the amendment of § 68 par. 3 Social Code's 10th Book.

- Amendments of the Alien and Asylum Law

- Data transmission between Alien and Asylum Offices and the Federal Office for the Protection of the Constitution

The Act recognizes the UN Security Council's Resolution 1373 as its basic source. The Federal Office for the Recognition of Foreign Refugees (renamed to Federal Office for Migration and Refugees by the new Immigration Act) and the Alien Offices all over the country shall spontaneously transmit personal information related to threats relevant for the task specified in §3 par. 1 BVerfSchG.

- Amendment of the Aliens and Asylum Procedure Act

a. Aliens' ID (§§ 5; 39 par. 1, 56a, 69 par. 2 AuslG, § 63 AsylVfG)

The new ID documents include, besides a photo and signature, other "biometrical data" as well as a "zone for automatic reading". The details

are to be elaborated by a Federal Home Office regulation. All governmental offices are allowed to use this data to fulfil their tasks.

b. Assessment of origin by speech analysis (§§41 par. 2 sentence 2, 78 par. 3, 4 AuslG; §16 par. 1 sentence 3, par. 5, 6 AsylVfG)

The public recording and analysis of a foreigner's voice is allowed to assess the asylum seeker's homeland or at least the region where he/she comes from.

c. Establishing identity by fingerprints (§§41 par. 3-6, 78 par. 2-4 AuslG; §16 AsylVfG)

Civil war refugees and asylum seekers could already be fingerprinted. Fingerprint information was centrally stored by the Federal Police. From now on other foreign nationals will be also fingerprinted when:

- They are rejected as asylum seekers or sent back to a safe "third country" (§26a par. 2 AsylVfG)
- Grounds for refusing a residence permit were established due to suspicion of extremism (§8 par. 1 Nr. 5 AuslG)
- In case of visa applications of nationals from states with problems of repatriation, and situations stated in §73 Art. 1 Immigration Act (additional visa investigation in specific situations)

Foreigners of at least 14 years of age, who enter Germany without permission, should be fingerprinted, as should be illegal residents or those aliens who are suspected of having applied for asylum in another EU-country.

d. Collection and use of identification marks (§78 par. 2-4 AuslG; §16 par. 5,6 AsylVfG)

Fingerprints and other information on identification should remain in custody of the Federal Police for 10 years. Their use is allowed generally for identity assessment or as evidence in criminal proceedings.

e. Participation requirement in visa procedures (§73 Art. 1 Immigration Act)

Agencies which issue visas (i.e., German embassies) are to retrieve information from the intelligence service, the Federal Office for the Protec-

tion of the Constitution, the Military Counter Intelligence, the Federal Police and the Customs Office about particular groups of foreign nationals in order to investigate whether the applicant has a history of extremism (grounds for refusing visa, §5 par. 4 Art. 1 Immigration Act).

f. Amendment of the Aliens' Central Record Act (Art. 11)

The Aliens' Central Register (Ausländerzentralregister - AZR) was given a statutory basis in 1994. It already disposes of a huge amount of information about foreign residents. Disproportionate interferences with the informational self-rule occur without a clear legal basis. The use of records by several security agencies represents a factually unfounded, unjustified and unequal treatment of aliens in comparison to Germans.

a. Information to be entered (§ 3 Nr. 5 AZRG)

Information about religion or belief shall be included in the Aliens' Central Register.

b. Data mining investigations (§§ 12, 31 AZRG)

A data mining investigation on the basis of AZR-data (including the visa-data) no longer requires the presence of a concrete danger in a particular case, but the prevention of a danger in general. Intelligence services will also be able to carry out data mining investigations in order to counter possible aggression against the Federal Republic of Germany, or harm to the monetary stability through foreign money forgery and international money laundering.

The second Counterterrorism package resulted in legislation that significantly invaded privacy. It received harsh criticism especially from the data-protection ombudsmen.

The International Terrorism Counter Fighting Act contains, to some extent, sunset legislation. The expiration date for some of its measures was set at January 11, 2007 (art. 22 par. 2). An evaluation shall be carried out before this deadline (par. 3 same article). The Federal Government prepared a report on May 11, 2005 and presented it to the Parliamentary Home Affairs Board, which accepted it on June 1, 2005. The measures evaluated included the reforms of the Federal Office for the Protection of the Constitution Act, the Military Counter Intelligence Act, the G 10 Act, the Security

Inspection Act and § 7 par. 2 of the Federal Criminal Office Act. The Home Affairs Board was satisfied with the way in which the involved agencies had fulfilled their obligations. However, what was presented does not amount to a serious attempt at evaluation. The evaluation is restricted to information that investigations have been carried out on the basis of amended statutes. From the use of new powers it is concluded that these powers are necessary and that the use that had been made of such powers was successful. If that would be accepted as evaluation, then governments would have “carte blanche” in the case of parliamentary decisions requiring evaluation of legislation.

“Third Counterterrorism Package”

In spring 2005 the Federal Home Office prepared a draft for the “Third Counterterrorism Package”. It aims at introducing new powers for the Federal Police (BKA), establishing new information systems for Counterterrorism and better communication and cooperation among security agencies.

After the terrorist attacks in London in summer 2005 there was consensus between the Government and the opposition parties about the necessity to pass a “third Counterterrorism package”. But the fact that federal elections were already carried out in late 2005 changed the scenario. All draft laws that are processed through the parliament are subject to the “discontinuity principle”. It is to be expected, however, that the new 'black&red' government-elect will pick up the draft again and develop it further.

Act on the Introduction of the European Arrest Warrant

As outlined earlier, the European Arrest Warrant was implemented on the basis of a statute that was declared unconstitutional by the Federal Constitutional Court (2 BvR 2236/04 July 18th 2005; see above).

Air Traffic Control Act

The Air Traffic Control Act responded on the one hand to the terrorist attacks of 9/11 in New York and Washington, and on the other hand, to an episode in Frankfurt on January 5, 2003 when a mentally ill pilot threatened to crash his small airplane into a building. On that day, fighter planes took off from Frankfurt airbase and tried to force the pilot to land. Controversially discussed was §14 par. 3 of the Act. It authorizes the shooting down of an airplane, if it can be assumed that the plane will immediately be

used as a weapon to threaten the lives of other persons, and if downing the plane is the only possibility way to save lives on the ground. The order is to be given by the Federal Defence Minister or his/her deputy and is to be carried out by the Air Force. Downing a plane under these circumstances was regarded to be an ultima ratio. It should have stepped in when an aircraft is either out of control or intentionally “transformed” into a weapon, and the risk that it causes great harm for people on the ground cannot be avoided otherwise. The Act came into force on January 11, 2005¹. The Federal President Horst Köhler signed it but stated serious doubts as regards compliance of §14 with the German Constitution. Two arguments backed up these doubts: first, justifying the sacrifice of human lives in order to rescue others on the ground does involve weighing up lives against other lives. Secondly, the downing of a plane would be carried out by the armed forces (Bundeswehr). However, the German Constitution prohibits deployment of the military on the territory of the Federal Republic of Germany and for issues of internal security.

Through a decision of the Federal Constitutional Court the act was declared to be unconstitutional (BVerfG, 1 BvR 357/05 as of 15. 2. 2006).

2.4 Dangerousness and incapacitation

Over the last two years a debate on preventative detention for terrorist offenders unfolded in Germany. The debate paralleled a discussion in the United Kingdom on the very same issue. The British Home Office Secretary some time ago announced plans for amending anti-terrorism legislation in order to allow for criminal trials that would be held in secret, before a security vetted judge and possibly state appointed defence councils who have been security cleared. More important still, the secretary voiced demand for lowering the current threshold of burden proof down from the beyond reasonable doubt standard to a balance of probability (www.guardian.co.uk/terrorism/). The former German Federal Minister of the Interior Schily thought then also about a need to introduce legislation which allows the for the detention of individuals deemed to be dangerous although past crimes cannot be proven (www.bmi.bund.de/). He considered creating special police detention laws that provide for the power to incapacitate individuals by way of detaining them (as long as dangerousness

¹ BGBl I 2005, 78. Modified by art. 49 of the Act from 21 June, 2005 I 1818.

prevails, see also the statement of the former Federal Minister of Interior, Spiegel Online, August 2, 2005; preventative detention (although restricted to 48 hours) is also considered in the Australian Draft Anti-Terrorism Bill 2005).

In fact, the first trial related to the WTC attacks which was held in Germany and resulted in the first instance conviction of Motassadeq (allegedly conspiring with those directly involved in the attacks and supporting the whole enterprise by channelling funds from Hamburg to North-America) demonstrates the type of problems that have to be encountered when applying due process standards in terrorist cases. The conviction was thrown out by the Supreme Court which argued that the standard of proof beyond reasonable doubt was in this case not fulfilled which in turn then led to the question whether such a system is able to deal effectively with terrorism (Safferling 2004).

While the new coalition government, in office since November 2005, agreed to postpone discussions about the introduction of preventative detention of dangerous terrorists, the new Federal Minister of the Interior now came up with a new proposal. He suggested the introduction of legislation that penalizes, for example, staying at a terrorist training camp.

In fact, the debates on how to respond to terrorist networks and how to deal with risks that cannot be responded to by way of carrying out ordinary criminal proceedings because evidence is too weak have led to three lines of thinking on how to deal with individuals assumed to pose significant terrorist threats.

*Incapacitating dangerous individuals on the basis
of assessments of dangerousness*

Current legislation that responds to dangerous individuals through preventive (or pre-emptive) detention is based upon rationales which have been accepted already in the 19th century. One form of preventive detention addresses psychiatric conditions which are assessed to create severe dangers for the individuals themselves or for others. Another form of preventive detention refers to the two track system of criminal sanctions which developed in many continental European systems of criminal justice. Here, the preventive track of criminal sanctions responds to dangerousness that, however, must be linked to past crimes and must be justified by an individual displaying the characteristics of a habitual offender. A third form of

preventive detention is found in police (or public order) laws which allow for (short term) detention if an individual is assessed to present an immediate danger. Such detention is limited to rather short periods of time (in Germany for example up to two weeks) and must be justified by an imminent danger (e.g., prediction of violent behaviour at the occasion of a soccer game).

Transnational organized crime and international terrorism both point towards a new category of dangerousness which does not result from insanity nor from chronic or career offending nor from a need to respond to an imminent and short term danger. It is either rational (market) behaviour or extremist attitudes which provoke assessments of (longterm) dangerousness. Insofar, there will not be indicators such as chronic past offending or a psychiatric diagnosis available but – according to ongoing debates – rather soft criteria like having spent time in an Al Qaeda training camp (see now the UK Draft Terrorism Bill 2005 where attendance at a place used for terrorist training shall be made a criminal offence), being part of a communicating network of extremists, voicing certain (extremist) ideas and convictions. However, public opinion and the political will in European societies will inevitably lead to such legislation in the future. This again demonstrates that it will be of paramount importance to establish procedures which will guarantee an independent (judicial) control of detention decisions as well as procedural fairness as requested by the European Convention on Human Rights.

*Creating new criminal law that penalizes behaviour
that indicates dangerousness*

A second line of thinking on how to respond to dangerous individuals concerns substantive criminal law that penalizes behaviour that, in the first line of thinking, is used as factors indicating dangerousness. The problem here, of course, concerns whether such dangerousness can be established in a way that justifies the creation of a criminal offence statute.

Lowering the threshold of proof in criminal proceedings

A third line refers to lowering the threshold of proof for selected (terrorist) criminal offences.

The debate on the risk, prevention and dangerousness also centers around the topic of “enemy criminal law” (Feindstrafrecht).

3. Summary

3.1 Legislation issues

The formal definition of terrorist offences is found in §§129a, b Criminal Code. With that the Federal Republic of Germany has implemented the EU framework decision on terrorism. §129a encloses a wide approach to terrorist offences and covers recruitment, training, preparatory acts, financing etc.

Special arrangements for preventive detention without charge in terror cases do not exist; however, §129a may serve as a ground to impose pre-trial detention without resorting to conventional grounds such as risk of absconding or obstruction of justice.

Terrorist suspects or convicted terrorists may be held incommunicado for up to 30 days if an immediate danger to the life of other persons can be established.

Crown witness legislation is currently available, but restricted to particular offence statutes. A general crown witness rule is currently being drafted.

Under the conditions outlined above, witnesses may be protected by the granting of anonymity. Intelligence services may withhold information (or witnesses coming from their ranks) by way of denying disclosure of information (justified with protecting eminent security interests) but then, such information may not be introduced as evidence.

3.2 Policies

As regards prevention and driving back of radicalisation and the development of extremism among sections of the population, initiatives have addressed, in particular, right wing extremism. The Federal Government is funding programmes that aim at reducing the influence of extremist ideologies, including providing for support for would be dropouts (see e.g., www.interkultureller-rat.de; www.exit-deutschland.de).

It is assumed that radicalisation of Muslims may take place through mosques, the internet and prisons (in particular for recruitment of young and marginalized immigrants). However, no research is available that could demonstrate whether such assumptions are valid.

No national frameworks exist (beside approaches to right wing extremism) that would serve as blueprints etc., for local approaches.

Dialogues rank high on the political agenda (in particular as regards dialogues between cultures, religion etc.). Muslim Councils exist and they participate in various conferences. Neither formally nor informally leaders of ethnic, religious or other organizations are assigned roles in preventing extremism.

A connection between integration of minorities and youth violence is made. Marginalization and disintegration are linked particularly to poor integration into the system of education and into the labour market. Recently, cultural integration in terms of language capabilities, knowledge and acceptance of Western values play a role in discussing the general phenomenon of “parallel societies”.

Monitoring of places where radicalisation takes place (or is assumed to take place) falls under the competence of internal intelligence services.

Radical organisations may also be banned by order of Ministry of Interior, if they are define themselves as being religious organizations.

Policy documents as regards means and aims with respect to prevention of radicalisation do exist in a general sense. However, they are not elaborated and reflect the particular perspectives of intelligence services, police or the Ministry of the Interior.

No general policy as regards the information of the public on radicalisation etc., exists.

Literature

Albrecht, H.-J. (1998): Organisierte Kriminalität – Theoretische Erklärungen und empirische Befunde, in: Deutsche Sektion der Internationalen Juristen-Kommission (Ed.): Organisierte Kriminalität und Verfassungsstaat. Heidelberg: Müller, pp. 1-40.

Albrecht, H.-J. (1998a): Money Laundering and the Confiscation of the Proceeds of Crime - A comparative view on different models of the control of money laundering and confiscation. In: The Europeanisation of Law. Ed. T. Watkin. United Kingdom Comparative Law Series, vol. 18, Alden Press, Oxford, pp. 166-207.

- Albrecht, H.-J. (1999): Die Determinanten der Sexualstrafrechtsreform. *Zeitschrift für die gesamte Strafrechtswissenschaft*, 111, pp. 863-888.
- Albrecht, H.-J. (2002): Fortress Europe? – Controlling Illegal Immigration. *European Journal of Crime, Criminal Law and Criminal Justice*, 10, 2, pp. 1-22.
- Albrecht, H.-J., Dorsch, C., Krüpe, C. (2003): Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen. Max-Planck-Institute for Foreign and International Criminal Law: Freiburg.
- Albrecht, H.-J., Fijnaut, C. (Eds.) (2002): The Containment of Transnational Organized Crime. Comments on the UN-Convention of December 2000. Freiburg: Edition iuscrim.
- Albrecht, H.-J.: Organisierte Kriminalität – Theoretische Erklärungen und empirische Befunde. In: Albrecht, H.-J. et al.: Organisierte Kriminalität und Verfassungsstaat. Heidelberg 1998, pp. 1-40.
- Antwort der Bundesregierung (2005): Auslagerung spezifischer Sicherheits- und Militäraufgaben an nichtstaatliche Stellen. Bt-Drucksache 15/5824, 24. 06.
- Arnold, J. (2001): Kriminelle Vereinigung und organisierte Kriminalität in Deutschland und anderen europäischen Staaten. In: Militello, V., Arnold, J., Paoli, L. (Eds.): Organisierte Kriminalität als transnationales Phänomen. Freiburg: Edition iuscrim, pp. 87-176.
- Arquilla, J., Ronfeldt, D. (Eds.) (2001): Networks and Netwars: The Future of Terror, Crime, and Militancy. Washington: Rand.
- Aust, S.: Der Baader-Meinhof-Komplex. Hamburg 1997.
- Beck, U. (2002): Das Schweigen der Wörter. Über Terror und Krieg. Frankfurt: Edition Suhrkamp.
- Benoist, A. de (2002): Die Wurzeln des Hasses. Ein Essay zu den Ursachen des globalen Terrorismus. Berlin: Edition JF.
- Berliner Beauftragter für Datenschutz und Informationsfreiheit: Sonderbericht. Berlin 10. 12. 2002.
- Berlit, U., Dreier, H. (1984): Die legislative Auseinandersetzung mit dem Terrorismus. In: Sack, F., Steinert, H. (Eds.): Protest und Reaktion. Opladen: Westdeutscher Verlag, pp. 227-318.
- Bloy, R. (2003): Möglichkeiten und Grenzen der Gewährleistung von Sicherheit durch Strafrecht. In: Momsen, C., Bloy, R., Rackow, P.

- (eds.): *Fragmentarisches Strafrecht. Beiträge zum Strafrecht, Strafprozessrecht und zur Strafrechtsvergleichung*. Peter Lang: Frankfurt a.M.
- Blumenwitz, D. (2002): *Einsatzmöglichkeiten der Bundeswehr im Kampf gegen den Terrorismus*. *Zeitschrift für Rechtspolitik*, 3, pp. 102-106.
- Bowden, M.: *The Dark Art of Interrogation. The most effective way to gather intelligence and thwart terrorism can also be a direct route into morally repugnant terrain. A survey of the landscape of persuasion*. *The Atlantic Monthly* October 2003
- Chalk, P., Rosenau, W. (2004): *Confronting the "Enemy Within" Security Intelligence, the Police, and Counterterrorism in Four Democracies*. RAND: Santa Monica.
- Council of Europe (2004): *The fight against terrorism - Council of Europe standards*. Council of Europe: Strasbourg.
- CPT (2003): *Report to the Government of the United Kingdom on the visit to the United Kingdom carried out by the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT) from 17 to 21 February 2002*. CPT/Inf (2003) 18. Strasbourg.
- CPT (2004): *Suspected international terrorists detained in the United Kingdom: new visit by the Council of Europe's Anti-Torture Committee*. News Flash. www.cpt.coe.int/documents/gbr/2004-03-24-eng.htm (14. 4. 2004).
- Crelisten, R., Özkut, I. (2000): *Counterterrorism Policy in Fortress Europe : Implications for Human Rights*. In: Reinares, F. (Ed.): *European Democracies Against Terrorism. Governmental Policies and Intergovernmental Cooperation*. Ashgate: Aldershot, pp. 245-272.
- Department of the Parliamentary Library (2002): *Terrorism and the Law in Australia: Legislation, Commentary and Constraints*. Research Paper No. 12, 2001-02. Melbourne: IRS Publications Office.
- Dishman, C. (2001): *Terrorism, Crime, and Transformation*. *Studies in Conflict & Terrorism* 24, 1, pp. 43-58.
- EC Commission, Working Document (2001): *The relationship between safeguarding internal security and complying with international protection obligations and instruments*. Brussels, 5 December 2001, COM, 743 final.

- European Council (2003): A secure Europe in a Better World. European Security Strategy. Brussels, 12 December 2003.
- Expertenkommission im Auftrag der Bundesregierung (23. 01. 2001): Bericht an den Nationalrat Verteidigungsdoktrin Analyse-Teil. Wien.
- FATF (2001): Money Laundering 2000-2001 Report. Paris.
- FATF (2002): Guidance for Financial Institutions in Detecting Terrorist Financing. FATF Secretariat: Paris.
- FATF (2003): The Forty Recommendations. FATF Secretariat: Paris.
- Federal Ministry of the Interior (2005): Fakten zur Evaluierung des Terrorismusbekämpfungsgesetzes. Berlin, May 11.
- Grässle-Münscher, J. (2002): Terror und Herrschaft. Die Selbstbespiegelung der Macht. Hamburg: Europäische Verlagsanstalt.
- Gressang, D. S. (2000): Terrorism and Sovereignty: Considering the Potential for Success. *Low Intensity Conflict & Law Enforcement* 9, 1, pp. 67-92.
- Groß, T. (2002): Terrorbekämpfung und Grundrechte. Zur Operationalisierung des Verhältnismäßigkeitsgrundsatzes. *Kritische Justiz*, 35, 1, pp. 1-17.
- Grosse Anfrage (2005): Auslagerung spezifischer Sicherheits- und Militäraufgaben an nichtstaatliche Stellen. Deutscher Bundestag Drucksache 15/0, 15. Wahlperiode, 18. Januar.
- Gurr, T.R. (1998): Terrorism in democracies: Its social and political basis. In: Reich, Walter (Eds.): *Origins of Terrorism*. Washington: Woodrow Wilson Center, pp. 86-102.
- Hassemer, W. (1992): Kennzeichen und Krisen des modernen Strafrechts. *Zeitschrift für Rechtspolitik*, pp. 378 - 383.
- Hermant, D., Bigo, D. (2000): Les Politiques de Lutte contre le Terrorism: Enjeux Francais. In: Reinales, F. (Eds.): *European Democracies Against Terrorism. Governmental Policies and Intergovernmental Cooperation*. Hampshire: Ashgate, pp. 73-118.
- Herzog, F. (1999): Geldwäschebekämpfung - quo vadis? *Zeitschrift für Wirtschafts- und Bankrecht*, 53, pp. 1905-1919.
- Herzog, F. (2003): Die Spuren des "schmutzigen Geldes" – Finanzermittlungen vor der Verdachtsschwelle. In: Hirsch, H.J., Wolter, J., Brauns, U. (eds.): *Festschrift für Günter Kohlmann zum 70. Geburtstag*. Köln, S. 427-450.

- Hess, H. (2002): Terrorismus und Weltstaat. *Kriminologisches Journal*, 34, 2, pp. 143-149.
- Hesse, H. A. (1994): *Der Schutzstaat. Rechtssoziologische Skizzen in dunkler Zeit*. Baden-Baden: Nomos.
- Hoffman, B., Morrison-Taw, J. (2000): A Strategic Framework for Countering Terrorism. In: Reinares, F. (Eds.): *European Democracies Against Terrorism. Governmental Policies and Intergovernmental Cooperation*. Hampshire: Ashgate, pp. 3-29.
- Hood, R. (2003): *The Death Penalty. A Worldwide Perspective*. 3rd ed., Oxford.
- Huber, B. (2002): Die Änderungen des Ausländer- und Asylrechts durch das Terrorismusbekämpfungsgesetz. *Neue Zeitschrift für Verwaltungsrecht*, 7, pp. 787- 794.
- Jahn, J. (2002): Verschärfte Finanzkontrollen nach Terroranschlägen. *Zeitschrift für Rechtspolitik*, 3, pp. 109-110.
- Jakobs, G. (2000): Selbstverständnis der Strafrechtswissenschaft vor den Herausforderungen der Gegenwart (Kommentar). In: Eser, A., Hassemer, W., B. Burkhardt (Eds.): *Die deutsche Strafrechtswissenschaft vor der Jahrtausendwende. Rückbesinnung und Ausblick*. München: Beck, pp. 47-56.
- Kilchling, M. (Ed.) (2002): *Die Praxis der Gewinnabschöpfung in Europa*. Max Planck Institute für Foreign and International Criminal Law: Freiburg.
- Kittrie, N. N. (2000): *Rebels with a Cause. The Minds and Morality of Political Offenders*. Boulder: Westview Press.
- Köhler, M.: Unbegrenzte Ermittlung und justizfreie Bundesgeheimpolizei: Der neue Strafprozeß? *Strafverteidiger* 1994, pp. 386-389.
- Kunz, K.-L. (2001): *Kriminologie*. 3. Auflage. Bern, Stuttgart, Wien: Haupt.
- Laqueur, W. (1987): *Terrorismus. Die globale Herausforderung*. Ullstein: Frankfurt, Berlin.
- Laqueur, W. (1998): *Die globale Bedrohung*. Berlin: Propyläen.
- Laqueur, W.: *Die globale Bedrohung*. Berlin 1998.
- Leman-Langlois, S., Brodeur, J.-P. (2005): Terrorism Old and New : Counterterrorism in Canada. *Police Practice & Research: An International Journal*, 6, pp. 121-140.

- Malcolm, W., Barker, D. (2002): Privacy and Surveillance: trouble ahead for communications providers. *New Law Journal*, 152, 7016, pp. 80-83.
- Maurer, A. (2002): §129b und Kronzeugenregelung. Alte Instrumente in neuem Gewand. *Bürgerrechte & Polizei* 70, 3, pp. 20-27.
- Mello, M. (2002): Friendly Fire: Privacy vs Security After September 11. *Criminal Law Bulletin*, 38, 2, pp. 367-395.
- Militello, V., Arnold, J., Paoli, L. (2001): Organisierte Kriminalität als transnationales Phänomen. Freiburg: Edition iuscrim.
- Militello, V., Huber, B. (2001): Towards a European Criminal Law Against Organized Crime. Freiburg: Edition iuscrim.
- Miller, W. (2000): Insurgency Theory and the Conflict in Algeria: A Theoretical Analysis. *Terrorism and Political Violence* 12, 1, pp. 60-78.
- Müller-Wille, B. (2004): For Our Eyes Only? Shaping an Intelligence Community Within the EU. The European Union Institute for Security Studies, Occasional Papers no. 50.
- Münkler, H. (2002): Die neuen Kriege. Rowohlt: Reinbek.
- Narr, W.-D. (2002): Ermächtigungsgesetze. Editorial. *Bürgerrechte & Polizei* 70, 3, pp. 1-9.
- Paeffgen, H.-U. (2002): „Vernachrichtendienstlichung“ von Strafprozeß- (und Polizei)recht im Jahre 2001. *Strafverteidiger* 22, 6, pp. 336-341.
- Parent, G.-A. (2002): Les événements du 11 septembre et la sécurité intérieure. *Revue internationale de criminologie et de police technique et scientifique* 55, 1, pp. 51-69.
- Peters, B.: RAF - Terrorismus in Deutschland. Stuttgart 1991.
- Proceedings of the Conference (2001): Integrated Security in Europe, a democratic perspective. Bruges, 14-17 November 2001. Brussels, Brugge.
- Sack, F. (1999): Jugendgewalt – Schlüssel zur Pathologie der Gesellschaft? in: Programmleitung NFP 40 (Eds.): Gewalttätige Jugend – ein Mythos? Bulletin Nr. 4. Bern: SFN, pp. 10.
- Sack, F. (2001): Prävention als staatliches Sicherheitsversprechen – Wandlungen des Gewaltmonopols in Deutschland, in: Komitee für Grundrechte und Demokratie (Eds.): Verpolizeilichung der Bundesrepublik Deutschland. Köln: hbo-druck, pp. 21-65.

- Safferling, C. J.M. (2004): Terror and Law – Is the German Legal System able to deal with Terrorism? – The Bundesgerichtshof (Federal Court of Justice) decision in the case against El Motassadeq. *German Law Journal* 5, pp. 515-524.
- Sarma, K. (2005): Informers and the Battle Against Republican Terrorism: A Review of 30 Years of Conflicts. *Police Practice & Research: An International Journal*, 6, pp. 165-180.
- Sassoli, M. (2004): The Status of Persons Held in Guantanamo under International Humanitarian Law. *Journal of International Criminal Justice* 2, pp. 96-106.
- Saul, B. (2003): International Terrorism as a European Crime: The Policy Rationale for Criminalization. *European Journal of Crime, Criminal Law and Criminal Justice* 11, pp. 323-349.
- Schünemann, B. (2003): Das Strafrecht im Zeichen der Globalisierung. *Goldammer's Archiv für Strafrecht*, 140, pp. 299-313, p. 299.
- Singer, P.W. (2003): *Corporate Warriors. The Rise of the Privatized Military Industry*. Ithaca, London.
- Singh Jafa, Y. (2005): Defeating Terrorism: A Study of Operational Strategy and Tactics of Police Forces in Jammu & Kashmir (India). *Police Practice & Research: An International Journal*, 6, pp. 141-164.
- Stegmann, A. (2004): *Organisierte Kriminalität. Feindstrafrechtliche Tendenzen in der Rechtssetzung zur Bekämpfung organisierter Kriminalität*. Bern.
- Stern, St. (2002): Heute Beschuldigter – morgen „Kron“-Zeuge. *Strafverteidiger Forum* 6, pp. 185-190.
- Tolmein, O. (2002): *Vom Deutschen Herbst zum 11. September. Die RAF, der Terrorismus und der Staat*. Hamburg: Konkret.
- Troosters, R. (2004): The European Union Framework Decision of 13th June 2002 on Combating Terrorism. In: Horvath, O. (ed.): *European Cooperation Against Terrorism*. Nijmegen, pp. 67-75.
- Turk, A.T. (2002): Policing International Terrorism: Options. *Police Practice and Research. An International Journal* 3, pp. 279-286.
- U.S. Department of Justice, Office of Legal Counsel (2002): *Memorandum for Alberto R. Gonzales, Counsel to the President*. Washington, August 1.

- United Nations Office on Drugs and Crime (2004): Money Laundering and the Financing of Terrorism: The United Nations Response. UNODC: Vienna.
- Van de Voorde, C. (2005): Sri Lankan Terrorism: Assessing and Responding to the Threat of the Liberation Tigers of Tamil Eelam (LTTE). *Police Practice & Research: An International Journal*, 6, pp. 181-200.
- Wächtler, H.: Dokumente und Materialien zur Kontaktsperre für Verteidiger. *Kritische Justiz* (1977), 395-412.
- Walker, C. (1992): *The Prevention of Terrorism in British Law*. 2. Auflage. Manchester: Manchester University Press.
- Walker, C. (2000): Briefing on the Terrorism Act 2000. *Terrorism and Political Violence* 12, 2, pp. 1-36.
- Wegner, C. (2002): Das Geldwäschebekämpfungsgesetz - Neue Pflichten für rechtsberatende Berufe und verfahrensrechtliche Besonderheiten. *Neue Juristische Wochenschrift*, 32, pp. 2276-2278.
- White House Memorandum (2002): Humane Treatment of al Qaeda and Taliban Detainees. Washington.
- Wittke, T.: Terrorismusbekämpfung als rationale politische Entscheidung. Frankfurt/M.
- Yeandle, M., Mainelli, M., Berendt, A., Healy, B. (2005): *Anti-Money Laundering Requirements: Costs, Benefits and Perceptions*. Z/Yen Limited: London.
- Zelman, J.D. (2001): Recent Developments in International Law: Anti-Terrorism Legislation – Part One: An Overview. *Journal of Transnational Law and Policy* 11, pp. 1-18.