Auswärtiges Amt

COUNTER-TERRORISM IMPLEMENTATION TASK FORCE CTITF
United Nations

14 December 2009

Invitation

Workshop on „Countering Terrorist Use of the Internet – Addressing Legal Aspects" in Berlin, 25-26 January 2010

Dear Colleague,

The Federal Foreign Office – Task Force/International Co-operation on Counter-Terrorism – and the United Nations Counter Terrorism Implemenation Task Force (CTITF) are jointly organizing a workshop on „**Countering Terrorist Use of the Internet – Addressing Legal Aspects**" which will be held in Berlin on 25-26 January 2010.

The workshop will focus on the effectiveness of legal frameworks devised to counter terrorist use of the Internet. Participants from national governments, international organizations, academia and civil society are called upon to share their experience in implementing and applying legal tools, to identify problems and shortcomings, and to exchange views on possible remedies.

The workshop forms part of a major project undertaken by the CTITF Working Group on Countering the Use of the Internet for Terrorist Purposes which aims at supporting Member States in their efforts to deal with terrorist use of the Internet. Subsequent workshops on „technical aspects" and „counter narratives" will complete the project. Its results are to be compiled and analysed, finally to be published in a comprehensive practical guide.

The Federal Foreign Office and CTITF cordially invite you or one of your colleagues to participate in the workshop and are looking forward to your attendance. Presentations are welcome, but we would kindly request that you limit your statements to 5-7 minutes in order to leave sufficient time for discussion.

A draft agenda, organizational details, and a registration form are enclosed. Further enclosed is a questionnaire which will inform the background research for this project. **We kindly ask you to complete the attached questionnaire regardless of whether or not you will be able to attend the workshop.** Thank you very much for your cooperation!

To RSVP or for any questions regarding this workshop please contact:

Mr. Jan Neutze
Counter-Terrorism Implementation Task Force
United Nations, New York
Email: neutze@un.org
Phone: +1-212-457-1767

We hope that you can participate in this timely workshop and look forward to your response.
Sincerely,

Eugen Wollfarth (Auswärtiges Amt)

Jean-Paul Laborde (CTITF)

For questions concerning the background research, the questionnaire or in case you are planning on making a presentation at the workshop, please contact Dr. Marco Gercke, Cybercrime Research Institute at gercke@cybercrime.de.

Auswärtiges Amt

COUNTER-TERRORISM IMPLEMENTATION TASK FORCE CTITF

United Nations

Registration Form

Workshop on "Countering Terrorist Use of the Internet – Addressing Legal Aspects"

Berlin, 25-26 January 2010

To RSVP by 8 January 2010 to:

Mr. Jan Neutze
Counter-Terrorism Implementation Task Force (CTITF)
United Nations
Phone: + 1-212-457-1767
Fax: +1-212-457-4037
neutze@un.org

DELEGATE INFORMATION **COUNTRY:**

Family Name

Name *Middle name*

Institution

Department

Address *Postal Code*

City

Phone (Please include country and area code) *Fax*

Mobile

E-mail

Auswärtiges Amt

COUNTER-TERRORISM IMPLEMENTATION TASK FORCE CTITF
United Nations

Workshop on „Countering Terrorist Use of the Internet – Addressing Legal Aspects" in Berlin, 25-26 January 2010

Organizational Details

Location of the Workshop:
The workshop will take place at the German Foreign Office in Berlin in the Adenauer Conference Room. Please sign in at the Foreign Office main entrance at Werderscher Markt 1, 10117 Berlin and you will be guided to the workshop conference room. For directions about the location, please see the Foreign Office website at:
http://www.auswaertiges-amt.de/diplo/en/AAmt/Erreichbarkeit,navCtx=57696.html
In case of any immediate query please contact Dr.M.Mimler at +49 (0)30 1817 1694 or Mr. W. Müller at +49 (0)30 1817 2930.

Questionnaire:
Attached to this invitation you will find a questionnaire developed by the CTITF Working Group on Countering the Use of the Internet for Terrorist Purposes. Responses to the questionnaire will serve to inform the project research. We kindly ask you to complete the questionnaire (whether you are able to attend the workshop or not) and submit it to Dr. Marco Gercke, Cybercrime Research Institute (gercke@cybercrime.de) by 31 December 2009.

Structure of the Workshop:
The workshop will be divided into five thematic sessions. There will be two or three impulse speakers at the beginning of each session who will help frame the issue and start the discussion. We strongly encourage your active participation in all sessions. If you are planning on making a presentation at the workshop, we kindly ask you to limit your contribution to 5-7 minutes in order to leave sufficient time for discussion among the participants.

Travel & Accommodation in Berlin:
Should you require accommodation in Berlin a number of hotels are located in close proximity to the Federal Foreign Office, such as
Arcotel JohnF, Werderscher Markt 11, 10117 Berlin, 030 405046-0, johnf@arcotel.at
Park Inn, Alexanderplatz, 10178 Berlin, 030 2389-0, reservations.berlin@rezidorparkinn.com
Novotel, Fischerinsel, 10179 Berlin, 030 20674-0, h3278@accor.com

Travel and accommodation costs can unfortunately not be reimbursed.

Contacts:
For questions about the overall project of the CTITF Working Group or the workshop in Berlin, please contact Jan Neutze, CTITF, United Nations at neutze@un.org or at +1-212-457-1767

Auswärtiges Amt

COUNTER-TERRORISM IMPLEMENTATION TASK FORCE CTITF
United Nations

Workshop on „Countering Terrorist Use of the Internet – Addressing Legal Aspects" in Berlin, 25-26 January 2010

25-26 JANUARY 2010
FEDERAL FOREIGN OFFICE, ADENAUER ROOM, BERLIN

AGENDA

DAY ONE, MONDAY, 25 JANUARY

8:30	**REGISTRATION**
9:00	**WELCOME AND INTRODUCTION** **Eugen Wollfarth**, *Head of Task Force - International Cooperation on Counter-Terrorism, Federal Foreign Office* **Jean-Paul Laborde**, *Chairman of CTITF, United Nations* **Richard Barrett**, *Co-ordinator, Al-Qaida and Taliban Monitoring Team, United Nations*
9:30	**KEYNOTE ADDRESS "COUNTERING TERRORIST USE OF THE INTERNET"** **Ambassador Dr. Georg Birgelen**, *Commissioner on Counter-Terrorism, Federal Foreign Office*
10:15	Coffee Break
10:30	**SESSION 1: "INTERNET-RELATED PROPAGANDA AND RECRUITMENT"** **Zahid Jamil**, *Jamil & Jamil, Pakistan*
12:30	Lunch
14:00	**SESSION 2: "INTERNET-RELATED TERRORIST FINANCING"** **Marc Goodman**, *Director IMPACT Alliance, Malaysia* **Daniel Thelesklaf**, *Co-Executive Director, Basel Institute of Governance, Switzerland* **Michael DeFeo**, *Advisor, UNODC & former U.S. Dept. of Justice official*
15:45	Coffee Break
16:00	**SESSION 3: "COMPUTER AND NETWORK-RELATED ATTACKS"** **Eneken Tikk**, *Head of Legal Team, NATO COE CCD, Estonia* **Claus Kreß**, *Law Professor, University of Cologne, Germany*
17:45	End of Day One

DAY TWO, TUESDAY, 26 JANUARY

9:00	**SESSION 4: "COLLECTION OF INFORMATION THROUGH COMPUTER AND NETWORK-TECHNOLOGY"** **Andrey Kulpin**, *Professor, Moskow State University*
10:45	Coffee Break
11:00	**SESSION 5: "COMMUNICATION THROUGH INTERNET-RELATED SERVICES"** **Phillip Brunst**, *Head of section on Information Technology Law and Legal Informatics at Max-Planck Institute for Foreign and International Criminal Law, Germany*
12:30	**CLOSING SESSION AND RECOMMENDATIONS**
13:30	End of Day Two

Legal aspects related to terrorist use of the Internet

Cybercri
Research Institute

Questionnaire

1. General Information

1.1 Background:

This questionnaire serves to inform the background research for a project of the **UN Counter-Terrorism Implementation Task Force (CTITF) Working Group on "Countering the Use of the Internet for Terrorist Purposes."** Responses submitted though this questionnaire will help the Working Group in preparation for an upcoming expert meeting which will take place in Berlin in January 2009. The meeting, jointly organized by CTITF and the German Federal Foreign Office, will focus in particular on the legal approaches to countering terrorist use of the internet, including – but not limited to – criminalization instruments, investigation instruments, as well as preventive elements.

Initial background research on national and international legal responses terrorist use of the Internet has shown a multitude of different approaches. The main goal of the questionnaire is to involve experts, practitioners, and analysts dealing with terrorist use of the internet by collecting responses to this questionnaire in order to ensure a more comprehensive picture of the different legal approaches pursued to counter terrorist use of the internet by different national governments and international organizations. The responses are intended to inform the project's background research, stimulate debate at the expert meeting, and guide the conclusions for the project's outcome document.

Please be advised that it is the intention of the CTITF Working Group to share the information gathered through this questionnaire with the members of the Working Group as well as those experts attending the Working Group meeting in Berlin. For any questions about the questionnaire or the research conducted for this project, please do not hesitate to contact the project lead researcher and drafter of the report, Dr. Marco Gercke of the Cybercrime Research Institute at gercke@cybercrime.de

1.2 Submission

Submissions should be made until **31.12.2009** to be included in the background paper prepared for the expert meeting. This word-document can be used to include comments and notes. To facilitate the preparation of the background paper it would be highly appreciated if relevant case studies, publications and example for legal approaches could be submitted as attached PDF-documents if possible.

Please send your responses to Dr. Marco Gercke at gercke@cybercrime.de

1.3 Contact information regarding the working group meeting

If you have any questions related to the upcoming expert meeting of the CTITF Working Group on "Countering the Use of the Internet for Terrorist Purposes" and the scope of the meeting, please contact Mr. Jan Neutze, CTITF, United Nations at neutze@un.org

2. Questionnaire – General Information

2.1 Categories for the Debate

The Working Group expert meeting will focus on the following five different categories of terrorist use of the internet:

- Internet-related Propaganda and Recruitment
- Internet-related Terrorist Financing
- Computer and Network-related Attacks
- Collection of Information through Computer and Network-Technology
- Communication through Internet-related Services

2.2 Structure of the Questionnaire

The questionnaire was designed to collect examples of successful investigations, reports about current or completed cases, as well as legal responses related to the five categories of terrorist use of the Internet.

- Information about legal responses is especially relevant in those areas where legal measures are considered an adequate response to an existing threat. To focus on existing threats (rather then discussing the extent of potential threats), we particularly welcome the submission of documented, fact based examples of cases, prosecutions, and legal measures on which they were based.
- The focus of the questionnaire is on the collection of different legal approaches to terrorist use of the internet. In addition to criminalization and investigation instruments, the background research will also cover preventive measures – submission of examples in this area are welcome.

3. Questionnaire – Main Part

3.1 Internet-related Propaganda and Recruitment

Over the past ten years there has been a dramatic increase in the number of violent extremist organizations maintaining websites informing their followers and the general public about their activities. According to the U.S. Institute of Peace, most of the these organizations – among them the PKK and Al Qaida – today maintain websites.[i] Terrorists have also started to use video communities (such as YouTube) to distribute video messages and propaganda.[ii] The use of websites and other forums signals a more professional public relations focus by terrorist groups.[iii] Websites and other media are used to disseminate propaganda,[iv] to describe and publish justifications of their activities[v] and to recruit[vi] new, and contact existing, members and donors.[vii]

Legal Response:

The fact that terrorist organizations can easily set up websites could be addressed by implementing registration obligations and mandatory verification procedures to ensure that the operators of such websites can be identified. Apart from the possibility of circumventing such measures by using illegally obtained identities,[viii] such approaches would require intensive administration from the industry or the state. Another approach would aim to criminalize the publication of information related to terrorist organizations. A number of countries already criminalize the publication of illegal content such as hate speech[ix] or propaganda.[x] The challenge in implementing this approach is to harmonise national legal standards, some of which strongly protect the freedom on speech, whilst avoiding a ban on legitimate reports about terrorist activities.

Contribution related to Legal Response:

-- please use this space to list any legislation either related to the prevention of criminalisation of such activities --

3.2 Internet-related Terrorism Financing

Tracing terrorists' financial transactions has become a key task in the fight against terrorism, particularly since the 9/11 attacks.[xi] There are several ways in which Internet services can be used for these transactions. Terrorist organisations can make use of electronic payment systems to enable online donations.[xii] They can use websites to publish information on how to donate, e.g., to direct supporters to the bank account, which should be used for the transaction. Several terrorist organisations have implemented systems for receiving online credit card donations, the IRA being one of the first to accept donations via credit card.[xiii] Other methods include operating fake web-businesses, online gambling, or sites using anonymous payment systems. Such businesses can be operated worldwide while making it difficult to prove that financial transactions are donations rather than regular purchases, which is further complicating investigations.[xiv]

Legal Response:

Over the past decade, a number of legal frameworks have been developed aimed at combating terrorism financing.[xv] These contain effective instruments with regard to financial institutions. They often do not, however, provide investigative authorities with the tools necessary to trace users of internet services and address the internet-related aspects of terrorism financing.

Legislation could address virtual currencies (including their use in their online games) and contain monitoring and detection obligations for commercial websites.

Contribution related to Legal Response:

-- please use this space to list any legislation either related to the prevention of criminalisation of such activities --

3.3 Computer- and Network-based Attacks

Critical infrastructure is widely recognised as a potential target for terrorist attacks as it is – by definition – vital for the stability of the state.[xvi] Infrastructure is considered to be critical if damage or destruction of this infrastructure would have a debilitating impact on the national or economic security of a state.[xvii] This concerns, in particular, electrical power systems, telecommunication systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems and emergency services. The vulnerability of critical infrastructure to network-based attacks is apparent from several incidents from the air transport industry: In 2004, the Sasser computer worm[xviii] infected millions of computers around the world, among them, computer systems of major airlines, which led to cancellations of flights.[xix] Airlines, such as Lufthansa, have also been affected by DoS attacks on their websites.[xx]

Legal Response:

Most countries already criminalize network-based attacks against computer systems. But other challenges remain: how to minimize the damage potentially caused by such attacks and how to cope with the difficulties in international investigations.

Contribution related to Legal Response:

-- please use this space to list any legislation either related to the prevention of criminalisation of such activities --

3.4 Collection of Information through Computer and Network-Technology

A large volume of information about terrorist methods and possible targets is available in the Internet. Websites on how to build bombs – even virtual training camps – provide instructions on the use of weapons in an e-learning approach.[xxi] In addition, sensitive or confidential information that is not adequately protected from search robots can be found via search engines.[xxii] There are signs that terrorists are exploiting this information. A similar incident was reported in Australia, detailed information about potential targets for terrorist attacks having been made available on government websites.[xxiii] In 2005, the press in Germany reported that investigators had found downloaded manuals on how to build explosives, on the computer of two suspects who then attempted to attack the German public transportation system with homemade bombs.[xxiv]

Legal Response:

The discussion about a response to the phenomenon currently focuses greatly on criminalisation of the publication of instructions on how to commit terrorist attacks. One example is the 2008 Amendment of the EU Framework Decision on combating terrorism.[xxv] In the introduction, the EU makes much of the fact that the existing legal framework criminalises aiding, abetting and inciting terrorism but does not criminalise the dissemination of terrorist expertise through the Internet.[xxvi] With the amendment, the EU purports to take measures to close the gap and bring the legislation closer to the Council of Europe Convention on the Prevention of Terrorism throughout the EU. Based on Article 3(1)(c)[xxvii] of the Framework, the member states are obliged, e.g., to criminalise the publication of instructions on how to use explosives, if the publisher knows that this information is intended to be used for terrorist-related purposes.

Contribution related to Legal Response:

-- please use this space to list any legislation either related to the prevention of criminalisation of such activities --

3.5 Communication through Internet-related Services

The use of information technology by terrorist organisations is not limited to running websites and conducting research in databases. In the context of the investigations after the 9/11 attacks, it was reported that the terrorists used e-mail communication in co-ordinating their attacks.[xxviii] The press reported that detailed instructions about the targets and the number of attackers had been exchanged via e-mail.[xxix]

Legal Response:

Since terrorists are increasingly able to exchange encrypted messages, intercepting terrorist communications has become much more complex.[xxx] While it is technically possible to intercept e-mail communication[xxxi], terrorists have started to use technical safeguards, such as encryption technology, to restrict access to the content of e-mail communications.[xxxii] The legal response to challenges such as the use of encryption technology is currently the subject of intense debate.[xxxiii] Solutions under consideration include restrictions on the power of encryption software,[xxxiv] the establishment of a key-escrow system[xxxv], and the creation of production orders.[xxxvi] As encryption technology is widely recognized as an essential component to maintaining cybersecurity, legal approaches addressing this issue are challenging.

Contribution related to Legal Response:

Cybercri
Research Institute

-- please use this space to list any legislation either related to the prevention of criminalisation of such activities --

Thank you very much for your input!

Marco Gercke on behalf of the CTITF Working Group on "Countering the Use of the Internet for Terrorist Purposes"

---

i *Weimann* in USIP Report, How Terrorists Use the Internet, 2004, page 3. Regarding the use of the Internet for propaganda purposes see as well: *Crilley*, 'Information Warfare: New Battlefields – Terrorists, Propaganda and the Internet', Aslib Proceedings, Vol. 53, No. 7 (2001), page 253.

ii Regarding the use of YouTube by terrorist organisations, see Heise Online News, 11 October 2006, available at http://www.heise.de/newsticker/meldung/79311; *Staud* in Sueddeutsche Zeitung, 05.10.2006.

iii *Zanini/Edwards*, 'The Networking of Terror in the Information Age' in Networks and Netwars: The Future of Terror, Crime, and Militancy, 2001, page 42.

iv US Homeland Security Advisory Council, Report of the Future of Terrorism, 2007, page 4.

v Regarding the justification see *Brandon*, 'Virtual Caliphate: Islamic Extremists and the Internet', 2008, available at http://www.socialcohesion.co.uk/pdf/VirtualCaliphateExecutiveSummary.pdf.

vi *Brachman*, 'High-Tech Terror: Al-Qaeda's Use of New Technology', The Fletcher Forum of World Affairs, Vol. 30:2, 2006, page 149 et seqq.

vii See *Conway*, 'Terrorist Use of the Internet and Fighting Back', Information and Security, 2006, page 16.

viii Regarding the consequence of ID-Theft for investigations see *Gercke*, 'Internet-Related Identity Theft', 2007, available at http://www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

ix See in this context for example the Additional Protocol to the Council of Europe Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at www.conventions.coe.int.

x An example is Sec. 86 German Penal Code:
'Section 86 Dissemination of Means of Propaganda of Unconstitutional Organizations (1) Whoever domestically disseminates or produces, stocks, imports or exports or makes publicly accessible through data storage media for dissemination domestically or abroad, means of propaganda:
1. of a party which has been declared to be unconstitutional by the Federal Constitutional Court or a party or organization, as to which it has been determined, no longer subject to appeal, that it is a substitute organization of such a party;
2. of an organization, which has been banned, no longer subject to appeal, because it is directed against the constitutional order or against the idea of international understanding, or as to which it has been determined, no longer subject to appeal, that it is a substitute organization of such a banned organization;
3. of a government, organization or institution outside of the territorial area of application of this law which is active in pursuing the objectives of one of the parties or organizations indicated in numbers 1 and 2; or 4. means of propaganda, the contents of which are intended to further the aims of a former National Socialist organization, shall be punished with imprisonment for not more than three years or a fine.'

xi The Commission analyzing the 9/11 attacks calculated that the costs for the attack could have been between USD 400,000 and 500,000. See 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, page 187. Taking into account the duration of the preparation and the number of people involved the cost per person have been relatively small. Regarding the related challenges see as well *Weiss*, CRS Report for Congress, 'Terrorist Financing: The 9/11 Commission Recommendation', page 4.

xii See in this context *Crilley*, 'Information Warfare: New Battlefields – Terrorists, Propaganda and the Internet', Aslib Proceedings, Vol. 53, No. 7 (2001), page 253.

xiii See *Conway*, Terrorist Use the Internet and Fighting Back, Information and Security, 2006, page 4.

xiv Regarding virtual currencies see *Woda*, Money Laundering Techniques with Electronic Payment Systems in Information and Security 2006, page 39.

xv For an overview see *Strauss*, 'Combating Terrorist Financing – Are Transition Countries the Weak Link?', 2009

xvi *Brunst* in *Sieber/Brunst*, 'Cyberterrorism – The Use of the Internet for Terrorist Purposes', Council of Europe Publication, 2007.

xvii US Executive Order 13010—Critical Infrastructure Protection. Federal Register, July 17, 1996. Vol. 61, No. 138.

xviii Sasser B Worm, Symantec Quick Reference Guide, 2004, available at http://eval.symantec.com/mktginfo/enterprise/other_resources/sasser_quick_reference_guide_05-2004.en-us.pdf.

xix *Schperberg*, 'Cybercrime: Incident Response and Digital Forensics', 2005 and 'The Sasser Event: History and Implications', Trend Micro, June 2004, available at http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/wp02sasserevent040812us.pdf.

xx *Gercke*, 'The Decision of the District Court of Frankfurt in the Lufthansa Denial of Service Case', Multimedia und Recht, 2005, page 868 et seq.

xxi For further reference see *Gercke*, 'The Challenge of Fighting Cybercrime', Multimedia und Recht, 2008, page 292.

xxii For more information regarding the search for secret information with the help of search engines, see *Long, Skoudis and van Eijkelenborg*, Google Hacking for Penetration Testers.

xxiii *Conway*, 'Terrorist Use the Internet and Fighting Back, Information and Security', Information & Security, 2006, page 18.

xxiv See Sueddeutsche Zeitung Online, 'BKA findet Anleitung zum Sprengsatzbau', 07.03.2007, available at http://www.sueddeutsche.de/deutschland/artikel/766/104662/print.html.

xxv EU Framework Decision on Combating Terrorism, COM (2007) 650.

xxvi Article 4 of the Framework Decision on combating terrorism states that inciting, aiding or abetting terrorist offences should be made punishable by the Member States. Article 2 of the same instrument requires Member States to hold those directing a terrorist group or participating in its activities criminally liable. However, these provisions do not explicitly cover the dissemination of terrorist propaganda and terrorist expertise, in particular through the Internet.

xxvii '[T]raining for terrorism' means to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of committing one of the acts listed in Article 1(1), knowing that the skills provided are intended to be used for this purpose.

xxviii The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, 2007, page 249.

xxix The text of the final message was reported to be: 'The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering.' The name of the faculties was apparently the code for different targets. For more detail see *Weimann*, 'How Modern Terrorism Uses the Internet', Journal of International Security Affairs, Spring 2005, No. 8; *Thomas*, 'Al Qaeda and the Internet: The Danger of "Cyberplanning"', 2003, available at http://findarticles.com/p/articles/mi_m0IBR/is_1_33/ai_99233031/pg_6; Zeller, On the Open Internet, a Web of Dark Alleys, The New York Times, 20.12.2004, available at http://www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position=;.

xxx See *Gercke*, 'The Challenge of Fighting Cybercrime', Multimedia und Recht, 2008, page 297.

xxxi *Branch*, 'Lawful Interception of the Internet', CAIA Technical Report 030606A, 2003, available at http://caia.swin.edu.au/reports/030606A/CAIA-TR-030606A.pdf.

xxxii Regarding the impact on computer forensic and criminal investigations, see *Huebner/Bem/Bem*, 'Computer Forensics – Past, Present And Future', No. 6, available at www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf.

xxxiii *Gercke*, 'The Challenge of Fighting Cybercrime', Multimedia und Recht, 2008, page 297.

xxxiv The limitation of the import of such powerful software is even characterised as 'misguided and harsh to the privacy rights of all citizens'. See for example: The Walsh Report – Review of Policy Relating to Encryption Technologies, Chapter 1.1.16, available at http://www.efa.org.au/Issues/Crypto/Walsh/walsh.htm.

xxxv *Lewis*, Encryption Again, available at http://www.csis.org/media/csis/pubs/011001_encryption_again.pdf.

xxxvi Such approach is for example contained in Sec. 49 of the UK Regulation on Investigatory Powers Act. For general information on the Act see *Brown Gladman*, 'The Regulation of Investigatory Powers Bill - Technically Inept: Ineffective against Criminals while Undermining the Privacy, Safety and Security of Honest Citizens and Businesses, available at http://www.fipr.org/rip/RIPcountermeasures.htm; Ward, Campaigners hit by decryption law, BBC News, 20.11.2007, available at http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/technology/7102180.stm.

United Nations Office on Drugs and Crime (UNODC)
"The Use of the Internet for terrorist purposes"
Dr. Hans-Georg Maaßen
Präsident des Bundesamtes für Verfassungsschutz
Eingangsstatement

Es gilt das gesprochene Wort!

(Anrede)

Ich habe heute die Ehre, Herrn Bundesinnenminister Dr. Friedrich zu vertreten, der aus terminlichen Gründen leider nicht hier sein kann.

Haben Sie bitte Verständnis dafür, dass ich zur Problematik, mit der wir uns heute beschäftigen nicht aus ministerieller, sondern aus einer spezifischeren Sicht, aus der Sicht der Nachrichtendienste vortrage.

(Virtuelle Lebenswelt und terroristische Aktivitäten)

Fundamentale technologische Neuerungen implizieren einer Vielzahl von Veränderungen. Das weiß jeder von uns aus seiner eigenen Lebenswelt. Die digitale Revolution wirkt sich auf extremistische und terroristische Bestrebungen aus: auf deren strukturelle und operative Herangehensweisen, auf Radikalisierungsprozesse und Mobilisierungsfähigkeit, manchmal sogar auf ihre ideologische Grundlagen, zumindest aber auf deren intellektuelle Dichte und Vermittlung

Die modernen Kommunikationstechnologien haben die Möglichkeiten von Extremisten und Terroristen enorm erweitert. Sie erreichen mit dem

Internet eine Breitenwirkung, wie sie auf herkömmlichen Wegen niemals gelingen könnte. Im Internet findet das statt, was Experten als „Cyber Mobilization" bezeichnen: der schnelle Aufbau netzwerkartiger Strukturen über geografische Grenzen hinweg, von Diskussionsforen über die kurzfristige Planung von Demonstrationen bis hin zur Bildung terroristischer Gruppen.

Soziale Netzwerke (wie etwa „Facebook") gewinnen dabei mehr und mehr an Bedeutung. Dort können ohne räumliche Grenzen Kontakte geknüpft und Interessengemeinschaften gebildet werden,. Neben dem Austausch von privaten Nachrichten über die Chatfunktion, ermöglichen sie den Aufbau von Kommunikationsplattformen, die nur für die Mitglieder offen sind.

Islamistische Terroristen bedienen sich ohne Vorbehalte moderner Technik. Es klingt paradox und doch ist es so: Rückwärtsgewandte Extremisten kämpfen mithilfe dieser Technologie gegen die politischen und sozialen Errungenschaften der Moderne. „Gotteskrieger", die einem archaischen Gesellschaftsbild anhängen, nutzen mit großer Selbstverständlichkeit die Möglichkeiten des Internets. Terror-Netzwerke sind auf moderne Kommunikationstechnologie angewiesen, wenn sie ihre Aktionsfähigkeit gewährleisten wollen.

Terroristische Zellen können Anschlagsplanungen besprechen, ohne dass sich die Terroristen je persönlich getroffen hätten. Diese virtuellen

Gruppentreffen finden ihre Ergänzung in virtuellen Trainingslagern, die der Vorbereitung auf den ganz realen Terrorismus dienen, mit Online-Handbüchern und Online-Videotheken oder auch mit Kampfsimulationen.

Das Internet dient Terroristen ebenso zur Koordinierung wie zur Rekrutierung.

Mit der virtuellen Vernetzung entsteht ein Gefühl der Zusammengehörigkeit und der Intensität des politischen Kampfes. Das trifft in besonderem Maße auf Anhänger des globalen „Jihad" zu, die in Wirklichkeit oftmals aus ganz unterschiedlichen Lebenswelten kommen.

Wir haben in den letzten Jahren mehrere „jihadistische" Internet-Propagandaoffensiven erlebt, zuletzt zu dem Mohammed-Schmähfilm. Dies reicht bis hin zu Mordaufrufen. „al-Qaida" verfügt mit dem „al-Fajr-Medienzentrum" sogar über eine zentrale Stelle zur Veröffentlichung von Videos und Verlautbarungen.

(Radikalisierungsprozess)

Radikalisierung findet heute nicht mehr nur (vielleicht kann man sogar sagen: nicht mehr überwiegend) in Organisationen und Gruppen statt, sondern im Internet als virtuelle Selbstvergewisserung und schließlich auch Selbstradikalisierung.

Arid UKA, der 2011 den ersten vollendeten islamistischen Anschlag in Deutschland ausführte und zwei US-amerikanische Soldaten tötete, ist ein solcher Fall. Die Auswertung seines „Facebook"-Profils machte seine Nähe zu islamistischen Missionierungsnetzwerken deutlich.

Wir stellen immer kürzere Radikalisierungsphasen fest. Radikalisierungsprozesse, die ohne erkennbaren Vorlauf stattfinden und selbst von der engeren Umgebung unbemerkt bleiben, erschweren es den Sicherheitsbehörden, die potenziellen Täter zu identifizieren.

(„individueller Jihad"/"elektronischer Jihad")

Die Digitalisierung bildet die materielle Grundlage für den „individuellen Jihad". Er gewinnt immer mehr an Bedeutung.
Jihadistische Organisationen, wie z.B. „al-Qaida", rufen ihre Anhänger auf, Anschläge auf eigene Faust und ohne organisatorische Anbindung durchzuführen.

Mit dem „individuellen Jihad" eng verwoben, ist der „elektronische Jihad".

Eine hochtechnisierte Gesellschaft wie unsere ist in hohem Maße störungsanfällig. Die aktuellen Stichworte hierfür sind Cyber-Krieg und Cyber-Terrorismus.

Wir wissen von einem Aufruf zur Gründung eines „Instituts für den elektronischen Jihad". Dort werden ausdrücklich Angriffe auf SCADA-

Systeme erwähnt („Supervisory Control and Data Acquisition"), auf Systeme zur Steuerung der Stromversorgung, von Wasser- und Gasnetzen aber auch der Systeme von Flughäfen, Bahnnetzen, Börsen und großen Banken.

Vor ziemlich genau einem Monat, am 18. September, wurden die Internetseiten amerikanischer Banken angegriffen. Verantwortlich zeichnete die „Cyber Fighters Izz ad-din al qassam", die ihre Aktion mit dem islamfeindlichen Mohammed-Film begründeten.

Dies hat zwar bei weitem nicht die Dimension von SCADA-Angriffen, zeugt aber gleichwohl von dem Willen, sich entsprechendes Wissen anzueignen und zum Einsatz zu bringen. Innerhalb der islamistischen Online-Community ist jedenfalls eine verstärkte Debatte über Angriffe über das Internet zu beobachten.

(Gegenmaßnahmen und Schluss)

Der transnationalen terroristischen Gefahr kann nur mit einer verstärkten nationalen und internationalen Kooperation wirksam entgegengetreten werden. Daran besteht kein Zweifel.

Auf internationaler Ebene findet ein wichtiger Erfahrungsaustausch statt, auch über die Methodik der Internetbearbeitung.

National müssen die Kompetenzen der Sicherheitsbehörden gebündelt werden. Deshalb haben wir einige Zentren aufgebaut, in denen die

Sicherheitsbehörden (Polizeien und Nachrichtendienste) zusammenarbeiten - jeweils selbstständig auf der Grundlage ihres eigenen gesetzlichen Auftrages, so das „Gemeinsame Internetzentrum“ (GIZ) im Bereich des islamistischen Terrorismus und in die Kooperationsplattform „Koordinierte Internetauswertung Rechtsextremismus“ (KIAR). Gegenwärtig prüfen wir, in welcher Weise Zentren auch für andere Phänomenbereiche aufgebaut werden können.

Die Bedrohung geht nicht allein vom islamistischen Terrorismus aus. Wenngleich Islamisten, Rechts- und Linksextremisten sich als Antipoden verstehen, übernehmen sie doch Strategien und Vorgehensweisen aus dem jeweils anderen Bereich. Anders Breivik, der 2011 in Norwegen mit zwei Anschlägen 77 Personen tötete, gab beispielsweise im Prozess an, von „al-Qaida“ gelernt zu haben.

Sicherheitsbehörden und Gesetzgeber sind gehalten, Entwicklungen in der Kommunikationstechnologie sorgfältig zu beobachten und – soweit dies möglich ist – auch zu antizipieren. Die Möglichkeiten der Sicherheitsbehörden müssen mit dieser Entwicklung Schritt halten.

Wir sehen einen steigenden Bedarf, durch eine offensive Nutzung des Internets an nachrichtendienstliche relevante Informationen zu gelangen. Dies ist eine notwendige Konsequenz aus der technologischen Entwicklung einerseits und den spezifischen Vorgehensweisen der Extremisten und Terroristen andererseits, nicht zuletzt auch vor dem

Hintergrund einer zunehmenden Professionalisierung und einer zunehmenden Nutzung von Verschlüsselungs- und Anonymisierungstechniken.

Auch unterhalb der Schwelle einer Online-Durchsuchung – sie ist dem Inlands-Nachrichtendienst in Deutschland nicht erlaubt – gibt es Aufklärungsmaßnahmen im Internet. Sie sind zwar weniger eingriffsintensiv, mit ihnen ist aber gleichwohl ein Zugang zu wichtigen Planungen und Verbindungsstrukturen möglich. Nur aus offen zugänglichen Quellen zu schöpfen, wird einer Gefahrenlage nicht gerecht, in der ein zu allem bereiter Gegner mit Konspiration und äußerster Brutalität vorgeht. Erst mit dem Einsatz nachrichtendienstlicher Mittel können rechtzeitig Informationen beschafft werden, die Terrorakte verhindern und Menschenleben retten.

Vielen Dank für Ihre Aufmerksamkeit

Draft Agenda

Launch of the UNODC's publication
on
"The use of the Internet for terrorist purposes"

22 October 2012

Federal Ministry of the Interior

9:30 *(Großer Vortragssaal, Federal Ministry of Interior)*	***Opening of the launching of the UNODC publication on "The use of the Internet for terrorist purposes"*** Ms. Johanna MIKL-LEITNER, Federal Minister of the Interior, Austria Mr. Yuri FEDOTOV, Executive Director of UNODC Mr. Sándor PINTÉR, Minister of Interior, Hungary Mr. James BROKENSHIRE, Security Minister, Home Office, UK Mr. Hans-Georg MAAßEN, President of the The Federal Office for the Protection of the Constitution, Germany
10:15 *(Großer Vortragssaal)*	***Coffee break***
10:15 *(Festsaal, Federal Ministry of Interior)*	***Press conference*** *Moderation: Mr. Hermann Muhr* Ms. Johanna MIKL-LEITNER, Federal Minister of the Interior, Austria Mr. Yuri FEDOTOV, Executive Director of UNODC Mr. Sándor PINTÉR, Minister of Interior, Hungary Mr. James BROKENSHIRE, Security Minister, United Kingdom Mr. Hans-Georg MAAßEN, President of the The Federal Office for the Protection of the Constitution, Germany
10:45	***Presentation of the publication*** **on "The use of the Internet for terrorist purposes"** ***Chair*****:** Marta REQUENA, Chief, Terrorism Prevention Branch (TPB), UNODC - **Overview of the publication on "The use of the Internet for terrorist purposes"**

	The United Nations action to counter the misuse of the internet for terrorist purposes, Richard BARRET, Chair, Working Group of the Counter-Terrorism Implementation Task Force (CTITF) on countering the use of the Internet for terrorist purposes **The UNODC action to counter the misuse of the internet for terrorist purposes**, Mauro MIEDICO, Chief of Section, TPB, UNODC
11:30	***National experiences on the use of the Internet for terrorist purposes*** Mr. Peter GRIDLING, Director, Austrian Federal Agency for State Protection and Counter Terrorism Ms., Moira MACMILLAN, Representative of the Crown Prosecution Service, United Kingdom Mr. Ehab Maher ELSONBATY, Senior Judge, Egypt Mr. Bin HU, Representative of the Permanent Mission of China to the UN in Vienna
12:30	***Discussion and Conclusion***
13:00	***Lunch***