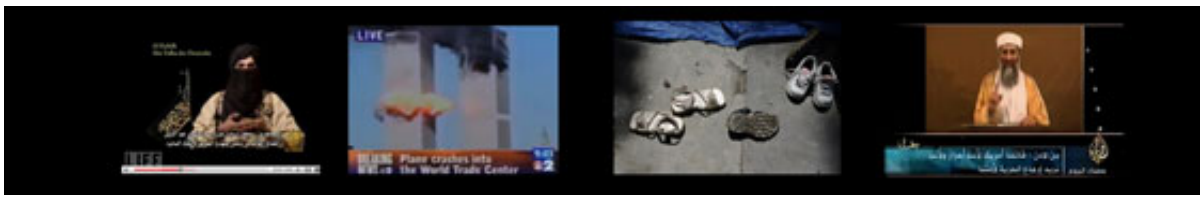
TERRORIST USE OF THE INTERNET AND LEGAL RESPONSE

Without doubt terrorist organisations today are using the Internet for various purposes. Unlike the early debate when the focus was on potential terrorist-related network-based attacks against critical infrastructure and the use of information technology in armed conflicts (cyberwarfare), it is widely recognised that the range of activities is more complex.(1)

Terrorist use of the Internet includes research, training, propaganda and communication.(2) But despite more intensive research many aspects are still uncertain as reports about concrete incidents often remain classified. The following article provides an overview of the different areas of terrorist use of the Internet and the concept of legal response.



I. Terrorist Use of the Internet

1. Propaganda

While ten years ago only 12 of the 30 foreign terrorist organisations listed by the U.S. State Department maintained websites,(3) in 2004 the United States Institute of Peace reported that almost all terrorist organisations have websites.(4) The Internet-related propaganda activities include the distribution of video messages(5) and the descriptions and justifications of activities.(6) The Internet has substituted traditional channels of distribution, particularly with regard to video messages.(7)

2. Collection of information

The Internet has proven to be highly useful for collecting information. Millions of websites provide information that can be used for legitimate as well as illegal purposes. One example are satellite pictures. High-resolution satellite pictures, previously available only to a handful of military institutions, are today made available by various Internet services.(8) Other examples include instructions on how to build bombs, and even virtual training camps, providing information on the use of weapons in an e-learning approach.(9) Such instructions are available on a large-scale online.(10)
In 2008, Western secret services discovered an Internet server that allowed for the exchange of training material and communications.(11) Several websites were reported to be operated by terrorist organisations to coordinate activities.(12) In addition, sensitive or confidential information that is not adequately protected from search robots can be found via search engines.(13) Terrorist organizations have started to explore this technology. In 2003, the U.S. Department of Defense was informed about a training manual linked to al-Qaida providing information on how to use public sources to find details about potential targets.(14) In 2005, the German press 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.(15)

3. Communication

In the investigations following 9/11, it was reported that the terrorists used e-mail communication to coordinate their attacks.(16) The press reported that detailed instructions about the targets and the number

of attackers had been exchanged via e-mail.(17) The threats related to a technology shift are also accentuated by the fact that the interception of Voice-over-IP calls is going along with significantly more challenge than the interception of regular phone calls.(18)

4. Use of information technology to prepare for “real world” attacks(19)

It has been reported that terrorists are using online videogames as part of their preparation for attacks. Various online games simulate the “real world” by allowing the user to manipulate characters (avatars) in a virtual world. Theoretically, those online games could be used to simulate attacks, though it is not yet certain to what extent they have been used to do so.(20)

5. Attacks against critical infrastructure

Over the past decades, more and more countries have turned into information societies.(21) Services such as online banking and telephone communications using Voice-over-Internet-Protocol (VoIP) are very popular.(22) But it is not only the communication sector that has shifted its services online: information technology and Internet services are today used to control and manage many functions in buildings, transportation systems, waterways and energy grids.(23)
Critical infrastructure is widely recognised as a potential target for terrorist attacks, as it is, by definition, vital for the stability of the State.(24) Infrastructure is considered to be frail, and its incapacity or destruction could have a debilitating impact on a State’s defence or economic security.(25) 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 civil disturbance caused by Hurricane Katrina highlights the dependence of developed societies on those services.(26)
Both the new means of communication and the use of information technology to control critical infrastructure have influenced terrorist organisations’ ability to use the Internet for attacks against critical infrastructure and to make it more vulnerable to attacks.(27) Interconnected systems that are linked by computer and communication networks are especially attractive targets.(28) A network-based attack would do more than cause a single system to fail. Rather, it would bring down an entire network of systems and their related infrastructure. Even short interruptions of services would cause huge financial damage to e-commerce businesses, government service providers and the security sector.(29)

II. Legal Response

The recognition of the threat associated with terrorist use of the Internet and the related challenges has led to various legal approaches to address the issue. The ones on a national level in particular show significant differences. With regard to systematic aspects, there are three different approaches of how countries are addressing the specific challenges of terrorist use of the Internet:

1. Applying existing cybercrime legislation, developed to cover non-terrorist related acts, to terrorist use of the Internet;
2. Applying existing legislation, developed to cover non-Internet related terrorist acts, to Internet-related acts as well;
3. Enacting specific legislation on terrorist use of the Internet.

1. Application of Cybercrime legislation

Some countries are using existing cybercrime legislation that was developed to cover non-terrorist related acts to criminalize terrorist use of the Internet. One example for such provision is Art. 2 of the Council of Europe Convention on Cybercrime,(30) which was developed to cover traditional cybercrime, but not specifically designed to address terrorist related acts:

Article 2 –Illegal access
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a

computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Based on the experiences with this approach, three aspects ought to be taken into consideration. Substantive criminal law provisions that were implemented to cover non-terrorist related acts (such as illegal access(31) or system interference(32)) might be applicable in terrorist-related cases, but very often the range for sentencing will differ from specific terrorism legislation. Depending on the dogmatic structure of procedural law this could influence the ability to use sophisticated investigation instruments that are restricted to terrorist or organised crime related investigation.
Secondly, and with regard to procedural instruments, the situation is slightly different. The application of cybercrime specific investigation instruments in cases of terrorist use of the Internet (such as the expedited preservation of computer data(33)) is going along with less challenges, since most countries do not limit the application to traditional cybercrime offences but to any offence involving computer data.(34)
Finally, regional instruments developed to address the challenge of cybercrime, but not specifically terrorist use of the Internet, often contain exemptions for international cooperation with regard to political offences. One example is Art. 27, paragraph 4.a of the Council of Europe Convention on Cybercrime.(35)

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements
[...] 3. Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.
4. The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:
a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
b) it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests. [...]

The provision authorizes parties to the Convention to refuse mutual assistance if it concerns an offence which the requested Party considers a political offence, or connected with a political offence.(36) As this is often the case when it comes to terrorist use of the Internet, such approach can hinder the investigation. To improve the situation the terrorist-specific legal frameworks, such as the 2005 Council of Europe Convention on the Prevention of Terrorism(37) contains an exclusion of the political exception clause in Art. 20.(38) With regard to the Convention on Cybercrime, the issue is only solved with regard to those countries that have signed and ratified both Conventions.

2. Application of existing (non Internet specific) terrorism legislation

Another approach is to use existing terrorism legislation to criminalise and prosecute terrorist use of the Internet. On example for a traditional instrument is the aforementioned Council of Europe Convention on the Prevention of Terrorism.(39)

Article 5 – Public provocation to commit a terrorist offence
1 For the purposes of this Convention, public provocation to commit a terrorist offence means the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed.
2 Each Party shall adopt such measures as may be necessary to establish public provocation to commit a terrorist offence, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

The Convention defines several offences, such as the above-mentioned public provocation to commit a terrorist offence: however, it does not contain provisions criminalising terrorist-related attacks against computer systems or specific data-related procedural instruments. However, especially with regard to

investigating Internet-related offences, specific procedural instruments are required as the investigation process differs significantly from traditional ones, and traditional instruments would therefore often fail.

3. Development of specific legislation dealing with terrorist use of the Internet

The third approach is the development of specific legislation addressing terrorist use of the Internet. One example is Section 4.f of the Draft ITU Cybercrime Legislation Toolkit.

Section 4. Interference and Disruption
[...] (f) Intent to Cause Interference or Disruption for Purposes of Terrorism.
Whoever commits interference and/or disruption pursuant to paragraphs (a) and (b) of this Section with the intent of developing, formulating, planning, facilitating, assisting, informing, conspiring, or committing acts of terrorism, not limited to acts of cyberterrorism, shall have committed a criminal offense punishable by a fine of [amount] and imprisonment for a period of [duration].

The International Telecommunication Union (ITU) is the UN organisation that has most responsibility for practical aspects of cybersecurity.(40) The aim(41) of the Draft Toolkit is to give countries the possibility of using sample language and reference material in the process of national cybercrime legislation development, that can assist, according to the Toolkit's developers, the "establishment of harmonized cybercrime laws and procedural rules."(42) The Toolkit was developed by the American Bar Association on the basis of a comprehensive analysis of the Council of Europe (CoE) Convention on Cybercrime and the cybercrime legislation developed by countries. It aims to be a fundamental resource for legislators, policy experts, and industry representatives, providing them with the framework to develop consistent cybercrime legislation. Moreover, in addition to traditional approaches, the Toolkit also contains several specific terrorist-related offences.(43)

* Dr. Marco Gercke is the Director of the Cybercrime Research Institute.
Mr. Daniel Thelesklaf is the Executive Director of the Basel Institute on Governance.

---

1 Gercke, 'Cyberterrorism, How Terrorists Use the Internet', Computer und Recht, 2007, page 62 et seq.
2 For an overview see Sieber/Brunst, Cyberterrorism – The Use of the Internet for Terrorist Purposes, Council of Europe Publication, 2007; Gercke, 'Cyberterrorism, How Terrorists Use the Internet', Computer und Recht, 2007, page 62 et seq.
3 ADL, Terrorism Update 1998, available at http://www.adl.org/terror/focus/ 16_focus_a.asp
4 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.
5 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
6 Regarding the justification see Brandon, 'Virtual Caliphate: Islamic Extremists and the Internet', 2008, available at http://www.socialcohesion.co.uk/pdf/VirtualCaliphateExecutiveSummary.pdf
7 So Weimann in USIP Report, How Terrorists Use the Internet, 2004, page 5.
8 Levine, 'Global Security', 27.06.2006, available at http://www.globalsecurity.org/org/news/2006/060627-google-earth.htm; regarding the discovery of a secret submarine on a satellite picture provided by a free of charge Internet Service see Der Standard Online, 'Google Earth: Neues chinesisches Kampf-Uboot entdeckt', 11.07.2007, available at http://www.derstandard.at/?url/?id=2952935
9 For further reference see Gercke, 'The Challenge of Fighting Cybercrime', Multimedia und Recht, 2008, page 292.
10 Brunst in Sieber/Brunst, 'Cyberterrorism – the use of the Internet for terrorist purposes', Council of Europe Publication, 2007; US Homeland Security Advisory Council, Report of the Future of Terrorism Task

Force, January 2008, page 5; Stenersen, 'The Internet: A Virtual Training Camp?', Terrorism and Political Violence, 2008, page 215 et seq.
11 Musharbash, 'Bin Ladens Intranet', Der Spiegel, Vol. 39, 2008, page 127.
12 Weimann, 'How Modern Terrorism Uses the Internet', 116 Special Report of the US Institute of Peace, 2004, page 10.
13 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.
14 'Using public sources openly and without resorting to illegal means, it is possible to gather at least eighty per cent of information about the enemy.' For further information, see Conway, 'Terrorist Use of the Internet and Fighting Back', Information & Security, 2006, page 17.
15 See Sueddeutsche Zeitung Online, 'BKA findet Anleitung zum Sprengsatzbau', 07.03.2007, available at http://www.sueddeutsche.de/deutschland/artikel/766/104662/print.html
16 The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, 2007, page 249.
17 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=;
18 Regarding the interception of VoIP to assist law enforcement agencies, see Bellovin and others, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP", available at http://www.itaa.org/news/docs/CALEAVOIPreport.pdf; Simon/Slay, "Voice over IP: Forensic Computing Implications", 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf
19 See US Commission on Security and Cooperation in Europe Briefing, 15.05.2008, available at http://csce.gov/index.cfm?FuseAction=ContentRecords. ViewTranscript&ContentRecord_id=426&ContentType=H,B&ContentRecordType=B&CFID=18849146&CFTOKEN=53; O'Brian, Virtual Terrorists, The Australian, 31.07.2007, available at http://www.theaustralian.news.com.au/story/0,25197,22161037-28737,00.html
20 Regarding other terrorist-related activities in online games see Chen/Thoms, 'Cyber Extremism in Web 2.0 – An Exploratory Study of International Jihadist Groups', Intelligence and Security Informatics, 2008, page 98 et seq.
21 For more information on the information society see Masuda, The Information Society as Post-Industrial Society; Dutta/De Meyer/Jain/Richter, The Information Society in an Enlarged Europe; Maldoom/Marsden/Sidak/Singer, Broadband in Europe: How Brussels can wire the Information Society; Salzburg Center for International Legal Studies, Legal Issues in the Global Information Society; Hornby/Clarke, Challenge and Change in the Information Society.
22 Regarding the new opportunities see for example: Communication From The Commission To The Council, The European Parliament, The European Economic And Social Committee And The Committee Of The Regions, Challenges for the European Information Society beyond 2005, page 3, available at http://ec.europa.eu/information_society/eeurope/i2010/docs/communications/new_chall_en_adopted.pdf. Regarding the extend of integration of ICTs into the daily lives and the related threats see Goodman, 'The Civil Aviation Analogy – International Cooperation to Protect Civil Aviation Against Cyber Crime and Terrorism' in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 69, available at http://media.hoover.org/documents/0817999825_69.pdf
23 Bohn/Coroama/Langheinrich/Mattern/Rohs, 'Living in a World of Smart Everyday Objects – Social, Economic & Ethical Implications', Journal of Human and Ecological Risk Assessment, Vol. 10, page 763 et seq., available at http://www.vs.inf.ethz.ch/res/papers/hera.pdf
24 Brunst in Sieber/Brunst, 'Cyberterrorism – The Use of the Internet for Terrorist Purposes', Council of Europe Publication, 2007.
25 US Executive Order 13010—Critical Infrastructure Protection. Federal Register, July 17, 1996. Vol. 61, No. 138.
26 Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve, GAO

communication, July 2007, available at http://www.gao.gov/new.items/d07706r.pdf
27 Sofaer/Goodman, 'Cybercrime and Security – The Transnational Dimension' in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, available at http://media.hoover.org/documents/0817999825_1.pdf
28 Lewis, 'Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats', Center for Strategic and International Studies, December 2002.
29 Shimeall/Williams/Dunlevy, Countering Cyber War, NATO Review, winter 2001/2002, available at http://www.cert.org/archive/pdf/counter_cyberwar.pdf
30 Council of Europe Convention on Cybercrime (CETS No. 185). For more details see: Sofaer, Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, Gercke, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 et seq.; Gercke, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et. seq; Aldesco, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1; Jones, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005; Broadhurst, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 et seq.
31 See for example Art. 2 Convention on Cybercrime.
32 See for example Art. 5 Convention on Cybercrime.
33 Art. 16 Convention on Cybercrime.
34 See in this context for example Art. 14 Convention on Cybercrime:
Article 14 –Scope of procedural provisions
1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.
2. Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
a. the criminal offences established in accordance with Articles 2 through 11 of this Convention;
b. other criminal offences committed by means of a computer system; and
c. the collection of evidence in electronic form of a criminal offence. [...]
35 Convention on Cybercrime, ETS 185.
36 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:
a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b. it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.
37 Council of Europe Convention on the Prevention of Terrorism, ETS 196.
38 Article 20 – Exclusion of the political exception clause
1 None of the offences referred to in Articles 5 to 7 and 9 of this Convention, shall be regarded, for the purposes of extradition or mutual legal assistance, as a political offence, an offence connected with a political offence, or as an offence inspired by political motives. Accordingly, a request for extradition or for mutual legal assistance based on such an offence may not be refused on the sole ground that it concerns a political offence or an offence connected with a political offence or an offence inspired by political motives. [...]
39 Council of Europe Convention on the Prevention of Terrorism, ETS 196.
40 Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks, European Union, Policy Department External Policies, 2009, page 17.
41 For more information see Gercke/Tropina, From Telecommunicaiton Standardisation to Cybercrime Harmonisation? ITU Toolkit for Cybercrime Legislation, Computer Law Review International, Issue 5, 2009, page 136 et seq.
42 ITU Toolkit for Cybercrime Legislation. Draft April, 2009, page 8. Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf
43 Sec. 2 d) (Unauthorized Access for Purposes of Terrorism), Sec. 3 f) (Unauthorized Access to or Acquisition of Computer Programs or Data for Purposes of Terrorism), Sec. 4 f) (Intent to Cause Interference or Disruption for Purposes of Terrorism), Sec. 6 h) (Intent to Furtherance of Terrorism).