COUNTER-TERRORISM IMPLEMENTATION TASK FORCE CTITF

CTITF Working Group Compendium

COUNTERING THE USE OF THE INTERNET FOR TERRORIST PURPOSES— LEGAL AND TECHNICAL ASPECTS

CTITF PUBLICATION SERIES

MAY 2011

United Nations
Counter-Terrorism Implementation Task Force

Working Group Compendium

Countering the Use of the Internet for Terrorist Purposes — Legal and Technical Aspects

May 2011

This is a shortened version of the report which can be found in full at:
www.un.org/terrorism/internet

United Nations
New York, 2011

About the United Nations Counter-Terrorism Implementation Task Force

The United Nations Counter-Terrorism Implementation Task Force (CTITF) was established by the Secretary-General in 2005 to ensure overall coordination and coherence in the counter-terrorism efforts of the United Nations system. CTITF is chaired by a senior United Nations official appointed by the Secretary-General and consists of 30 United Nations system entities and INTERPOL.

The United Nations Global Counter-Terrorism Strategy, which brings together into one coherent framework decades of United Nations counter-terrorism policy and legal responses emanating from the General Assembly, the Security Council and relevant United Nations specialized agencies, has been the focus of the work of CTITF since its adoption by the General Assembly in September 2006 (General Assembly resolution 60/288).

The Strategy sets out a plan of action for the international community based on four pillars:

- Measures to address the conditions conducive to the spread of terrorism;
- Measures to prevent and combat terrorism;
- Measures to build States' capacity to prevent and combat terrorism and to strengthen the role of the United Nations system in this regard;
- Measures to ensure respect for human rights for all and the rule of law as the fundamental basis of the fight against terrorism.

In accordance with the Strategy, which welcomes the institutionalization of CTITF within the United Nations Secretariat, the Secretary-General in 2009 established a CTITF Office within the Department of Political Affairs to provide support for the work of CTITF. Via the CTITF Office, with the help of a number of thematic initiatives and working groups, and under the policy guidance of Member States through the General Assembly, CTITF aims to coordinate United Nations system-wide support for the implementation of the Strategy and catalyse systemwide, value-added initiatives to support Member State efforts to implement the Strategy in all its aspects. CTITF also seek to foster constructive engagement between the United Nations system, international and regional organizations, the private sector, and civil society on the implementation of the Strategy.

United Nations
Department of Political Affairs
Counter-Terrorism Implementation Task Office
One United Nations Plaza
New York, NY 10017

Website: www.un.org/terrorism/cttaskforce

Contents

	Page
Background	v
Executive summary	ix
Chapter I. Legal Aspects	1
Overview	1
Challenges	2
Overview of legal responses to terrorist use of the Internet	3
A. Internet-related attacks (cyberattacks)	3
B. Illegal content	4
C. Communication	5
D. Terrorist financing	5
Strategic approaches	6
A. States apply existing cybercrime legislation, developed to cover non-terrorist-related acts, to terrorist use of the Internet	6
B. Application of existing (non Internet specific) terrorism legislation	7
C. Development of specific legislation dealing with terrorist use of the Internet	7
Protection of fundamental rights	8
Conclusion and recommendations	8
Endnotes	10
Chapter II. Technical Aspects	17
Overview	17
Cybercrime and Terrorist Use of the Internet: Understanding the Nexus	18
The Technologies	19
A. The Internet as an Open Source Information Tool	19
B. Identity & Attribution	21

Page

C. Data Encryption/Obfuscation 24
D. The Internet as a Tool for Propaganda & Radicalization 27
E. Social Networking 31
F. Fundraising & Alternative Payment Systems 33
G. Tactical Communications 35
H. Unlawful Access to a Computer System/"Hacking" 36
I. Botnets/Computer Network Attacks 38
J. Emerging and Future Technologies 41
Conclusions and Recommendations 44
Endnotes 45

Report Contributors 51

Background

1. In the Global Counter-Terrorism Strategy, adopted by the General Assembly in September 2006, Member States pledge to "coordinate efforts at the international and regional level to counter terrorism in all its forms and manifestations on the Internet". The Strategy also highlights the need to do so "with due regard to confidentiality, respect for human rights and in compliance with other obligations under international law". United Nations Security Council Resolution 1624 (2005) calls upon states "to take measures that are necessary and appropriate, and in accordance with their obligations under international law, to prohibit by law incitement to commit terrorist acts and to prevent such conduct". And the report of the Secretary-General of the United Nations 'Uniting against terrorism: recommendations for a global counterterrorism strategy' of 27 April 2006, argues that Resolution 1624 provides a basis for criminalizing such acts committed through the Internet.

2. The Working Group on Countering the Use of the Internet for Terrorist Purposes, which is one of the eight Working Groups of the United Nations Counter-Terrorism Implementation Task Force (CTITF) that aim to enhance coordination and coherence of the United Nations counter-terrorism efforts, has sought to establish what instruments (laws and conventions), programmes, resources, as well as technical means are used to counter the use of the Internet for terrorist purposes and identify areas where future engagement may be necessary.

3. To assist Member States in identifying challenges and opportunities in countering the use of the Internet for terrorist purposes, the CTITF Working Group undertook a three-stage project from October 2009 to April 2011 researching and analyzing legal, technical, and counter-narrative aspects. To this end, the Working

Group—working with senior research advisors—facilitated debate within a multi-disciplinary expert group that included experts from governments, regional organizations, academia, civil society, and the private sector.

4. The recent project undertaken by CTITF Working Group served as a follow-up to the group's initial report released in February 2009, which broadly addressed issues related to terrorist use of the Internet for the purposes of fundraising, training, recruitment, secret communication, data mining, propaganda and radicalization, as well as cyber attacks. The earlier report concluded that terrorist use of the Internet should be addressed via a multi-disciplinary approach involving experts in counter-terrorism, technology, law, public policy, law enforcement and human rights.

5. To effectively take stock and assess the various legal approaches employed in countering the use of the Internet for terrorist purposes, the Working Group sent a questionnaire to experts from various countries and institutions. Those approaches were the subject of discussion during a conference hosted at the German Foreign Ministry (Auswärtiges Amt) in Berlin in January 2010. Chapter I of this publication aims to provide an overview of the challenges related to legal solutions and highlight different approaches developed at the international, regional and national level. The unabridged version of this report on legal aspects is available at www.un.org/terrorism/internet.

6. The Working Group recognizes that the use of the Internet for terrorist purposes can not be addressed nor resolved solely through legal solutions alone: any effective approach must include a solid understanding and appreciation of the technical aspects of ICT (information and communications technology). In order to ensure such a comprehensive approach, the Working Group held a second workshop of international experts in Redmond, Washington (USA) in February 2010 which was hosted by the Microsoft Corporation. Chapter Two of this publication summarizes the findings of the Working Group on the technical challenges and solutions available for countering the use of the Internet for terrorist purposes.

7. The UN Global Counter-Terrorism Strategy includes a second reference to the role of the Internet in counter-terrorism. Specifically, it describes Member States' commitment to "use the Internet as a tool for countering the spread of terrorism." The third stage of the CTITF Working Group project thus focused on ways to use the Internet in countering the appeal of terrorism. To this end, the Working Group organized a major conference in Riyadh, Saudi Arabia, in January 2011, which brought together around 150 policy makers, experts and practitioners from the public sector, international organisations, industry, academia and the media. Several States participated at ministerial or ambassadorial level. Policy recommendations and the conference summary are also available at www.un.org/terrorism/internet. The Working Group is currently undertaking an in-depth study on this topic which will be available in the latter half of 2011.

Members of the CTITF Working Group on Countering the Use of the Internet for Terrorist Purposes:

- Monitoring Team of the 1267 Committee (co-chair)
- CTITF Office (co-chair)
- Alliance of Civilizations (AoC)
- Counter-Terrorism Executive Directorate (CTED)
- Department of Public Information (DPI)
- International Criminal Police Organization (INTERPOL)
- Office of the High Commissioner for Human Rights (OHCHR)
- Special Rapporteur on Promotion and Protection of Human Rights While Countering Terrorism
- United Nations Educational, Scientific and Cultural Organization (UNESCO)
- United Nations Interregional Crime and Justice Research Institute (UNICRI)
- United Nations Office on Drugs and Crime (UNODC)

Executive summary

Chapter I. Legal Aspects

8. Preventing as well as investigating terrorist use of the Internet requires adequate legislation as well as effective technical solutions. The challenges presented differ in important ways from those identified in the fight against more traditional terrorist activity. As a result of the available network technology and the multitude of Internet-based services, these challenges range from preventing the availability of instructions on how to commit terrorist acts to monitoring the use of encryption technology in terrorist communications.

9. There has been a wide range of legal responses to these phenomena. Not only do the formulation of criminal legislation and procedural instruments vary, but so too does the strategic approach. It is possible to identify three key trends:

   (*a*) some countries apply existing cybercrime legislation to terrorist use of the Internet;

   (*b*) some countries apply existing counter-terrorism legislation to Internet-related acts; and,

   (*c*) some countries have enacted specific legislation on terrorist use of the Internet.

10. While (*c*) is certainly the most advanced approach, the dominant solutions are currently (*a*) and (*b*), though many legal frameworks addressing terrorism were developed during a time when the threats relating to terrorist use of the Internet were not immediately apparent.

Chapter II. Technical Aspects

11. Rapid developments in technology represent both a challenge and a tool for global efforts to counter terrorism. While the vast number of peaceful social causes and political organizers have benefited from new technologies, evidence shows that terrorist groups do exploit social media communities, including for recruitment, fundraising, and propaganda.

12. As terrorist groups turn to technical tools to organize, plan, run, finance and support their activities, their increasing reliance on technology also makes them vulnerable to government scrutiny. Governments are developing increasingly sophisticated techniques to identify and track potential terrorists. Rapid advances in technology also permit non-governmental organizations and researchers to detect and monitor the online activities of suspected terrorists in cyberspace. Thousands of suspected terrorist websites have been catalogued by various entities around the world.

13. Technology alone is no panacea for combating terrorism, including terrorist use of the Internet. Technical approaches should be enshrined in appropriate legal frameworks, which – in turn – should be part of a comprehensive public policy response that support and clarify the role of technology in combating and countering terrorist activity on the Internet.

14. There is a need for enhanced cooperation between the public and private sectors; as most of the technical infrastructure upon which terrorists are planning, financing and supporting their illegal activities is owned wholly or in part by private entities, there is a strong need for leveraging existing expertise within the private sector and for increased information-sharing among stakeholders. Most experts agreed that greater progress could be made against terrorist use of the Internet, and cyber-security issues in general, with closer cooperation between the public and private sectors.

15. There is an important role for technology not just in the identification of and response to terrorist use of the Internet, but also in countering the narratives of terrorist groups. The wide variety of

technological tools, such as social media networks and online video and chat rooms, offers opportunities to engage with vulnerable communities and potential sympathizers and dissuade them from pursuing a path of violent extremism.

Chapter I
Legal Aspects*

Overview[1]

1. The Internet has innumerable positive features, but also provides a platform for illegal activities,[2] terrorism among them. In the 1990s, the main concern was that terrorist organizations might launch network-based attacks against critical infrastructure, such as transportation and energy supply ("cyber terrorism").[3] This view of terrorist use of the Internet began to change after the 2001 attacks in the United States. Although the 9/11 attacks were not cyberattacks, the perpetrators used the Internet extensively in planning and financing the operation and in communicating with the Al-Qaida leadership.[4,5] In addition to these uses of the Internet by terrorists, the March 2009 Report of the CTITF Working Group on Countering the Use of the Internet for Terrorist Purposes lists training, recruitment, data-mining, propaganda and radicalization.[6]

2. The measures discussed to address these issues are as diverse as the terrorist activities themselves. As the Internet is based on technology, the debate has tended to focus on technical countermeasures such as the blocking of websites; but it goes beyond that. As underlined in the 2009 Report of the CTITF Working Group, there are also legal aspects to consider. Apart from fundamental problems of defining "terrorism" and "terrorist intent", issues such as the protection of human rights, the legality of investigative instruments and

* This chapter would not have been possible without the research, expert interviews, and careful analysis by Dr. Marco Gercke, Director of the Cybercrime Research Institute in Cologne, Germany. The Working Group is also grateful to the numerous experts from Member States, international and regional organizations, non-governmental organizations, academia, and the private sector who have contributed to this chapter with providing their insights and comments.

the applicability of criminal law provisions in counter-terrorist work, are also relevant. This report considers some of these legal issues associated with dealing with terrorist use of the Internet.

Challenges

3. Strategies to fight cybercrime in general and terrorist use of the Internet in particular currently attract a lot of attention. The reason for this is not just that some of the methods are new and therefore require intensive research, but also that the investigation of crimes involving network technology—such as use of the Internet for terrorist purposes—presents particular difficulties.

4. Some of these arise from the ability of offenders to use software tools[7]—such as those designed to locate open ports or break password protection—while committing an offence.[8] In addition, an offender who plans an attack can find detailed information on the Internet that explains how to build a bomb.[9] Although information like this was available before the Internet was developed, it was much more difficult to access. Discussion on the correct legal response ranges from a criminalization of the production, sale or even possession of tools primarily designed to commit sophisticated computer attacks,[10] to criminalizing the publication of critical information.[11]

5. Another challenge is related to the identification of suspects. Although users leave multiple traces while using Internet services, offenders can hinder investigations in particular by disguising their identity. Some countries address these challenges by implementing legal restrictions[12] (for example Italy, where public Internet access providers are required to identify users before allowing them access).[13]

6. Finally, offenders can use automation to scale up their activities, such as through hacking attacks.[14] Up to 80 million hacking attacks occur every day[15] as a result of the availability of software tools[16] that can attack thousands of computer systems in hours.[17] But it is not only automation that causes difficulties in investigating and preventing such attacks. Offenders can use "botnets" to commit powerful

attacks—illustrated for example by the attack against computer systems in Estonia in April 2007.[18] Analysis of the attacks suggests that they were committed by thousands of computers within a "botnet",[19] or group of compromised computers running programs under external control.[20]

Overview of legal responses to terrorist use of the Internet

7. While the 2009 Report of the CTITF Working Group identified several possible terrorist activities involving the Internet,[21] a legal response is relevant to four: Internet-related attacks, illegal content, communication and financing of terrorism.

A. Internet-related attacks (cyberattacks)

8. The popularity of the Internet has had a significant impact on the development of societies worldwide.[22] There is a global procession of countries that are either becoming, or have already become information societies.[23] The transition process is in general characterized by an emerging use of information technology to access and share information.[24] This process has increased the vulnerability of critical infrastructure, as demonstrated by the Stuxnet Computer Worm, discovered in 2010, which focuses on computer systems that control critical infrastructure. Several computer-related attacks have been detected in the last years that—based on the context—could be characterized as politically motivated. The best known are attacks against computer systems in Estonia (2007)[25] and Georgia (2008).[26]

9. The legal response to Internet-related attacks is mainly linked to criminalizing the relevant acts. Two different approaches exist: the application of cybercrime provisions to terrorist-related acts, and the implementation of specific legislation focusing on terrorist attacks only. Regional legal frameworks[27], such as the 2002 Commonwealth Model Law on Computer and Computer Related Crime,[28] the European Union Framework Decision on Attacks against Information Systems and the Council of Europe Convention on Cybercrime[29]

all contain provisions that can be used to prosecute offences such as interference with computer systems. Some of the regional legal frameworks extend criminalization to data interference[30] and even to the production of tools that may be used to commit such offences.[31] Such provisions not only criminalize non-terrorist-related acts but are also applicable to terrorism. However, other countries and model laws include specific legislation dealing with terrorist-related attacks against computer systems. Examples are Section 66F of the Indian Information Technology Act 2000, amended in 2008, and Section 4f of the Draft ITU Cybercrime Legislation Toolkit.[32]

10. The discussion during the working group meeting highlighted that, in general, applying existing legislation was a better option than designing specific laws from scratch. An advantage of the more general approach is that it is not necessary to prove the intent to commit an act of terrorism in order to prosecute an offender.

11. An evaluation of the attacks in Estonia leads to several additional conclusions related to procedural law. One aspect is the need for effective instruments that enable competent authorities to collect quickly the evidence required to determine the extent of the attack, identify offenders and end ongoing attacks. Another potential issue revealed by analysis of the response to the attack against Estonia is the fact that procedural instruments were related to the specific communication. An investigation into botnet attacks involving various computer systems on both the offender's side as well as the victim's side can lead to difficulties as it might not be possible to determine two partners that define a specific communication.

B. Illegal content

12. While activities like recruitment, publication of propaganda material or the collection of information about potential targets appear at first sight to be substantively different, in all cases material is either made available or obtained through impersonal as well as personal communication. The working group emphasized the importance of balancing preventing and investigating offences linked to terrorist use of the Internet with the need to protect freedom of speech.[33]

Legal approaches to criminalize the publication of propaganda should not interfere with the right to freedom of expression.

13. There are different approaches to this issue and a basic distinction between the application of non-Internet specific legislation to terrorist-related material made available online and the development of Internet-specific legislation. Furthermore, while some countries focus on criminalizing the publication of material others focus on the effect by criminalizing incitement. One example of a non-Internet-specific approach is Article 10 of the Russian Federal Law 149-FZ of 27.07.2006 on Information, Information Technologies and Protection of Information. It is again possible to distinguish between Internet-specific and technology-neutral approaches. One example of an Internet-specific approach is Article 5 of the Chinese Computer Information Network and Internet Security, Protection and Management Regulations.

C. Communication

14. The investigation of the 9/11 attacks found that the terrorists had used e-mail to coordinate their attacks.[34] As means of communication for terrorist organisations exist equally outside the Internet, the use of communication systems does not seem to be an Internet-specific topic. However the debate within the working group highlighted that certain Internet-specific challenges might require specific responses. The focus of the discussion in this context concerned the variety of services available, traceability, interception of communications and encryption.

D. Terrorist financing

15. Following the attacks of 11 September 2001, tracing terrorists' financial transactions became a key task.[35] Here too the Internet plays a role. Discussion during the expert workshop, however, highlighted the uncertainty concerning the scope and extent of the use of the Internet for terrorist financing purposes, as many experts believe that funds transfers for terrorist purposes continue to be made predominately in cash.

16. However, as terrorist organisations and their financiers seek ways to disguise and conceal the source of terrorist financing, Internet payment systems will likely play a greater role as they offer a number of advantages to terrorist financiers.[36] For example, terrorist organizations can make use of electronic payment systems to enable online donations.[37] In addition, they can use websites to publish information on how to make donations.[38] Such publication of information is addressed, for example, by United Arabic Emirates Federal Law No 2 of 2006 on Prevention of Information Technology Crime. Instruments to enable competent authorities to confiscate property of value are contained, for example, in the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the Financing of Terrorism.[39]

Strategic approaches

17. States have adopted three different approaches when addressing the specific challenges of terrorist use of the Internet:

A. States apply existing cybercrime legislation, developed to cover non-terrorist-related acts, to terrorist use of the Internet.

18. There are three aspects in this context that need to be taken into consideration.

(*a*) Substantive criminal law provisions introduced to cover non-terrorist-related acts such as data interference[40] or system interference[41] may apply to terrorist-related cases, but the range for sentencing will differ from convictions under specific terrorism legislation.

(*b*) The deployment of cybercrime-specific investigation instruments in cases of terrorist use of the Internet (such as the expedited preservation of computer data[42]) can be advantageous as most countries do not limit the application of sophisticated

investigation instruments to traditional cybercrime offences but include any offence involving computer data.

(*c*) Regional instruments developed to address the challenge of cybercrime, but not specifically terrorist use of the Internet, often contain exemptions for international cooperation. One example is Art. 27, paragraph 4 (*a*), of the Council of Europe Convention on Cybercrime.[43]

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

19. One example of a traditional instrument is the Council of Europe Convention on the Prevention of Terrorism from 2005.[44] The Convention defines several offences such as public provocation to commit a terrorist offence[45] and recruitment for terrorism[46] but does not, for example, contain provisions criminalizing terrorist-related attacks against computer systems.

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

20. One example is Section 4f of the ITU Cybercrime Legislation Toolkit. The International Telecommunication Union (ITU) is the United Nations organization that has most responsibility for practical aspects of cybersecurity.[47] The aim[48] of the Toolkit, presented in draft in 2009 and revised in 2010, is to give countries sample language and reference material for the development of national cybercrime legislation, so as to assist, according to the Toolkit's developers, the "establishment of harmonized cybercrime laws and procedural rules".[49] It aims to be a fundamental resource for legislators, policy experts and industry representatives in order to provide them with a pattern for the development of consistent cybercrime legislation. In addition to traditional approaches, the Toolkit contains several specific terrorist-related offences.[50]

Protection of fundamental rights

21. Discussions within the working group and the expert workshop highlighted the importance of well-balanced legal approaches that take into consideration the most efficient way of criminalizing certain conduct or providing the competent authorities with tools to carry out investigations or prevent activity while at the same time protecting fundamental rights. This is especially relevant with regard to procedural instruments. One example is Sec. 53 of the United Kingdom's Regulation of Investigatory Powers Act 2000,[51] which addresses the increasing use of encryption technology by obliging the suspect of a crime to support the work of law enforcement agencies by disclosing the key. While this appears to be a legal solution to the challenge, there are concerns that the obligation is in conflict with the fundamental protection of a suspect against self-incrimination.[52]

22. Also, while it is theoretically broadly possible to criminalize propaganda material, the debate about the criminalization of xenophobic material highlights the potential difficulties of a broader application. One of the main difficulties related to provisions criminalizing xenophobic material is to keep a balance between ensuring freedom of speech[53] on the one hand and preventing the violation of the rights of individuals or groups on the other. The difficulties over the negotiation of the Council of Europe Convention on Cybercrime[54] and the need for and subsequent status of the signatures/ratifications of the Additional Protocol[55] demonstrate that the need to protect freedom of expression would hinder a number of countries from undertaking such an approach.

Conclusion and recommendations

23. While further research would enable an evaluation of the efficiency of the varying approaches to the problem, these conclusions and recommendations are limited to the issues discussed above.

24. Addressing terrorist use of the Internet presents challenges that develop in line with the technology. The problem is not static and

legal measures will generally follow technical developments rather than foresee them. The working group recommends careful analysis of current challenges and future trends to ensure that any legal response to terrorist use of the Internet remains effective. In this respect, given the nature of the Internet, global initiatives are likely to have most impact .

25. Unlike computer and network technology, which is to a large degree globally harmonized already enabling users around the world to access the same services over the Internet,[56] cybercrime legislation and other specific legal responses to terrorist use of the Internet lack a common approach.[57] The issue of harmonization of legislation is highly relevant as a large number of countries base their mutual legal assistance regimes on the principle of "dual criminality".[58] The transnational dimension of terrorism highlights difficulties in cooperation—especially with regard to illegal content. Member States may therefore wish to consider implementing existing regional instruments (such as the Commonwealth Model Law on Cybercrime and the Council of Europe Convention on Cybercrime) as well as relevant international initiatives such as the United Nations Convention against Transnational Organized Crime.

26. The use of traditional cybercrime legislation as well as non-Internet-specific anti-terrorism legislation to address terrorist use of the Internet gives rise to several potential problems. In addition to implementing legislation on cybercrime and traditional forms of terrorism, States may wish to consider—if gaps are discovered—developing specific legislation to address terrorist use of the Internet while avoiding criminalizing conduct that is not criminalised outside the Internet. States may wish to pay special attention to seeking a harmonized approach in order to facilitate international cooperation.

27. As investigations today benefit from more sophisticated technology, legal safeguards become more important. The need for well-balanced legal approaches that take into consideration the most efficient way of criminalizing certain conduct or providing the competent authorities with the tools to carry out investigations while protecting fundamental rights is self-evident. Thus, States may wish to take into

consideration the importance of a measured approach with regard to technical solutions, procedural instruments as well as criminal law provisions.

28. Technical solutions for the removal and prevention of terrorist postings on the Internet, whether incitement or instruction, must also benefit from adequate legal provisions. These are unlikely to exist without international agreements on definitions and on mutual assistance. In the absence of such agreements, and given the ability of terrorist groups to ensure the resilience of their Internet presence, informal agreements between States and between national authorities and Internet service providers in the private sector are likely to have more effect in the short to medium term than any legal provisions.

Endnotes

1 This report is informed by the discussions and outcomes of a workshop on "Countering Terrorist Use of the Internet" with a focus on legal issues, organized in Berlin, Germany (January 2010) by the CTITF Working Group on Countering the Use of the Internet for Terrorist Purposes. The workshop was co-organized and supported by the German Federal Foreign Office.

2 *Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes*, 2009, page 3.

3 Gercke, Cyberterrorism, "How Terrorists Use the Internet", Computer und Recht, 2007, page 62 et. seq.

4 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", *The 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=;

5 CNN, News, 04.08.2004, available at: http://www.cnn.com/2004/US/08/03/terror.threat/index.html.

6 *Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes*, 2009, page 5-8.

7 "Websense Security Trends Report 2004", page 11; "Information Security—Computer Controls over Key Treasury Internet Payment System", United States General Accounting Office, July 2003, page 3; Sieber, *Council of Europe Organised Crime Report 2004*, page 143.

8 Ealy, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention", page 9 et seq., available at: http://www.212cafe.com/download/e-book/A.pdf.

9 One example is the "The Terrorist's Handbook"—a pdf-document that contains detailed information how to build explosives, rockets and other weapons (See www.capricorn.org/~akira/home/terror.html).

10 See in this context, for example, Art. 6, Council of Europe Convention on Cybercrime.

11 Regarding the criminalization of terrorist-related training material, see EU Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism, 28.11.2008, 2008/919/JHA.

12 Gercke, *Understanding Cybercrime: A Guide for Developing Countries*, ITU 2009, Chapter 6.2.11.

13 Decree-Law 27 July 2005, no. 144.—Urgent measures for combating international terrorism. For further information on the Decree-Law, see, for example, the article "Privacy and data retention policies in selected countries", available at: http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

14 Ealy, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention", page 9 et seq., available at: http://www.212cafe.com/download/e-book/A.pdf.

15 The Online-Community HackerWatch publishes regular reports on hacking attacks. Based on their sources, more than 250 million incidents were reported in only one month (August 2007). Source: http://www.hackerwatch.org.

16 Regarding the distribution of hacking tools, see: CC Cert, "Overview of Attack Trends", 2002, page 1, available at: http://www.cert.org/archive/pdf/attack_trends.pdf.

17 See CERT Coordination Center, "Overview of Attack Trends", 2002, page 1.

18 Regarding the attacks, see: Lewis, "Cyber Attacks Explained", 2007, "A cyber-riot", *The Economist*, 10.05.2007, available at: http://www.economist.com/world/europe/PrinterFriendly.cfm?story_id=9163 598; "Digital Fears Emerge After Data Siege in Estonia", *The New York Times*, 29.05.2007.

19 See Toth, "Estonia under cyber attack", http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.

20 See Ianelli/Hackworth, "Botnets as a Vehicle for Online Crime", CERT Coordination Center, 2005, page 3.

21 *Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes*, 2009, page 5-8.

22 Related to the development of the Internet, see Yang, Miao, ACM International Conference Proceeding Series; Vol. 113; Proceedings of the 7th international conference on Electronic commerce, Page 52-56, Association for Computing Machinery.

23 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*.

24 World Summit on the Information Society, Document WSIS-03/GENEVA/DOC/5-E, December 2003, available at: http://www.itu.int/wsis/docs/geneva/official/poa.html

25 Tikk/Kaska/Vihul, "International Cyber Incidents: Legal Considerations", NATO CCD COE, 2010, page 18 et. seq; Ashmore, "Impact of Alleged Russia Cyber Attacks", *Baltic Security & Defence Review*, Vol. 11, 2009, page 8 et seq.

26 Tikk/Kaska/Rünnimeri/Kert/Talihärm/Vihul, "Cyber Attacks Against Georgia: Legal Lessons Identified", 2008, page 4; Hart, "Longtime Battle Lines Are Recast In Russia and Georgia's Cyberwar", *Washington Post*, 14.08.2008; "Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks", European Union, Policy Department External Policies, 2009, page 15, Ashmore, "Impact of Alleged Russia Cyber Attacks", *Baltic Security & Defence Review*, Vol. 11, 2009, page 10.

27 The working group discussed briefly if the Council of Europe Convention on Cybercrime shall be characterized as a regional or international instrument. In this context the Council of Europe pointed out that the Convention was negotiated with the support of four non-member states (Canada, Japan, South Africa and the United States) and "100 jurisdictions around the world have either acceded/sought accession to, or have based their national legislation on, this Convention" and the instrument should therefore be labeled international. However, taking into account that the Convention is characterized as a regional approach by different UN Resolutions (see, for example, GA Res. 64/211), that apart from the United States no country outside Europe so far ratified the instrument, and finally that the Council of Europe could not provide more information (like a list of countries) that would enable a verification of the provided number of "100 jurisdictions", the drafter decided to use the common characterization of the Council of Europe Convention on Cybercrime as regional instrument.

28 "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information see Bourne, *2002 Commonwealth Law Ministers Meeting: Policy Brief*, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.; Angers, "Combating Cyber-Crime: National Legislation as a Pre-requisite to International Cooperation" in: Savona, *Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research*, 2004, page 39 et seq.; United Nations Conference on Trade and Development, *Information Economy Report 2005*, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

29 *Council of Europe Convention on Cybercrime* (CETS No. 185), available at: http;//conventions.coe.int. Regarding the Convention on Cybercrime see Sofaer, "Toward an International Convention on Cybercrime" in Seymour/Goodman, *The Transnational Dimension of Cyber Crime and Terror*, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; Gercke, "The Slow Wake 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, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; Jones, "The Council of Europe Convention on Cybercrime, Themes and Critiques", 2005, available at: http://www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; 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; Adoption of Convention on Cybercrime, *International Journal of International Law*, Vol 95, No.4, 2001, page 889 et seq.

30 See, for example, Art. 4 Convention on Cybercrime.

31 See, for example, Art. 5 Convention on Cybercrime.

32 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.

33 Regarding the principle of freedom of speech see Tedford/HerbeckHaiman, "Freedom of Speech in the United States", 2005; Barendt, "Freedom of Speech", 2007; Baker, "Human Liberty and Freedom of Speech"; Emord, "Freedom, Technology and the First Amendment", 1991. Regarding the importance of the principle with regard to electronic surveillance see Woo/So, "The case for Magic Lantern: September 11 Highlights the Need for Increasing Surveillance", *Harvard Journal of Law & Technology*, Vol. 15, No. 2, 2002, page 530 et seq; Vhesterman, "Freedom of Speech in Australian Law, A Delicate Plant", 2000; Volokh, "Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law", *Loyola University Chicago Law Journal*, Vol. 33, 2001, page 57 et. seq., available at: http://www.law.ucla.edu/volokh/harass/religion.pdf; Cohen, "Freedom of Speech and Press: Exceptions to the First Amendment", CRS Report for Congress 95-815, 2007, available at: http://www.fas.org/sgp/crs/misc/95-815.pdf.

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

35 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 costs 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.

36 http://www.fatf-gafi.org/searchResult/0,3400,en_32250379_32237295_1_1_1_1_1,00.html

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

38 Weimann in USIP Report, "How Terrorists Use the Internet", 2004, page 7.

39 Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the Financing of Terrorism, ETS 198.

40 See, for example, Art. 4 Convention on Cybercrime.

41 See, for example, Art. 5 Convention on Cybercrime.

42 Art. 16, Convention on Cybercrime.

43 Convention on Cybercrime, ETS 185.

44 Council of Europe Convention on the Prevention of Terrorism, ETS 196.

45 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.

46 Article 6—Recruitment for terrorism

1. For the purposes of this Convention, recruitment for terrorism means to solicit another person to commit or participate in the commission of a terrorist offence, or to join an association or group, for the purpose of contributing to the commission of one or more terrorist offences by the association or the group.
2. Each Party shall adopt such measures as may be necessary to establish recruitment for terrorism, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

47 *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks*, European Union, Policy Department External Policies, 2009, page 17.

48 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.

49 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

50 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).

51 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; *ABA International Guide to Combating Cybercrime*, page 32.

52 Regarding the discussion about the protection against self-incrimination under the United States law, see, for example, Clemens, "No Computer Exception to the Constitution: The First Amendment Protects Against Compelled Production of an Encrypted Document or Private Key", *UCLA Journal of Law and Technology*, Vol. 8, Issue1, 2004; Sergienko, "Self Incrimination and Cryptographic Keys", *Richmond Journal of Law & Technology*, 1996, available at: http://www.richmond.edu/jolt/v2i1/sergienko.html; O'Neil, "Encryption and the First Amendment", *Virginia Journal of Law and Technology*, Vol. 2, 1997, available at: http://www.vjolt.net/vol2/issue/vol2_art1.pdf; Fraser, "The Use of Encrypted, Coded and Secret Communication is an 'Ancient Liberty' Protected by the United States Constitution", *Virginia Journal of Law and Technology*, Vol. 2, 1997, available at: http://www.vjolt.net/vol2/issue/vol2_art2.pdf; Park, "Protecting the Core Values of the First Amendment in an age of New Technology: Scientific Expression vs. National

Security", *Virginia Journal of Law and Technology*, Vol. 2, 1997, available at: http://www.vjolt.net/vol2/issue/vol2_art3.pdf; "Hearing before the Subcommittee on the Constitution, Federalism, and Property Rights of the Committee on the Judiciary", United States Senate, 105th Congress, Second Session on Examining the Use of Encryption and Mandatory Access in Digital Communications, Focusing on Proposals to Balance Privacy Rights with Law Enforcement Concerns, available at: http://www.loc.gov/law/find/hearings/pdf/00139296461.pdf.

Regarding the discussion in Europe about self-incrimination, in particular with regard to the European Convention on Human Right (ECHR) see Moules, "The Privilege against Self-Incrimination and the Real Evidence", *The Cambridge Law Journal*, 66, page 528 et seq.; Mahoney, "The Right to a Fair Trail in Criminal Matters under Art. 6 ECHR", *Judicial Studies Institute Journal*, 2004, page 107 et seq.; Birdling, "Self-incrimination goes to Strasbourg: O'Halloran and Francis vs. United Kingdom", *International Journal of Evidence and Proof*, Vol. 12, Issue 1, 2008, page 58 et seq.; Commission of the European Communities, *Green Paper on the Presumption of Innocence*, COM (2006) 174, page 7, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0174:FIN:EN:PDF.

53 Regarding the principle of freedom of speech see: Tedford/HerbeckHaiman, "Freedom of Speech in the United States", 2005; Barendt, "Freedom of Speech", 2007; Baker, "Human Liberty and Freedom of Speech"; Emord, "Freedom, Technology and the First Amendment", 1991; Regarding the importance of the principle with regard to electronic surveillance see Woo/So, "The Case for Magic Lantern: September 11 Highlights the Need for Increasing Surveillance", *Harvard Journal of Law & Technology*, Vol 15, No. 2, 2002, page 530 et seq; Vhesterman, "Freedom of Speech in Australian Law: A Delicate Plant", 2000; Volokh, "Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law", *Loyola University Chicago Law Journal*, Vol. 33, 2001, page 57 et. seq., available at: http://www.law.ucla.edu/volokh/harass/religion.pdf; Cohen, "Freedom of Speech and Press: Exceptions to the First Amendment", CRS Report for Congress 95-815, 2007, available at: http://www.fas.org/sgp/crs/misc/95-815.pdf.

54 *Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime*, No. 4.

55 Regarding the list of states that signed the Additional Protocol see Gercke, *Understanding Cybercrime: A Guide for Developing Countries*, ITU 2009, Chapter 5.1.4.

56 Regarding the technical standardization see OECD, *Internet Address Space: Economic Considerations in the Management of IPv4 and in the Development of IPv6*, 2007, DSTI/ICCP(2007)20/FINAL; Regarding the importance of single technical as well as single legal standards, see Gercke, "National, Regional and International Approaches in the Fight Against Cybercrime", *Computer Law Review International*, 2008, page 7 et seq.

57 Regarding the relation between technical and legal standards in fighting cybercrime, see "Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including cases of cybercrime", *Working Paper for the 12th United Nations Congress on Crime Prevention and Criminal Justice*, Brazil, 2010, A/CONF.213/9.

58 Dual criminality exists if the offence is a crime under both the requestor and requesting party's laws. Regarding the dual criminality principle in international investigations, see "United Nations Manual on the Prevention and Control of Computer-Related Crime", 269; Schjolberg/Hubbard, "Harmonizing National Legal Approaches on Cybercrime", 2005, page 5.

Chapter II
Technical Issues*

Overview

1. While it would be wrong to make broad generalizations about the technical skills of terrorists, there is evidence to suggest that many terrorists in organizations such as Al-Qaida, are well-educated and trained in the use of computer systems. Participants noted that terrorist websites were increasing in technical sophistication, moving well-beyond basic HTML, to include widespread use of other scripting languages and web applications such as PHP, ASP and JSP. [1, 2, 3] There is now little difference between the technical sophistication of Middle Eastern terrorist websites and those of the U.S. Government, except that terrorist websites take greater advantage of multimedia techniques, including embedded audio and video files.[4]

2. The rapid development of new technologies and their adaptation by terrorists pose significant public policy and legal challenges for law enforcement. International law and public policy remain far behind the pace of technological development. As prior CTITF efforts have specifically addressed issues of law and policy, this report will focus on the technologies themselves and how terrorists are exploiting them to their advantage. Of course technology itself is neither good nor evil: it can be used for both positive and negative objectives; therefore, when applicable, this report also aims to address

* This chapter would not have been possible without the research, expert interviews, and careful analysis by Marc Goodman, Director of the Future Crimes Institute in San Francisco, USA. The Working Group is also grateful to the numerous experts from Member States, international and regional organizations, non-governmental organizations, academia, and the private sector who have contributed to this report with providing their insights and comments.

the counter-measures that governments, the private sector, and civil society/academia can take against the use of Internet technology by terrorist organizations.

Cybercrime and Terrorist Use of the Internet: Understanding the Nexus

3. Evidence suggests that a number of terrorist organizations fund their activities by engaging in traditional forms of online criminality, such as credit card fraud and intellectual property theft. In June 2007, three British residents, Tariq al-Daour, Waseem Mughal, and Younes Tsouli, were charged with using the Internet to incite murder. Evidence presented showed that the men had used stolen credit card information to purchase goods such as night vision goggles, global positioning devices, airplane tickets and prepaid mobile phone cards to provide direct tactical support for terrorist operations. The trio reportedly made fraudulent charges totaling more than 3.5 million U.S. dollars and was in possession of a database containing nearly 40,000 stolen credit card accounts.[5] In another case, Bali Bomber Imam Samudra funded his attack in which more than 200 people were murdered with an estimated $150,000 US, which he obtained by hacking into Western bank accounts and credit lines.[6] Moreover, Samudra wrote a book while in jail in which he shared his hacking and "carding" techniques with his disciples, encouraging them to take their "holy war" to cyberspace by committing credit card fraud.[7, 8]

4. Participants noted the existence of the vast, organized, cybercrime underground—one which was willing to sell its services to the highest bidder, regardless of ideology or agenda. Thus there was nearly unanimous concern regarding terrorist organizations leveraging the technical talents of existing organized cyber criminals. Organized cybercrime groups, particularly those in Eastern Europe and parts of Asia, widely advertised sophisticated cyber attacks tools, such as "botnets" for rent or sale on the Internet, (see section 5.9 for further detail on botnets). While this remained a concern, there was

no publicly available evidence presented to prove that terrorists had already hired hackers from organized crime groups or that they had rented a massive botnet army to conduct an advanced technical attack against a target of interest. That said, there was a high degree of agreement among participants that the offensive cybercrime tools developed by organized crime would make a powerful addition to the arsenal of terrorist tools and it was merely a matter of time before terrorists took advantage of these capabilities.

The Technologies

A. The Internet as an Open Source Information Tool

5. **Target Acquisition and Research:** The globally distributed network has created new opportunities for terrorists to research a potential target. For example, it is often possible to find for free on the Internet detailed building schematics, photographs and even satellite imagery. In 2006 an organization linked to Al-Qaida reportedly produced a 26-page manual providing detailed instructions on how best to exploit the Google search engine.[9] According to media reports, during a 2007 operation in Basra, Iraq, British Army officials discovered numerous Google Earth printouts which showed in great detail buildings inside the British base in Basra, with tented accommodations, lavatory blocks and light armored vehicles clearly marked.[10] Based upon further evidence uncovered, British officials deduced the information was being used to plan an attack on their base. In other cases, such as the 2007 planned attempt by terrorists to blow up fuel tanks at New York's John F. Kennedy International Airport, court records indicate that terrorists utilized Google Earth as a means of obtaining detailed aerial photographs of their intended target.[11] Furthermore, evidence from the 2009 attacks in Mumbai, India indicated that terrorists used a wide variety of open source Internet tools, including Google Earth and Maps to plan their assault on the city.[12] Terrorists can also mine a variety of other sources, such as social networking sites, to uncover the names and addresses of individuals

affiliated with a target, such as hotel or embassy staff, as well as data on their family connections and their networks.

6. **Data Mining:** The emergence of the Internet has allowed both the public and private sector to put vast amounts of information online. While doing so has provided significant cost savings, it has also created significant opportunities for terrorists and others to conduct data mining operations, searching out with precision, the exact details needed to conduct or facilitate a terrorist attack. In a January 2003 report, the United States Secretary of Defense warned his personnel that at least 700 gigabytes of Defense Department data was publicly available on government websites and that one needed to assume that this data was being accessed by terrorists to gain insight into the department's plans, programs and activities.[13] Moreover, an Al Qaida training manual uncovered in Afghanistan advised terrorists that by "using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of information about the enemy."[14] In addition, incidents such as the 2011 "Wikileaks" disclosures, which unveiled more than 250,000 diplomatic cables, provide government assessments on the state of terrorist organizations, their plans and intentions, and therefore reveal the extent of their knowledge.[15]

7. **Education and Training:** Some counterterrorism experts have referred to the Internet as a "terrorist university," a place where terrorists can learn new techniques and skills to make them more effective in their attack methodologies. Widely available online are documents such as the "Mujahideen Poisons Handbook" that contains various "recipes" for homemade poisons and poisonous gases.[16] Similar information on hostage taking, bomb making and guerilla tactics is also available in a wide variety of other sources such as the "Anarchist Cookbook" and the "Sabotage Handbook."[17] The 600 page "Encyclopedia of Jihad" is also widely available online and includes chapters such as ""how to kill," "explosive devices," "manufacturing detonators" and "assassination with mines." On-line magazines, such as Inspire, and many terrorist websites also provide training and ideas for terrorist attacks, and the development and widespread

availability of the Internet has made it possible to create readily accessible "virtual training camps".

8. **Countermeasures and opportunities:** All participants recognized the dual positive and negative effects of Internet technologies. For example, high quality 3-D maps might be of value to terrorists, but they had infinitely greater positive applications. In addition, participants noted that terrorists were not merely consumers of digital content, but were increasingly becoming content producers as well. Numerous governments, security services and NGOs frequently accessed the data disseminated on terrorist websites and leveraged it for intelligence and law enforcement purposes.

B. Identity & Attribution

9. In 1993, during the early days of the Internet, cartoonist Peter Steiner famously drew a cartoon for the New Yorker magazine of two dogs sitting in front of a computer screen. One dog, touting the advantages of the new medium, happily told the other "On the Internet, nobody knows you're a dog."[18] The cartoon demonstrates one of the primary advantages and disadvantages of Internet communication: anonymity. The anonymous nature of the Internet has been a boon for people all over the world seeking or posting political, religious, or even medical information and many view anonymity on the Internet as promoting freedom of speech and human rights. Conversely, both criminals and terrorists have used the anonymity of the net to their full advantage, often with impunity.

10. Today's online identity challenges stem from the fact that when the original Internet architecture was conceived and constructed, no rigorous means of identification was engineered into the network itself. However, the Internet does provide for a means of numeric identification via an Internet protocol address, a unique identifier which is transmitted with every step taken on the Internet and which allows the Internet to route traffic to the appropriate destination.[19] Just as each telephone has a unique numeric identifier, so too does each Internet connection. Thus for example, an Internet protocol address

is routinely attached to an email to show the source network and user from whom the email is sent. By visiting sites such as www.whois.com, it is possible to do a "whois lookup" and determine for example that the Internet protocol address 157.150.34.32 is registered to the United Nations.

11. From an investigative perspective, it is of course useful to know the Internet protocol address of an email sent, as it can potentially lead to the real-world location of a criminal or terrorist. Unfortunately, knowing that an email may have originated from any particular domain does not tell investigators who may have sent that email. Further information would be required, such as the network logs showing the individual who was logged into a particular computer at the time. Due to the high storage costs involved, these logs are only kept for a limited period and in some case, are not kept at all. Without the specific computer logs, counter-terrorism investigators might be able to determine that a message was sent from a particular computer host in a particular country, but would not be much further along in identifying the individual concerned.

12. Many terrorists are well aware of the Internet protocol addressing system and take steps to ensure their location data is not transmitted as part of their online activities. Simple solutions are to send emails from anonymous cyber-cafes, unsecured wireless access points, or through previously hacked or compromised computers belonging to third parties. Often criminals and terrorists will purposefully route their Internet traffic through multiple countries and jurisdictions, making their communications nearly impossible to trace.

13. Many more sophisticated methods exist to remain anonymous online, including through the increasing number of cost free anonymization services such as the I2P Network and the Tor Project, each of which uses a variety of peer-to-peer and encryption technologies to hide Internet protocol addresses.[20] These anonymization services utilize a proxy server computer that acts as an intermediary and a privacy shield between the client computer and the rest of the Internet.[21] In effect, the proxy acts on the original user's behalf to protect any personal information from being shared with destination points on the

Internet beyond the proxy, and as such, users are able to "spoof" or alter their IP address. These proxy services have increased in sophistication in recent years and now often utilize a peer-to-peer networking approach to prevent the user's identity from remaining in any single central third-party site that could disclose a user's identity.

14. Participants additionally identified two emerging technologies as potential targets for terrorist abuse: the growing use of mobile computing technologies and the rapid spread of "cloud computing."[22] More and more mobile phones are providing access to the Internet and the wide availability of non-registered SIM cards in many countries allows users to make phone calls, send text messages and surf the Internet without any form of identification required. In addition, the wide availability of "bullet-proof" hosted cloud computing resources means that terrorists are able to host their propaganda and digital content online with little fear of identification or reprisal. Bullet-proof domain hosting companies are "legitimate businesses" that primarily sell their services to illegitimate organizations. They primarily locate their businesses in jurisdictions with little international law enforcement cooperation and routinely and deliberately ignore any international legal requests for information about their clients. Bullet-proof hosts allow their customers great flexibility in the material hosted, whether spamming or pornography, and as such they have become the preferred option for international organized crime groups. Participants assessed terrorists would increasingly avail themselves of bullet-proof hosting services as a means of protecting their identities and ensuring the distribution of their online content.

15. Anonymity in cyberspace makes it vastly more difficult to attribute criminal or terrorist activities to any one group or individual. The lack of attribution techniques was viewed as one of the major obstacles in effectively responding to terrorist use of the Internet. Without attribution, it was impossible to determine if a particular cyber attack or intrusion was the work of a lone teenage hacker testing his skills, an international organized crime group seeking to commit a major financial fraud, a terrorist entity launching a denial of service attack against a vital critical infrastructure or a nation-state engaging in

cyber-warfare. In this regard, participants agreed that more trustworthy forms of identity in cyberspace would be required in order to have any deterrent effect on terrorist use of the Internet. Several proposals for more robust identity systems were put forward, but participants noted the need to balance carefully requirements for identification in cyberspace with relevant human rights and data privacy concerns.[23]

16. Countermeasures and opportunities: Participants noted a variety of policy and legal measures that could enhance the ability of competent authorities to respond to the challenges posed by terrorist anonymity on the Internet. These varied from some jurisdictions requiring identification from those using a cyber café or purchasing a SIM card, though it was noted that determined terrorists could readily obtain false identification documents. Another was to implement mandatory requirements for data retention, such as the March 2006 European Union directive 2006/24/EC which requires that EU communications providers retain certain data necessary to identify and trace the source of a particular electronic communication.[24] From a technical perspective, several tools were discussed, such as those developed by the Dark Web Terrorism Research project which allowed investigators to use artificial intelligence and language analysis techniques to improve identification of terrorists in online forums.

C. Data Encryption/Obfuscation:

17. Terrorists additionally use widely available technical tools, such as data encryption, to obscure and protect their activities.[25] For example, Ramzi Yousef, convicted for his involvement in the first World Trade Center Bombing in 1993, used encryption to hide details of a plot to destroy U.S. airliners. Police discovered the encrypted files on a computer in his Manila apartment in 1995.[26] Another terrorist, Wadih El Hage, who was indicted for the 1998 bombings of two United States embassies in East Africa sent encrypted e-mails to associates in Al-Qaida according to court papers. In the Yousef case, it took law enforcement authorities more than a year to break the encryption algorithm used by the terrorist.[27] Since the early 1990's,

the availability of encryption has become much more widespread and its use far easier, removing the barrier to entry for less technically sophisticated terrorists. Online email services, such as Hushmail, seamlessly permit users to utilize encryption services in an easy to use webmail interface.[28]

18. More recently, terrorist encryption techniques have become decidedly more technically complex and sophisticated. Encryption key lengths have increased since the days of Ramsey Yousef and 256 bit encryption keys are now widely available as part of the Advanced Encryption Standard (AES). The longer the encryption key, the longer it would take competent authorities to "brute-force" the decryption of any encoded terrorist message. For example, using a computer capable of guessing 10^{18} potential keys per second, it would still take a super-computer $3x10^{51}$ years to find the key necessary to read the message. To put the amount of time and computing power required into perspective, $3x10^{51}$ years is longer than the age of our solar system.

19. Terrorists can also use other data encryption techniques to keep their communications secret, such as multiple encryptions of the same files. Much like a Matryoshka doll, an encrypted file can be contained within an encrypted file, hidden within another encrypted file, making decryption all but impossible. Former British Airways employee Rajib Karim who allegedly exchanged electronic messages with an Al-Qaida cleric in Yemen in 2010 utilized such a technique.[29] Karim plead guilty in November 2010 to a variety of terrorist charges and was reported to have used multiple encryption techniques to protect 320 gigabytes of data files, including the use of complex ciphers, nested-encryption and data-obfuscation.

20. Evidence has shown that terrorist organizations are somewhat distrustful of commercially available encryption technologies. To this end, many encryption programs have been made available as "open source" downloads, allowing terrorists to check the software for hidden backdoors that might assist law enforcement authorities to identify them.[30] In addition, some terrorist groups have started to compile their own encryption products and advertise them as

programmes for secure communications through networks with the highest technical level of encoding."[31]

21. Several terrorist groups, including Al-Qaida have been reported to be utilizing steganography techniques[32] to provide a degree of communications security to their operational activities.[33] Steganography, derived from the Greek for "hidden-writing", allows an electronic message to be hidden inside another type of computer file. For example, a word document containing the planning details of an imminent attack could be hidden in a digital photograph of the Eiffel Tower or the latest Star Wars movie file, the presence of which would likely be highly undetectable by authorities. The advantage of steganography over encryption is that law enforcement authorities readily recognize encrypted files and are willing to dedicate resources to attempt decryption, while with steganography, police are unlikely even to realize that a hidden file exists.[34] Commonly available steganography programs include Hiding Glyph, Vecna, TrueCrypt, F5, mp3stego and Steganos Privacy Suite. Law enforcement officials are attempting to improve their skills in Steganalysis, the craft of uncovering and revealing the use of steganography, but so far there is no consistently available tool for detecting the use of steganography in a computer file.

22. Another online technique terrorists can utilize to their advantage is the growing number of places to hide on the Internet. In other words, the sheer volume of data being produced every day is so large, with so many new programs, websites, chat program and micro-blogging sites emerging, that it has become increasingly easy merely to hide within the noise. Recently, a senior executive of Google Inc. noted that humanity created more data every two days in 2010 than it had from the dawn of time through 2003.[35] Much of this data is coming from user-generated content sites such as YouTube, Twitter, Facebook, Flickr and the like. As the number of gaming sites, auction sites, virtual worlds, instant messaging services, VoIP (Voice over IP) services and micro-blogging services continue to expand, terrorists will have more places to hide and law enforcement officials will have vastly expanded areas in which to look for signs of terrorist activity online.

23. Countermeasures and opportunities: While certain technological developments could in theory help break computer encryption more rapidly, the time required to brute-force attack a lengthy encryption cipher would still be in the billions of years. As such, competent authorities needed to explore other techniques for obtaining a terrorist's pass-phrase, whether compelling disclosure in a legal proceeding, or using innovative investigative techniques and social engineering to determine the cipher key. Overall, the techniques available to law enforcement are limited in their effectiveness and thus, for the foreseeable future, terrorists will continue to benefit from data hiding techniques such as encryption and steganography.

D. The Internet as a Tool for Propaganda & Radicalization

24. Terrorists have become adept and leveraging the Internet as a tool for propaganda, radicalization, recruitment and psychological warfare. The ability of terrorists to spread their propaganda via technological tools is nothing new and prior to the widespread use of the Internet many terrorist organizations produced CDs, DVDs and other media to get their message out. Some, such as Hezbollah, began producing video games long ago, including the 2003 program "Special Force" which encouraged players to assassinate the then Israeli Prime Minister Ariel Sharon. The game reportedly sold more than 10,000 copies throughout the Middle East and Europe and was available in English, French, Arabic and Farsi. A member of the game's design team noted that the game was created to spread the organization's values and ideas.[36]

25. Since then, numerous terrorist organizations have taken their message to cyberspace. By the late 1990s, Al-Qaida already had launched its first website.[37] According to one noted cyber terrorism expert, the number of terrorist websites grew in the ensuing decade from fewer than 100 to nearly 5,000.[38] While exact statistics are not available, the University of Arizona's Dark Web project has reported collecting data from more than 10,000 unique terrorist or terrorist-affiliated websites[39] and all major groups have established them including

Aum Shinrikyo, Ansar al Islam, the Japanese Red Army, the Popular Front for the Liberation of Palestine, the al Aqsa Martyrs Brigades, Hezbollah, Hizb-ul Mujehideen in Kashmir, the Liberation Tigers of Tamil Eelam, the Irish Republican Army, the Shining Path (Sendero Luminoso), the Basque ETA Movement and FARC (the Armed Revolutionary Forces of Colombia).[40]

26. Terrorists continue to improve the quantity, quality and sophistication of their Internet propaganda and recruitment efforts. One report noted that in 2002, the Al-Qaida media arm As-Sahab had issued only six audio or video web messages. By 2007, the number had increased to nearly 100 multimedia files.[41] Increasingly violent and explicit videos of suicide bombings and other attacks were posted online, having a noted propaganda effect.

27. Often terrorist websites enable chat or commenting technologies which allow individual visitors to post information, pose questions, or suggest topics for discussion. While many of these sites are open to the general public, others require passwords or introductions by other members in order to be admitted. The vetting process can continue and as users rise in the ranks or show particular aptitude or commitment, they can access increasingly restricted portions of the site. Often communication is moved from the web forum to other communications channels, such as IRC (Internet Relay Chat) forums, VoIP/mobile phone conversations or in-person meetings. Of course the webmasters of these sites can lurk in the background, monitoring all the activity of those accessing their sites and thus can flag particular individuals, often young and idealistic, for recruitment or other operational activity in support of the terrorist cause.

28. Countermeasures and opportunities:

    (*a*) While the growing web presence of terrorist organizations poses a variety of public safety and security challenges, it also creates opportunities for competent authorities to gain insights into their activities. However, participants were divided on the best approach to take in response to violent or criminal content posted by terrorists in cyberspace. Some countries and

jurisdictions are adamant that the content should be taken down and access blocked, but while blocking access to content within one's own jurisdiction may be feasible and legal, doing so internationally is more complicated.

(*b*) Whether through legal processes served on the web hosting company or via other technical means, some participants argued for an active means of blocking public access to terrorist websites. One of the available technical tools for doing so is by establishing a national firewall system,[42] But although a national firewall and content filter could in theory prevent access to a wide variety of offensive content ranging from child pornography to explicit beheading videos, the distributed nature of the Internet makes this approach imperfect and raises a number of privacy and human rights concerns. Also the material could be posted on multiple sites around the world, each with a slightly different name, making content blocking a challenge, or it could be moved onto closed or password-protected forums. Moreover, by using any number of widely available proxy-servers and anonymizers, it is often possible to bypass national content filtering systems.

(*c*) In addition, the growing availability of "fast-flux" (for fast fluctuation) hosting techniques makes it nearly impossible for national authorities to block access to terrorist or other malicious content with complete assurance.[43] Fast flux is a technique which continuously moves the location of a website, email or domain name system server from computer to computer in an effort to hide its activity and make detection more difficult. In such cases, any "black list" of offensive sites would be rendered useless. Even more advanced website hiding techniques, such as "double-flux" allow the domain name servers (DNS) which resolve web host names to be moved rapidly from server to server, so although the website visitor is able to view the desired content, intermediary proxies prevent visitors from knowing the actual web server hosting the content. To complicate matters further, it is also possible to encrypt the various systems in use as a means of further frustrating investigators

and authorities attempting to block or limit access to these sites. From 2009–2010, the Internet Corporation for Assigned Names and Numbers (ICANN) studied the problem of fast-flux technologies, noting their ability to assist criminals and terrorists in cyberspace.[44]

(*d*) Given the significant impediments to blocking terrorist content in cyberspace, some participants raised the possibility of utilizing even more active measures, such as the launching of distributed denial of service (DDOS) attacks against terrorist websites.[45] Doing so, however, has many challenges. First, the legality of such an approach under international law is highly suspect. Second, given the lack of robust attribution tools, it is quite possible that any DDOS attack might be misdirected at an innocent party. For example, hundreds of companies or organizations can be hosted on any particular web server, thus legitimate businesses, NGOs and medical providers could share a same server with a terrorist organization and so suffer from an attack directed against it. In addition, terrorists and criminals often use hacked and compromised websites of third parties to host their content. Doing so has many benefits, including frustrating attempts at attribution and avoiding the actual costs of web hosting, which can be high given the volume of multimedia content on terrorist websites. The experiences of one company in California are typical: the firm had no idea it was hosting video content of an Al-Qaida beheading until its hosting costs sky-rocketed due to frequent downloads of the video.[46]

(*e*) Given the aforementioned difficulties in blocking terrorist content in cyberspace, many participants preferred to monitor the online activities of terrorists and exploit them for intelligence and law enforcement purposes. Some participants also noted that allowing terrorist websites to remain operational provided an opportunity to influence the discussion in online forums,and use them as avenues for countering terrorist narratives.

(*f*) A number of projects had been undertaken in this field and several were presented at the CTITF Expert Workshop. For

example, in 2009, Interpol launched a new unit known as "Monitoring Assessment and Partners" (MAP) whose goal was to monitor terrorist websites and disseminate any valuable information uncovered to national police forces around the world. Certain governments had also initiated their own specialized efforts, including the Federal Republic of Germany which had established its "Joint Internet Centre" (Gemeinsames Internetzentrum—GIZ), a multi-agency effort to gather information on terrorist activities in cyberspace. In addition, in May 2007, the European Union's European Police Office (Europol) established a secure online portal known as "Check the Web" which allows police officials to share data uncovered online on individual terrorists and terrorist organizations.[47] The secure site is available to police services in all 27 EU member states and includes links to monitored websites, as well as to a database of police officials with expertise in examining these sites, including their language capabilities and technical expertise.[48]

E. Social Networking

29. Social networking sites, such as Facebook, YouTube, Myspace, Bebo, Hi5, Habbo, Orkut, Badoo, QZone, Renren and Twitter are experiencing massive increases in membership worldwide.[49] Facebook alone has over 500,000,000 members.[50] Social networking services such as these are used by all age groups, but younger people tend to use them at a much higher rate.[51] Research indicates that social networking sites, leveraged by tech-savvy terrorist organizations, have a particular appeal among this demographic, and groups associated with Al-Qaida have made clear their intention to use social networking to spread their message.[52] By some estimates, nearly 90 per cent of online terrorist activity takes place using some form of social networking tools, whether independent bulletin boards, Paltalk or Yahoo Groups.[53, 54]

30. A U.S. Department of Homeland Security report from late 2010 uncovered numerous cases of suspected terrorists sharing operational data in multiple languages on social networking sites, such as

methods for building improvised explosive devices (IEDs).[55] Social networking services have all the features of standard websites, and more, allowing terrorists to use them for propaganda, training, recruitment, fund raising, secret communication, data mining and radicalization. Some terrorist groups, however, remain suspicious of social networking sites such as Facebook, and have specifically warned fellow extremists to avoid organizing on the site for fear of detection.

31. In a prescient October 2008 report, one country's military intelligence officials noted the possibility for terrorists to exploit microblogging sites such as Twitter, to aid them in conducting real-time terrorist operations.[56] Just one month later a group of terrorists attacked numerous locations in Mumbai, India, and used all the advanced information technologies available to them in an attempt to gain an operational advantage over police, the military and their victims. As well as using Google Earth satellite imagery and handheld GPS devices to plan and perpetrate their attack,[57] reports indicate that they received live updates from their handlers on their Blackberry mobile phones with regard to the location of hostages, especially foreigners.[58] The Mumbai attacks were also noteworthy for the vast use of social media by the public to document the event. Almost immediately thousands of Twitter "Tweets" began to describe what was happening; photos of the incident were posted on Flickr; a live map of affected areas was generated on Google Maps, and a Wikipedia page dedicated to the attack was published and updated in near real time.[59, 60] The level of tactical detail, including photographs and location data, provided instantaneously by members of the public could have greatly assisted the attackers. Concerned about that possibility, a Tweet was posted: "Indian government asks for live Twitter updates from Mumbai to cease immediately. ALL LIVE UPDATES —PLEASE STOP TWEETING."[61]

32. Social networking services can provide significant intelligence to terrorists in cyberspace. Users freely share vast amounts of personal information in social networking spaces making it easy to find many targets of interest, such as the names of diplomats working at an

embassy, as well as their pictures and those of their spouses and children. In response, numerous governments, especially military officials, have issued warnings to their personnel to be circumspect concerning data they reveal on Facebook, Twitter, and other networks.

33. Countermeasures and opportunities: Just as social networks provide rich target data to potential terrorists, so too can they yield numerous leads for law enforcement and security officials. Terrorists who participate in social media sites subject themselves to potential social network analysis techniques in which an entire network of friends, family and contacts can be mapped out by officials for identification,[62] providing a powerful tool in the fight against terrorism, especially when used in combination with large data sets of terrorist Internet activity such as Europol's "Check the Web" project or the University of Arizona's "Dark Web" program. Moreover, governments can also leverage social media to their advantage as a means of delivering a counter narrative to the terrorist and extremist ethos, as does one noted program in Indonesia.[63]

F. Fundraising & Alternative Payment Systems

34. The Internet has provided terrorists new ways of raising, spending and hiding money. Terrorists use a variety of techniques to raise funds online for their extremist activities. Following a popular business trend, many have turned to e-commerce, selling CDs, DVDs, T-shirts and books as a means of raising cash.[64] An even easier approach is merely to "accept donations" and many terrorist organizations have added links to their sites which advise visitors how to donate funds electronically via bank transfer (IBAN, SWIFT and BIC account numbers provided), via credit card or even by PayPal.[65] Many terrorist organizations also create so-called "charitable organizations" through which they solicit funds promising to use the money to feed and cloth the poor, though their true intent is to use the money to fund acts of violence.[66] Increasingly, many social networking services, such as Facebook, Myspace and Youtube also allow charities to raise and solicit funds via their sites.[67] Moreover, the new trend in mobile software applications (apps) for cellular telephones

has not gone unnoticed by charities and there are numerous charity apps available for download or as plug-ins for social networking sites.[68] Several terrorist organizations are already using social networking applications as the latest method for raising money for their activities.

35. Cybercrime as a means of fundraising. There is substantial evidence that terrorist organizations are using the proceeds from traditional cybercrime, such as online credit card fraud, identity theft and telecommunications fraud to fund their operations. Even in the dawn of the Internet revolution, terrorists were exploiting technology as a means of fundraising. In one early case from 1997, the Tamil Tigers compromised a computer system at Sheffield University in England and captured the user IDs and passwords of faculty members. They then used the compromised accounts to send out messages asking donors to send money to a charity in Sri Lanka.[69] In another case, according to the U.S. Federal Bureau of Investigation, a terrorist cell based in Spain with ties to Al-Qaida used stolen credit cards for numerous purchases of logistical items for the cell.[70] They also reportedly used stolen telephone and credit cards to communicate with affiliated groups in Pakistan, Afghanistan and Lebanon. Terrorists also use phishing scams to defraud innocent parties into providing their credit card details. In another documented case from 2003, an email arrived in a victim's inbox advising her to update her eBay account information. Upon doing so, the victim unwittingly provided credit card details to an Al-Qaida affiliate in the UK, Tariq al-Daour, who committed fraud with the card. Al-Daour later pleaded guilty to a terrorism charge of using the Internet to incite murder.[71] As noted previously in section 4.1 of this report, the terrorist bombings in Bali were also funded partially via online credit card fraud.[72] For further examples of cybercrime funding terrorist activities, see "Terrorist Financing and the Internet" in Studies in Conflict & Terrorism.[73]

36. Money Laundering and Alternative Payment Systems: Emerging technologies are also making it easier for terrorists to hide and move money around the world. Though unsubstantiated, news reports have indicated that terrorists may be using online gambling sites as a means

of laundering funds.[74] Another terrorist technique for transferring and laundering money discussed by participants was the exploitation of stored-value cards which were anonymous, untraceable, reusable and universally accepted. These cards could be transported across borders, with little difficulty and settlement was instantaneous, without any required intermediary. Participants also expressed concern regarding the potential abuse of emerging payment systems, such as mobile phone payments (m-pay), which could also potentially facilitate terrorist financing and money laundering.[75]

37. Countermeasures and opportunities: While the Internet and alternative payment systems made it easier for terrorists to fundraise, commit crimes and launder funds, participants also noted that at least some of these activities leave behind valuable clues that could be exploited by law enforcement. By bringing terrorist finance online and away from more traditional systems, such as Hawala, there was the potential for greater transparency in these financial transactions.[76] That said, many of the new forms of payment and money remain unregulated by international authorities and thus often remain difficult to detect.

G. Tactical Communications

38. Emerging technologies were making it easier and cheaper for terrorists to communicate and increasingly difficult for authorities to monitor these communications for public safety reasons. Email, chat rooms, mobile phones, SMS, VoIP, social networks, virtual worlds and micro-blogging sites were creating enormous volumes of communications data, allowing terrorists to hide among the noise. In addition to the numerous communications protocols themselves, there was a significant proliferation of devices: conversations could take place on cell phones, laptop computers, computing tablets, consumer electronics and gaming devices, many of which were obtained without providing any subscriber information. Mobile phone usage had climbed to nearly 4.6 billion subscriptions at the end of 2010,[77] and some predictions suggest that the number of Internet-connected devices will top 50 billion by 2020.[78] While the overwhelming

majority of these devices will be used for peaceful and legal purposes, the sheer volume of alternative places and methods that terrorists can use to communicate with one another will continue to present a significant challenge.

39. Given the online communication options, terrorists may achieve a significant level of operational security by limiting their interaction to cyberspace. To protect their identities and security online, terrorists have developed an elaborate layered security approach to ensure only trusted and vetted individuals are admitted. While the general public can visit many terrorist related websites, those seeking to volunteer or support the "cause" are directed to more secure chat-rooms. After proving themselves in these secured spaces, they may eventually be granted access to an even more select and vetted forum. The process continues on and on, frequently with required recommendations from trusted members of a terrorist cell for participation. Naturally, only vital operational issues are discussed in the most secured spaces, posing a challenge for law enforcement officials hoping to infiltrate these virtual communities.

40. Countermeasures and opportunities: In theory, less person-to-person communication and more online communication might provide authorities with additional opportunities to detect and respond to terrorist activities. As noted previously, however, the sheer volume is overwhelming and provides a significant challenge to timely analysis. Participants noted that there was great opportunity for member states to leverage communications technologies to allow for better information sharing amongst governments, NGOs and the private sector in an effort to improve data sharing among the parties.

H. Unlawful Access to a Computer System/"Hacking"

41. Many incidents have shown that terrorist groups are capable of utilizing hacking skills, to gain unauthorized access to the information systems of others. Software vulnerabilities, poorly chosen passwords and social engineering techniques provide ample opportunity for terrorists to attack the confidentiality, integrity and authenticity of data systems. One such terrorist-hacker, Younis Tsouli, was arrested

by British authorities in October 2005.[79] Tsouli hacked under the pseudonym/online name "Irhabi007," Arabic for terrorist 007. Tsouli used his hacking skills to break into university and government systems around the world, posting terrorist content, such as beheading videos, on the websites of unwitting parties, such as the State of Arkansas, in the United States. Moreover, Tsouli actively taught others the art of hacking as well as provided information to terrorists on how to maintain their own information security and anonymity online. He posted a training seminar on hacking websites to the "Ekhlas" forum and provided details on dozens of vulnerable websites that others could hack to further various terrorist purposes. While it might be easy to dismiss Tsouli as a mere "geek" or computer specialist, in fact, he was actively engaged in a variety of real world terrorist activities and was lauded by Abu Musab al Zarqawi, then the leader of Al-Qaida in Iraq, as an essential fighter for the cause. Ultimately he was charged by police in the UK with offenses including conspiracy to murder, conspiracy to cause an explosion, conspiracy to obtain money by deception and offences relating to the possession of articles for terrorist purposes and fundraising.

42. The tools: Terrorist hackers have access to the same toolset as other members of the hacker underground. The terrorists often do not require high levels of sophistication to be successful. They need not develop their own software attack tools, but can merely use the tools created and freely shared by others. These include a wide variety of computer viruses, Trojans, worms, sniffers, spyware, keystroke loggers, network vulnerability analyzers and rootkits.[80]

43. The purpose: Terrorists engage in hacking activities for a wide variety of reasons, including committing cyber crime for financial gain, to vandalize the pages of others for the purposes of propaganda, to host media-rich content on the servers of others without cost and to destroy the data of perceived enemies. In addition, hacking the systems of others can provide valuable insight into a target in the lead-up to a real-world kinetic attack.

44. Hacktivism: This word is an amalgam of the terms "hacking" and "activism" and takes a variety of formats, such as the defacement of

targeted websites or blocking their access by the general public.[81] These types of attacks, though not particularly high-level or terrorist in nature, can cause significant disruption and embarrassment to the affected party. Hacktivism has often been called politically motivated cybercrime and has occurred often in regional political disputes.

45. The Insider Threat: Hacking need not occur over great distances via the Internet, but can also be accomplished by trusted insiders as well. There are documented cases of terrorists or their affiliates obtaining trusted positions within organizations and using their access to facilitate unauthorized activities. One such example occurred when members of the Japan-based Aum Shinrikyo cult—the same group that was responsible for the gassing of the Tokyo subway in 1995—obtained a sub-contract to provide technical support to the Tokyo Metropolitan Police Department. Their insider status gave them access to sensitive data and could have been further exploited to violate the integrity of police databases.[82]

46. Countermeasures and opportunities: Given the current level of insecurity in today's information systems, participants assessed that terrorists would continue to employ hacking techniques well into the future. Yet, as terrorists themselves began to rely increasingly on information and communications technologies, there were opportunities for government authorities under the appropriate rule of law to gain remote access to terrorist information systems as well. In addition, relevant competent authorities could also use computer "honeypots" to detect terrorist hacking methods and use the knowledge to improve computer security, particularly in high-value information systems.[83]

I. Botnets/Computer Network Attacks

47. While terrorists have demonstrated their abilities to gain unauthorized access to individual computer accounts or even into multiple computer hosts, there is potential for them to do significantly greater damage through the "weaponization" of information systems. A widespread computer network attack could disrupt, deny,

degrade, manipulate or destroy any information resident on a target computer network, or even the entire network itself. As nations around the world have come to rely upon information systems for their daily survival, an attack against these systems could have devastating effect. In particular, critical information infrastructures—such as energy, water supply, telecommunications, government and emergency services, health care and banking—would make attractive targets for any terrorists intent on doing serious and widespread damage.[84] While much attention has been paid to a wide scale critical infrastructure attack, none has occurred to date. That said, there have been many reported incidents of isolated, non-terrorist attacks against specifically targeted critical infrastructure.

48. The "Botnet" Threat: Botnets, or "Bot Networks," are made up of vast numbers of compromised computers that have been infected with malicious code, and can be remotely-controlled through commands sent via the Internet.[85] Tens or even hundreds of thousands of these infected computers can be controlled and directed to disrupt or block Internet traffic for targeted victims.[86] Botnets are also commonly used to distribute spam, viruses and other forms of malicious computer code and are the tool of choice for transnational cybercriminals in the digital underground. Botnets work by inundating targeted computers with hundreds of thousands of requests for information, more requests than could possibly be handled, in so called "distributed denial of service" (DDOS) attacks, thereby preventing access by legitimate users.[87]

49. Attacks Against Nation States—The Case of Estonia: In the Spring of 2007, a massive botnet attack took place in which government and private sector computer systems in Estonia became widely unavailable.[88, 89] In the early days of the cyber attack, government websites that normally receive around 1,000 visits a day reportedly were receiving 2,000 visits every second and according to the Estonian Defence Minister, more than one million computers worldwide were engaged in the attack.[90] The Estonia case was notable as it represented a significant paradigm shift in offensive cyber operations: though the nation was clearly being attacked, it was not clear whether the attack was a case of cyber crime, cyber terrorism or cyber warfare due to

a lack of decisive attribution techniques. What is clear, however, is that a determined individual or group of individuals can have a significant disruptive effect on the national critical infrastructures of a nation state.

50. Attacks for Rent: One of the key features of botnet attacks is that one need not build or own the botnet in order to mount an attack. Botnets are widely available for rent in the digital underground at rates from $200-300 US per hour, making them available to even the poorest terrorist organization.[91] The price of a botnet increases significantly with its size, for example, the Shadow botnet, created by a 19 year old hacker from the Netherlands comprising over 100,000 infected computes, was put on sale for $36,000 US.[92] The wide availability to terrorists and criminals of this attack mechanism allows them to cause significant damage with limited resources and without the need to own any of the attack vehicle. Rather, through the clever insertion of malware, they can get innocent parties to attack one another by focusing the force of a botnet against an intended target.

51. SCADA/Industrial Control System Vulnerabilities: Supervisory Control and Data Acquisition (SCADA) systems are the computers that monitor and regulate the operations of most critical infrastructure sectors such as power generation and water delivery. SCADA systems automatically monitor and adjust switching, manufacturing, and other process control activities, based on digitized feedback data gathered by sensors.[93] SCADA systems are computers that control physical things, such as the pressure levels in a pipeline or whether or not a dam is open or closed. While many of these systems use older, proprietary technologies, they are increasingly being connected to the Internet, thereby providing terrorists a potential avenue of attack against critical information infrastructures. SCADA attacks are not theoretical; they have already occurred. For example, in 1997, a hacker was able to access the communication systems at the airport in Worcester, Massachusetts, in the United States, disrupting telephone service to the airport control tower and disabling the ability of approaching aircraft to turn on the runway landing lights.[94] In another instance, a former employee of an Australian

waste management utility accessed the computer systems of the utility to release thousands of liters of raw sewage in Queensland, destroying both flora and fauna and causing evacuations of the general public.[95] Not surprisingly, terrorists are also exploring attacks against SCADA and other critical infrastructure systems. For example a computer seized at an Al-Qaida office in Kabul, Afghanistan, contained models of a dam, made with structural architecture and engineering software that enabled the planners to simulate its catastrophic failure. The U.S. Federal Bureau of Investigation has uncovered numerous instances of Al-Qaida conducting online target research and surveillance on emergency telephone systems, electrical generation and transmission plants, water storage and distribution facilities, nuclear power plants and gas storage networks.[96]

52. Countermeasures and opportunities: Counter measures for DDOS and botnet attacks are difficult to achieve, especially as perpetrators adjust their methods of operation. For example, first generation botnets organized themselves with central command and control locations, allowing security officials to go after a central node and potentially disarm the botnet. In response, botnet criminals adjusted their operations and migrated towards "peer-to-peer" botnets, which due to their decentralized architecture, were much more resilient against mediation efforts undertaken by security officials.[97] Participants again raised the issue of possibly "hacking-back" as a means of responding to botnet attacks. Yet as noted elsewhere, the practice is complicated by the difficulty of correct attribution of the source and because most of the machines in the botnet are unwitting and unwilling participants in the attack.

J. Emerging and Future Technologies

53. This report has focused on technologies that are widely used today and those that have already been exploited, at one level or another, by terrorists. Participants in Redmond, however, noted that technology is far from static; in fact its development proceeds at an exponential pace. While these technologies may be distributed unevenly around the world, the trend is for them eventually to be accessible to a broad

section of the global population, as may be seen in the enormous growth in mobile telephony. Coming developments in robotics, genetic engineering, virtual reality, cloud computing, nanotechnology and artificial intelligence, to name a few, will likely effect the way of life of large numbers of people in the 21st century.[98]

54. Virtual Worlds: Advancing developments in virtual reality have been cited often as of potential value to terrorists, whether using virtualized 3D versions of buildings and cities to practice and rehearse their operational plans or as a means of communication. The same could readily be said of many online gaming systems and massively multiplayer online role-playing games (MMORPGS).[99] While the extent of the threat has been debated, many see the potential for abuse, with the United States Congress holding public hearings on Al-Qaida's reported use of "Second Life."[100] In 2007, the director of Australia's High Tech Crime Centre (AHTCC) noted that terrorists can gain training in games such as World of Warcraft in a simulated environment, using weapons that are identical to real-world armaments.[101] The AHTCC director further noted a new form of "terrorism" in which new terrorist organizations, such as the "Second Life Liberation Army," were being created in purely virtual worlds to combat a whole new set of perceived grievances. Thus virtual "terrorist organizations" have been established to throw virtual bombs at virtual buildings—causing real damage to virtual code.[102] While the extent of the risk from virtual world terrorist activities is debated, the vast growth of virtual economies (those selling purely virtual goods and services) is agreed to be valued at a minimum $5 billion US annually.[103] Virtual worlds often have their own virtual currencies such as Linden dollars, QQ coins and World of Warcraft gold which are openly traded (with little or no regulation) in exchange for hard currencies such as the Renminbi, Pound or Euro.[104] Given the opportunities, it would not be surprising to see terrorists in the future exploiting new forms of money for the purposes of fundraising, terrorist finance and money laundering.[105]

55. Robotics: Though once the province of science fiction, robots are increasingly appearing in various contexts around the world. There

are robots that help care for elderly people in Japan, robots that vacuum the floors in houses in the United States and robots that kill terrorists around the world. In fact, many military services have embraced robotics and there are thousands of ground-based robots systems and unmanned aerial vehicles (UAVs) on patrol in combat or post-war environments.[106, 107] These machines are well-armed, lethal and have killed hundreds. As robots continue to proliferate in society, participants assessed they could potentially become yet another technological attack tool for terrorists. In a recent article on robotics and crime, authors demonstrated numerous examples of organized crime groups using home made robots to commit a variety of offenses, including drug smuggling.[108] YouTube is replete with hobbyists showing home made robots that perform elaborate tasks such as tracking and shooting people with paint balls or water pistols—a pastime ideal for terrorist adaptation. iPhone controlled micro-UAVs could be built for very small sums of money and readily fly over any crowd to deliver a biological, chemical or explosive device.[109] Unfortunately, terrorist interest in robotics is not merely theoretical: in December 2009, terrorists were able to hack into sophisticated American military UAVs as they patrolled the skies over Iraq.[110] Incredibly, they were able to do so with a piece of software they purchased on the Internet for a mere $26 US. The software allows terrorists to intercept video feeds emanating from the classified Predator drones, though apparently does not give them control over the device's weapons systems (at least, not yet).

56. Countermeasures and opportunities: Technology is constantly on the march, with newer and cheaper devices being introduced all the time. As such, it is not surprising that terrorists will attempt to use them in novel and innovative ways. Responsible authorities will have to remain vigilant to these developments and study their potential terrorist abuses for planning and contingencies purposes. If not, nation-states may be caught off-guard by a new and unexpected application of technology that could cause serious public harm.

Conclusions and Recommendations

57. Technology proves to be a double-edged sword in the fight against terrorism. Terrorists have realized its potential and use technological tools for their communications, training, propaganda, recruitment, fundraising and operational planning. Conversely, government security and law enforcement officials can leverage these tools as well to gain greater insight into terrorist activities.

58. Privacy and Human Rights: As more and newer electronic devices enter our lives, they have the potential to be a great force for good as well as for harm. Proliferating and ubiquitous mobile phone, CCTV systems, RFID tags, location-based services, laptops, i-tablets, wireless gaming systems, smart-roadways, GPS enabled cars and electronic financial transactions can provide near-universal situational awareness for those capable of leveraging these technologies to their advantage. Participants believed it important to ensure a balance between human rights and public safety in the use and exploitation of these tools, with vigorous and open public debate.

59. Public Private Partnerships: Given that the majority of the infrastructure that underpins global information and communication systems is owned and managed by the private sector, governments should consider partnering with the private sector in formulating strategic responses to the terrorist threat. Participants from both government and the private sector noted that national governments often asked for information and assistance from the private sector, but shared precious little information in return. Hence, governments may wish to consider exploring opportunities to improve information-sharing, both between the public and private sectors and with relevant non-governmental/research organizations. This is particularly an issue as more and more civil society institutions develop expertise in penetrating terrorist chat rooms and tracking the online activities of terrorists in cyberspace. Some participants suggested considering a broader strategy in combating terrorist use of technologies, to include a public health model employed by entitles such as the World Health Organization—one where information is shared among all parties, public and private, rich and poor to ensure

that attacks against our common global information infrastructure are limited in frequency and severity.[111]

60. A Multi-Pronged Approach: Terrorists have considerably updated their modus operandi to leverage technology to their full advantage. While the purpose of this report has been to address technical issues in countering terrorist use of the Internet, technology alone will not solve this problem. Even when the right technical tools are in place, further human analysis is required to respond to terrorist activity in cyberspace. For these reasons, a multi-pronged approach will undoubtedly be required to deal with terrorist use of the Internet. As noted in other CTITF research studies, there is a critical need for international law and public policy to respond to an ever-evolving terrorist threat. Moreover, technical and legal approaches should be combined with effective counter-narratives aimed at discrediting terrorist rhetoric and countering the appeal of terrorism altogether (see Report on the CTITF Conference on Counter-Narratives of February 2011 for more detail[112]). In order to counter the use of the internet for terrorist purposes more effectively, governments may wish to consider an approach that combines legal, technical and ideological components.

Endnotes

1 See http://www.php.net/ for further.

2 http://www.w3schools.com/asp/asp_intro.asp

3 http://www.apl.jhu.edu/~hall/java/Servlet-Tutorial/Servlet-Tutorial-Overview.html

4 Jialun Qin et al., "Analyzing Terror Campaigns on the Internet: Technical Sophistication, Content Richness and Web Interactivity," International Journal of Human-Computer Studies, November 1, 2006, vol. 65, p.71–84.

5 Brian Krebs, "Three Worked the Web to Help Terrorists," The Washington Post, July 6, 2007, p. D01. http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501945.html.

6 http://news.discovery.com/tech/internet-fraud-finances-terrorism.html.

7 http://en.wikipedia.org/wiki/Carding.

8 http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html.

9 "Terrorists Launch Google Guide," The Jawa Report, November 29, 2006

10 Harding, T. (2007), "Terrorists 'Use Google Maps to Hit UK Troops' The Telegraph Online, available at: http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/01/13/wgoogle13.xml.

11 http://news.cnet.com/8301-10784_3-9725253-7.html.

12 http://www.telegraph.co.uk/news/worldnews/asia/india/3691723/Mumbai-attacks-Indian-suit-against-Google-Earth-over-image-use-by-terrorists.html.

13 McCullagh, Declan, 'Military Worried About Web Leaks.' CNET News 16 January 2003, available at: http://news.com.com/2100-1023-981057.html.

14 See "Dot-Com Terrorism," The New Atlantis, Number 5, Spring 2004, pp. 91–93, available at: http://www.thenewatlantis.com/publications/dot-com-terrorism.

15 http://www.guardian.co.uk/world/2010/nov/28/how-us-embassy-cables-leaked.

16 Weimann, G. (2004b). How Modern Terrorism Uses the Internet, Special Report (United States Institute of Peace), 116.

17 Brunst, P., "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet," in A War on Terror? : The European Stance on a New Threat, Changing Laws and Human Rights Implications," 2009.

18 Peter Steiner, page 61 of July 5, 1993 issue of The New Yorker, (Vol.69 (LXIX) no. 20).

19 http://en.wikipedia.org/wiki/IP_address.

20 See http://www.i2p2.de/ and http://www.torproject.org/ as examples.

21 For information on proxy servers and how they work, visit: http://windows.microsoft.com/en-US/windows-vista/What-is-a-proxy-server.

22 http://computer.howstuffworks.com/cloud-computing.htm.

23 See for example, Scott Charney "The Evolution of Online Identity," IEEE Security and Privacy, vol. 7, no. 5, pp. 56–59, Sep./Oct. 2009.

24 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

25 For an introduction to encryption techniques, visit http://www.washingtonpost.com/wp-srv/politics/special/encryption/encryption.htm.

26 http://www.fas.org/irp/congress/1998_hr/s980128f.htm.

27 Ibid.

28 Available at www.hushmail.com.

29 A detailed overview of the techniques employed was reported by the Wall Street Journal and is available at: http://online.wsj.com/article/SB10001424052748704570104576124231820312632.html.

30 Brunst, P., "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet," in A War on Terror? : The European Stance on a New Threat, Changing Laws and Human Rights Implications," 2009.

31 Sedarat, F., "Jihadi Software Promises Secure Web Contacts," Reuters Online, 2008, available at: http://www.reuters.com/article/2008/01/18/us-internet-islamists-software-idUSL1885793320080118.

32 http://www.usatoday.com/tech/news/2001-02-05-binladen-side.htm.

33 A description of steganography is available at: http://www.garykessler.net/library/steganography.html.

34 For a detailed overview on terrorist use of steganography, visit: http://www.sans.org/reading_room/whitepapers/stenganography/analysis-terrorist-groups-potential-electronic-steganography_554.

35 http://techcrunch.com/2010/08/04/schmidt-data/.

36 http://www.nytimes.com/2003/05/18/world/aftereffects-beirut-video-game-created-militant-group-mounts-simulated-attacks.html?pagewanted=all&src=pm.

37 http://www.nytimes.com/2006/06/25/books/review/25worth.html.

38 http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005.

39 http://ai.arizona.edu/research/terror/.

40 Conway, Maura. "Terrorist Web Sites: An Empirical Analysis" Paper presented at the annual meeting of the International Studies Association, Le Centre Sheraton Hotel, Montreal, Quebec, Canada, Mar 17, 2004, available at: http://doras.dcu.ie/504/.

41 Sedarat, F., "Jihadi Software Promises Secure Web Contacts, Reuters Online, 2008, available at: http://www.reuters.com/article/internetNews/idUSL1885793320080118.

42 For an in-depth discussion on the topic of government web filtering and various forms of censorship of Internet content, see Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace, by Deilbert R., MIT Press, 2010 and Access Denied: the Practice and Policy of Global Internet Filtering, by Deilbert, R, MIT Press 2008.

43 For further information, see: http://www.honeynet.org/papers/ff.

44 The full report is available at: http://gnso.icann.org/issues/fast-flux-hosting/fast-flux-initial-report-26jan09.pdf.

45 For an explanation of distributed denial of service attacks, visit: http://www.us-cert.gov/cas/tips/ST04-015.html.

46 http://www.usatoday.com/tech/news/computersecurity/2004-06-19-hackers-post-video_x.htm.

47 See http://www.europol.europa.eu/index.asp?page=news&news=pr091013.htm.

48 http://www.theregister.co.uk/2007/05/31/eu_web_terror/.

49 http://en.wikipedia.org/wiki/Social_network_service.

50 http://blog.facebook.com/blog.php?post=409753352130.

51 http://stakeholders.ofcom.org.uk/market-data-research/media-literacy/medlitpub/medlitpubrss/socialnetworking/summary/.

52 http://www.telegraph.co.uk/news/worldnews/3885367/Al-Qaeda-plans-to-wage-holy-war-on-Facebook.html.

53 http://www.washingtonpost.com/wp-dyn/content/discussion/2006/04/11/DI2006041100626.html.

54 For a detailed background on terrorist use of social networking services, see "Terror on Facebook, Twitter, and Youtube," in the Brown Journal of World Affairs, 2010 by Gabriel Weimann, available at: http://www.bjwa.org/article.php?id=E0957T6u4xbxptB39OxJir92zulpVddWGH9QInXI.

55 http://publicintelligence.net/ufouoles-dhs-terrorist-use-of-social-networking-facebook-case-study/.

56 http://www.wired.com/dangerroom/2008/10/terrorist-cell/.

57 http://www.washingtonpost.com/wp-dyn/content/article/2008/12/02/AR2008120203519.html.

58 http://www.telegraph.co.uk/news/worldnews/asia/india/3534599/Mumbai-attacks-Terrorists-monitored-coverage-on-UK-websites-using-BlackBerry-phones-bombay-india.html.

59 http://en.wikipedia.org/wiki/2008_Mumbai_attacks.

60 http://www.telegraph.co.uk/news/worldnews/asia/india/3530640/Mumbai-attacks-Twitter-and-Flickr-used-to-break-news-Bombay-India.html.

61 http://edition.cnn.com/2008/WORLD/asiapcf/11/27/mumbai.twitter/.

62 http://www.independent.co.uk/news/world/politics/terrorist-facebook-ndash-the-new-weapon-against-alqaida-1774041.html.

63 http://asiancorrespondent.com/28651/social-media-helps-indonesia-battle-terrorism/.

64 Brunst, P., "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet," in A War on Terror? : The European Stance on a New Threat, Changing Laws and Human Rights Implications," 2009.

65 http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005.

66 See http://www.un.org/terrorism/pdfs/CTITF_financing_ENG_final.pdf, chapter on Alternative Remittance Systems for further, Chapter 4, Section D.

67 http://www.guardian.co.uk/society/2010/nov/20/social-media-raise-funds-charities.

68 http://www.squidoo.com/top10facebookcharityapps.

69 Vatis, M., "Cyber Terrorism and Information Warfare: Government Perspectives," in Cyber Terrorism and Information Warfare, Y. Alexander and M. S. Swetnam, eds.

70 http://www.fbi.gov/news/testimony/financing-patterns-associated-with-al-qaeda-and-global-terrorist-networks.

71 http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501153_pf.html.

72 Alan Sipress, "An Indonesian's Prison Memoir Takes Holy War Into Cyberspace," Washington Post, December 14, 2004, p. A19.

73 Jacobson, Michael(2010) 'Terrorist Financing and the Internet', Studies in Conflict & Terrorism, 33: 4, 353–363, available at: http://pdfserve.informaworld.com/961630__919769800.pdf.

74 http://www.telegraph.co.uk/technology/4060727/Terrorists-launder-cash-through-online-gambling.html.

75 http://mashable.com/2011/04/06/mobile-payments-commerce/.

76 For an explanation of Hawala systems, http://www.interpol.int/Public/FinancialCrime/MoneyLaundering/hawala/.

77 http://www.itu.int/net/pressoffice/press_releases/2010/06.aspx.

78 http://gigaom.com/2010/04/14/ericsson-sees-the-internet-of-things-by-2020/.

79 http://www.washingtonpost.com/wp-dyn/content/article/2006/03/25/AR2006032500020.html.

80 Definitions of each of these terms are available at: http://arstechnica.com/security/news/2004/11/malware.ars

81 http://www.wired.com/techbiz/it/news/2004/07/64193..

82 http://news.bbc.co.uk/2/hi/asia-pacific/662172.stm.

83 For an explanation of honeypots, see http://www.sans.org/security-resources/idfaq/honeypot3.php.

84 For further information on critical infrastructure protection, see http://www.dhs.gov/files/programs/critical.shtm and http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm.

85 For an explanation of a botnet network, see: http://us.norton.com/theme.jsp?themeid=botnet.

86 "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," a Report of the U.S. Congressional Research Service, January 2008, http://www.fas.org/sgp/crs/terror/RL32114.pdf.

87 http://www.us-cert.gov/cas/tips/ST04-015.html..

88 http://www.nytimes.com/2007/05/29/technology/29estonia.html.

89 http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

90 http://online.wsj.com/public/article/SB117944513189906904-__3K97ags67ztibp8vLGPd70WXE_20070616.html.

91 Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," a Report of the U.S. Congressional Research Service, January 2008, http://www.fas.org/sgp/crs/terror/RL32114.pdf.

92 For an overview of botnet economics, see Kaspersky Lab's report on the topic available at: http://www.securelist.com/en/analysis?pubid=204792068.

93 "Botnets, Cybercrime and Cyberterrorism," p. 25.

94 http://www.justice.gov/criminal/cybercrime/juvenilepld.htm.

95 http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/.

96 http://www.ellen-bomer.com/Osama/Cyber-Attacks.html.

97 http://www.csoonline.com/article/216450/peer-to-peer-botnets-a-new-and-growing-threat-.

98 An overview of these emerging technological security threats is available at www.future-crimes.com.

99 http://en.wikipedia.org/wiki/Massively_multiplayer_online_role-playing_game.

100 http://virtuallyblind.com/2008/04/01/congress-virtual-worlds/.

101 http://www.theaustralian.com.au/news/features/virtual-terrorists/story-e6frg6z6-1111114072291.

102 http://www.foreignpolicy.com/articles/2008/02/19/terrorists_in_second_life.

103 http://news.bbc.co.uk/2/hi/technology/8425623.stm.

104 See https://www.virwox.com/ as an example of a virtual currency exchange house.

105 Wm. Mitchell L. Rev. 5159 (2008-2009) Funding Bin Laden's Avatar: A Proposal for the Regulation of Virtual Hawalas, by Landman, Stephen I.

106 http://www.wired.com/dangerroom/2011/02/1-in-50-troops-robots/.

107 http://en.wikipedia.org/wiki/Unmanned_aerial_vehicle.

108 See "The Coming Robot Crime Wave," in the IEEE's Computer Magazine, by N. Sharkey, M. Goodman and N. Ross, available at: http://www.computer.org/portal/web/computingnow/0910/whatsnew/computer.

109 http://www.wired.com/dangerroom/2009/08/new-use-for-your-iphone-controlling-drones/.

110 For further information, see http://online.wsj.com/article/SB126102247889095011.html.

111 See http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/internethealth.aspx as an example of application of a public health model to cyber security.

112 Available at http://www.un.org/terrorism/internet.shtml.

Report Editors

Richard Barrett, Coordinator, Monitoring Team of the 1267 Committee

Jan Neutze, Programme Officer, Counter-Terrorism Implementation Task Force Office

Principal Researchers

Marco Gercke, Director, Cybercrime Research Institute (Cologne, Germany)

Marc Goodman, Director, Future Crimes Institute (San Francisco, USA)

Report Contributors

CTITF members

Counter-Terrorism Implementation Task Force Office

Jean-Paul Laborde

Monitoring Team of the 1267 Committee

Jahyun Han

International Monetary Fund

Gianluca Esposito

United Nations Office on Drugs and Crime—Terrorism Prevention Branch

Jo Dedeyne

Cecilia Ruthstrom-Ruin

Counter-Terrorism Committee Executive Directorate

Syed Haider Shah

INTERPOL

Jacques Courteau

Alexander Lim

CTITF members (cont.)

Office of the High Commissioner for Human Rights

Anne Charbord

United Nations Interregional Crime and Research Institute

Francesco Candelari

Alma Pintol

United Nations Department of Public Information

Robert Neshovski

Janos Tisovszky

Other international organizations

Council of Europe (CoE)

European Union (EU)

North Atlantic Treaty Organization (NATO)

Organization for Cooperation and Security in Europe (OSCE)

Member States experts

Canada

Germany

India

Indonesia

Russian Federation

Spain

The Netherlands

Tunisia

USA

Private sector experts

Jamil & Jamil (Karachi, Pakistan)

Martins de Almeida - Advogados (Rio de Janeiro, Brazil)

McAfee

Private sector experts (cont.)

Microsoft
Symantec
Team Cymru
World Check

Academia and civil society

Center on Global Counterterrorism Cooperation (Washington, DC)
Cybercrime Research Institute, (Cologne, Germany)
Future Crimes Institute (San Francisco, USA)
Institute of Governance (Basel, Switzerland)
London School of Economics (London, United Kingdom)
Max Planck Institute for Foreign and International Criminal Law (Freiburg, Germany)
Moscow State University (Moscow, Russian Federation)
Pontifícia Universidade Católica, (Rio de Janeiro, Brazil)
University of Arizona (Phoenix, USA)

The Counter-Terrorism Implementation Task Force is grateful to the Governments of Germany and The Netherlands for their generous support of this project.