

Counter-Terrorism Implementation Task Force (CTITF)

**Report of the Working Group on
Countering the Use of the Internet for Terrorist Purposes**

February 2009

Table of Contents

Table of Contents	1
Executive Summary	2
Introduction	3
Framing the issue	4
Specific concerns	5
<i>i. Cyber-attacks</i>	<i>5</i>
<i>ii. Fundraising</i>	<i>5</i>
<i>iii. Training</i>	<i>5</i>
<i>iv. Recruitment</i>	<i>6</i>
<i>v. Secret communication</i>	<i>6</i>
<i>vi. Data mining</i>	<i>6</i>
<i>vii. Propaganda</i>	<i>6</i>
<i>viii. Radicalization</i>	<i>7</i>
Analysis of measures for countering the use of the Internet for terrorist purposes	7
<i>i. Use of the Internet to perform terrorist attacks by remotely altering information on computer systems or disrupting the flow of data between computer systems</i>	<i>8</i>
<i>ii. Use of the Internet as an information source for terrorist activities</i>	<i>13</i>
<i>iii. Use of the Internet as a means for disseminating content relevant to the advancement of terrorist purposes</i>	<i>15</i>
<i>iv. Use of the Internet as a means for supporting communities and networks dedicated either to pursuing or supporting acts of terrorism</i>	<i>22</i>
The Internet as a tool to counter the spread of terrorism	27
Protecting human rights	31
Conclusions and Recommendations	32
ANNEX I: INFORMATION SOURCES	36

Executive Summary

The Internet is a distinctively global medium. It has the potential to bring communities together, ensure equal access to information, and empower populations; yet at the same time it provides a platform for mal-doers to advance their criminal goals and engage in and organize terrorist acts. In the Global Counter-Terrorism Strategy, adopted in September 2006, Member States pledged to ‘coordinate efforts at the international and regional level to counter terrorism in all its forms and manifestations on the Internet’ and to ‘use the Internet as a tool for countering the spread of terrorism, while recognizing that States may require assistance in this regard,’ and with the requirement that they do so ‘with due regard to confidentiality, respecting human rights and in compliance with other obligations under international law.’ This report was drafted by the Working Group on Countering the Use of the Internet for Terrorist Purposes which is one of the nine Working Groups of the United Nations Counter-Terrorism Implementation Task Force (CTITF), which aims to provide a common, coherent and focused counter-terrorism framework for entities of the United Nations system.

The Report presents an overview of approaches taken, primarily by Member States, towards countering use of the Internet for terrorist purposes. It suggests all uses of the Internet for terrorist purposes can be classified according to four basic types of Internet use: (1) Use of the Internet to perform terrorist attacks by remotely altering information on computer systems or disrupting the flow of data between computer systems; (2) Use of the Internet as an information source for terrorist activities; (3) Use of the Internet as a means for disseminating information relevant to the advancement of terrorist purposes and (4) Use of the Internet as a means for supporting communities and networks dedicated either to pursuing or supporting acts of terrorism. The latter two are the areas in which terrorism and the internet appear most obviously to convert into a distinct, new phenomenon, which may require specific types of counter-strategies.

The paper gives special attention to the use of counter-narratives on the Internet and to protecting human rights. It concludes by suggesting some ideas for future UN work in this area. These include:

- Facilitating Member States sharing best practices
- Building a database of research into use of the Internet for terrorist purposes.
- Conducting more work on countering extremist ideologies that are spread through the Internet.
- Explore the added value, viability, and desirability of creating international legal measures aimed at limiting the dissemination of terrorist content on the Internet.
- Fostering partnerships with the private sector and industry. These non-traditional stakeholders play an important role in protecting data and developing safeguards, and in establishing standards of acceptable content.

Introduction

1. The Internet is a distinctively global medium. The unique way in which it has developed as a free and open resource, for the common benefit of humanity, is the source of both its strength and weakness. It has the potential to bring communities together, ensure equal access to information, and empower populations; yet at the same time it provides a platform for mal-doers to advance their criminal goals and engage in and organize terrorist acts.

2. In the Global Counter-Terrorism Strategy, adopted in September 2006, Member States pledged to ‘coordinate efforts at the international and regional level to counter terrorism in all its forms and manifestations on the Internet’ and to ‘use the Internet as a tool for countering the spread of terrorism, while recognizing that States may require assistance in this regard,’ and with the requirement that they do so ‘with due regard to confidentiality, respecting human rights and in compliance with other obligations under international law.’

3. The Working Group on Countering the Use of the Internet for Terrorist Purposes is one of the nine Working Groups of the United Nations Counter-Terrorism Implementation Task Force, which aims to provide a common, coherent and focused counter-terrorism framework for entities of the United Nations system. The Working Group has sought to establish what instruments (laws and conventions), programmes, and resources have been dedicated to countering the use of the Internet for terrorist practices. Information has been collected at a national, regional and international level, as well from industry, civil society and academia. Based on this information, the Working Group has sought to map existing practice and identify areas where future engagement may be necessary.

4. The aim of this report¹ is two-fold: a) to present an overview of approaches taken, primarily by Member States, towards countering use of the Internet for terrorist purposes; b) to propose an

¹ This report would not have been possible without the research, expert interviews, and careful analysis of Member States responses to the Working Group by Mr. Gilbert Ramsay of the University of St. Andrews. 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.

analytical framework appropriate for categorising the different aspects of the issue, and solutions that may be applicable. The report concludes by examining what further actions may be appropriate, particularly on the part of the United Nations.

Framing the issue

5. While there is as yet no internationally agreed definition of terrorism,² it is a matter of wide consensus that terrorism is not an ideology so much as a strategy of violent action. It is conceivable that an act of terrorist violence could be carried out by means of the Internet; however, thus far, terrorist violence is considered to be an offline activity. Terrorism is a means of communication; its purpose is not completed by the violent action itself, but rather through the wider message of intimidation transmitted to a public audience. Any act of terrorist violence is preceded by a sequence of events and actions, which being social rather than physical, can also occur by means of the Internet.³

6. For this reason, ‘use of the Internet for terrorist purposes’ is a complex term, which can describe a number of very different activities. Responses of Member States to the Working Group questionnaire confirmed this.⁴ Some focused almost exclusively on measures relating to cyber-security and cyber-crime; others focused on measures for countering organizational and propagandistic uses of the Internet. Most described measures relevant to either terrorism or to cyber-security, with relatively few giving details of initiatives specifically relating to terrorism and the Internet.

7. From the responses provided by Member States to the Working Group, one important limiting factor to the discussion of the use of the Internet for terrorist purposes emerged. There appeared to be an overwhelmingly greater interest in what can be broadly referred to as ‘Al-Qaida-type’ terrorism

² The United Nations defines terrorism indirectly by relying on 16 international legal instruments for the prevention and punishment of terrorist acts. These define “terrorist acts.” (<http://www.un.org/terrorism/instruments.html>). For the diversity of legal definitions of terrorism internationally, see ‘The Definition of Terrorism’, a report to the UK Parliament by Lord Carlile of Berriew, presented by the Secretary of State for the Home Department, March 2007.

³ See Max Taylor and John Horgan, ‘A Conceptual Framework for Addressing Psychological Process in the Development of the Terrorist’, *Terrorism and Political Violence*, 18 (2006).

⁴ See Annex on “Information Sources”.

than any other form and manifestations of terrorist violence. This is also true in the academic field, which is heavily focused on Al-Qaida use of the Internet. Only two States referred to the maintenance of websites by terrorist organizations in general.

8. Al-Qaida-type terrorism is not the only type of terrorism that benefits from the Internet, nor is it the sole concern of Member States. Other terrorist organizations use the Internet, in some cases with a high degree of sophistication. Furthermore, there has been a rise in the incidence and severity of politically motivated cyber-attacks carried out on behalf of a range of religious and ethno-nationalist agendas, which while they may not constitute terrorism, are of increasing security concern.

Specific concerns

9. In the course of its consultation with Member States, the Working Group encountered a number of specific concerns:

i. Cyber-attacks

10. A large proportion of the overall material submitted to the Working Group related, broadly speaking, to the topic of cyber-security. However, only two States listed cyber-attacks by terrorists as one of the threats that concerned them.

ii. Fundraising

11. Four States specifically mentioned terrorist fundraising on the Internet as a concern. One state suggested that terrorist organizations raised funds by means of computer games and phishing, although it noted that this was not yet the case within the country itself. Another noted that it had found relatively little evidence of systematic fundraising. A number of other States implied that they considered this issue relevant by describing measures they were taking against it.

iii. Training

12. One State argued that the Internet was used 'extensively for training purposes'. According to another, the Internet was an important vehicle for 'indoctrination and training'. Definitions of what

constitutes 'training' on the Internet were not consistent, however. As one State pointed out, 'not all of the material available on the Internet is realistic, reliable or (safely) usable.'⁵ Experts indicate, for example, that this kind of material is far from sufficient to allow the commission of an attack.⁶ Other States framed the issue in terms of the dissemination of instructional materials.

iv. Recruitment

13. Six States expressed concern about the use of the Internet for terrorist recruitment. However, they differed in what they understood by this; for some, recruitment was closely associated with radicalization, and one suggested that 'interactive forms of recruitment' and 'self ignition' were the concern, suggesting a more 'bottom up' understanding of recruitment than normally assumed.

v. Secret communication

14. Three States mentioned secret communication among the most important uses of the Internet for terrorist purposes, though not necessarily at a high level of sophistication. Ordinary email, sent from publicly available computers in Internet cafes, was one example given of how terrorists communicate anonymously through the Internet.

vi. Data mining

15. Three States wrote that they considered data mining on the Internet to be an important use of the medium by terrorists or for terrorist purposes. The Al-Qaida terrorist manual captured in Afghanistan notes that 'using sources openly available, it is possible to gather at least 80 per cent of all information acquired about the enemy.'

vii. Propaganda

16. Concern over use of the Internet to transmit terrorist propaganda was a commonly expressed concern. In some state jurisdictions content that advocates violence is illegal; in others it is not. The radical ideology that caused most concern appeared to be that of Al-Qaida and its related

⁵ *Jihadis and the Internet*, A report by the Dutch National Counterterrorism Coordinator, p.83.

⁶ See Anne Stenersen, 'The Internet: A Virtual Training Camp?' *Terrorism and Political Violence*, 20:2 (2008).

organizations. Affiliated media foundations such as Al Sahab, Al Fajr and the Global Islamic Media Front were listed as key outlets for Al-Qaida propaganda, and a wide range of types of Al-Qaida-related material was identified.⁷ Another ideology mentioned in detail by one State was that of the extreme right. However, there was some question as to whether this material is best understood as terrorism or as cyber-hate.

17. There was little assessment of the extent to which terrorist propaganda on the Internet can inspire individuals to commit offline acts of terrorism. One State did observe, however, that there are known cases of individuals who claim to have been persuaded to undertake violent terrorist activities after reading online propaganda. Imam Samudra, who was responsible for the 12 October 2002 Bali bombings, was cited as an example.

viii. Radicalization

18. The issue of radicalization on the internet was addressed directly by only one State. Several others dealt with it indirectly, discussing the potential of the internet as a vehicle for recruitment and disseminating propaganda.⁸

Analysis of measures for countering the use of the Internet for terrorist purposes

19. The range of uses of the Internet mentioned by States suggests that there is no single, integrated approach possible to address the issue of ‘use of the Internet for terrorist purposes’. Professor Sieber of the Max Planck Institute in his legal and threat analysis for the Council of Europe *Cyber-terrorism: The Use of the Internet for Terrorist Purposes*⁹ draws a distinction between ‘terrorism-specific gaps’

⁷ One country, for example, provided the following typology: - Key sites consisting of the major official home pages of international, regional or national groups that adopt Al-Qaida ideology; - Distributors' sites include various web portals. These sites can be purely information sites with updated links to Al-Qaida-related web sites and debate groups such as Yahoo and PalTalk, or they may be sites consisting of information boards and registration boxes for electronic news letters; - Producers' sites consisting of web sites for various Al-Qaida-related media groups such as the Global Islamic Media Front.

⁸ The report of the CTITF Working Group on Addressing Radicalization and Extremism that Lead to Terrorism dealt at some length with the concerns of States regarding the issue of radicalization on the Internet. It is available at <http://www.un.org/terrorism/pdfs/Report%20of%20the%20Working%20Group%20-%20Workgroup%202.pdf>

⁹ *Cyber-terrorism - The use of the Internet for terrorist purposes*, 2008, Council of Europe.

and ‘Internet-specific gaps’. This suggests two possible approaches: what do terrorists (and supporters of terrorism) achieve using the Internet? Or, what special capabilities does the Internet give to terrorists? The Working Group has adopted the latter as it relates more closely to the issue of ‘countering’, by getting closer to the online source of the concern.

20. It is possible to group uses of the Internet for terrorist purposes under four main headings:

- i. Use of the Internet to perform terrorist attacks by remotely altering information on computer systems or disrupting the flow of data between computer systems;
- ii. Use of the Internet as an information source for terrorist activities;
- iii. Use of the Internet as a means for disseminating information relevant to the advancement of terrorist purposes; and
- iv. Use of the Internet as a means for supporting communities and networks dedicated either to pursuing or supporting acts of terrorism.¹⁰

21. While these categories can overlap, they provide a basis for considering what options are available in terms of countering the uses to which terrorists put the Internet.

i. Use of the Internet to perform terrorist attacks by remotely altering information on computer systems or disrupting the flow of data between computer systems

22. States and industry do not always speak the same language when it comes to examining terrorist threats on the Internet. States are more concerned about non-disruptive uses of the Internet by or for terrorists than they are about cyber-terrorism in its commonly understood sense.¹¹ The Internet industry, when the word ‘terrorist’ was mentioned, was often very eager to discuss issues such as cyber-attacks, malware, and similar threats. The reason for this may relate more to definition than to a genuinely different understanding of the threat. To the information technology industry, precise political considerations about the distinction between terrorists and other criminals are less important

¹⁰ Sieber’s approach, which focuses more on operational outcomes for terrorists, perceives three basic areas: cyber-attacks, dissemination of content and operational use.

¹¹ See, for example, Dorothy Denning, ‘Activism, Hacktivism and Cyber-terrorism: The Internet as a Tool for Influencing Foreign Policy’ in Arquilla and Ronfeldt ed. *Networks and Netwars, the Future of Terror, Crime and Militancy* (RAND: 2002).

than the practical issue of how best to protect the infrastructures upon which it bases its business. For States, however, distinguishing between cyber-crime in the broader sense and terrorist cyber-crime specifically is a matter of some importance.

23. Cyber-attacks certainly exist, and are a growing concern. Whether or not a cyber-terrorist attack has so far occurred depends very much on how it is defined. According to many academic definitions of cyber-terrorism and the approach to terrorism thus far enshrined in the sixteen international counter-terrorism instruments, any cyber attack qualifying as ‘terrorist’ would ultimately still have to cause damage in the ‘real world’: for example, by interfering with a critical infrastructure system to the extent of causing loss of life or severe property damage. However, as dependence on online data and services increases, an attack that resulted only in widespread interruption of the Internet could, in future, cause sufficient devastation to qualify as a terrorist attack. However, categorizing such attacks as terrorist remains controversial.¹² The damage resulting from such attacks, while potentially economically significant, but to date their impact has been more on the level of a serious annoyance. Extending the word ‘terrorist’ to such forms of activity therefore may risk overstretching the term.

24. Cyber-attacks for political purposes are technically no different from cyber-attacks for ordinary criminal purposes. Indeed, politically motivated cyber-attacks to date have not been particularly significant when compared with the worst attacks carried out by criminals for financial or personal reasons. However, politically motivated cyber-attacks are likely to differ in the scope of their targeting. The denial of service attack on Estonia in 2007 is an example of this. While, by volume of traffic, a far larger example of a denial of service attack is provided by an incident in which a company providing an anti-spam service was effectively destroyed by spammers, the victims were nonetheless relatively few. By contrast, in the Estonian case, the attackers succeeded in affecting news websites and online banking services used by a very high proportion of the population.¹³ In future, it is possible that a terrorist attack might take over the supervisory control and data acquisition system

¹² Martin Scheinin, the United Nations Special Rapporteur on Human Rights While Countering Terrorism holds that ‘crimes of cyber-terrorism need to be defined with the same precision as other forms of terrorist crime. There must be an intention and a real risk of causing death or serious bodily harm among members of the public, plus a terroristic intent, either to cause fear among the population or to compel the government to do or not to do something’.

¹³ ‘Hackers take down most wired country in Europe’, *Wired*, 21 August 2007.

(SCADA) of a major public utility, such as a power plant.¹⁴ Such a targeted attack would not correspond closely to current patterns of ordinary cyber-criminality but could make sense to a politically motivated attacker.

25. Finally, it is conceivable that terrorists could target the entire Internet. One way this could occur would be through an attack on the Internet's domain name system (DNS).¹⁵ The DNS is, in itself, extremely robust, since it is operated on thirteen separate root servers. However, one security expert within the Security and Stability Advisory Committee of the Internet Corporation for Assigned Names and Numbers (ICANN) suggests that there are other ways through which the servers are potentially vulnerable. For example, an attack on the routing system by which requests for IP addresses reach the servers would be difficult to recover from rapidly.

26. While many of the necessary measures required for addressing political (and potentially, terrorist) cyber-attacks are the same as those required for addressing cyber-crime in general, it appears that the threat of politically motivated cyber-attacks, and the possibility of terrorist cyber-attacks invite some distinct measures at the political level.

27. From a legislative point of view, one question is to what extent a definition of cyber-terrorism is required in order to recognize the threat such attacks could pose. Two States mentioned that they their legal codes formally defined 'cyber-terrorism', while a further three mentioned that terrorist intent could be considered for sentencing purposes in the context of any criminal activity carried out by means of the Internet. The two formal definitions provided differed significantly in the breadth of their understanding of what constituted the offence, suggesting that an important future consideration for States wishing to legislate against cyber-terrorism will be the arrival at a reasonable consensus as to what such an offence entails.

¹⁴ Recently, a security researcher succeeded in hacking into the control systems of a nuclear power plant. 'America's Hackable Backbone', Forbes, 22 August 2007.

¹⁵ This is the distributed system which enables computers to resolve verbal names (uniform resource locators or URLs such as www.un.org) into numerical Internet Protocol (IP) addresses for individual computer systems (in this case, 157.150.195.10). Readers who wish to gain a better understanding of how the DNS works are referred to 'The Domain Name System Explained for Non-Experts' in *Internet Governance: A Grand Collaboration* publication of the UN ICT Task Force, Series 5 <http://www.unicttaskforce.org/perl/documents.pl?id=1392>

28. Another issue relates to responsibility for coordinating preparation and response. Traditionally, most of the day-to-day work of providing cyber-security has been carried out by the private sector, and this will undoubtedly continue to be the case. Software companies play a key role in producing malware solutions, providing security products, researching and producing intelligence on the evolution of cyber-criminal threats, looking out for vulnerabilities, providing incident response capabilities and lobbying for better cyber-crime laws. However, as cyber-attacks are politicized, as government moves online, and as national citizens become increasingly dependent on services with an Internet dimension, the provision of cyber-security has become a matter of national interest as well. This may sharpen arguments for closer governmental supervision of industry self-governance on security issues.¹⁶

29. At the national level, therefore, States are increasingly beginning to take responsibility for overseeing the cyber-security of national critical infrastructure, even though much of this is in private hands. A number of States described measures that they were taking, in collaboration with the private sector, in this regard.

30. Since the Internet is a global entity there is, inevitably, a regional and international aspect as well. At present, the lack of uniform cyber-crime laws and agreed international procedures means that, in practice, such situations are handled by means of informal and personal arrangements. For example, in the case of the cyber-attacks on Estonia, aspects of the situation requiring international cooperation were handled through the trusted relationship between a handful of highly respected individuals and the attacking computers' ISPs.¹⁷ In computer emergencies there is often no obvious place to go for help.¹⁸

¹⁶ A recent report on American national cybersecurity has called for greater state supervision. See *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*.

http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf. However, there remains strong industry scepticism as to the value of more government intervention in the provision of cybersecurity.

¹⁷ This point was made in a discussion with Fred Baker and John Klensin at a meeting of the Internet Engineering Task Force in Dublin (June 2008).

¹⁸ These points were raised in the panel discussion 'The Dimensions of Cybersecurity and Cyber-crime: A Mapping of Issues and our Current Capabilities' at the December 2008 meeting of the IGF in Hyderabad. Panellists were Patrick Falstrom, Marc Goodman, Alexander Ntoko, Michael Lewis, Guishan Rai and Jayantha Fernando. Transcript available from http://www.intgovforum.org/cms/workshops_08/main_dimensions.html

Countering use of the Internet to perform terrorist attacks by remotely altering information on computer systems or disrupting the flow of data between computer systems

31. States, industry and academia overwhelmingly agree that the single most important political contribution to the fight against cyber-crime generally, and cyber-attacks by terrorists in particular, is the development and expansion of sensible, interoperable cyber-crime laws. Several organizations are working on this. The Council of Europe Convention on Cyber-crime has achieved wide acceptance as a model for international cyber-crime legislation, even beyond its immediate signatories.¹⁹ The International Telecommunications Union is building on its work by developing a cyber-law ‘toolkit’. A number of other organizations are working at the regional level to promote uniform cyber-crime laws, an example being the Gulf Cooperation Council, which has produced a model cyber-crime law intended particularly for Arabic States.

32. More specifically relevant to a possible cyber-terrorist attack, however, are attempts to build capabilities for protection of infrastructure and incident response at the regional and international levels. One of two recent examples is IMPACT, the International Multilateral Partnership Against Cyber Threats hosted in Malaysia. This initiative aims to perform a number of such functions, providing a worldwide forum for government and industry; an international incident response capability; cyber-security training, and security testing and certification. Another is the North Atlantic Treaty Organisation (NATO) Cyberdefence Centre of Excellence in Tallinn, Estonia, a research centre which aims to be able to provide security expertise to interested members of the Alliance. However these initiatives remain relatively embryonic. Other organizations have promoted discussion and collaboration between their members, such as the Association of Southeast Asian Nations (ASEAN), the Organization of American States (OAS) and the Shanghai Cooperation Organisation (SCO).

33. Despite positive steps forward, any progress towards international institutions for cyber-security will necessarily be gradual. At present critical cyber-incident management at the global level depends

¹⁹ This is not to say that the Convention on Cyber-crime is without its critics. Some argue that the convention offers insufficient safeguards to privacy and that its extradition arrangements ought to require that the defendant’s offence is against the law in both the country in which she/he is accused and the country from which the extradition is sought.

on personal networks of trust within a small circle of computer scientists and engineers. Replacing this relatively ad hoc way of working will be difficult and will require the establishment of institutions that can demonstrate trustworthiness, reliability and capacity.

ii. Use of the Internet as an information source for terrorist activities

34. The Internet provides unparalleled access to information, whether legitimate or illegitimate, either of which can provide terrorists with a valuable service. Two examples serve to illustrate this: On 26 November 2008, gunmen launched a series of well-coordinated and devastating attacks on locations in Mumbai, India. In order to reach their targets and navigate the city centre as efficiently as possible, it is claimed that they used both hand-held GPS devices²⁰ and satellite data freely available on the Internet, allegedly from the application Google Earth.²¹ On 4 July 2007, Tariq al-Daour, a British citizen of Palestinian origin, pleaded guilty to conspiring to incite murder through his assistance to another defendant, Younis Tsouli, who had been creating websites to facilitate the distribution of propaganda originating, in particular, with Al-Qaida in Iraq. Daour's main contribution had been to provide stolen credit card details, which he had purchased from underground forums specializing in the sale of such illegally obtained information.²²

Countering use of the Internet as an information source for terrorist activities

35. In both cases the Internet was as a source of information, however the type of information was very different. In the first, the information obtained was legally obtained from an application overwhelming used for innocent purposes. In the second, the information was clearly illegal and should not have been available on the Internet.

36. The problem of terrorist access to useful but legitimate content is one that Member States have not

²⁰ According to the dossier of evidence on the attacks provided by the Indian government to the Pakistani government, GPS devices were found among the possessions of one of the Mumbai terrorists captured and interrogated by Indian police. Report available from: http://www.nefafoundation.org/miscellaneous/FeaturedDocs/mumbai_dossier1.pdf

²¹ 'Google Earth accused of aiding Mumbai terror attacks', *The Times* (London, UK), 10 December 2008.

²² Tariq Al Daour purchased credit card details from the online criminal forum 'Shadowcrew'. See e.g. 'Data Breaches: What the Underground World of "Carding" Reveals' by Kimberley Kiefer Peretti, US Department of Justice *Santa Clara Computer and High Technology Journal* 25 2008.

resolved. There are instances in which providers have been required to remove or reduce resolution of images of secret or sensitive installations. However, these would not cover a major civilian area such as the centre of Mumbai. And given terrorists' tendency to attack civilians and soft targets (to many a definitional requirement of terrorism), such measures are likely to be limited as a counter-terrorist tool. Reportedly, Indian courts have considered banning Google Earth within India. But such a measure, while understandable in the circumstances, could prove to be a double-edged sword even in the event of another attack since such applications can also benefit the emergency services.

37. Moreover even if Google Earth had been unavailable, the same data would still be accessible from more than a dozen other online sources, not to mention the GPS technology that was also reportedly employed in this instance, or low-technology sources such as a drawing on a paper napkin obtained from an informant.²³ In this case, it would appear that the only answer lies in the better application of a good, vigilant counter-terrorism policy, cognizant of the new capabilities of terrorist groups and counterbalanced by the even greater capabilities that such technology gives to state agencies²⁴. There is simply no obvious Internet solution.

38. By contrast, the case of Tariq al-Daour tells an opposite story. Here, the act (quite apart from its terrorist ramifications) is a straightforward example of cyber-crime. Indeed, the forum from which many of al-Daour's stolen credit card numbers were obtained was subsequently shut down after a criminal investigation. This appears to be an instance where the most appropriate tools to deal with a 'terrorist' use of the Internet are those applicable to ordinary law enforcement scenarios.

39. These two cases illustrate a wider theme that runs through State responses to the Working Group questionnaire, namely that the existence of innovative terrorist activity does not necessarily mean that existing measures are obsolete and that new custom-built approaches must be drawn up. The solutions may lie in the more effective application of existing tools and approaches.

²³ See: Google Earth: Don't blame us for terrorist attacks, *Times Online*, 30 January 2009, at http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article5615916.ece

²⁴ According to Google Geolocation Services, all images on Google Earth are more than a year old. US law states that all photographic data from all US satellites must be solely accessible to the US government for the first twenty four hours after it is obtained. Other governments employ similar rules.

iii. Use of the Internet as a means for disseminating content relevant to the advancement of terrorist purposes

40. Content dissemination is a core feature of many uses of the Internet for terrorist purposes. Indeed, technically speaking, all use of the Internet entails the dissemination of data in one way or another. It is central to use of the Internet for propaganda, or for 'training'. The dissemination of ideological material is also generally seen as an important factor in the process of radicalization. Uses of the Internet for purposes such as fundraising can also entail certain types of Internet content, such as websites of front charities. The discussion to follow will aim to identify the types of material disseminated on the Internet relevant to terrorism, and to consider specifically how States have approached the issue of suppressing such material.

41. Content available from the Internet can be divided into static and dynamic categories. Static content consists of items such as websites, which appear as relatively constant locations on the net. Dynamic content consists of items such as documents, images, sound or video. Until 2001 the presence of terrorist organizations on the Internet was predominantly through static websites. Since then, particularly Al-Qaida type terrorism, has tended to move to a model which is more dependent on dynamic content in the form of productions by a range of semi-official media foundations. In order to disseminate this content, an elaborate and increasingly controlled pyramid system of bulletin board forums has evolved.²⁵ After September 2008, this system was disrupted when the four major forums at the head of it became unavailable. Since then, Al-Qaida's media product distribution network seems to have moved to previously second tier forums.²⁶ While Al-Qaida is highly sophisticated in its use of the Internet, it is not unique. Websites and forums are used by almost all terrorist organizations,²⁷ and sophisticated video productions can be found on the Internet from a number of

²⁵ See Daniel Kimmage, 'The Al-Qaida Media Nexus' a special report of Radio Free Europe/Radio Liberty March 2008. According to Evan Kohlmann of NEFA, Al-Qaida use of the Internet for propaganda purposes has gone through three phases: originally static websites such as www.azzam.com and www.neda.com were the organisation's primary platform. When these closed, the organisation began to rely on a looser system of video dissemination. Following the arrest of Younis Tsouli (irhabi007) by British police, it created a more formalised structure, based on a system of core forums run by the Al Fajr media centre.

²⁶ For example, Al-Faloja and Shumukh forums

²⁷ See Maura Conway 'Terrorist Websites: Their Contents, Functioning and Effectiveness in Philip Seib (ed) *Media and Conflict in the 21st Century* (New York: 2005)

politically violent groups.²⁸

42. While many experts regard terrorism as fundamentally an act of communication, the Internet appears to change the nature of terrorist communication in ways that are still to be fully understood. On the one hand, the Internet allows terrorist groups more than ever before to make their messages available unmediated by others. This undermines strategies that aim to limit the oxygen of publicity to terrorists through careful media management.²⁹ At the same time, the Internet may serve to subvert the normal structure of terrorist propaganda. Terrorist propaganda divides into three fundamental categories: propaganda intended for wider publics, propaganda for the terrorists' 'constituency' and propaganda intended for members of the terrorist group itself.³⁰ With the Internet it becomes more difficult for terrorists to tailor their messages in this way. For example, 'internal' documents may become accessible to wider audiences. Another feature of terrorist information dissemination on the Internet is a blurring of the distinction between the role of members of the terrorist group and that of supporters of the group's ideology, who may play key roles in generating unofficial content relating to the organization or disseminating and assembling the organization's official content.

Countering use of the Internet as a means for disseminating content relevant to the advancement of terrorist purposes

43. Given the difficulty of creating a single definition for terrorism-related content on the Internet, the issue of countering the dissemination of such material tends to be addressed at a political level through a number of laws and approaches. Depending on the jurisdiction, some items of content that may be related to terrorism may already be illegal without recourse to terrorism laws. This could include, for example, videos featuring graphic depictions of real life terrorist violence, or material expressing racist or hateful views of particular ethnic or religious groups.

44. By contrast, official material attributable to terrorist groups could be largely inoffensive. This is

²⁸ Videos, music and similar materials expressing support for politically violent groups as diverse as, for example, ETA, the PKK, the Tamil Tigers, FARC-EP and The Naxalites, can be readily found on the Internet.

²⁹ Gabriel Weimann *Terror on the Internet: the New Arena, the New Challenges* United States Institute of Peace, 2006

³⁰ See for example Joanne Wright *Terrorist Propaganda: The Red Army Faction and the IRA, 1968-1986* (London: 1991)

the case with many official websites of terrorist groups, perhaps particularly ethno-nationalist groups.³¹ There may nonetheless be an objection to such content on the grounds that it fulfills a part of a terrorist group's wider strategic agenda and thereby adds value to its acts of violence. One State proposed that this approach be adopted at an international level by producing an international level agreement creating an obligation on Internet providers to identify owners of websites they host, and a simultaneous international agreement to deny websites to individuals and groups identified as engaging in terrorism. Such a proposal would certainly need to take into account human rights considerations.

45. In other cases, it may be considered necessary to create new legislation dealing with certain categories of content that may be particularly relevant because of their availability via the Internet. The most obvious example of this is provided by the Council of Europe Convention on the Prevention of Terrorism, which contains provisions against 'public provocation to commit a terrorist offence' and the dissemination of material relating to terrorist training. This approach has been partially adopted by the European Union New Framework Agreement on Countering Terrorism.³² 'Public provocation to commit a terrorist offence' may be regarded as a more worrying issue on the Internet, where highly inflammatory material may be disseminated in the hope that someone will act on its suggestions, but where there is not a direct connection between the provocateur and the individual provoked. At the same time, the potential limitations that such a broad law might place on a fundamental human right to freedom of expression are cause for concern.³³

46. Lastly, there exist a handful of laws that deal with certain types of content in an Internet-specific context. The clearest example being Saudi Arabia's provision in its new law on information crimes which criminalizes 'Publishing a website for a terrorist organization on an electronic network, or a computer system, or disseminating it in order to facilitate communication with the leaders of these, or

³¹ See Gabriel Weimann and Yariv Tsfati 'www.terrorism.com: terrorism on the Internet' *Studies in Conflict and Terrorism* 25:5 2005

³² Joanne Mariner, director of the terrorism and counter terrorism programme of Human Rights Watch pointed out to the Working Group that the EU has adopted a narrower approach to criminalising speech on the Internet, framed in terms of 'incitement' rather than 'provocation' to violence.

³³ Jennifer Daskal, another specialist at Human Rights Watch, raised a similar point at the OSCE hosted follow-up conference on the use of Public Private Partnership in Countering Terrorism

to circulate their thinking, or publishing how to manufacture explosives.’ Another, more limited example is provided by the special provisions relating to terrorism-related information on the Internet in the 2006 Terrorism Act in the United Kingdom.

47. Even with legislation outlawing the various categories of terrorism-related content, identifying the relevant material amongst the overwhelming volume of information available on the Internet is a difficult task. In the case of other content that may be illegal, such as child pornographic or racist hate material, a common approach is to take advantage of the power of the Internet to allow end users to report content that they consider suspicious.

48. This can happen in two ways. Material can be reported to its host, in which case the host may choose voluntarily to remove it, or it can be reported to another agency, which may use legal sanctions to attempt to force its removal. Notwithstanding the importance of due process and the right to a fair trial, the problem with the latter course is that the necessary due process is likely to be too slow to provide a useful instrument, particularly for countering dynamic content.

49. In some very specific cases countries may find ways around this legal issue. For example, the United Kingdom has a reverse presumption of innocence with regard to material believed to portray the sexual exploitation of children.³⁴ This means that trained staff at the hotline for countering illegal content, the Internet Watch Foundation, can identify such material and, if it is on a server in the United Kingdom, have it removed. A similar situation pertains with hotline services elsewhere. Moreover, some countries employ a similar approach for racist or hate-related material. According to the hotline that deals with child pornography and National Socialist material in Austria, this is possible because there are very specific legal definitions regarding such material.

50. Since terrorism-related material is much harder to define than these examples, and since, inevitably, it is often difficult to distinguish from legitimate political expression, hotlines are generally reluctant to extend their activities in this direction. However, this is possible in principle. Two States

³⁴ This point was made in a discussion with Fred Langford of the United Kingdom Internet Watch Foundation.

reported that they were looking into employing a hotline approach to address extremist content relating to terrorism. One remarked that relatively few reports of such material had actually been made by the public, who found it difficult to determine what constituted illegitimate content in this context.

51. In the United Kingdom the law does in principle provide a possible mechanism for the expedited removal of terrorism-related material in some circumstances via the following provision in the 2006 Terrorism Act:

52. 'The Terrorism Act 2006 allows a UK police constable to serve a notice on the person(s) responsible for hosting the unlawfully terrorism-related material on the Internet. The notice requires that the material be removed or modified within two working days. Failure to comply with this notice is not an offence but the person on whom the notice is serviced will not be capable of using the statutory defence of non-endorsement should s/he be charged with glorifying or supporting terrorism'.

53. A complementary approach that could help expedite the identification of illegal, terrorism-related material is the construction of a database of known examples. At a regional level the European Police Office (Europol) through its '*Check the Web*' project is compiling a database of extremist materials found on the Internet. It is intended to serve as a resource for police forces of EU member States and is expected to facilitate the rapid identification of particular documents for evidential purposes. A similar initiative exists in the United Kingdom through the Dedicated Viewing Unit of the UK specialist counterterrorism police branch SO15. However, the legal complexities and contextual factors involved mean that this approach cannot by itself identify a known item as illegally terrorist.

54. Even where undesirable content can be identified, it is not necessarily easy to remove it. If the content reported is illegal, and is hosted within the jurisdiction of the laws which make it so, then removing it is, in principle, relatively straightforward, particularly in the case of static content. Many States made clear that they would remove any websites established for terrorist purposes hosted within their national jurisdiction, but dynamic content is hard to pursue, particularly if it migrates

away from the web onto a peer-to-peer network which, particularly if their users are security-aware, may be difficult to identify and disrupt.

55. If content is illegal in one country, but is hosted in another, then removing it is difficult, though not necessarily impossible. It may be, for example, that a company with international operations chooses to conform to the laws of another State regarding content, rather than forego business in that country. However, this is not a consistently effective approach. An alternative is to filter for illegal content at the local level. Filtering, however, has a number of disadvantages. Depending on how heavily the State wants to filter, it may be expensive and may reduce the speed and performance of the Internet nation-wide. It also makes the Internet less robust at the national level, as it confines what is otherwise a highly redundant system to a limited number of chokepoints where data can be analysed and, if necessary, dropped. Finally, filtering is never 100% successful, and can usually be beaten by a determined Internet user.³⁵ However, filtering technologies have improved, and with the advent of hybrid URL filtering, filtering has increasingly become a commercially practicable reality for certain kinds of content.

56. At present, filtering is employed by ISPs in a number of countries, particularly for the purpose of targeting images relating to child sexual exploitation. Some ISPs have also begun actively tracking suspected use of the Internet for downloading copyright material. A number of countries employ filtering against a wider range of content. According to one State, it is presently used to block websites violating laws against terrorism-related material hosted outside the country where the site's host has refused to remove it.

57. In other jurisdictions, however, filtering out terrorism-related material has been rejected as an option on the grounds that the legal obstacles and the likely costs to legitimate commerce are prohibitive. This was, notably, the conclusion of the report carried out by the European Commission accompanying the proposal for a new European Council framework decision on combating terrorism,

³⁵ See Johnny Ryan, 2007 *Countering Militant Islamist Radicalisation on the Internet: A User Driven Strategy to Recover the Web* Institute of European and International Affairs (Dublin) 2007. Fred Baker (fellow, Cisco systems) and Danny O'Brien (international outreach officer, Electronic Frontier Foundation) made similar points to the Working Group.

in which the idea of a Europe-wide filtering system for the Internet was rejected.³⁶ This does not mean that commercial filtering packages may not be deployed against this material on a voluntary basis by, for example, parents or schools. Two States mentioned that they were encouraging such an approach. EuroISPA, the world's largest association of Internet Service Providers, has been keen to stress that, notwithstanding the limited cases mentioned above, ISPs still wish to be seen as neutral conduits for data rather than active gatekeepers for legal content. There is generally strong resistance to the idea of ISPs being used to block access to terrorism-related content.

58. When content is reported directly to its host, rather than a national authority, then removal is (initially at least) at the host's discretion. If the host is in a jurisdiction where the content in question is not illegal, the host may nonetheless choose to remove it if it conflicts with the acceptable use agreement under which the material is hosted. In fact, voluntary action has resulted in a very large amount of allegedly terrorism-related material being removed. One civil society group which is dedicated to the monitoring of particularly Al-Qaida-related material, claims to have succeeded in having over 1000 websites taken down simply by contacting their hosts and informing them of their content. This approach can be formalised through the introduction of established 'notice and take down' procedures agreed between government and industry. Another State said that it was introducing this approach as part of an industry-led self-governance approach to illegal content.

59. Some websites, particularly official sites of terrorist organisations and Internet forums closely associated with them, are hosted in locations where it is unlikely that the host will respond to a request that they be removed. In one State, many sites containing extreme right-wing material, which while not illegal, were vulnerable to being voluntarily terminated by commercial hosts, are now hosted on privately run servers.³⁷ The same is true for highly secret 'warez' sites dedicated to disseminating illegal 'cracked' copies of popular software.³⁸ However, a large proportion of terrorism-related material is hosted by responsible companies and is in violation of the acceptable use agreements that

³⁶ See the 'Commission Staff Working Document: Accompanying Document to the Proposal for a Council Framework Decision Amending Framework Decision 2002/475/JHA on combating terrorism'.

³⁷ Mark Potok of the Southern Poverty Law Center.

³⁸ Kevin Mitnick and William L. Simon *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers* (Indianapolis: 2005) p182.

they have with their customers. For this reason, terrorism-related material on the Internet often has a short life span in any one location. This is somewhat frustrating for frequenters of terrorism-related forums, where a common complaint is that a certain content item is no longer accessible at the location provided in a previously posted link. Unfortunately, however, the speed with which material may be uploaded and downloaded, and the diversity of options for making it available show that these measures generally result in an annoyance rather than a major disruption.

iv. Use of the Internet as a means for supporting communities and networks dedicated either to pursuing or supporting acts of terrorism

60. The Internet is a fundamentally interactive medium and very few communications are inevitably one way. Even websites may readily become interactive platforms, incorporating within them forums and instant messaging. As a result, the Internet offers great potential as a means for sustaining social networks and communities. Many of the uses of the Internet for terrorist purposes mentioned by States have their origins in, or are significantly assisted by, the interactive possibilities of the Internet. Operational planning, internal discussion and recruitment are all outcomes of the Internet that are fundamentally interactive.

61. Communities on the Internet formed around shared ideological support for the activities of a terrorist group are collective enterprises that play an important role in giving meaning and context to individual content items.³⁹ Moreover, the Internet gives individuals what may be satisfying and low-cost opportunities to participate directly in the work of a terrorist movement through activities such as propaganda dissemination, fundraising, or 'hacktivism'.⁴⁰ As well as being of benefit to terrorist groups in its own right, it is possible that some individuals involved in these sorts of activities may thereby become interested in making a deeper commitment to the cause, for example by becoming involved in real life violence. Alternatively, the social network contacts made in the course of such

³⁹ This point is made in the Dutch report *Jihadis and the Internet*.

⁴⁰ Max Taylor, Professor of International Relations and director of e-learning at the Centre for the Study of Terrorism and Political Violence, University of St Andrews observes that there may be 'criminogenic properties' to the Internet explained by perceptual psychological theories of 'affordance'. The idea would be that certain activities (such as clicking on a link) come so naturally to the human mind that they weaken inhibitions against criminal activity that might otherwise exist.

activity may create new possibilities for involvement, such as joining a terrorist training camp.⁴¹

62. Nonetheless, the case for seeing extremist Internet communities as a decisive factor in an increased incidence of terrorist violence is contestable. The marked difference in the level of actual violence arising from equally vigorous ideological communities dedicated respectively to Al-Qaida-related terrorism and extreme right militancy suggests that, while such communities may be an important precondition for campaigns of terrorist attacks, they may not be a sufficient condition in themselves.⁴² Another consideration is the scale of involvement in radical online communities compared to the actual number of individuals involved in violence. The fact that the largest neo Nazi forum has over 120,000 members,⁴³ and just one of the large Al-Qaida-affiliated forums had, at the time of its closure, over 80,000 members,⁴⁴ may suggest that involvement in online communities supporting violence is not in itself a very strong predictor of involvement in violence. Finally, history shows that flattened, networked terrorist movements of the type believed to be sustained by the Internet already existed long before the invention of the Internet.⁴⁵

Countering use of the Internet as a means for supporting communities and networks dedicated either to pursuing or supporting acts of terrorism

63. It is possible to disrupt virtual communities in a number of ways. Since many communities on the Internet are based around a virtual 'place' such as a website or bulletin board, removing this site may be one way to disrupt the community. Moreover, since new radical online communities are likely to be relatively easy to infiltrate at the moment they are established, creating alternative, trusted forums

⁴¹ A number of recent terrorist plots have involved individuals making contacts via the Internet to visit a terrorist training camp. An example of this is provided by the NEFA report by Evan Kohlmann 'Anatomy of a Homegrown Terror Cell'.

⁴² According to the TE-SAT EU Terrorism Situation and Trend Report of 2008, most European countries do not classify their extreme right wing groups as 'terrorist'. One act of extreme right wing terrorism was reported in Europe in 2008: the vandalising of a Jewish graveyard in Portugal. Increasing numbers of convictions of right wing extremists involving explosives have, however, been reported. By far the most frequent types of terrorist attack were carried out by 'separatist' groups (532 out of a total of 583). Such groups are not particularly notable for use of the Internet for organisational (as opposed to propaganda) purposes.

⁴³ Mark Potok, Southern Poverty Law Center

⁴⁴ Posted on Al-Hisbah forum, late October 2008. According to this posting, this number was reached after the forum amalgamated with the defunct 'Al Boraq' forum. Given that this posting appeared to relate to an internal strategic discussion rather than propaganda purposes, it seems likely to be accurate.

⁴⁵ James L Gelvin 'Al-Qaida and Anarchism: A Historian's Reply to Terrorology' *Terrorism and Political Violence* 20:4 2008

may be a difficult process.⁴⁶

64. The reverse may also be the case. Just as Internet content in the form of websites and forums provides the virtual space in which virtual communities of support may form, so too there is necessarily a human network behind the dissemination of terrorism-related content. Pursuing such individuals is therefore one way to disrupt terrorism-related content: a fact underscored by several cases in which alleged propagandists have been arrested and convicted.⁴⁷

65. Particularly given the threat of arrest looming over those who participate in the dissemination of terrorist propaganda, monitoring communities dedicated to sharing such material can become a powerful disruptive weapon in its own right. Today, forums discourage members from posting requests to join terrorist training camps or, in some cases, posting training material.⁴⁸ At the same time, there is evidence that, as with other persecuted communities on the Internet, rather than being destroyed by surveillance, communities supporting terrorism will tighten, switch to less traceable means and continue their work.⁴⁹ Whether this will make them more or less dangerous in terms of the emergence of violence is uncertain.⁵⁰

66. At present, Internet communities that offer ideological support for terrorism do still exist on publicly accessible forums. However, the more serious examples of networking support for terrorism on the Internet have for some time taken limited steps to preserve a measure of secrecy. At one end, this involves meeting on password-protected forums. Such forums serve to preserve a veil of privacy over the activities of the community. However, they are not very secure, as the anonymity of the Internet means that they are inherently vulnerable to infiltration, particularly when the forum is first

⁴⁶ This concern was raised on Al-Hisbah forum in late October 2008 in a thread discussing the closure of the other three major Al Fajr affiliated forums.

⁴⁷ Examples are the arrest and subsequent conviction of Younis Tsouli in the United Kingdom, individuals associated with the Global Islamic Media Front in Germany, and with Minbar-SOS in Belgium.

⁴⁸ 'The Internet: A Virtual Training Camp?'

⁴⁹ A posting to al-Hisbah discussed the possibility of movement to a decentralised network based on encrypted email.

⁵⁰ Despite continued persecution, communities devoted to copyright violation, child pornography and other crimes persist, and have found progressively more ingenious means of exploiting Internet technology: see, for example 'Child Pornography and Sexual Exploitation of Children Online' a report of ECPAT International for the World Congress III against Sexual Exploitation of Children and Adolescents' by Ethel Quayle with Lars Loof and Tink Palmer pp 39-44

set up.⁵¹ Within the forums private chat facilities can add a further layer of secrecy because they are internal to the forum and cannot be monitored in the same way as ordinary instant messenger channels.⁵² Individuals may also communicate on a one-to-one basis using a variety of other methods for maintaining confidentiality; some of these are relatively well-known and effective, such as publicly available encryption, and other, more exotic techniques such as when two or more people share a password to a web mail account and read each other's messages saved to the 'drafts' folder, or use 'invisible ink' where a short, innocent message is followed by a longer one written in white text on a white background. Commercially available steganography is also used.⁵³

67. Monitoring the Internet communications of individuals who are sensible, computer-literate and determined to keep them secret is not an easy task. Publicly available encryption is effectively unbreakable, and techniques such as the use of a shared draft folder or a chat service within a forum, make monitoring harder still. There is of course still a flow of data packets between the individual user's computer and the server hosting the account, which is in principle vulnerable to a 'packet sniffer' placed at an appropriate place in the network, but this is harder if a proxy server is used and an equally effective counter-measure is to use a publicly accessible computer, for example in an Internet café. To combat this latter tactic, a number of countries are taking steps to ensure greater regulation of Internet cafes.

68. The problem of locating individuals responsible for certain items of content, particularly websites, has prompted a trend towards stricter standards for hosting providers in terms of knowing their customers. ICANN has recently increased the frequency with which it checks the accuracy of its *Whois* database on registrants of websites.⁵⁴ A number of States mentioned that they were looking to improve their ability to identify individuals linked to Internet content, and one proposed that their should be Know Your Customer regulations for companies that host content on the Internet, enforced

⁵¹ Conversations with several individuals who have successfully infiltrated online forums suggest that doing so is especially easy at this stage.

⁵² Reported by Evan Kohlmann at the Working Group Stakeholders' Event

⁵³ Reported in a presentation by Tom Quiggan of CSIS, Canada at the European Expert Network meeting in the Hague, October 2008

⁵⁴ See 'ICANN's Whois Data Accuracy and Availability Programme: Description of Prior Efforts and New Compliance Initiatives' ICANN 27 August 2007.

at the international level.

69. A number of States reported on ways in which they were extending the provision for surveillance of the Internet by law enforcement and conducting increased research on Internet-based terrorism-related phenomena. One described its policy in terms of preventive surveillance; another mentioned creating a special police cell specifically devoted to the task of monitoring terrorism on the Internet; a third did this through a special directorate in the Interior Ministry. One State expressed its willingness to share the results of its research on the phenomenon of terrorism on the Internet, and proposed that the United Nations establish a database of research in the area.

70. It is still possible to gain useful information on terrorism-related activities via the Internet without sophisticated surveillance techniques. Psychological properties of the Internet such as disinhibition, and the relative looseness of online networks, in which individuals only develop good security practice as they deepen their involvement, mean that it is possible even for private individuals to infiltrate communities that support terrorism. Such individuals vary in their level of responsibility and professionalism, and there have been accusations of 'Internet vigilantism' against some. Nonetheless, this is an example of how the nature of the Internet can work against, as well as in favour of terrorist activity. It is well known in virtual communities that online presentation may not be the same as real life identity. Individuals who participate in communities on the Internet should not automatically expect that the people they talk to are who they say they are.⁵⁵ Individuals who infiltrate communities supporting terrorism provide an example of the power of the Internet to stimulate voluntary contributions to a collective good.

71. Private or civil society initiatives that have played an important role in investigating terrorism include commercial services that penetrate bulletin boards and monitor websites sympathetic to terrorist groups. A number of human rights organisations with a focus on anti-Semitic and racist activities have also expanded their activity into collecting and monitoring terrorist-related materials on the Internet. For example, the Simon Wiesenthal Foundation currently maintains records of around

⁵⁵ The power of Internet communications to facilitate the creation of alter egos has been frequently observed. For a fairly early example see Sherry Turkle *Life on the Screen: Identity in the Age of the Internet* (New York: 1995)

8,000 terrorism-related sites.⁵⁶ A number of academic projects also operate in this area such as the Dark Web Portal, a project that uses automated computing methods to capture and analyse extremist and terrorism-related activities on the Internet, including websites, forums and videos.⁵⁷

The Internet as a tool to counter the spread of terrorism

72. The Internet is not an unmitigated blessing for terrorists. On the one hand, it supports communities that support terrorism, but on the other, these same communities, by the very fact that they democratise opportunities for access are highly vulnerable to infiltration even by self-motivated amateurs. When one individual in such a global network is arrested, dense interconnections and lack of good tradecraft can lead to the disruption of multiple plots. While the Internet allows anyone to obtain the necessary information to build a bomb, in practice, inexperienced individuals who have attempted to do so have usually met with unimpressive results.⁵⁸

73. In the area of message dissemination, the same is true. While the Internet gives terrorist organisations unprecedented freedom to disseminate their messages directly to an audience, it also threatens terrorist organisations with loss of control over media strategy, with enthusiastic amateurs sometimes causing embarrassment through over zealous freelancing.

74. Generally, the Internet appears to strengthen ways of working which are based on collaboration, community and contributions from individuals. This applies to counterterrorism as well as to terrorism. When individuals report unacceptable content to its host, or decide, out of personal interest, to monitor extremist communities or use the Internet to inform people about terrorism and counterterrorism, these are all examples of how the power of the Internet may be used to take on terrorism.

⁵⁶ Richard Eaton, Simon Wiesenthal Foundation.

⁵⁷ Professor Hsinchun Chen described the work of the Dark Web Portal project of the Eller Business School, University of Arizona to the Working Group. See also the 'The Dark Web Portal Project: Collecting and Analyzing the Presence of Terrorist Groups on the Web' in *Intelligence and Security Informatics* (Heidelberg: 2005)

⁵⁸ See Marc Sageman *Leaderless Jihad: Terror Networks in the 21st Century* (Philadelphia: 2008) p113.

75. It is also the case that the Internet gives just as much freedom to those who wish to oppose the views of terrorist groups as those who wish to promote them. Just as terrorist videos have been disseminated or reverentially re-edited by enthusiastic volunteers, they have also been parodied, lampooned and defaced by others.⁵⁹ This invites the possibility that a more effective strategy than attempting to restrict terrorist material on the Internet may be to use the Internet as a means of countering terrorist arguments.

76. There are some obstacles to doing this. The inherent diversity of the Internet is such that it is difficult to oblige people to engage in debate beyond their existing comfort zone. On the Internet, everyone is free to choose, or to create, an environment that reflects his or her beliefs. If an individual who supports a terrorist group finds him or herself in an online space in which the legitimacy of terrorist violence is being questioned, he or she may simply choose to go elsewhere. If the community is dedicated to promoting views sympathetic to terrorism, those who challenge these views may simply be ejected.⁶⁰

77. Other obstacles are political. Much as states may wish to counter arguments to the claims made by terrorist groups about the legitimacy and necessity of their actions, the very involvement of states, particularly if these are the very states terrorists have declared to be their enemies, may undermine rather than reinforce the strength of these viewpoints.⁶¹ Those who oppose terrorist violence in the terrorists' constituency may be viewed as complicit in the machinations of the enemy. These are difficulties of which states engaging in the promotion of alternative views are well aware. As a result, States have adopted a number of different approaches.

78. The first and perhaps the most obvious way for States to present an alternative message on the Internet is simply to create websites expressing alternative views to violence. The State Department of

⁵⁹ Daniel Kimmage 'Fight Terror with YouTube' New York Times July 1 2008

⁶⁰ This problem derives from what is sometimes referred to as the 'long tail' of the Internet. Its implications for civil society and the public sphere are explored in, e.g. Cass Sunstein *Republic.com 2.0* (Princeton 2007)

⁶¹ Specifically with regard to attempts to counter the message of the Al-Qaida brand of terrorism, the scholar Olivier Roy writes in a recent paper: 'To promote 'good Islam' through governmental means is to give the kiss of death to liberal Muslim thinkers'. (Olivier Roy 'Al-Qaida in the West as a Youth Movement: The Power of a Narrative' MICROCON Policy Working Paper 2 November 2008)

the United States maintains a site on ‘identifying misinformation’ that is ‘devoted to countering false stories that appear in extremist and other web sources’. Such an approach has value but any views expressed directly by a State may seem inherently unreliable and unattractive to the target audience, which may simply avoid such sites.⁶²

79. Another approach is to adopt a multi-media strategy. Here governments are at a relative disadvantage when restricted to the Internet, where they must compete on more or less equal terms with a number of rival viewpoints; but their superior resources count when disseminating a message across a number of outlets including mass media, promotion of community activism and the education system. Two States proposed this, and in many countries one of the strengths of this approach is that independent media outlets will only publish stories on their merits, so giving them more credibility.

80. A third approach entails providing support for existing moderate alternatives to terrorism. There are many such initiatives, some backed by governments, some by civil society groups.⁶³ Despite the strengths of such approaches, if not carefully handled, there is a risk that genuine movements may be seen as tainted and as having lost credibility once government backing for them is discovered.

81. A fourth approach is to attempt targeted interventions in radical forums. For example, one State surveyed encourages volunteers to post on radical forums supporting terrorism and to present alternative views. In the United States, the Digital Outreach Team is an official state-sponsored group that posts messages on forums where radical views are expressed. These postings are officially attributed to the United States, but may stimulate dialogue nonetheless. A difficulty here is that the posters may be expelled from the more radical forums, thus limiting their ability to get their message

⁶² An administrator of an Islamic forum popular with individuals expressing support for terrorism said ‘The problem I find is that you start listening to a speaker that you may not be familiar with, go to two or three lectures maybe. The next thing you find is they condemn the mujahideen here and there or start being apologetic about terrorism in Islam. For me, that’s enough to switch off.’ – reported in the report ‘Virtual Caliphate: Islamic Extremists and their Websites’ by James Brandon, Centre for Social Cohesion

⁶³ See for example, Ustaz Mohamed bin Ali ‘Responding to Terror Ideology on the Internet: the Singapore Experience’ report of the International Centre for Political Violence and Terrorism Research, S. Rajaratnam School of International Studies, Singapore.

across.⁶⁴ Where government does not officially claim responsibility but is involved, the same problems of undermining credibility could surface. Where it does, there is a risk that this will prejudice people against the content of the message.

82. The difficulty that States face increases the importance of the role of civil society in opposing support for terrorism on the Internet. Indeed, many of the initiatives that governments support, they do so in partnership with civil society. Inevitably, the most powerful voices against violence come from within the communities that terrorist groups target. The power of cultures and civilisations to find within themselves the capacity to defeat violent extremism is a substantial resource against terrorism in all its forms and manifestations, and there may be scope for further work at an international level to empower this process. One State suggested that: ‘The United Nations should consider whether it could do more to support civil society organisations, particularly those with an online presence, to enhance the effect of these organisations worldwide.’ The rapid reaction media response mechanism of the Alliance of Civilisations already provides a good example of this.

83. There are other, less conventional ways in which civil society groups may use information to counter violent extremists. An example is the work of the Southern Poverty Law Centre, an American civil rights law practice which specialises in working against hate groups, especially of the extreme right, and which has deployed a number of ingenious practices, often involving techniques of investigative journalism which have resulted in discrediting, sowing internal dissent in, and otherwise disrupting such movements.⁶⁵ This provides a strong example of how a free flow of public information can counter extremist groups that thrive on secrecy and present a false image of strength and integrity. Indeed, one State pointed out that one of the most serious blows to support for extremist ideologies among individuals in that country was the public realisation of the true nature of such movements, as evidenced by the indiscriminate violence they practiced.

⁶⁴ ‘At State Dept. Blog Team Joins Muslim Debate’ *New York Times* 22/9/07

⁶⁵ Mark Potok, as above.

Protecting human rights

84. The United Nations Global Counter-Terrorism Strategy reaffirms the obligation of States to comply with their obligations under international law, including human rights law, in all measures taken to counter terrorism. Human rights and security are often regarded as two sides of the same coin, since neither can exist without the other. Effective counter-terrorism measures and the promotion of human rights are not conflicting goals, but complementary and mutually reinforcing. However, to the extent that there is a tension between them, it is evident in concerns over measures against use of the Internet for terrorist purposes. The Internet is a powerful vehicle for the exercise and protection of human rights of freedom of opinion and expression, and freedom from interference in privacy. It is these very properties that make it such a valuable medium for terrorists and extremists who support terrorism. Governments have no less right to govern illegal activity taking place on the Internet than anywhere else. However, terrorism-related content is not a readily definable category, and the line between such content and legitimate political expression may not always be clear. Therefore, it is imperative that any measures aimed at policing and reducing terrorism-related activities/content on the Internet must be carried out in full respect for human rights, with the utmost circumspection, and that any restriction is prescribed by law, in pursuit of a legitimate purpose, and respects the principles of necessity and proportionality.

85. Applying the term terrorism too widely, particularly in the case of activities such as denial of service attacks may be inappropriate. In that vein, it is essential that in the definition of any terrorist offense, criminal liability is limited to clear and precise provisions based upon the principle of legality. Secondly, concerns have been raised as to the legitimacy of broad offences relating to incitement or provocation to terrorist violence, or training for terrorism on the Internet. A third area of concern relates to measures taken by governments to monitor the Internet, as these may necessarily entail the unwarranted capture and retention of private communications data from ordinary citizens, as well as suspected criminals. These concerns have become more serious as governments have increasingly attempted to push for the preservation of traffic data for longer periods, and as ISPs have begun to play a more proactive role in monitoring for certain types of activity, for example copyright violation.

86. These concerns are real, and it will be important to ensure that, as initiatives are developed for countering the use of the Internet for terrorist purposes, and for fighting cyber-crime more generally, they are taken into account. At the same time, it must be accepted that there may be features of the Internet that create previously unforeseen necessities for law enforcement. While the complexity and magnitude of the challenges facing States in their efforts to combat terrorism can be significant, it is essential that they act within the framework of international human rights law. Terrorist groups using the Internet have often proved to be their own worst enemies when information about their indiscriminate violence has come to light. To the extent that the Internet is, fundamentally, about a better and more democratic flow of information, and so it is about both the exercise of human rights and, through the enjoyment of these rights, the empowerment of individuals to stand up against the violence of terrorists.

Conclusions and Recommendations

87. Perhaps the single most compelling conclusion to emerge from the Working Group's activities has been that there is no single, easily identified 'use of the Internet for terrorist purposes'. Terrorism could occur on, or by means of, the Internet, but it is disputable whether it has happened yet. Terrorists use the Internet in a variety of different ways, many of which are indistinguishable from ways in which everyone else uses it. Finally, and most confusingly, the Internet hosts a great deal of activity and material that may be related to terrorism. But establishing firm connections between online social actions and offline terrorist violence is not always straightforward. As is appropriate for such a complex issue, States have for the most part not adopted a 'one size fits all' approach. Rather, they have taken different measures aimed at tackling different aspects of the problem.

88. In the main, tackling terrorism on the Internet does not call for measures different from those employed for tackling either terrorism in general, or cyber-crime in general. However, there are some specific difficulties that may call for new approaches. Central to the problem is the point that content of various types and interactions of various types may support the continued survival of a social phenomenon, one of the products of which is terrorist violence. Necessarily, this phenomenon closely

resembles the expression of religious and political opinion, which is a protected human right. Knowing when such expression crosses the line into illegal conspiracy or incitement to violence can be difficult. It may also be somewhat academic, since available means to suppress even content which is definitely illegal are clumsy or ineffective, or both. This being the case, it is tempting to devise strategies that work with the Internet rather than against it, employing its capacity for facilitating grass roots organization and information dissemination. However, despite the existence of a number of such projects, there is a severe shortage of good information that allows an assessment of their effectiveness. If mismanaged, they could do more harm than good.

89. Throughout the Working Group consultations, one theme that emerged constantly was the extent to which Member States recognise their limitations in this area. There are many ways in which States can contribute to the fight against terrorism on the Internet. Better coordination within States, as well as the sharing of best practice between States, is critical. The United Nations could play a useful role in assisting with this latter process.

90. At the international level, States have suggested a number ways in which the United Nations might contribute:

- i. Through facilitating Member States sharing of best practices.
- ii. Through building a database of research into use of the Internet for terrorist purposes.
- iii. Through more work on countering extremist ideologies.
- iv. Through the creation of international legal measures aimed at limiting the dissemination of terrorist content on the Internet.

91. These are all areas that require further consideration and consultation with Member States. In particular, any measures that would limit a certain category of terrorist or extremist content at an international level would obviously require particularly careful review given the ambiguities of definition and human rights considerations, let alone the difficulties of enforcement. To avoid duplication of responsibilities, such discussions would also have to take into account current work by the United Nations in the wider area of Internet governance. A possible alternative to a rigidly legal

approach to countering terrorist content dissemination might be an approach based on what one well-known terrorism law academic suggested could be thought of as a ‘FATF for the Internet’. Naturally this, too, is an idea which would require careful review, particularly as, in the final analysis, the effects of terrorist propaganda on individual radicalization are not yet well understood, and are questioned by some.⁶⁶

92. Another possible area for international action identified by the report is in the field of cybersecurity. However, given that there is not yet an obvious terrorist threat in this area, it is not obvious that it is a matter for action within the counter-terrorism remit of the United Nations. If a more concrete threat of terrorist cyber-attacks does materialise in future, it might be a more appropriate and longer-term solution to consider a new international counter-terrorism instrument against terrorist attacks on critical infrastructure in general. The definition of critical infrastructure could, if necessary, be updated (perhaps by protocol to the treaty) to include information infrastructure, if this becomes important. However, any such treaty would have to be carefully phrased so as not to criminalise all non-violent activities (such as certain types of political direct action) that could result in disruption of transport, power or information systems.

93. Counter-narrative work holds exciting promise, but is still in its infancy and requires further exploration. There is no question that the United Nations can and should improve its own capacity to promote its core values on the Internet, possibly by looking at innovative ways to build online communities.

94. One clear conclusion of the Working Group is the relevance of actors outside the traditional political sphere in countering terrorism on the Internet. Industry clearly has an important role to play, not just in maintaining the stability of the Internet and providing the means to protect data from would-be attacks, but also to safeguard standards of acceptable content. However, it should be recognised that a great deal is already done in this regard. While it may be difficult to remove content

⁶⁶ See ‘Terrorism in the Age of the Internet’ in *Leaderless Jihad: Terror Networks in the 21st Century* by Marc Sageman (Philadelphia: 2008). Sageman made similar points to the Working Group.

from the Internet, the contortions of terrorist propaganda distribution on the Internet demonstrate that the Internet is not an entirely unregulated safe haven for any kind of content, no matter how extreme.

95. Finally, there is an enormous role for civil society – both in the form of formal organizations and, as ordinary Internet end-users. At times, States or international organizations may be able to support this work, and they should take every opportunity to do so. At other times, it may be that the very populism terrorists seek to exploit on the Internet will, if left alone, contain the seeds of their downfall.

ANNEX I: INFORMATION SOURCES

In March 2008, the Working Group sent a letter to all 192 Member States of the United Nations asking for information on laws, conventions, resources and initiatives relevant to countering the use of the Internet for terrorist purposes and using the Internet as a tool to counter the spread of terrorism. It was suggested that, in addition to measures explicitly related to this issue, that States might also wish to submit details of measures they had taken relevant to countering cyber-attacks or the dissemination of terrorism-related content in general.

To date, thirty-one States⁶⁷ have responded to this letter, and these responses provide the first source of information for this report. While this can by no means be taken as a definitive or scientific sample, it is believed that these responses do nonetheless provide a useful picture of how the issue is understood and approached at the state level.

The second major source for the report has been the proceedings of a ‘stakeholders’ event’ held in New York from 11 to 12 November 2008. This event brought together a range of expertise from industry, regional and international organizations, and civil society organizations specializing in relevant issues as well as academic experts on the issue. Finally, the report has benefited from a number of interviews, correspondences and discussions with relevant individuals and institutions as well as a review of relevant literature.

⁶⁷ These were: Afghanistan, Algeria, Australia, Austria, Belarus, Belgium, Bosnia and Herzegovina, Canada, Finland, Germany, Iceland, Japan, Jordan, the Kingdom of Saudi Arabia, Malta, Morocco, the Netherlands, New Zealand, Nigeria, Norway, Oman, Pakistan, Poland, Portugal, the Russian Federation, Senegal, Serbia, Spain, Switzerland, the United Kingdom and the United States of America.