DRAFT DOCUMENT

The content of this document has been discussed with partners and participants in the Clean IT project and has met a degree of consensus, but individual participants do not necessarily agree with all parts of the text. No partner or participant has committed to this text yet.

Clean IT draft document

Reducing terrorist use of the Internet

FOR PUBLICATION

This document was drafted after the fourth Clean IT workshop (Utrecht, September 2012) and internal consultation between Clean IT participants

NOTE:
The aim of the Clean IT project is to facilitate a dialogue between public and private organizations on terrorist use of the Internet and how to reduce this. This document will be the main deliverable of the Clean IT project. At this stage, the document is still 'work in progress' and is open for discussion. Comments can be sent to editorialboard@cleanITproject.eu. This draft will be used as input for the Clean IT conference in Vienna (November 2012), during which the participants will further discuss the text. The content of this document has been discussed with Clean IT partners and participants and has met a degree of consensus, but individual partners and participants do not necessarily agree with all parts of the text. No partner or participant has committed to this text yet.

DRAFT DOCUMENT

The content of this document has been discussed with partners and participants in the Clean IT project and has met a degree of consensus, but individual participants do not necessarily agree with all parts of the text. No partner or participant has committed to this text yet.

Contents

Executive summary

PM

Definitions

Terrorist offences

The European Union (EU) has defined terrorist offences as 'intentional acts which, given their nature or context, may seriously damage a country or an international organization where committed with the aim of: seriously intimidating a population, or unduly compelling a Government or international organization to perform or abstain from performing any act, or seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization" (EU Framework Decision, 13 June 2002 on combating terrorism). The EU has identified the following offences that are linked to terrorist activities: 'public provocation to commit a terrorist offence, recruitment for terrorism, and training for terrorism' which can also be committed in the online environment (Framework Decision 2008/919/JHA, 28 November 2008, amending the 2002 Framework Decision).

Internet companies

In this document, the term "Internet companies" refers to companies providing diverse services on the Internet. This document differentiates Internet access providers, Internet content delivery and content publishing companies, where appropriate. It also mentions webhosting companies and social media. A more detailed categorization would be and may be used, where appropriate: providers of access, browsers, chat boxes, certificates, domain registration, e-mail services, end-user control filters, exchange points, hosting, messaging systems, search engines, social networks, e-commerce sites, voice-over Internet protocol and web forums.

1. Preamble

(by governments)

A. Terrorism can be regarded as the unofficial or unauthorized use of violence or intimidation in the pursuit of political aims. Terrorism does not recognize borders and may affect all states and people, including European Union (EU) Member States and citizens. Individual terrorists and groups of terrorists intend to seriously threaten the democratic values of our societies and to the rights and freedoms of our citizens. Even small-scale terrorist activities can have a disruptive impact on society. Acts of terrorism are criminal and unjustifiable, and should be treated as such.

B. The Internet has become very important to modern society. It is now a regular feature in the daily lives of individual citizens, interest groups, businesses and public organizations. The vast majority of Internet use is legal and beneficial to its users. The Internet plays a positive role in our lives and societies and online freedom and access to the medium should always be protected. However, the Internet is also used for illegal purposes: it is used for many forms of cybercrime, including the attack of critical infrastructures. The Internet is also used for terrorist purposes. Although terrorist activities are illegal under European legislation,[1] some activity still takes place within Europe with help of the Internet, while terrorist use of the Internet also emanates from outside the EU.

C. Terrorists use the Internet on a daily basis. From a technical perspective, terrorist use of the Internet is not substantially different from regular, legal use of the Internet. Terrorists use the same popular, easy to use or more advanced Internet services as other users do, and they also use tools to conceal their identity and activities. Terrorists do not primarily use the Internet as a weapon to attack other targets, but mainly as a resource. Terrorist activities on the Internet can be found in the easy to access part of Internet where social media are used, and many forms of user-generated content are exchanged. This is also the place where violent propaganda material is spread, and the process of finding new recruits for terrorist acts and radicalization begins. Those who are interested are attracted to more ideological websites and social media that often contain illegal material. The illegality of content may depend, however, on the context in which the material is presented. These ideological websites often glorify and encourage violence, and are used to distribute training manuals and other information on how to commit terrorist acts. The Internet is also used to plan and organize deadly attacks. This takes place in hidden parts of the Internet, the hard-to-access terrorist forums.

[1] From this point onwards, the term ‘terrorist use of the Internet’ is used in this text.

D. While in practice it is difficult to evaluate whether specific content or activity is actually terrorist, some activities on the Internet are clearly not, such as political speech, reporting about terrorism in the media, non-violent extremism, hacktivism and the academic study of terrorism.

E. It is practically impossible to bring all terrorist activities on the Internet to a complete stop. Nevertheless, governments and NGOs have a task in limiting terrorist activities and protecting society from the impact of terrorist attacks. To reduce chances of terrorist attacks, it is also necessary to reduce terrorist activities on the Internet. Because the Internet is largely privately owned and operated, a public-private approach is required to reduce the terrorist use of the Internet.

F. From a legal perspective, it is a challenge to reduce the terrorist use of the Internet because:
- The Internet is not a single virtual society that possesses the characteristics of an individual state governed by the rule of law. This means that every national law becomes operative within the 'space' of the Internet.
- It is often difficult to determine which content on the Internet is illegal, also because illegality depends on the context in which it is presented and can differ between EU Member States and even worldwide.
- Illegal content itself does not always lead to radicalization and terrorist acts, while content that does contribute to radicalisation is not always illegal.
- Many activities of (potential) terrorists start in ordinary, easy accessible parts of the Internet and are not illegal.
For the above-mentioned reasons, it is necessary to discuss and distinguish between unequivocally illegal content or activities and cases where it is not clear whether the content or activities are illegal.

G. There are also practical difficulties related to solving the challenge of the terrorist use of the Internet:
- There is an imbalance in knowledge between governments and industry; governments are typically specialized in legal, policy and constitutional issues, while the industry holds the technical expertise.
- Reducing terrorist use of the Internet requires communication and procedures that go beyond organizational or territorial borders, and most procedures are limited to individual companies or public organizations on national levels.

H. This document is a result of the Clean IT project and will be made available to the public. Organizations that commit to this document will thereby commit to the general principles formulated in it and will thereby also agree to join the future dialogue and cooperation that has started with the Clean IT project. Organizations will make public on their own website that they have committed and joined. All organizations that join will increase their efforts to reduce terrorist use of the Internet, and can choose on a voluntary basis which of the best practices described below they will implement.

2. General Principles

(by all participants)

The partners in the Clean IT project believe that any action taken to reduce the terrorist use of the Internet should be guided by this set of general principles:

I. All organizations should make clear that terrorist use of the Internet is unacceptable.

II. Any action taken to reduce the terrorist use of the Internet, whether by governments of by private entities, must comply with national and European laws and regulations, and respect fundamental rights and freedoms, including access to the Internet, freedoms of assembly and expression, privacy and data protection.[2] In no way, private entities are bound by this document to perform any action which could not be introduced by legislation for constitutional or human rights issues.

III. Actions to reduce terrorist use of the Internet must be effective, proportionate and legitimate. Reducing the terrorist use of the Internet requires trans-organizational cooperation, and should be incorporated as much as possible in existing programmes, systems and procedures.

IV. In cases of unequivocally unlawful terrorist use of the Internet immediate and proportionate action should be taken in order to stop this unlawful situation.

V. In cases of probable terrorist use of the Internet, when the unlawfulness is not clear to one the organizations that should take action, the organizations involved will avoid status-quo situations as much as possible within their respective legal obligations. If organizations or individuals cannot agree, procedures should be in place and be used where courts will determine what is unlawful.

VI. Terrorist use of the Internet should be prevented as much as feasible. Actions to make it more difficult for terrorist to attain their goals should always be transparent and proportionate.

VII. Internet access providers, content delivery, hosting and publishing companies are not responsible for terrorist content or terrorist activity on their network, but can assist to make it more difficult for terrorists to attain their goals.

VIII. All organizations should be sufficiently equipped, transparent, professional and predictable regarding their activities to reduce terrorist use of the Internet.

IX. Internet users should have the means to avoid being subjected to terrorist use of the Internet or at least should have user-friendly mechanisms available to them as much as feasible to report what (they believe) is terrorist use of the Internet.

[2] Add references from Council of Europe, UN, and ITU and EU.

X. Long-term public-private dialogue and cooperation, based on mutual trust and understanding, are required to explore new and better ways of reducing the terrorist use of the Internet.

3. Best Practices

The partners in the Clean IT project consider the following best practices to be useful in reducing the terrorist use of the Internet, provided they are implemented in compliance with the general principles mentioned above. Implementing best practices is voluntary and is the full responsibility of each individual organization.

3.1 Proactive best practices

Best Practice 1: Legal framework and government policies

Challenge:
Terrorist use of the Internet is not always clearly explained, while it is very difficult to apply existing legislation on unlawful terrorist activities to the technical reality of cyberspace. Every EU Member State uses its own sovereign powers to implement legislation and government policies, but these are not always tailored to the increased and cross-border terrorist use of the Internet. Differences between national legislation make it complicated for LEA and Internet companies to deal with terrorist use of the Internet.

Best practice:
The legal framework and governmental policies to reduce the terrorist use of the Internet should be clearly explained to users, NGOs, LEAs and Internet companies to make their work more effective. Increased efforts and international coordination will help to reduce the transnational terrorist use of the Internet.

Explanatory note:
Many governments include reducing the use of the Internet for terrorist purposes as an integral part of their security strategies and in foreign policy and stimulate international cooperation in this field. All Member States regulation is based on the implementation of the EU Framework Decision of 13 June 2002 on combating terrorism and EU Framework Decision 2008/919/JHA of 28 November 2008. More analysis and explanation of differences in states' legislation will help practitioners in reducing the international aspects of terrorist use of the Internet.

The Council Regulation (EC) No 881/2002 of 27 May 2002 (art 1.2) for example, is not widely known by practitioners that aim to reduce the terrorist use of the Internet. This regulation states that providing Internet services is included in providing economic instruments to Al-Qaeda (and other terrorists persons and organisations designated by the EU) and therefore an illegal act. Also Youth protection legislation protects in some cases against terrorist use of the Internet.

Remaining questions to be addressed in Vienna:

- In some Member States legislation is or will be adapted to oblige Internet companies to report security breaches in their networks. If Clean IT best practices are endorsed and implemented by individual organizations, it should not be necessary to create similar legal

obligations for terrorist use of the Internet. Is it useful to address this point here?

- In some Member States Internet companies are obliged by law to provide LEAs with all necessary customer information for investigations of terrorist use of the Internet. Are their gaps in this respect on a European level and if so, should this be addressed?
- Do all EU Member States have clear procedures in place with regard to clarification of unlawfulness of terrorist use of the Internet? Is it useful to include this in the explanatory note?

Best Practice 2: Business conditions

Challenge:
Not all Internet companies state clearly in their business (or service) conditions that they will not tolerate terrorist use of the Internet on their platforms, and how they define terrorism. This makes it more difficult to decide what to do when they are confronted with (potential) cases of terrorist incitement, recruitment and training on their platform.

Best practice:
Some Internet companies do explicitly include terrorist use of the Internet, with a definition or examples, in their terms of service/business conditions, stating that such use is unacceptable. Some Internet companies effectively enforce this policy.

Explanatory note:
This best practice does not require any European standard. Internet companies can define and/or give examples of what is terrorist use of their services, and do so for legal, ethical or business reasons. Access providers should refrain from developing these policies, as access-blocking is not a recommendable option. Acceptable use policies do not create new legal rights for third parties, but solely govern the relationship between the respective service provider and customer. It is recommended that companies have sufficiently staffed and capable abuse departments and are consistent and transparent in how they deal with abuse of their networks and violations of their business conditions.

Remaining questions to be addressed in Vienna:

- How to handle terrorist use of platforms in languages abuse departments do not master?
- Would it be useful to develop a benchmark to evaluate if Internet companies have enough capacity for their abuse departments in relation to their number of users and the volume of (possible) terrorist use of their service? If so: who should develop this benchmark?

Best Practice 3: Awareness

Challenge:
Terrorist use of the Internet is currently not widely known or understood. Children, teenagers, young adults, the circle that surrounds them and the public in general should be made aware of terrorist use of the Internet. Professionals involved should know what to do when they are confronted with terrorist content or someone who is radicalizing.

Best Practice:
Cyber security awareness, education and information programs exist in a number of EU Member States, and some of them include terrorist use of the Internet.

Explanatory note:
In increasing awareness, education and information on terrorist use of the Internet, best results might be expected if governments, LEAs, Internet companies cooperate in, and NGOs lead awareness programs. Increased awareness amongst Internet users will probably lead to more reports of terrorist use of the Internet. Governments have specific knowledge about terrorist activities and threats. It would help Internet companies in becoming more aware of terrorist use of the Internet if this kind of information is shared actively by governments.

It is important to address Internet users in general, and vulnerable persons in particular, about the dangers of the Internet and how to recognize online signs of radicalization. Awareness programs should be creative and appeal to the younger generation. This can be done by involving youth in developing programs, using the latest technology, involving former radicals and victims and implementing counter-narrative policies.

Remaining questions to be addressed in Vienna:

- Should awareness programs also target user activity (to report terrorist activities on the Internet), the quality of notifications and existing helplines?
- Should awareness programs specifically address the role of hate speech and extremism on the Internet as an important catalyst of radicalization?

3.2 Detection best practices

Best Practice 4: No automated detection, unless...

Challenge:
While users, LEAs, NGOs and Internet companies do report a number of (potential) cases of terrorist use of the Internet, only automated detection systems can process large volumes of content and activities on the Internet. Some governments, LEAs, NGOs and Internet companies use such software systems to point to potential cases of terrorist use of the Internet, but these systems are often not precise and effective, can be costly, while their use is not made clear to Internet users and could be endangering Internet freedom or even be illegal.

Best practice:
Automated detection systems should **not** be used, unless the following conditions are met. After being pointed to potential cases of terrorist use of the Internet by the automated systems, (specialized) employees from governments, LEAs, NGOs should decide what actions are required. In addition, the use of automated systems is only recommended for open source observation purposes, only when this is in accordance with (national) legislation and if organisations are transparent about the fact they are using these systems and on how these systems are used.

Explanatory note:
If automated detection is used, the systems should be published and made known to Internet users/customers, including at least a general description of their working. These systems should only be used by Internet companies to signal to their abuse officers where on their platforms there might be cases of terrorist (and other illegal) use of the Internet. These systems should never be used to automatically remove content and make decisions that can have legal implications for Internet users. If these conditions are respected, and the use of these systems is in accordance with (national) legislation and these systems are deemed accurate enough, implementation might be considered. Automated detection might become more accurate if it searches for known terrorist organization content, activities and imagery (i.e. logo's) as this is proven technology in other market sectors.

Remaining questions to be addressed in Vienna:

- Is the use by governments and LEAs sufficiently regulated and do they respect the conditions? Should this best practice be limited to private sector only?
- Does accordance with national legislation mean they can be used to crawl the Internet regardless of national borders?
- Many detection systems available on the market are not tailored to terrorist use of the Internet. Is there a market anyway for these systems?
- If detection systems are used to search for specific keywords, what distinguishes them from common search engines?
- Would it be useful to address in this best practice what else should be done with automatically detected information? I.e., how long should this be stored and what can be done to prevent

the loss of evidence of terrorist use of the Internet?

3.3 Reporting best practices

Best Practice 5: Flagging mechanisms

Challenge:
Internet users currently do not have enough easy ways of reporting terrorist use of social media. In addition, Internet users are not used to reporting what they believe is illegal. As a consequence, some terrorist use of the Internet is currently not brought to the attention of Internet companies and LEAs.

Best practice:
Some websites with user generated content offer simple and user friendly flagging systems on their platforms. These systems allow end-users to flag alleged terrorist activities and thereby bring potential abuse to the attention of the Internet service provider. This allows the company to assess (il)legality and take appropriate action and if necessary inform the authorities.

Explanatory note:
Flagging is a useful method of notifying Internet companies about potential terrorist use of the Internet. User-friendly flagging systems have a separate, specific category to flag cases of terrorism and radicalizing. The service providers also explain to their users how these flagging systems work. This practice is primarily meant for websites that provide user generated content. Flagged content means that possible illegal content is brought to the attention of the service provider, and from that point they are not excluded from liability for the information stored on their networks.[3]

Anonymous flagging should be possible and respected, while Internet companies can also extend a higher credibility status to trusted flagging organizations, like specialized NGOs. Higher credibility statuses should serve to prioritize handling reports. Individual users could also be provided higher credibility status based on their (calculated) reputation in successfully reporting abuse.

Governments and LEAs should primarily use formal ways of notifying Internet companies. In some Member States flagging is also regarded as a formal notification. If governments and LEAs use flagging systems apart from their formal/legal procedures, they make clear this is exclusively meant as bringing the alleged terrorist use of the Internet to the actual knowledge of the provider (see also: notice and take action).

Remaining questions to be addressed in Vienna:

- *Does this best practice apply only to social media platforms/communities? Or is it technically possible and helpful to use flagging systems on other platforms? For VOIP it is unclear for example, how about forums?*
- *Should this best practice include the possibility to make flagging systems available for subgroup moderators to remove content after it being flagged by subgroup users?*

[3] Article 14 E commerce directive.

Best Practice 6: End-user browser button

Challenge:
While user generated content platforms can offer 'flagging' opportunities, hosted websites often lack such a mechanism. Moreover, there is not one international, user friendly reporting mechanism available to all Internet users, irrespective of which part of the Internet they are using at the moment they notice what they think is terrorist use of the Internet. Comparable systems to report spam and phishing sites already exist as an option or add-on in browsers.

New practice:
On a European level a browser based reporting button could be developed to allow end users to report terrorist use of the Internet.

Explanatory note:
Webhosting companies do not want terrorist use of their networks, but are technically, economically, legally or practically limited in detection of their clients' content . If those clients do not have proper notification mechanisms for abuse, Internet users cannot signal the terrorist use of the Internet in a user-friendly way. In those cases, webhosters can play an intermediary role. In some countries webhosting companies in coordination with LEAs offer banners that clients can add to their website on a voluntary base to report alleged illegal content. Similar mechanisms exist for phishing sites and malware. A more systematic approach to help hosting companies to be notified by Internet users about alleged terrorist (and other illegal) use of the Internet is a reporting button in a browser. This is a user-friendly notification tool to webhosting companies for hosted websites (and other parts of the Internet) that do not offer flagging tools or don't have effective abuse departments. The application should also be considered for mobile devices and operating systems.

The reporting button will send an automated signal to the hosting company involved, which will allow them to contact their client (the website owner) so the client can take appropriate action. The client and / or the webhoster can also contact the authorities if necessary. The system works only for known webhosters, or webhosters that register to this service. As this is a new practice, a pilot is recommended to experiment and evaluate the added value of this system, as well as to solve legal/jurisdictional, procedural and technical issues.

Remaining questions to be addressed in Vienna:

- Should this system be limited to signal web hosting companies, or should authorities and/ or specialized NGOs be involved? If so, under which conditions?
- Can open source code be used for this system?
- Would each report have to get a ticket number, allowing LEAs to know if the provider already took action?
- Would implementing this system make the 'flagging' best practice unnecessary? Or would all or some social media still prefer or be necessitated to have their own flagging mechanisms?
- Which are the first steps that need to be undertaken in order to start an experiment/pilot?

Best Practice 7: Referral units and hotlines

Challenge:
Internet companies do have potential cases of terrorist use of the Internet reported to them, but they often lack the required specialist knowledge about terrorism to determine whether it is illegal. In addition, determining what is illegal is primarily a law enforcement role. In other cases, Internet companies lack the language skills they need to make a judgment on the meaning and therefore on the legality of the content or other terrorist activity. In addition, some existing industry operated hotlines do not (explicitly) include terrorist use of the Internet as one of the abuse areas that could be reported to them. As a consequence a large number of potential cases of terrorist use of the Internet are not dealt with adequately.

Best practice:
Some governments and LEAs maintain one or more referral organization(s), to which Internet companies, NGOs and end-users can report potential cases of terrorist activity on the Internet. The referral organization analyzes whether content is illegal and take appropriate action if necessary. Some industry operated hotlines do explicitly aim to also handle terrorist use of the Internet.

Explanatory note:
Well-organized referral units (government) and hotlines (private sector), having an appropriate team behind them with the needed competences and skills, will help Internet service providers to handle notifications about terrorist use of the Internet more effectively and efficiently. This is especially the case if Internet service providers are not sure whether notification of terrorist use of the Internet is illegal or not.

The role of an LEA operated referral unit is to assess Internet content and where it is deemed unlawful have the material removed and coordinate any prosecutions for offences which may have been disclosed. For regional and local police units the referral unit offers more expertise in dealing with (potential) terrorist use of the Internet.

Private sector hotlines provide a mechanism for the public to report content or use of the Internet that they suspect to be illegal. Hotlines analyze the reports to determine if the content is illegal under their national legislation, and if so, will perform a "trace" on the web to identify where it appears to be located (source country). With this data, the hotline will then pass the information to the relevant stakeholders (internet service provider or LEA) for further action.

Referral units and hotlines should technically be able to receive all kinds of terrorist use of the Internet (i.e. websites, videos, messages, emails, profiles) and if both exist within one Member State they should have excellent cooperation. As a secondary task they can contribute to awareness, education and information efforts on terrorist use of the Internet. For example, governments and LEAs could help Internet companies by sharing information on specific phenomena of illegal content and have programs to educate web moderators. Governments can also subsidize competent NGOs that substantially contribute to reducing terrorist use of the Internet and radicalizing content on the Internet.

Remaining questions to be addressed in Vienna:

- Should it always be possible for persons reporting a case to a hotline/referral unit to be informed as to the progress, check the status themselves and the results of the investigation following their report? Or should this only be available to trusted parties?

- Is it feasible that referral units / hotlines be organized in such a way as to be able to handle referrals in the (very) uncommon languages often used in cases of terrorism? Would a system or network of trusted translation agencies be recommendable?
- Should this best practice include an explanation on cooperation with referral units in other countries, including handing over cases to more competent or authoritative units?

3.4 Reactive best practices

Best Practice 8: Notice and take action procedures

Challenge:
When Internet companies are notified of probable cases of terrorist use of the internet, the procedure to handle these reports is not always effective and efficient. Internet companies have liabilities both to respond to the reporter and to protect the services they deliver to their users. Sometimes LEAs notify Internet companies to bring terrorist use of the Internet to the actual knowledge of the provider. From their formal role LEAs can also order Internet companies to remove illegal content. The difference between these two actions is not always clear to Internet companies. In addition, when LEAs order to remove content, these orders suffer sometimes from being insufficiently specific or inappropriate to the company being approached.

Best practice:
Some individual Internet companies have their own effective and efficient notice and take action procedures and some have agreed to use a standard for notice and take action. In some EU Member States LEAs apply a standard for take down orders.[4]

Explanatory note:
Legally there are two forms of reporting alleged illegal content:

(1) *a notification brings the content to the actual knowledge of the Internet service provider, which means they are not excluded anymore from liability for the information stored on their networks according to the E-commerce directive.*
(2) *an order is a binding request to an Internet service provider by a competent authority.*

Notifications
Notice and take action applies to any service provided that consists of the storage of information provided by a recipient of the service, for example: providers of chat boxes, e-mail services, file sharing, hosting, social networks, e-commerce sites, and web forums. Effective notice and take action procedures imply that notified unequivocally illegal content is removed as fast as possible. This best practice will only work if the quality of notifications is sufficient. Notices should be specific (unambiguously identify the material in question), proportionate (matching the offence and limiting collateral damage to other users) and appropriate to the service offered by the Internet company. In case of terrorist use of the Internet it is important to contextualize the terrorist content and describe how it is breaching (national) legislation.

If it is unclear whether the content is illegal or not, effective notice and take action procedures make clear that Internet service providers have an intermediary role to avoid status-quo situations. The ultimate goal is that every notification is handled carefully and that appropriate action is taken (which is not necessarily the take down of the content). However, in some EU Member States it is possible for the service provider to ask the reporter and the content provider to settle the dispute and to wait for a final decision. This situation should always be limited in time. If the content is kept online in the meantime, the service provider can ask the reporter for a promise of indemnification.

[4] The European Commission´s DG Market is also developing a European Notice and Take Action framework.

(Court) orders

From the perspective of Internet companies the above mentioned qualifications for notices should at least also apply for formal orders by LEAs. Internet companies would like to easily recognize the competent authorities, especially if they are based in other countries. If LEAs notify apart from their formal/legal procedures, they should make clear this is exclusively meant as a means of bringing the alleged terrorist use of the Internet under the provider's attention.

Remaining questions to be addressed in Vienna:

- What is the status of DG Market initiative to establish a horizontal framework for notice and take action and can there be any conflict with this best practice?
- How should Internet companies handle imperfect notices and orders? Should they reply to the reporter that information is missing or incorrect and wait for a response?
- Would it be useful to address in this best practice that actions taken (like removal of content) should not make it impossible or more difficult for LEAs to investigate the origin and who is responsible for the terrorist use of the Internet?

Best Practice 9: Points of contact

Challenge:
Governments, Internet companies, LEAs and NGOs do not always know whom to contact on the issue of terrorist use of the Internet.

Best practice:
Some governments, LEA, Internet companies and NGO's have points of contact for (among others) terrorist use of the Internet. These points of contact are stable, remain points of contact for a reasonable period and develop relations with their most important counterparts in other organizations.

Explanatory note:
A network of trusted and listed points of contact facilitates cooperation between organizations committed to reduce the terrorist use of the Internet. Points of contact are experts able to represent their organization preferable on a daily or even 24/7 basis.

Remaining questions to be addressed in Vienna:

- To establish a professional system of points of contacts, are detailed working procedures and a central (EU) database and host organization required? Should this be included in this best practice?

Best Practice 10: Cooperation in investigations

Challenge:
When LEAs suspect illegal use of the Internet for terrorist purposes and contact Internet companies to assist in investigations of third parties, cooperation between the two is not always effective and efficient.

Best practice:
Some Internet companies and LEAs agreed on how to cooperate efficiently, effectively and lawfully in investigations of probable illegal terrorist activity on the Internet.

Explanatory note:
The legal base of LEAs investigations should always be clarified. LEAs and Internet company have very different backgrounds and fields of activities, but have in common that they want to reduce terrorist use of the Internet. Exchanging knowledge between LEAs and Internet companies (as well as amongst each other) can increase expertise, improve mutual understanding and lead to better cooperation in investigations. LEAs should respect the technical integrity of the company involved in the investigations ("do not pull the plug on the servers which might affect other entities than the ones targeted in the operations" and "make a copy rather than take the server"). The legal base of investigations should always be clear and be presented. If an investigation needs additional efforts made by Internet companies that already took reasonable precautions to reduce the terrorist use of the Internet, it is reasonable they ask for adequate compensation by government.

Remaining questions to be addressed in Vienna:

- Should Internet companies and LEAs publish their policies on which data they share and how long data is stored after investigations end?
- If Internet companies remove illegal, terrorist content, after a (civilian) notification, they can consider informing LEA. Should this be addressed in this best practice?
- Would it be helpful if in case of investigations LEAs and Internet companies each appoint a single point of contact?
- Cooperation between different national governments might also help to operate more effectively in reducing the terrorist use of the Internet. It might be helpful if governments could reduce the time needed for international (legal) action against content in another Member State. Should this point be added to this best practice?

Best Practice 11: Sharing abuse information

Challenge:
Most Internet companies have to deal with few cases of terrorism on their platforms. When illegal content is removed, terrorists often try and succeed to post it on other Internet companies services.

New practice:
Some Internet companies share information on other kinds of abuse of their network with each other, using a trusted intermediate partner company. This private sector practice could be extended to include known terrorist use of the Internet.

Explanatory note:
Systems to share known abuse information via a trusted third partner organization and its databases with known abuse information already exist. These systems often make use of e-mail as it is reliable. Data with a time-stamp is exchanged using formats like xarf (http://x-arf.org) that allows the exchange of many kinds of abuse data like videos, pictures, IP-addresses, email addresses. Only data that is formally confirmed as terrorist use of the Internet, taking into account national legislation, should be added to these systems.

Remaining questions to be addressed in Vienna:

- *Can hotlines and referral units participate in the sharing of terrorist abuse information?*
- *What restrictions does privacy regulation impose on this practice?*

Best Practice 12: Voluntary end-user controlled services

Challenge:
Various kinds of voluntary end-user controlled services exist to identify, log access to or block unwanted or illegal content. However, end-user controlled services rarely include terrorist use of the Internet. Technology for detecting, logging access to or blocking of terrorist use of the Internet is often not mature enough to be precise and effective and risks blocking content that should be free to access.

Best practice:
Parental and other voluntary end-user controlled services that effectively include terrorist use of the Internet.

Explanatory note:
In general, blocking and filtering options are considered as a "bad practice", especially if it is used at state level or if it is otherwise forced on Internet users. Filtering and controlling access on private networks cannot stop illegal web use completely - it is predominantly a tool to prevent accidental and/or casual exposure to illegal content. Filtering by Internet access companies at infrastructure level should not be promoted. Nevertheless, at a parental / end-user level individuals should not be limited in the possibilities to protect themselves or their children from what they believe is inappropriate. Vendors already categorized and have the potential to control access to some 'terrorist, race-hate, extremism' content through the use of keywords, phrases and known URLs. This can be a helpful tool e.g. for parents that want to protect their children from radicalization attempts.

Remaining questions to be addressed in Vienna:

- It is not clear whether end user controlled services specific for terrorist use of the Internet are profitable for commercial use. Should this point be addressed?
- Should in this description of this best practice be included that the precise working of such systems must be transparent and made clear (by vendors) to end-users?

3.5 Learning best practices

Best Practice 13: Research and Advisory Organisation

Challenge:
The understanding of what is terrorist use of the Internet is the result of many individual public and private organizations studying terrorist use of the Internet and sharing their expertise. In terrorist use of the Internet there is no one coordinating and academic authoritative body to which all organizations involved are likely to refer.

New practice:
An academic organization (on sub-national, national and/or international level) that is respected by all parties, to explore in depth what is terrorist use of the Internet, and how best to reduce it.

Explanatory note:
An organisation as proposed here should be part of a university and can provide research and advice on terrorist and other content which is recognised as dangerous throughout the EU and in each individual Member State. The organisation should act independently, i.e. without political interference. Possible fields of work are:

- Legislation & jurisprudence;
- Academic work on the subject;
- Known terrorist use of the Internet;
- Information on the technologies used by terrorists.

Remaining questions to be addressed in Vienna:

- Would it be useful if this organization also gives advice on how abuse departments of Internet companies, referral units and hotlines should handle (procedures and protocols) reports, notifications and automatically detected terrorist use of the Internet?
- Which institute is most comparable and should be taken as example for this best practice?