NOTE: This document was drafted after the first Clean IT conference (Berlin, June 2012). The first part (preamble) is meant to be adopted by governments, the second part by all participants. This document is 'work in progress' and is open for discussion. Comments can be sent to editorialboard@cleanITproject.eu and will be used as input for the Clean IT workshop in Utrecht, the Netherlands (September 2012) and the Clean IT conference in Brussels (November 2012), during which the participants will finalize this draft.

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 FD, 13 June 2002 on combating terrorism). The European Union 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' also when committed (intentionally) in the online environment (FD 2008/919/JHA, 28 November 2008).

Internet companies

In this document the term "Internet companies" refers to companies providing divers services on the Internet, like Internet access and content delivery or publishing. "Internet companies" can refer to 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. Each kind of Internet company can make specific contributions to reducing terrorist use of the Internet.

Preamble (by governments)

1. Terrorism does not recognize borders and may affect states and people, irrespective of their geographical location, thus including EU States and citizens. Individuals and groups who believe that they can advance their political aims by using terror, pose a serious threat to the democratic values of our societies and to the rights and freedoms of our citizens, especially by indiscriminately targeting innocent people. Even small-scale terrorist activities can have a disruptive impact to society. Acts of terrorism are criminal and unjustifiable, and must be treated as such under all circumstances.

2. The Internet has become very important to modern society, the daily lives of individual citizens and for businesses and economic innovation. Most use of the Internet is legal and beneficial to its users. The Internet plays a positive role in our lives and societies. Nevertheless, the Internet is also used for illegal purposes, including terrorism, supporting terrorism and encouraging terrorism.

3. Cyber terrorism covers a range of illegal activities, including conducting cyber-attacks or targeting the Internet itself. Terrorists use the Internet on a daily basis to spread violent propaganda material, glorify and encourage violence, radicalize and recruit individuals, distribute training manuals and other knowledge on how to commit terrorist acts. The Internet is even used to plan and organize deadly attacks. The use of the Internet for terrorist purposes takes place within Europe, but for a large part also emanates from abroad, including from befriended nations. The use of the Internet for terrorist purposes is

illegal by European legislation.[1]

4. From a technical perspective, terrorist use of the Internet is not substantially different than regular, legal use of the Internet. Terrorists use the same popular, easy to use Internet services as other users do, but terrorists use these as platforms for propaganda, recruitment and training. They also use tools to conceal their identity and activities.

5. From a legal perspective, it is a challenge to counter the terrorist use of the Internet because:
   - The Internet is no 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 and the illegality of content might differ between EU countries.
   - The (illegal) content itself does not always lead to radicalization and terrorist activities, 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 or not.

6. There are many difficulties related to solving the problem of the terrorist use of the Internet:
   - The necessary knowledge for effective cooperation is unbalanced; governments are specialized in legal and constitutional issues, while the industry has the technical expertise.
   - Procedures usually cover public or private organizations on national level, while combating the terrorist use of the Internet requires communication and procedures that go beyond organizational or territorial borders.
   - Policies of public and private organizations contribute to a safer and lawful use of the Internet. Abuse policies for Internet services do not always include terrorist use of the Internet and are not always applied effectively. In addition, law enforcement activities and government policies are not always tailored to counter the terrorist use of the Internet.
   - Hiding ones real identity on the Internet is easy and common practice.
   - The fast growth of leading Internet companies poses organizational challenges to incorporate legal compliance and knowledge of security issues, including terrorist use of the Internet.
   - It is not always clear how additional security measures, including automated technologies, would relate to privacy protection and the openness of the Internet.

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

General Principles (by all participants)

Traditional types of regulation are not likely to solve all the above mentioned problems. The partners in the Clean IT project (Internet user organizations, Internet companies, Non-Governmental Organizations (NGOs), Law Enforcement Agencies (LEAs) and governments), believe that implementation of a set of best practices, guided by general principles including first and foremost respect for fundamental rights and freedoms, co-created in an open dialogue between the public and private sector, can contribute to reducing the terrorist use of the Internet. Organizations committing to this document will adopt the following general principles:

7. Reducing the terrorist use of the Internet can become more effective and efficient if all organizations involved increase their efforts and increase mutual cooperation.

8. The best practices that will be implemented to reduce terrorist use of the Internet must be effective as well as proportional and legitimate.

9. Additional measures should be incorporated as much as possible in existing programmes, organisations, systems and procedures.

10. All organizations involved must proactively make clear and explain that terrorist use of the Internet is unacceptable, raise awareness of as well as prepare to contribute to reducing terrorist use of the Internet.

11. Public and private organisations will comply with national and European laws and regulation. Any action taken to reduce the terrorist use of the internet, will respect fundamental rights and freedoms, including access to the Internet, freedoms of assembly and expression, privacy and data protection.

12. Internet access providers, content delivery companies and content publishing companies provide services on the Internet and from that perspective have an intermediate position between LEA and persons that use the Internet for terrorist purposes. In case of unequivocally unlawful use of the Internet immediate and proportionate action should be taken in order to stop this unlawful situation. In case organisations involved cannot agree: courts determine what is unlawful.

13. Terrorist use of the Internet must be prevented as much as possible.

14. Internet content delivery and content publishing companies do not have as a primary task to detect terrorist use of their services, but are willing to help in reducing terrorist use of the Internet. These Internet companies must be transparent about the use of automated detection systems for this purpose, these systems must always be consistent with laws and regulations and these systems will not be used to automatically judge (il)legality of or end activities or content.

15. For Internet users it must be made easier and be made possible on more parts of the Internet to report terrorist use of the Internet. Internet companies that offer services to publish information of users, as well as LEAs, must offer reporting mechanisms to Internet users to report terrorist use of the Internet to the Internet company involved or LEA responsible.

16. All organizations must strive to increase both efficiency and effectiveness in reducing the terrorist use of the Internet. Internet companies and LEAs should work and cooperate in a predictable, transparent, professional and respectful manner.

17. Long term public-private cooperation is necessary and will further increase effectiveness and efficiency. While implementing the best practices, all organizations must share knowledge and expertise, as well as to continue to evaluate and improve these general principles and best practices described below. This takes place in a permanent, European platform for public-private dialogue.

Best Practices (by all participants)

Governments, LEAs, NGOs and Internet companies can decide on a voluntary base, complying to the above mentioned general principles, to implement the following proactive, preventive, detective, reactive and learning best practices.

Proactive best practices

18. Government policies.
    Problem: Governments must take an active role in reducing terrorist use of the Internet. However, government policies that address illegal terrorist use of the Internet are not in all cases clearly defined, consistent, tuned to the realities of the Internet, fully implemented, efficient or clearly explained. In addition, some European Union Member States have extensive policies, while others do not, and policies differ between governments, thus limiting synergy.
    Goal: Governments need to implement comprehensive and effective policies, while reducing the differences between national policies to reduce terrorist use of the Internet.
    Benefits: This best practice will make governments, LEAs, NGOs and Internet companies more effective in reducing terrorist use of the Internet.

19. Legislation
    Problem: Waht is terrorist use of the Internet is not always adequately defined or clearly explained. This is also the case for law enforcement and Internet companies mechanisms to deal with terrorist use of the Internet. There are differences in (il)legality between national legislations, which limits both LEA and Internet companies effectiveness in dealing with terrorist use of the Internet.
    Goal: What is illegal terrorist use of the Internet and what are the powers and/or obligations LEAs and Internet companies have, and the relevant procedures, must be clearly stated in national and EU legislation, enforced and explained to users, NGOs, LEAs and Internet companies.
    Benefits: This best practice will make it easier for Internet companies, LEAs, NGOs and governments to assess (il)legality and take action. More cases of terrorist use the Internet will be dealt with.

20. Service/business conditions and acceptable use policies.
    Problem: Not all Internet companies state clearly that they will not tolerate the illegal terrorist use of the Internet on their platforms. 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.
    Goal: Internet companies should ban the illegal terrorist use of the Internet in their terms of service/business conditions and acceptable use policies, and effectively enforce this policy.

Benefit: This best practice would make it easier for Internet companies to take action against clients that use their platform for terrorist purposes. Thereby they can reduce the scale of terrorist incitement, recruitment and training opportunities.

21. Awareness, education and information.
    Problem: The terrorist use of the Internet is currently not widely known and sometimes not well understood. Cyber security awareness, education and information programs exist in a number of European countries, but often do not include terrorism.
    Goal: Children, teenagers, young adults, the circle that surrounds them and the public in general should be (made) aware of the dangers on the Internet, including terrorist use of the Internet. Professionals should know what to do when they are confronted with terrorist content or someone who is radicalizing.
    Benefit: This practice would result in more users who report abuse, increased quality of reporting and reacting to abuse reports. An increased number of real cases of terrorist use of the Internet can be dealt with, and therefore the scale of terrorist incitement, recruitment and training opportunities can be reduced.

Preventive best practices

22. Real identity policies
    Problem: Terrorists (and other criminals) profit from the anonymity that large parts of the Internet offer. Even though anonymity to other users is logical and desirable for some Internet services, for many it is not a necessity. Terrorists are less likely to use services in which they are easily recognizable to other users.
    PM

23. Police patrol on social media
    Problem: Less than in the physical world, Internet users realize their behaviour must be within laws and social norms. On the Internet, users are hardly ever confronted with or reminded of the presence of LEAs, signalling that abusive behaviour will have consequences. On social media platforms, where there is a lot of social interaction, terrorists currently feel secure enough to spread their propaganda on a vast scale and recruit others.
    Goal: LEAs will be visible and active on most relevant social media platforms to deter, detect and react to terrorist use of social media.
    Benefits: Police patrolling on social media will reduce terrorist incitement, recruitment and learning.

Detection best practices

24. Automated detection systems.
    Problem: 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, thus detect far more (possible) terrorist use. Some LEAs, NGOs and Internet companies use such systems to try and detect terrorist activity, but these systems are often not mature enough to be precise and effective, while the use of these systems is not made clear to Internet users and could be endangering Internet Freedom or even be illegal.
    PM

Reporting best practices

25. Flagging/report button systems.
    Problem: Internet users currently don't have enough easy ways of reporting terrorist use of the Internet. In addition, Internet users are not used to report what they believe is illegal. As a consequence, a large part of the terrorist use of the Internet is currently not brought to the attention of Internet companies and LEAs.
    Goal: Providers of specific Internet services should offer simple and user friendly flagging/report button systems on their platforms. Internet companies, as well as LEAs, governments and NGOs should encourage Internet users to use these systems.
    Benefit: This best practice would increase the number of (potential) cases of terrorist use of the Internet that are reported to Internet companies and LEAs. This will allow them to assess (il)legality and take appropriate action, resulting in more real cases being dealt with.

26. Reporting button for websites.
    Problem: Many websites do provide users with an (e-mail)address to report abuse, and effectively handle complaints of abuse. However, terrorist (related) websites usually do not. While many social media platforms offer 'flagging' opportunities and react to their users complaints, few web hosting companies offer similar reporting tools and therefor receive few notifications of terrorist use of websites they host.
    PM

27. Referral units/hotlines.
    Problem: Internet companies have to determine (il)legality of reported cases of (potential) terrorist abuse of their platforms, while they are sometimes lacking the specialist terrorism knowledge or are not willing to fulfil what they regard as a law enforcement role. In other cases Internet companies lack the language skills they need to make a judgment. As a consequence a large number of potential cases of terrorist use of the Internet are not dealt with adequately.
    Goal: Governments or LEAs should have national referral units, to which Internet companies, NGOs and end-users can refer (potential) cases of terrorist activities on the Internet. The referral unit will then determine (il)legality and take appropriate action if necessary.
    Benefits: This best practice will reduce all kinds of terrorist activity on the Internet.

<u>Reactive best practices</u>

28. Notice and take action.
    Problem: When LEAs notify individual Internet companies of probable cases of terrorist use of the Internet, cooperation between a LEA and an Internet company in some cases is not effective or efficient.
    Goal: Internet companies and LEAs need to cooperate effectively, efficiently and in accordance with (national) legislation in notice and take action procedures.
    Benefit: This best practice would result in more cases of illegal terrorist use of the Internet being dealt with, faster and with less effort.

29. Points of contact
    Problem: Governments, Internet companies, LEAs and NGOs not always know whom best to contact on the issue of illegal use of the Internet for terrorist purposes.
    Goal: There should be points of contact for terrorist use of the Internet within each government, LEA, Internet company and NGO. These points of contact should be stable;

they should remain points of contact for a longer period and develop relations with their most important counterparts in other organizations.
Benefits: Establishing points of contact would increase the effectiveness of all types of cooperation to reduce illegal, terrorist use of the Internet.

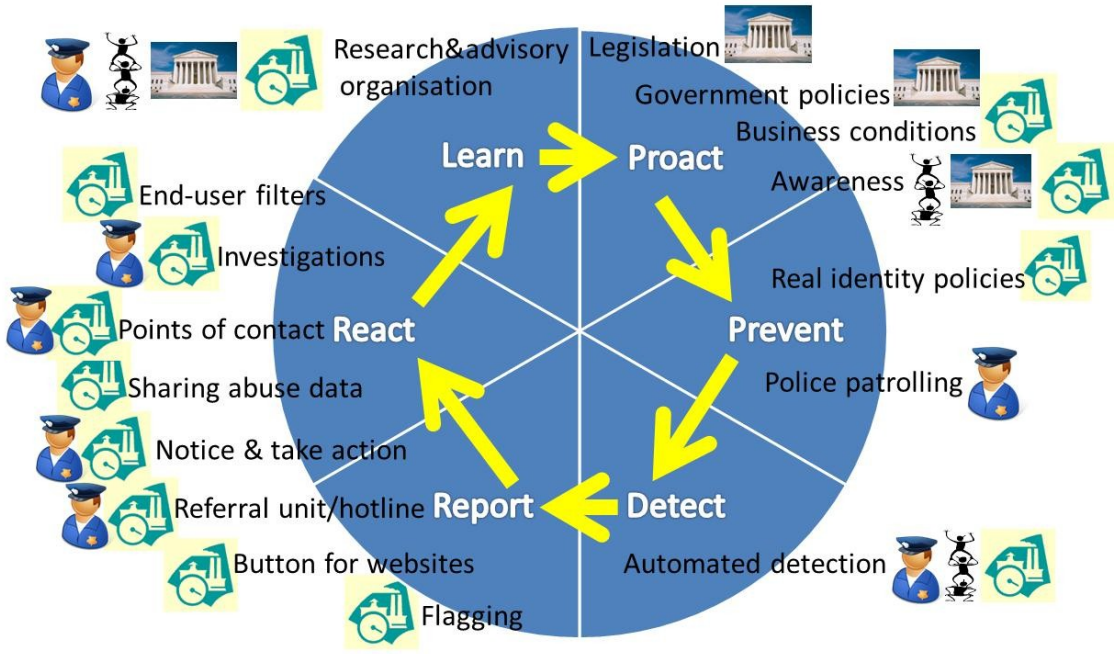
30. Cooperation in investigations.
Problem: When LEAs suspect illegal use of the Internet for terrorist purposes and contact Internet companies to assist in investigations, cooperation between the two is not always effective and efficient.
Goal: Internet companies and LEAs need to cooperate efficiently, effectively and lawfully in investigations of probable illegal terrorist activity on the Internet.
Benefits: This best practice would result in more real cases of terrorist use of the Internet being prosecuted.

31. Sharing abuse data.
Problem: Most Internet companies have to deal with few cases of terrorism on their platforms. When illegal material is removed, terrorists often try to post it on other Internet companies services. Terrorist use of the Internet would be significantly reduced if information removed by one Internet company will not be allowed by large numbers of other companies.
Goal: Internet companies should share data on cases of illegal, terrorist use of the Internet with each other, preferably in automated processes, using trusted partner companies.
Benefits: This best practice would reduce terrorist incitement, recruitment and training.

32. End-user controlled filters.
Problem: Unlike for other types of illegal use of the Internet, few end-user controlled filters that effectively reduce terrorist use of the Internet are currently available.
Goal: Parents and other users should be educated and offered the choice to install end-user control services to identify, log access to or block terrorist and radicalizing content.
Benefits: This best practice would reduce the accessibility of terrorist content and thereby the terrorist incitement, recruitment and learning.

Learning best practice

33. European Research and Advisory Organisation
Problem: There is a lot of unclarity about what is terrorist use of the Internet. Currently there is no organization that gathers and exchanges information on terrorist use of the Internet, both on the pan-European threat and what is different between European countries.
Goal: An organization that is trusted by all parties, should be created to assist LEAs, NGOs and Internet companies in reducing terrorist use of the Internet. This organization will provide advice on what is terrorist use of the Internet.
Benefits: This best practice will reduce terrorist incitement, recruitment and learning on the Internet.



Implementation (by all participants)

34. This document will be published and disseminated to Internet companies, LEAs, governments and NGOs. These organizations will be invited to commit to increasing their efforts to reduce terrorist use of the Internet, and to join a new European, public-private format for dialogue and cooperation to reduce terrorist use of the Internet. Organizations will publish that they have committed and joined.

35. Organizations that commit to this document, commit to the general principles and agree join the dialogue and cooperation, and to seriously consider implementing most if not all the best practices in this document where applicable to them and as far as they do not already apply these. A document containing detailed recommendations on how precisely to implement the best practices has been developed. This will only be shared among organizations that commit and join, and will be further developed with these organizations in the permanent dialogue.