CLEAN IT PROJECT – DETAILED RECOMMENDATIONS DOCUMENT FOR BEST PRACTICES AND PERMANENT DIALOGUE

CONFIDENTIAL / NOT FOR PUBLICATION / LIMITED DISTRIBUTION

This document is not for publication. The recipient may share this document only with others within their organization on a "need-to-know" basis.

NOTE: this document contains detailed recommendations on how to implement the best practices identified in the Clean IT project. It will be developed further in the months ahead. After the end of the Clean IT project it will only be shared with organizations that have committed to implementing the best practices. It will be developed further with these organizations participating in the Clean IT permanent public-private dialogue platform.

Items in this document are not obligatory to organizations to implement, but have met a high degree of consensus, except for the sections 'to be discussed'. Items in the 'to be discussed' sections are either new, need reformulating or are contested. The items formulation includes three degrees to of whether organizations committing to the Clean IT 'draft document' are expected to implement the detailed recommendations in this document: what they 'must', what they 'should' if no specific, pressing situation or interest prevents them to, and what they 'could implement if they want.'

This document will be discussed and developed further in Clean IT project meetings, in Working Groups and the future permanent platform for public-private dialogue.

CLEAN IT PROJECT – DETAILED RECOMMENDATIONS DOCUMENT FOR BEST PRACTICES AND PERMANENT DIALOGUE

CONFIDENTIAL / NOT FOR PUBLICATION / LIMITED DISTRIBUTION

This document is not for publication. The recipient may share this document only with others within their organization on a "need-to-know" basis.

Contents

Implementation

To be discussed:

1. **After committing to this document, organizations will implement the best practices according to the following time schedule.**

   - **Within half a year:**
     - **Governments will review and decide on policies;**
     - **Internet companies will include terrorist use of the Internet in their business conditions and acceptable use policies;**
     - **Existing hotlines will explicitly include terrorist use of the Internet;**
     - **Organizations will appoint Points of Contact.**
   - **Within a year:**
     - **Governments will review and decide on improving legislation;**
     - **LEAs will start a national referral unit, and Internet companies of a country will jointly start a hotline;**
     - **LEAs and Internet companies will implement procedures for notice and take action;**
     - **LEAs and Internet companies will implement procedures for cooperation in investigations;**
     - **LEAs will start patrolling on social media;**
     - **Internet companies will start using flagging systems;**
     - **Internet companies will start to share abuse information;**
     - **A Points of Contact System will be operational;**
     - **National LEAs will implement a police reporting buton.**
   - **Within two years:**
     - **Governments, LEAs, NGOs and Internet companies will do all they can to promote the use and increase the effectiveness of end-user controlled filters on of terrorist use of the Internet;**
     - **Governments, LEAs, NGOs and Internet companies will implement improvements on awareness, information and education,**
     - **Governments, LEAs, NGOs and Internet companies will create European Research and Advisory Organization on terrorist use of the Internet;**
     - **Governments, LEAs, NGOs and Internet companies will start to use automated detection systems;**
     - **Internet companies will implement real identity policies on their platforms;**
     - **At the European level a browser or operating system based reporting button system will be developed and introduced.**

2. **For each best practice an expert, participating organization will be sought to volunteer to coordinate implementation and gather additional detailed recommendations.**

3. **The European Commission will be approached to consider finding a European organization that will adopt the results of Clean IT, continue its activities and host the new European, public-private**

dialogue and cooperation format to reduce terrorist use of the Internet. This organization will organize regular European meetings with a diversity of participants. Participants can be both organizations that have committed to this document and organizations that are considering to commit, as well as experts that give presentations. Discussions will cover the problem of terrorist use of the Internet, how to reduce it and the implementation and up-dating of this document.

4. There will be European Clean IT Working Groups on each of the best practices described above, as well as on research, on new technology (i.e. IPV6, web 3.0, cloud computing, TOR and Internet-via-TV) and new types of terrorist use of the Internet. All organizations that commit to this document are allowed to join the Working Groups. For each best practice one organization is willing to coordinate the implementation, chair the Working Group and lead the dialogue on updating this document and the detailed recommendations on this best practice.

5. Governments that commit to this document will start a national Clean IT dialogue and cooperation format within half a year.

6. Organizations that commit to this document and join the dialogue and cooperation will try to influence policies of other organizations and try to convince them to join and implement the best practices in this document. They will stimulate societal debate about the threat posed by terrorist use of the Internet. This document will also be discussed with the European Commission, other EU Member States, the United States and other befriended non-EU governments, as well as LEAs, NGOs and Internet companies from these countries.

Legal framework

Recommendations:

a. All States committing to the Clean IT document must implement the EU FD 2002 and EU FD 2008;
b. All States must implement the EU Data Directive;
c. Differences States legislation must be analyzed and States must aim for convergence if no specific national interests or conditions warrant differences;
d. When they become aware themselves or are made aware by users or NGOs of terrorist use of the Internet within their infrastructure, Internet companies must be obliged by law to report terrorist use of the Internet to LEAs;
e. Internet companies must be obliged by law to provide LEAs with all necessary customer information for investigations of terrorist use of the Internet;
f. It must be legal for police officers to 'patrol' on social media. This includes having a profile, joining user groups, sending and receiving messages, on the platform;
g. Any organization must be allowed by law to provide for the implementation of end-user controlled filters for the Internet use of their employees.

To be discussed:

1. **Knowingly providing hyperlinks on websites to terrorist content must be defined by law as illegal just like the terrorist content itself;**
2. **States must make clear that original terrorist content and terrorist activities on the Internet of people and organisations on the UN/EU/national terrorist sanction list is illegal and should not be allowed on Internet company platforms;**
3. **It must be legal (under privacy legislation) for Internet companies to ask (new) customers/users to identify themselves towards the company, in order to apply real identity policies;**
4. **It must be legal for LEAs to make Internet companies aware of terrorist content on their infrastructure ('flagging') that should be removed, without following the more labour intensive and formal procedures for 'notice and take action';**
5. **Judges, Public Prosecutors and (specialized) police offers must be legally allowed to order by means of a notice and take action procedure to (temporarily) remove terrorist content from the Internet;**
6. **Legislation must make clear Internet companies are obliged to try and detect to a reasonable degree (costs of and availability of technology for detection) terrorist use of the infrastructure and can be held responsible for not removing (user generated) content they host/have users posted on their platforms if they do not make reasonable effort in detection;**
7. **Companies providing end-user controlled filtering systems and their customers should be obliged by law to report cases of illegal use of the Internet for terrorist purposes they encounter;**
8. **It should be legal and obligatory for Internet companies to store data on terrorist content removed from their platform until they can hand this data to LEA;**
9. **Governments must start a full review of existing national legislation on reducing terrorist use of the Internet, after this start improving legislation and puting more effort into explaining existing legislation;**

10. **The Council Regulation (EC) No 881/2002 of 27 May 2002 (art 1.2) should be explained 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;**
11. **(National) legislation should make clear that knowingly sending false reports to Internet referral units is illegal and punishable, just like intentionally false calling of '911' in (some) countries is.**
12. **Youth protection legislation must (be expanded to) include protection against terrorist use of the Internet.**

Government Policies

Recommendations:

a. Governments must reduce the time needed for international (legal) action against content in another country;
b. Governments and LEAs could help Internet companies by sharing information on specific phenomena of illegal content and have programs to educate web moderators;
c. Governments should (help) starting or support referral organization(s) for users, NGOs and Internet companies to report to and handle potential cases of the use of the Internet for terrorist purposes;
d. Governments must strive to good cooperation between LEA's and Internet companies;
e. Governments should stimulate self-regulation by Internet companies;
f. Governments must make sure competent agencies have enough capacity to deal effectively with the use of the Internet for all kinds of terrorist purposes;
g. Governments must increase awareness programs to the general public;
h. Governments (and LEA's) must include reducing the use of the Internet for terrorist purposes in foreign policy and international cooperation or increase efforts in this field;

To be discussed:

1. **Governments must have LEA's or intelligence agencies monitor terrorist use of the Internet, but only monitor specific threats, not primarily the population as a whole and all Internet use;**
2. **Governments must have clear policies on intelligence gathering and when to take action, against terrorist or radicalizing content on the Internet;**
3. **Governments must have specialized police officer(s) 'patrol' on social media;**
4. **Governments must include reducing terrorist use of the Internet as an integral part of their Cyber Security Strategy;**
5. **Governments must stimulate mid-term (> 5 year) technological development as well as stimulate research and academic discussion;**
6. **Governments must disseminate lists of illegal, terrorist websites;**
7. **Governments must disseminate lists of domain names that can are not allowed to be registered, to prevent terrorist propaganda;**
8. **Governments must subsidize competent NGOs that substantially contribute to reducing terrorist use of the Internet and radicalizing content on the Internet;**
9. **Governments should implement filtering systems to block or detect civil servants to illegal, terrorist use of the Internet;**
10. **Governments should subsidize the initial development of software for sharing between Internet companies specific data of terrorist use of the Internet;**
11. **Governments should include Internet companies' track record on reducing terrorist use of the Internet as a criterion in purchasing policies and Public Relation policies;**
12. **Governments could have programs to educate web moderators;**
13. **Governments could implement counter narrative policies and projects.**

End-User Controlled Filters

Recommendations:

a. End-user filtering is the responsibility of the private network owners and operators. They have direct responsibility for the online environment that they provide to their users;
b. 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 illegal content;
c. Attempted access to defined illegal content from within private networks is generally not recorded and on that basis not legally required to be reported to the relevant authorities by the network owner;
d. Governments and LEAs should (through a trusted international intermediary) provide regular, clear and precise information of what is illegal content and activities to known filtering vendors. The information as a minimum should include:
    - the specific URL (or domain if appropriate);
    - the submitting organization;
    - the legislative reference;
    - the jurisdiction where the content is considered to be illegal;
    - the date submitted;
    - a referral contact email / telephone number;

    The information could also include:
    - identification of the elements of page which are deemed to be illegal to enable on-going 'product training';
e. End-user filter providers should enable their products to be configured with specific network owner OPT-IN categorisation 'blocklists. For example: UK Government Illegal Content List;
f. The blockpage when attempting to access known illegal content should have the option to display the reason, organisation, jurisdiction and legislative reference for the blocking action. A process to challenge the block directly with the issuing organisation should be instigated - this should not be through the vendor or private network owner;
g. Increased levels of security (physical, data, personnel) will be required when dealing with terrorist content or information;
h. Private network operators that use filtering technology already provide their users protection from 'inappropriate content' – this includes all manner of content that does not fit with their culture and objectives. The term 'inappropriate' in this context is subjective and based on the type, level and quality of the filtering the organization users.
i. 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. Regular briefings by governments and LEAs would enable these content categories to be updated and maintained ensuring more accurate filtering. It should be considered best practice to ensure that the briefings covered a wide range of international content.

To be discussed:

1. **Companies providing end-user controlled filtering systems should use the output of the proposed the European Advisory Foundation;**
2. **Companies providing end-user controlled filtering systems should provide users the choice to block any terrorist content and terrorist activity by persons and organizations on the UN/EU/national terrorism sanction lists. The company should include data to this end in its systems, so this content can be detected;**
3. **All kinds of Internet companies, LEAs and NGOs, but not governments, should promote the use of end-user controlled filters among their clients, the public and supporters;**
4. **Filtering by companies at infrastructure level should not be promoted;**
5. **Social media platforms should offer their users filters that block access to or warn for terrorist content;**
6. **Browser companies should offer their users parental control or other end-user control filters based on the blacklist principle;**
7. **End-user controlled filters must meet market standards (ie CEN/PC 365).**

Flagging/Report Button Systems

Recommendations:

a. Flagging/report button systems must be implemented.
b. Users must be provided an way to flag/report terrorism and radicalizing content as a separate, specific category to flag/report. Technologies for this include description fields, drop down lists and links to special reporting pages;
c. Providers of chat boxes, e-mail services, messaging systems, social networks, retailing sites, voice over Internet protocol (if technically possible the session and/or the user) and web forums, must have flagging systems.
d. Hosted websites must have an easily visible abuse reporting email addresses or contact form. Creating a browser/operating system based reporting tool that would signal abuse to hosting companies should be developed;
e. How flagging/reporting works must be explained by service providers to their users.
f. The anonymity of the reporter must be preserved. Reporter details must never be shown to content owners;
g. Internet companies must be sufficiently (quantity and quality) staffed or supported to handle reports. Recognizing illegal, terrorist use of the Internet requires specialist knowledge on terrorism, (national) legislation and (national) cultural differences;
h. Reports of (potential) cases of terrorist use of the platform must be analyzed. Clearly illegal terrorist activity must be reported to LEAs immediately;
i. Specialized NGOs should actively flag what is (deemed) illegal terrorist content;
j. LEAs should primarily use formal ways of notifying Internet companies (notice and take action). In some countries flagging is also regarded as a formal notification;
k. Internet companies could extend a higher credibility status to trusted flagging organizations, like LEAs and specialized NGOs. Users could also be provided higher credibility status based on their (calculated) reputation in successfully reporting abuse. Higher credibility statuses should not lead to automatic removals, but rather serve to prioritize handling reports or assist in deciding on (il)legality;
l. Governments, LEAs, NGOs and Internet companies should encourage flagging/reporting as a way of notifying Internet companies on terrorist use of the Internet.

To be discussed (new or contested):

1. **Small Internet companies should also organize handling reports of terrorist activity on the infrastructure. This could be done by outsourcing this work to a (specialized) company.**
2. **Outsourcing abuse handling should not limit the ability to rightly decide on (il)legality.**
3. **On Voice over IP services it must be possible to flag users for terrorist activity. If messaging systems are attached, it must also be possible to flag specific messages. Some Voice over IP technologies allow for conversations to be flagged;**
4. **Internet companies offering users the opportunity to create their own subgroups, should make flagging/reporting buttons available on these subgroups (and for the moderators to remove content after being signaled).**

Service/Business Conditions

Recommendations:

a. No wording of European standard service/business conditions or abuse policy should be recommended. What may well be recommended is a best practice how to handle abuse, and how to make such policy transparent;
b. Acceptable use policies do not create new legal rights for third parties, but solely govern the relationship between the respective service provider and customer, unless stated otherwise (e. g. a "reaction guarantee" towards everyone within the context of complaints about alleged copyright violations in order to avoid lawsuits).
c. Local law and what is considered as unwanted by local society must be a decisive factor. "Unwanted by local society" might refer to content which is fully legal and which may also be in line with terms and conditions of the relevant service provider. Internet companies may or may not declare content unwanted for ethical or business reasons, on which there should be no recommendation;
d. Access providers should refrain from developing these policies, as access-blocking is not a recommendable option;
e. Internet companies must have sufficiently staffed and capable abuse departments or services to effectively enforce policy;
f. Internet companies should assure that content that has been removed once can not be uploaded onto the platform again, including when the content has been slightly modified if this can be achieved technologically and at reasonable cost. This does not apply to content which is only removed because of the context which it has been presented in;
g. Before Internet companies remove illegal, terrorist content, they should inform LEA and store the blocked data for possible LEA investigations. LEAs should very quickly, e. g. within three days, make further arrangements;
h. If possible technologically and only to reasonable costs, Internet companies should use automated processes to search or detect potentially unacceptable use (according to a defined policy);
i. Service/business conditions and abuse policies should not be very detailed in describing terrorist activity. A very detailed description will very likely cause gaps;
j. If two persons/institutions are arguing about legality/illegality, it should be possible for the service provider to ask those persons/institutions to settle the dispute and to wait for a final decision (agreement or a court decision). If the content is kept online meanwhile, the service provider should not be liable in that case, except where the illegality is obvious. The service provider should have the possibility to make removal dependent on a promise of indemnification made to the service provider (this problem does not arise in case of a court order).

To be discussed (new or contested):

1. **Service/business conditions should point at the UN/EU/national terrorist sanction lists as the first reference for determining what is terrorist content and terrorist activity;**
2. **The use of platforms in languages abuse specialists or abuse systems do not master should be unacceptable and preferably technically impossible.**

3. **Providers of chat boxes, e-mail services, hosting, messaging systems, social networks, retailing sites, voice-over Internet protocol and web forums, must include terrorist use in their service/business conditions and acceptable use policies;**
4. **Different types of Internet companies need to include banning terrorist use of their services in different ways;**
5. **Internet companies should effectively enforce their ban of terrorist use of their platform. This includes having abuse departments with the required expertise, capacity proportionate to their number of users (for which a benchmark will be developed) and the volume of terrorist use of their service.**

Notice and Take Action

Recommendations:

a. Notification is a message by a competent national law enforcement authority or Public Prosecutor ordering an Internet company to take action against terrorist use of the Internet;
b. Internet companies should remove content as fast as possible;
c. Internet companies must have clear and fast procedures to take action after receiving notifications;
d. LEAs must contextualize the likely terrorist content and describe how it is breaching (national) legislation;
e. LEAs must be very specific on the type of information at Internet companies they want removed, including storage of disputed data and where (locally or worldwide) it should be removed;
f. Development and implementation of a EU standard format for notice and take action is not be desirable;
g. Internet companies should send a reply to all notifications send to them by recognizable authorities and specialized NGOs;
h. In some cases LEAs must send notice that access to content must be blocked;
i. In some cases LEAs must send notice that domain registration must be ended+
j. In some cases notice and take action procedures must lead to security certificates of sites to be downgraded.

To be discussed (new or contested):

1. **For this best practice 'Internet companies' applies to: providers of chat boxes, e-mail services, file sharing, hosting, messaging systems, social networks, e-commerce sites, voice-over Internet protocol and web forums;**
2. **In case an Internet company does not agree that the national competent authority is correctly pointing at terrorist use of the Internet, it does not have to and should not be forced to take action;**
3. **Meta data of terrorist use of the Internet, once being ended by an Internet company, should be shared with as many as possible other Internet companies (see best practice 'sharing abuse data').**
4. **The content or other data about the terrorist use of the Internet taken action against, should be stored and handed to LEA (see best practice 'investigations').**

Investigations

Recommendations:

a. LEAs should exchange knowledge on the complexity and workings of the Internet as well as the role of the Internet company involved in their investigations;
b. LEAs must 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 / data should not be ceased by taking the physical deviced but by making a mere copy);
c. Feedback on anonymous cases to the ISP's involved in investigations is desirable. This should preferably be done through federations;
d. The Legal base of the request should always be clear and must be presented;
e. Better streamlining of contact points in case of an investigation is desirable ("a single point of contact");
f. A system of adequate compensation by government in case of investigations and efforts made by ISP's should be put in place.

To be discussed:

1. **Internet companies and LEAs must publish their policies on which data they share and how long data is stored after investigations end.**
2. **How best to organize international investigations?**
3. **How should privacy be protected?**
4. **Is legislation on investigating adequate? Is clear what an Internet company must provide as information, including what it should store as information?**

Awareness

Recommendations:

a. Governments, LEAs, Internet companies and NGOs should cooperate to increase awareness, education and information on illegal, terrorist use of the Internet;
b. Preferably, public and/or privately funded NGOs should lead awareness, education and information programs. Government campaigns can help, while Internet companies can support these initiatives and publish more information on terrorism on their websites.
c. Expertise on reducing the use of the Internet for terrorist purposes must also be shared internationally, outside the EU;
d. Awareness of options for Internet users to report for terrorist use of the Internet should be increased;
e. Governments and LEAs could send e-mail threat updates and general information on terrorist activity on the Internet relevant to Internet companies (and NGOs);
f. Governments and LEAs must increase knowledge about the complexity of the Internet and the different roles individual ICCs have;
g. Governments, LEAs, NGOs and Internet companies could employ or use former terrorists and victims to reduce radicalization online.
h. There should be educational programs on Internet literacy on schools an educational institutes. These programs should (also) address terrorist use of the Internet and its dangers, particularly to vulnerable persons.
i. Awareness programs on radicalization through the Internet should be developed, including how Internet users can recognize the signs of radicalization.
j. Awareness programs should be creative and appealing to the younger generation. This can be done by involving youth in developing programs, using the latest technology and involving former radicals and victims.

To be discussed:

1. **Existing programs and organizations should be used and expanded as much as possible;**
2. **There is a need to increase user activity and the quality of notifications, also by education professionals in governments, LEAs, NGOs and Internet companies.**
3. **Governments, in cooperation with LEAs, NGOs and Internet companies, must establish new or expand the scope of existing helplines for terrorist use of the Internet.**

Points of Contact

Recommendations:

a. A trusted points of contact system should facilitate cooperation between organisations committed to implementing the Clean IT results on a strategic and policy level;
b. Points of contact must be experts able to represent their organization as well as be able to reach the right persons within their own organization;
c. Points of contact should always be available;
d. Between points of contact a culture of openness, stimulating to be contacted and to get into contact, needs to be created;
e. Government points of contact should come from counter-terrorism authorities and serve as the primary point of contact in cross border issues;
f. National and European lists of points of contact should be provided to other points of contact on a "need to know" basis.

To be discussed (new or contested):

1. **A European organisation, preferably Europol, should operate and host this points of contact system;**
2. **The points of contact system should use secure communication lines (email, telephone, dissemination of contact information, document sharing);**
3. **Persons in the points of contact systems that are regularly and repeatedly complained about their performance, should be removed from the system, and replace by another person from the same organisation;**
4. **Large Internet companies should not have to deal, if they do not want to, with too many individual LEAs and NGOs, but only a few representatives. It would be good if regular telephone calls are organised to discuss overall contacts and cooperation. It would also be desirable to channel requests to these companies via a limited number of (government or LEA contacts);**
5. **Only persons committed to implementing the Clean IT 'draft document' practices should be included in the Points of Contact System. Plus some recognized and 'logical' LEA, government and academic/research specialists.**

Research and Advisory Organization

Recommendations:

a. The Organization will provide research and advice on terrorist and other content which is recognised as dangerous throughout the EU and in each individual country;
b. The Organisation should be independent, with a 'partnership' stature in the EU;
c. The relation with the EU will depend on the specific design and therefore legal and authoritative standing of the Organisation, however best practice is promulgated, it needs to be recognised as neutral;
d. The Organization should be part of a University, as academic funding provides a means of support without political interference;
e. The organization must include staff drawn from, not representatives of, governments, LEAs, Internet companies, NGOs and academic institutions;
f. The Organization should provide advice on:
    - Legislation & jurisprudence;
    - Academic work on the subject;
    - Material that can be researched and used for 'machine-learning';
    - Known terrorist and extremist content;
    - Hate Speech;
    - Information on the technologies used by terrorists;
g. The Organization must be a collator of material and an authoritative source of materials recognised as terrorist content. The Organisations database should be secure as the material kept within it would be dangerous. Its content must be shared without running the risk that it gets out and is misused. An Academic institution may provide the most effective balance on how to handle dangerous materials in a transparent way;
h. The Organisation should take on the challenge of trying out different categorisations of content to see which work, as at this stage there is not clear which single effective model it should adopt;
i. The Organization must work with organizations who code machines like filters and web crawlers for the provision of learning materials. It will be a centre of excellence for the techniques that they would need to develop in analysing material to understand its impact and therefore likely harm.

To be discussed:

1. **(How) should this organization be under democratic control?**
2. **How should this organization ensure transparency?**
3. **What is the relation between this advisory organization and the organization hosting or created as a successor to the Clean IT?**
4. **What is the relation with the best practice of sharing abuse data?**
5. **How should this organization be governed?**
6. **What legal issues need to be discussed for creating such an organization?**

Share Abuse Data

Recommendations:

a. Exchange via email should be preferred as e-mail is reliable and there is no need for an institution to run and maintain a system that is exchanging the data;
b. Since it is very important to use existing mechanisms, xarf (http://x-arf.org) must be used as a format for data exchange. This format is very easy to understand, implement and process. It is already used for other kinds of reports and can be extended in an easy way. This way the exchange of data will be open for any future types of abuse data;
c. Any kind of content or abuse data could be shared (videos, pictures, IP-addresses, email addresses). This must include a timestamp. Everything else is optional. For all different kinds of reports the mandatory and optional information that should be shared must be defined. To define this the need and (il)legality of attaching and sharing the terrorist content must be considered, as well as the differing (il)legality in various countries.
d. Terrorist content should not be stored centrally in the sharing system, for security reasons. It might be interesting to consider including LEAs, Europol, the proposed European Advisory Organization or academic institutions in the system, to point them at the content involved;
e. To start increasing the amount of reports of terrorist content being shared through the system, data providers such as filter vendors, LEAs and NGOs that keep track on such activities must be invite and start to participate. With a few institutions like this involved the system can easily be scaled to more and more institutions. Maybe some kind of small software that helps reporting is needed, which must be developed and which can make it easier to scale reporting in later stages.

To be discussed:

1. **As to Internet companies this best practice applies to: providers of chat boxes, domain registration, e-mail services, end-user control filters, hosting, messaging systems, social networks, e-commerce sites, voice-over Internet protocol and web forums;**
2. **Would it be wise to allow only trusted NGOs to participate?**
3. **How should privacy be guaranteed? Should persons/organisations have a way to request being taken out of the system, just like with spam?**
4. **Is legislation adequate for sharing terrorist abuse data?**
5. **Is participation by LEAs covered by existing legislation?**
6. **Should hotlines and referral units participate in the sharing of terrorist abuse information?**

Referral Units/Hotlines

To be discussed (new):

1. **Each country should have a LEA operated referral unit and an Internet industry operated hotline;**
2. **All persons and organizations, all Internet users must be allowed to alert hotlines and referral unit;**
3. **All kinds of terrorist use of the Internet must be allowed to be reported to the units/hotline (websites, videos, messages, emails, profiles);**
4. **Referral units/hotlines must operate a webpage for Internet users to report (among others) terrorist use of the Internet.**
5. **Persons reporting a case to a hotline/referral unit should be informed as to the progress, check the status themselves and the results of the investigation following their report.**
6. **Referral units should be operated by police officers.**
7. **Referral units of different countries should coordinate their services for very uncommon languages often used in case of terrorism, making sure they can collectively handle (potential) terrorist content in any language.**
8. **Police coming across terrorist use of the Internet should hand these cases to their (national) referral unit, having more expertise in dealing with (potential) terrorist use of the Internet.**
9. **National referral units should build relations with other national referral units. Potential cases of terrorist use of the Internet should be handled by/handed over to the (legally) most competent national referral unit (language skills, terrorists involved, jurisdiction).**
10. **Referral units must contribute to awareness, education and information efforts on terrorist use of the Internet.**
11. **Referral units should have excellent cooperation with all other relevant national agencies and authorities in law enforcement and intelligence;**
12. **Referral units should be legally allowed to send notifications or otherwise start Notice and Take action procedures;**
13. **Referral units must develop and maintain working relations with (most relevant) Internet companies and their industry representatives**
14. **Referral units/hotlines must promote the 'reporting button for hosted websites', which is one of the other best practices in Clean IT.**

Real Identity Policies

To be discussed (new):

1. **Internet companies must only ask customers/users to identify themselves if (national) (privacy) legislation allows this.**
2. **In this best practice 'Internet companies', unless specified, refers to: providers of chat boxes, domain registration, e-mail services, hosting, messaging systems, social networks, e-commerce sites, voice-over Internet protocol and web forums;**
3. **A number of Internet services, platforms or formula's for clear reasons require anonymity of users towards each other or towards the Internet company offering this service. This includes services for human-rights activists in undemocratic societies;**
4. **Internet companies must allow only real, common names. These must be entered when registering. On request of the Internet company, a registrant must provide proof of the real or common name. Internet companies can request to prove the real or common name also after a user has been flagged, signalled or reported.**
5. **Social media companies must allow only real pictures of users;**
6. **Internet companies must implement verified billing processes for users;**
7. **Internet companies must know and store the real identity and contact information of users and customers, in order to provide at least this information to LEAs in case of an investigation into (potential) terrorist use of the Internet.**

Virtual community policing

To be discussed (new):

1. **Virtual community policing must be used to find and connect to persons in danger to get radicalized.**
2. **To reduce terrorist use of the Internet virtual community police officers should (also) be active on those social media platforms known for terrorist or radicalizing activity.**
3. **Virtual community policing must be used to discuss with and state to Internet users what is terrorist use of the Internet, and what will be the consequences of illegal behavior.**
4. **Virtual police officers should be easily recognizable, make clear they are real policemen, and use their real photo's, names and various ways to contact them.**
5. **Virtual police officers should use easy to understand ('popular') language, friendly icons and profile photographs, in order to lower the threshold of being contacted and in order to be effective in combination with (often younger) users of the social medium.**
6. **Virtual community policing must be used to show law enforcement is present, is watchful, in order to prevent terrorist use of the Internet and make regular users feel more secure.**
7. **Virtual police offers must organize ways that other users of the social media can 'follow' or 'link' (to) them to increase awareness of terrorist use of the social medium and what is being or can be done against it.**
8. **Virtual police officers should become members in extremist and terrorist fora as much as possible, subscribe to news, mailing and alerts etc. to be able to detect any terrorist content or activity.**
9. **Virtual police officers do not have additional legal authority, meaning no different powers than LEA has in dealing with terrorist use of the Internet.**
10. **Virtual police officers should contact the abuse department of the social medium or 'flag' in case of terrorist use of the Internet, as well as the criminal investigations department of LEA or intelligence services.**
11. **Virtual police officers should act on any terrorist content or activity they encounter, not only which is (clearly) related to their country, geographical unit or specialism.**
12. **Virtual police officers should also discuss with parents the dangers of radicalization of their children via social media.**

Semi-automated detection

To be discussed:

1. Automated detection systems must be used by LEAs, NGOs and Internet companies (in this best practice referring to providers of access, browsers, chat boxes, e-mail services, exchange points, file sharing, hosting, messaging systems, social networks, e-commerce sites, voice-over Internet protocol and web forums).
2. The use of automated detection systems by Internet companies must be published and made known to their Internet users, including a general description of its working;
3. The use of automated detection systems must be in accordance with national legislation;
4. Accordance with national legislation should be established and published on a regular basis by an independent accountant in conformity with EDP auditing standards;
5. Automated detection systems should comply with market standards;
6. Automated detection could search for known terrorist organizations logo's, content (video's, pictures and publications), IP-adresses, names, email adresses, hyperlinks, keywords (ideological terminology, cursing);
7. Governments and LEAs must offer assistance to Internet companies developing or using automated detection systems;
8. Automated detection systems should only be used to signal to abuse officers where on their platforms might be terrorist use of the Internet. These systems must not be use to automatically remove content of users;
9. All terrorist use of the Internet signaled by the automated detection system and after that judged as such by the abuse officer of an Internet company, must be removed from the Internet, and put to the attention of LEA as soon as possible;
10. All terrorist use of the Internet signaled by the automated detection system and after that judged as such by an NGO must be put to the attention the Internet company and the competent LEA as soon as possible;
11. All terrorist use of the Internet signalled by the automated detection system and after that judged as such by a LEA officer must start a notice and take action procedure towards the Internet company as soon as possible.

Police button

To be discussed (new): NB 1-11 and 12-15 are about 2 different reporting button systems.

1. **Like it is used in a number of EU Member States, LEAs should develop and offer for free to Internet companies a national police reporting button;**
2. **The technology for the system (logo, hyperlink, secure messaging etc) must be developed, financed and owned by LEA;**
3. **LEA must invite and cooperate with (the most important) Internet companies in their country to develop, implement and promote the system;**
4. **The police reporting button system must be user friendly and allow anonymous reporting;**
5. **The system must allow to attach hyperlinks, video's, pictures etc. to a report to the police;**
6. **Internet companies should offer their users the police reporting button or add the police button to the websites they host;**
7. **Governments, LEAs, Internet companies and NGOs will promote the implementation and use of this reporting button (in media, on websites, at schools/universities);**
8. **LEAs must put effort into motivating moderators and other frequent 'users' of Internet platforms to send tip-offs for unusual behavior and radicalization;**
9. **LEAs must analyze all tip-offs sent via the system;**
10. **LEAs must have sufficient capacity to operate the system and handle tip-offs;**
11. **LEAs must record the usefulness of each tip-off, calculate the reputation of persons (IP-addresses), and respond faster to persons with higher reputation rank.**

12. **At the European level a browser or operating system based reporting button must be developed;**
13. **The browser or operating system base reporting button must send a signal to the Internet company involved, which will take appropriate action;**
14. **The system will also send a signal to LEA, which after some time will check whether it is satisfied with the action taken by the Internet company and could chose to start a formal notice and action procedure,**
15. **Governments will start drafting legislation that will make offering such a system to Internet users obligatory for browser or operating system service company as a condition of selling their products in this country or the European Union.**