Reducing terrorist use of the Internet

The result of a structured public-private dialogue between government representatives, academics, Internet industry, Internet users and non-governmental organizations in the European Union.

Reducing terrorist use of the Internet

The result of a structured public-private dialogue between government representatives, academics, Internet industry, Internet users and non-governmental organizations in the European Union.

Clean IT project, January 2013

Contents

Introduction

Internet and counter-terrorism
The Internet plays a positive role in our lives and societies, but it is also used for illegal purposes, including terrorism. Terrorist use of the Internet has been researched in the past, and attempts have been made to include terrorist use of Internet in the fight against terrorism. None of these attempts, however, were based on a systematic dialogue with the private sector and civil society. Such government-only initiatives run the risk of resulting in legislation which is technically unfeasible, unworkable, insufficiently supported by end users or in conflict with fundamental rights and freedoms.

The Internet is largely operated by private organizations, and it is there and in civil society that most Internet expertise is concentrated. Conversely, law enforcement agencies and intelligence services possess the most knowledge about terrorist activities. Public-private dialogue is therefore a logical approach in identifying the best instruments to reduce terrorist use of the Internet.

In 2010 the targeted call for proposal "illegal use of internet" was published under the programme "prevention and fight against crime". The European Commission called for public-private cooperation to develop and exchange efficient methods of monitoring the Internet for terrorist content and combating it.

Experienced by an earlier cooperation with Germany and United Kingdom in the preceding project "Exploring the Islamist extremist web of Europe", the Netherlands submitted a project proposal called "Clean IT".

Clean IT project
The objectives of the Clean IT project were:

a. To start a constructive public-private dialogue about terrorist use of the Internet.

Because the Internet is a collective good, the ambition is to have an equal representation of public and private interests. It is vital, moreover, that all participants in the dialogue share the same perception of what is understood to be terrorist use of the Internet. The Clean IT meetings were set up to accommodate both these aims.

b. To draft a set of "general principles" that are supported by both public and private parties.

The project did not aim to find results in a legislative form. The "general principles" have the status of a code of conduct, as encouraged for example by the European Commission in article 16 of the E-commerce guideline. The general principles are supported by the parties involved and provide direction on how to deal with terrorist use of the Internet.

c. To identify "best practices" which, after possible modification, could in the opinion of the Clean IT participants contribute to a successful reduction of the impact of terrorist use of the Internet.

Because the Clean IT project had a non-legislative approach, the results cannot be binding in any way. The use of best practices and compliance with the general principles cannot be enforced legally. Organizations are free to use the results of Clean IT, but the implementation of these results is not included in the project objectives and responsibilities.

Project organization

The project was started in June 2011 with the financial support of the European Commission and five government partners: from Belgium (Coordination Unit for Threat Analysis), Germany (Federal Ministry of the Interior), the Netherlands (National Coordinator for Counterterrorism and Security), Spain (Centro Nacional de Coordinación Antiterrorista) and the United Kingdom (Office for Security and Counter Terrorism). During the course of the project six government partners were added: from Austria (Federal Ministry of the Interior), Denmark, Greece (Hellenic Police), Hungary (Counter-terrorism Centre), Romania (Romanian Intelligence Service) and Portugal (Polícia Judiciária). The Clean IT project organised an innovative process by which public and private sector organizations engaged in an open and constructive dialogue. In this dialogue, both terrorist use of the Internet and possible ways to further reduce it were explored. The project team facilitated this dialogue. Clean IT scheduled six two-day meetings (in Amsterdam, Madrid, Brussels, Berlin, Utrecht and Vienna) in which groups of 20-60 participants met. Meetings consisted of presentations and open discussions aimed at reaching consensus.

The document

This document is a product of the Clean IT project and was published in January 2013. It reflects the combined views of the participants as a whole on how to reduce terrorist use of the Internet. Individual participants or the organizations they represent do not necessarily agree with all parts of the text. Some parts of the document might still trigger the need for further, detailed discussions.

This document consists of three parts. The 'Preamble' was drafted by government participants only, because it is primarily a task of governments to describe the threat of terrorism, and how terrorists use the Internet, why it is difficult to reduce terrorist use of the Internet, and why public and private organizations should discuss and cooperate to reduce terrorist use of the Internet. The last section of the 'Preamble' (H) invites all organizations interested or involved to join in a permanent public-private dialogue, to commit to the general principles and/or choose which best practices to implement.

The 'General Principles' in Chapter 3 determine nine conditions for any action taken to reduce the terrorist use of the Internet. The participants endorsed these nine principles.

Chapter 4 puts forward twelve best practices that could reduce terrorist use of the Internet in the EU. As these emerged from a public-private dialogue, any future implementation can only be voluntary and according to existing laws and regulations. For each best practice, in a separate paragraph, the challenge that best practice is meant to overcome, what the best practice consists of, as well as more detailed explanations of and considerations on the best practice are described.

The Clean IT project team,
The Hague, January 2013.

1 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, 2002/475/JHA of 13 June 2002 on combating terrorism). The EU has further identified the following offences as being 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).

Terrorist use of the Internet
In this document "terrorist use of the Internet" refers to the use of the Internet for terrorist purposes, which is illegal, including for public provocation (radicalisation,[1] incitement, propaganda or glorification), recruitment, training (learning), planning and organizing terrorist activities.

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 is and may be used, where appropriate: providers of access, browsers, chat boxes, e-mail services, end-user controlled filters, hosting, messaging systems, social networks, e-commerce sites and web forums.

Competent authority
In this document "competent authority" refers to a public organization that has the authority, in its jurisdiction, to authoritatively act on terrorist use of the Internet. Which public organization(s) are competent authorities differs between EU Member States and may include the police, specialised agencies, courts and ministries.

General principle
A "general principle" is a fundamental and guiding idea or belief that should be applied in activities or thinking about reducing terrorist use of the Internet, including the best practices and dialogue described in this document.

Best practice
In this document "best practice" refers to existing instruments or concepts, as identified by participants, to reduce terrorist use of the Internet.

[1] Radicalisation is a process by which an individual or group comes to adopt increasingly extreme ideals and aspirations, and as a result might become violent/commit acts of violence.

2 Preamble

A. Terrorism does not recognize borders and may affect all EU Member States and citizens. Individual terrorists and groups of terrorists intend to seriously threaten the democratic values of our societies and 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 EU legislation, some terrorist use of the Internet still takes place within the EU, while terrorist use of the Internet also emanates from outside the EU. [2]

C. Terrorists use the Internet on a daily basis. Terrorists do not primarily use the Internet as a weapon to attack other targets yet, but mainly as a resource. From a technical perspective, terrorist use of the Internet is not substantially different from regular, legal use of the Internet. Terrorists use the same easy to access, easy to use or more advanced Internet services as other users do. Terrorists use social media to spread violent propaganda material and begin the process of finding new recruits and radicalisation. Those who are interested are attracted to more ideological websites, which often glorify and encourage violence, and which are used to distribute training manuals and other information on how to plan, organize and commit deadly attacks and other serious crimes.[3]

D. While in practice it is difficult to assess whether specific content or activity is actually terrorist, some activities on the Internet are not, such as political speech, reporting about terrorism in the media and research on terrorism for academic purposes.

E. Reducing terrorist use of the Internet will reduce other terrorist activities and reduce the likelihood of terrorist attacks. Public organizations and NGOs have a duty to protect society from terrorist attacks, but because the Internet is largely privately owned and operated, a public-private approach is required to reduce the terrorist use of the Internet.

[2] Europol, 'TE-SAT 2012, EU Terrorism Situation and Trend Report', The Hague, 2012, pages 10-11. The Security Council of the United Nations (2010, resolution number 1963) expressed "concern at the increased use ... by terrorists of ... the Internet, for the purposes of the recruitment and incitement as well as for the financing, planning and preparation of their activities."

[3] See for a longer description of terrorist use of the Internet i.e. "The use of the Internet for terrorist purposes", United Nations Office on Drugs and Crime, Vienna/New York, 2012, pages 3-12.

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 governed by one system of rule of law.
   - 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 worldwide and even between EU Member States.
   - EU and Member States legislation and jurisdiction covers only a part of the Internet.
   - Illegal content itself does not always lead to radicalisation 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.

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 and has direct access to the infrastructure.
   - Reducing terrorist use of the Internet requires communication and procedures that go beyond organizational or territorial borders; communication and procedures which often do not exist, are complicated or difficult to follow.
   - The Internet and terrorist tools and techniques to use it are changing continuously.

H. Organizations choose on a voluntary basis to commit to the general principles, to join the dialogue that has started with the Clean IT project, and/or to implement the best practices described in this document.

3 General Principles

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 oppose the use of the Internet for terrorist purposes as defined in the first section. This requires organizations to be sufficiently resourced, accountable, innovative, reliable and professional regarding their activities to reduce terrorist use of the Internet, taking their capacities and goals into account.

II. Any action taken to reduce the terrorist use of the Internet, whether by governments or by private entities, must comply with national provisions, EU and other international legal instruments, and respect fundamental rights and civil liberties, including access to the Internet, freedoms of expression and assembly, the right to privacy and data protection.

III. This document does not suggest action which cannot be introduced by legislation for constitutional or human rights reasons.

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

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

VI. In cases of suspected terrorist use of the Internet, when an activity is not deemed unequivocally illegal, but might be considered as harmful, organizations (i.e. competent authorities and ISPs) will first try to resolve the situation among themselves as quickly as possible within their respective legal obligations and competences. At all times, organizations have the right to refer the case to the competent court or seek other legal remedy which the applicable laws provide.

VII. Even in cases where Internet access providers, content delivery, hosting and publishing companies are not legally responsible for terrorist content or terrorist activity on their network, they will still act in accordance with the aims of this document and assist to reduce terrorist use of the Internet within their means.

VIII. Internet users should have the means to avoid being subjected to terrorist use of the Internet. User-friendly mechanisms should exist to facilitate reporting of terrorist use of the Internet.

IX. Further public-private dialogue and cooperation, based on mutual trust and understanding, are necessary to ensure the continuation and future enhancement of efforts to reduce terrorist use of the constantly evolving Internet.

4 Best Practices

The partners in the Clean IT project consider the following best practices to be useful in reducing terrorist use of the Internet, provided they are implemented in compliance with the general principles. Therefore the best practices are to be conducted within the limits of applicable legislation and respect fundamental rights and civil liberties. Implementing best practices is voluntary and is the full responsibility of each individual organization.

4.1 Proactive best practices

Best Practice 1: Legal framework

Challenge:
Terrorist use of the Internet is not always clearly explained, while it can be 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, 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 competent authorities and Internet companies to deal with terrorist use of the Internet.

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

Explanatory note:
All measures taken to reduce terrorist use of the Internet must be in accordance with human rights and fundamental rights and freedoms. 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 Member States' legislation will help practitioners in reducing the international aspects of terrorist use of the Internet. Member States should have clear procedures in place to end terrorist use of the Internet. The legal framework to reduce terrorist use of the Internet must be clearly explained to users, NGOs, Internet companies and competent authorities to make their work more effective. Also youth protection legislation protects in some countries against terrorist use of the Internet. Governments should not put too much pressure on organizations when explaining legislation, e.g. by threatening to use (legitimate but) very invasive measures. Putting too much emphasis on terrorist use of the Internet could also have a chilling effect on freedom of expression. Explanation of legislation should be balanced and based on adequate analysis of relevant (national) legislation.

Best Practice 2 : Government policies

Challenge:
Governments should take an active role in reducing terrorist use of the Internet. However, policies on reducing terrorist use of the Internet are not always comprehensive, clearly defined or explained, governments differ in being able to keep up with the rapidly developing Internet while for some governments, dialogue with Internet companies and NGOs is rather new. In addition, policies on reducing terrorist use of the Internet differ between governments, which limits synergy.

Best Practice:
Governments that have a strategy in place are willing to lead in reducing terrorist use of the Internet and are well equipped to do so. Governments strive for efficient international cooperation and stimulate cooperation with Internet companies and NGOs to reduce terrorist use of the Internet.

Explanatory note:
Many governments include reducing terrorist use of the Internet as an integral part of their security strategies and in foreign policy and stimulate international cooperation in this field. Governments should make sure competent authorities have enough capacity to deal effectively with the use of the Internet for all kinds of terrorist purposes. The time needed for international (legal) action against content in another country could be reduced. Some governments strive for good cooperation between competent authorities and Internet companies. Internet companies and competent authorities could be assisted by governments by sharing information on terrorist use of the Internet (see also the best practices 'Awareness' and 'Sharing abuse data'). Governments could stimulate self-regulation by Internet companies and organize programs to educate web moderators.

Best Practice 3: Terms and conditions

Challenge:
Not all Internet companies state clearly in their terms and 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 and conditions, stating that such use is unacceptable. Some Internet companies effectively enforce this policy.

Explanatory note:
This best practice does not require any EU 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. In this best practice "Internet companies" does not refer to access providers. Access providers should refrain from including terrorist use of the Internet in their terms and conditions, as access-blocking is not a recommendable option. Terms and conditions do not create new legal rights for third parties, but solely

govern and clarify the relationship between the respective Internet company and its customer. In contrast, the illegality of terrorist use of the Internet affects the relationship between the customer and the (Member State, representing the interests of the) general public. 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 terms and conditions. Small and medium Internet companies might not have the capacity to maintain a well-staffed abuse department and understand the language in which potential terrorist use of their service takes place. In this case it would be best to forward possible cases of terrorist use of the Internet to hotlines, referral units or competent authorities.

Best Practice 4: Awareness

Challenge:
Terrorist use of the Internet is currently not widely known or understood. The public in general, but especially vulnerable groups like children, teenagers and young adults and the circle that surrounds them are largely unaware that they are being targeted by terrorists and terrorist groups for incitement and recruitment. Professionals like frontline workers 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, competent authorities, 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 radicalisation. 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.

Awareness programs should inform where to find help on or report terrorist use of the Internet, as well as provide examples of known cases of terrorist use of the Internet. Awareness projects should inform about the full extent of terrorist programs using the Internet, including radicalisation starting from hate speech, address psychological effects and group dynamics in radicalisation, and provide examples of this.

Awareness programs should not violate the right to non-discrimination, while creating a culture of fear and stigmatisation must be avoided.

4.2 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 competent authorities.

Best practice:
Some websites with user-generated content offer simple and user-friendly flagging systems on their platforms, having a separate, specific category for terrorist use of their service.

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. The service providers should also explain to their users how these flagging systems work and otherwise stimulate its use. This practice is primarily meant for social media or websites that provide user-generated content, but it could be considered to make the technology more widely available where this is technologically possible. 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 (E-commerce directive, 2000/31/EC of 8 June 2000, article 14e).

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. Abuse of the flagging mechanism should be prevented as much as possible.

Governments and competent authorities should primarily use formal ways of notifying Internet companies. In some Member States flagging is also regarded as a formal notification. If governments and competent authorities 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 the best practice of notice and take action).

Best Practice 6: End-user browser mechanism

Challenge:
While content portals (like social networks, image or video portals) can offer 'flagging' opportunities, other platforms (like 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.

Best practice:
A browser-based reporting mechanism could be developed to allow end users to report terrorist use of the Internet.

Explanatory note:
Webhosting companies and other content platform providing Internet companies that do not offer a single point for reporting to end-users, do not want terrorist use of their networks, but are technically, economically, legally and/or practically limited in detection of their clients' content. If those clients do not have proper reporting mechanisms for abuse, Internet users cannot report the terrorist use of the Internet in a user-friendly way. In those cases, these Internet companies can play an intermediary role. In some countries Internet companies in coordination with competent authorities offer banners that clients can add to their website on a voluntary basis to report alleged illegal content. Similar mechanisms exist for phishing sites, spam and malware, as an option or add-on in browsers or mail client software. A more systematic approach to help Internet companies to be notified by Internet users about alleged terrorist use of the Internet is a reporting mechanism that is implemented in the standard distribution of a browser, or, as a fallback solution only, is offered as a plugin for browsers. This is a user-friendly notification tool to Internet companies that do not offer flagging tools or do not have effective abuse departments. This mechanism should also be considered for the browsers of mobile devices and their operating systems. While being developed, at for example the EU-level, the mechanism should have an open architecture, allowing non-EU organizations to start using it as well later on.

The reporting mechanism will send an automated signal to the Internet company involved, which will allow them to contact their client (the content owner) so the client can take appropriate action. The client and or the host can also contact the competent authorities if necessary (see the best practice of referral units). The system works only for known hosts: hosts that register to this service. As such a mechanism needs to be organized and developed, a pilot is recommended to experiment and evaluate the added value of this system, as well as to solve legal/jurisdictional, organizational, procedural and technical issues. Abuse of the reporting mechanism should be prevented as much as possible.

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. 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 competent authorities 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 takes 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 (public sector) 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 possible terrorist use of the Internet that is reported to them is illegal or not.

The role of a public sector operated referral unit is to assess Internet content and where it is deemed unlawful to have the material removed and coordinate any prosecutions for offences which may have been identified. For regional and local police units the referral unit offers more expertise in dealing with (potential) terrorist use of the Internet. Referral units need to be advertised and promoted. Referral units' authority must be grounded in legislation, while any referral unit must work according to local legislation and within its jurisdiction. As legislation differs between EU Member States, referral units' activities might differ as well. Referral units should be in regular contact with relevant Internet companies, also to ensure actions are coordinated as much as necessary. Internet companies should only refer cases in which it is reasonable to think there is terrorist use of the Internet, not refer all that is reported to them. As cases of terrorist use of the Internet can be transnational, referral units need excellent working relations with referral units in other Member States and outside the EU.

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 competent authority) for further action.

Referral units and hotlines should technically be able to receive all kinds of terrorist use of the Internet (e.g. websites, videos, messages, emails, profiles) and if both exist within one Member State they should have excellent cooperation. Referral units and hotlines would benefit from a points of contact system as proposed in best practice number 9.

As a secondary task referral units and hotlines can contribute to awareness, education and information efforts on terrorist use of the Internet. For example, governments and competent authorities 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.

4.3 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 competent authorities notify Internet companies to bring terrorist use of the Internet to the actual knowledge of the provider. From their formal role competent authorities 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 competent authorities

give an 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 competent authorities apply a standard for take down orders.

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.
(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. Notifications 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 competent authorities send an insufficient notification, the Internet company addressed should always reply as soon as possible and explain in detail the insufficiency. (Insufficient reports by other organizations or by individuals should merely be replied to with a standardized message stating the report was insufficient.)

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.

Notice and take action procedures should be surrounded with clear procedures and guarantees for the right of free speech and the right to a fair trial.

Orders

From the perspective of Internet companies the above mentioned qualifications for notices should at least also apply for formal orders by competent authorities. Internet companies would like to easily recognize the competent authorities, especially if they are based in other countries.

Best Practice 9: Points of contact

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

Best practice:
Some governments, competent authorities, Internet companies and NGOs have points of contact for terrorist use of the Internet.

Explanatory note:
A network of trusted and listed points of contact facilitates cooperation between organizations committed to reducing the terrorist use of the Internet. Points of contact are experts able to represent their organization, preferably on a daily or even 24/7 basis. To establish a professional system of points of contacts, detailed working procedures and a central database, facilitated by an EU (level) organization, will be required. These points of contact should be identified by role and their contact details published. Where possible the people occupying these roles should remain in them for a reasonable period and develop relations with their most important counterparts in other organizations.

Best Practice 10: Cooperation in investigations

Challenge:
When competent authorities 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 competent authorities have agreed on how to cooperate efficiently, effectively and lawfully in investigations of probable illegal terrorist activity on the Internet.

Explanatory note:
The legal base and purpose of competent authorities' investigations should always be clarified. It should be made clear what the legal status of the request for cooperation is: if it is mandatory, based on legislation, or voluntary, at the discretion of the Internet company to which the request is directed. Cooperation should be standardized, but human contact remains important. Internet companies have very different backgrounds and fields of activities, but have in common that they want to reduce terrorist use of the Internet. Exchanging knowledge can improve mutual understanding and lead to better cooperation in investigations. Competent authorities 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"). If an investigation needs additional efforts made by Internet companies that already took reasonable precautions to reduce terrorist use of the Internet, it is reasonable they ask for standardized adequate compensation by government.

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.

Best practice:
Some Internet companies share information on other kinds of abuse of their network with each other, using a trusted intermediate partner organization. This private sector practice could be extended to include confirmed illegal 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, including privacy and data protection legislation, should be added to these systems. Competent authorities and NGOs might help start such a sharing system by providing the information on formally confirmed terrorist use of the Internet they possess. Gathering information for this system should be done by providing information on a case by case basis, from cases of confirmed terrorist use of the Internet. Matching the information in the system with information on the Internet companies' service will enable to assess more efficiently whether this content is illegal. The legal status of the trusted third party organization, its tasks and competencies, procedures (of information gathering and qualification) and guidelines must be clear and transparent.

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, voluntary end-user controlled services rarely include terrorist use of the Internet. Technology for detecting, logging access to or blocking 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 address terrorist use of the Internet.

Explanatory note:
In general, blocking and filtering options are considered 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 have already categorized

and have the potential to control access to some 'terrorist, race-hate, extremism' content through the use of keywords, phrases and known website addresses. This can be a helpful tool e.g. for parents who want to protect their children from radicalization attempts. All voluntary end-user controlled services must comply with EU and/or Member States regulations, i.e. on data protection and privacy. Development of accurate sources of information on what constitutes terrorist use of the Internet in each jurisdiction is considered a priority, to which the founding of an authoritative Research and Advisory Organization, as is described in the next best practice, could contribute. Any website addresses list or other information on what should be regarded as terrorist use of the Internet should be (treated) jurisdiction specific and be optional to implement by providers of these filtering services and end-users. Content that is blocked by using such information should have an optional information page that displays the reason, jurisdiction, contact information and method to redress inaccuracies of the supplier of this information.

4.4 Learning best practices

Best Practice 13: Research and advisory organization

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 single coordinating and academic authoritative body to which all organizations involved are likely to refer.

Best practice:
An academic network (on sub-national, national and/or international level) that is respected by all parties, to expand existing knowledge on terrorist use of the Internet, and how best to reduce it.

Explanatory note:
An organization as proposed here should be part of a university and would be able to provide research and advice on terrorist use of the Internet throughout the EU and in each individual Member State. This organization should (among others) gather and combine the research that has been done on terrorist use of the Internet, and share this with others in its network. The organization should act independently, i.e. without political interference. The organization should (among others) facilitate meetings between and projects of academics and practitioners. Possible fields of work are:

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

Dit is een uitgave van:

Ministerie van Veiligheid en Justitie
Nationaal Coördinator Terrorismebestrijding
en Veiligheid
Postbus 20301 | 2500 EH Den Haag
www.rijksoverheid.nl/venj

Januari 2013 | Publicatienr: J-16813