COUNCIL OF THE EUROPEAN UNION

GENERAL SECRETARIAT

Brussels, 22 December 2011

CM 6026/11

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC 21.11.2012

ENFOPOL

COMMUNICATION

REQUEST FOR CONTRIBUTION

from:	Dutch delegation
to:	Terrorism Working Party
Contact:	twg@consilium.europa.eu
Tel./Fax:	+32.2-281.3945, +32.2-281.58.90
Subject:	Questionnaire to identify best practices used to limit Internet use by terrorists and extremists

Delegations will find enclosed a questionnaire prepared by the Dutch delegation aiming at identifying best practices used to limit Internet use by terrorist and extremists in relation to the "CleanIT" project.

Delegations are kindly asked to **send their replies by 1 April 2012** at the latest to the following e-mail address: questionnaire@cleanitproject.eu.

National Coordinator for
Counterterrorism and Security
Ministry of Security and Justice

> Return address Postbus 16950 2500 BZ The Hague

Members Counter Terrorist Working Group

Coordination and Crises Management Department

Oranjebuitensingel 25
2511 VE The Hague
Postbus 16950
2500 BZ The Hague
www.nctv.nl

Contact
DELETED

Date 16 December 2011
Concerning Questionnaire

Project name
Clean IT

Our reference
www.cleanitproject.eu

Please quote date of letter and our ref. when replying. Do not raise more than one subject per letter.

Dear Sir, Madam,

The internet plays a central role and is of great strategic importance for terrorists and extremists. It is a critical tool for generating funds, recruits, support, propaganda, communication, coordination and planning. Those phenomena were studied during the EU project "Exploring the Islamist extremist Web of Europe - Analysis and Preventive Approaches", that was finalised in October 2009. The overriding objective of this study was to contribute to preventing radicalization through the internet and to develop ways and means to address Islamist extremist content on internet. This project identified several best practices in Germany, The United Kingdom, The Czech Republic and The Netherlands.

Although some interesting national best practices were identified, it was not always clear how to apply them effectively, because:

- Content on the internet is difficult to locate, and is duplicated easily or automatically;
- In a lot of cases, information on internet crosses geographical borders and is therefore not submitted to one single legal system;
- The use of internet makes it possible that unlawful activities are undertaken in one part of the world, but affect multiple places on the other side of the world, within a split second.
- The national legal systems, based on the E-commerce directive (2000/31/EC), regulate the conditions under which information society service providers can be held liable for third party illegal content when they act as "online intermediaries". However, it does neither regulate how to act in case of illegal use of the internet nor does it define in which way public and private parties can exercise their common responsibility to keep the Internet clean from terrorist activities.

The conclusions of the foregoing project comprehend that prevention of Internet crime is of common interest to governments, security authorities, the internet sector and internet users. The response should consist of a wide range of approaches and include a number of partners.

New project: Clean IT

Coordination and Crises Management Department

Date
16 December 2011

Our reference
www.cleanitproject.eu

To deal with terrorism and extremism in the virtual world, traditional law enforcement approaches are not always effective. In addition to regulatory approaches, public-private partnerships can cause a breakthrough in deadlocked talks between government and industry. The internet is in most countries predominantly privately owned, while industry has much more knowledge and capacity to keep the Internet 'clean'. Solutions to this problem can be found in direct cooperation between Member States and the Internet industry.

To contribute to the prevention of the misuse of the Internet for terrorist purposes, a non-legislative approach should be developed. This should lead to a type of non-legislative 'framework' that consists of:

- General principles, to be used as a guideline or gentlemen's agreement on how to fight the illegal use of the Internet. These principles should fill the gap between Member States' (national) regulation and private initiatives / best practices and should be adopted by all partners. It should state what the responsibilities of the different parties are, and which concrete steps public and private partners can take in order to fight illegal use of Internet.
- Best practices that can be implemented voluntarily in order to achieve increased law-compliance on the Internet.
- A platform for dialogue for public and private partners to strengthen the fight against the illegal use of the Internet.

The Netherlands (National Coordinator for Counter Terrorism and Security) has therefore submitted a project proposal in partnership with Germany (Federal Ministry of the Interior) , United Kingdom (Office for Security and Counter Terrorism), Belgium (Coordination Unit for Threat Analysis), and Spain (Centro Nacional de Coordinación Antiterrorista). This project is called "Fighting the illegal use of the Internet with public-private partnerships from the perspective of counter terrorism" (short name: Clean IT) and is submitted under the Programme "Prevention of and Fight against Crime" 2010. The project is granted, partially funded by the European Commission, and started last summer.

Aim of the new project

The strategy followed by the Clean IT project (www.cleanitproject.eu) is to have open discussions in a trusted environment between the Internet industry, government, law enforcement, non-governmental organisations and user organisations on making the Internet a more secure and safe environment. The objective is to identify general principles, and practices as well as methods for permanent dialogue that can limit the use of the Internet by terrorists and extremists. These principles, practices and methods will be written down in a draft covenant. The particular nature of this project is that we will put the private sector in the lead of this drafting process, and monitor that the covenant will have support from both public and private organisations. The principles and practices should be non-legislative because they will be adopted on a voluntary basis with support from the industry. It should also be possible to implement them quickly in any European Member State, or even worldwide. But it is possible however, that one of the results will be a call for better regulation. Please find the latest updates for the project in the progress report, which we included.

Different tracks

In the Clean IT project public and private organisations from Belgium, Germany, The Netherlands, Spain and The United Kingdom attend workshops and conferences to discuss common identified problems and give input into the drafting process. Participants are not restricted to these countries, representatives from other countries and companies are welcome as long as they have an active and constructive contribution based on their experience in the field. During the project, the number of on-line and off-line participants will grow gradually.
A separate track of the Clean IT project aims to identify practices to limit the use of the Internet by terrorists and extremists in all European Union Member States. These practices will be used as input for the draft covenant too. Best practices can be related to Internet monitoring, filter mechanisms, subsidising non-governmental organisations, notice-and-take down agreements with the Internet industry, flagging tools, real name policies, research, education and awareness programmes.

Questionnaire

With this questionnaire we intend to gather information on practices that limits the use of the Internet for terrorist purposes. In addition we would like to establish contact with experts in both public and private organisations that would be interested in participating in Clean IT and follow-up projects. In time the Clean IT project could develop into a permanent platform for dialogue.

Please answer the following questions according to your own knowledge and insight. Please contact a few other experts if needed, but no detailed and thorough study is required. This questionnaire is also distributed to some known trusted experts from the industry and Internet Service Provider Associations in different countries.

Further contact

If you need explanation, have questions or want to comment: please send an email to questionnaire@cleanitproject.eu or call Dr Michiel de Weger, 00 31 6 149 161 35.

Please return this questionnaire and send documents to questionnaire@cleanitproject.eu no later than April 1, 2012. In mid-May 2012 we will send you a report based on the questionnaires we received from you and other European Union Member States. We will ask sending your comments before the end of May 2012. The main findings of this report will be presented at the Clean IT conference in Berlin, in June 2012. Some weeks after the conference we will send you a finalised report by email.

Kind regards,

DELETED

Coordination and Crises Management Department

Date
15 December 2011

Our reference
www.cleanitproject.eu

Questionnaire to identify best practices used to limit Internet use by terrorists and extremists

For the purposes of the CleanIT project 'best practices' are to be understood as measures such as Internet monitoring, filter mechanisms, provision of subsidies to non-governmental organisations, 'notice-and-strike down' agreements with the Internet industry, flagging tools, real name policies, research and, education or awareness programmes.

QUESTIONS

1. How Internet use by terrorists or extremists is limited in practice in your country? If there is no general policy, are you aware of any best practices used in this field and if so, what are these? *Please list any best practices applied or planned in your country, and if possible provide a hyperlink to the website where more information can be found.* *Please describe in detail each practice providing information on actors, actions, governance, costs, effects and if possible contact details (name, e-mail address, mobile phone number) of a person that can be contacted for more information.*
Answer:
2. Which types of Internet use by terrorists and extremists are regarded as problematic in your country? *Please give examples of cases where the application of practical measures could help limiting Internet use by extremists and terrorists.*
Answer:

3. Who in your country would be interested in participating (receiving e-mails with updates, and invitations to meetings, and providing comments on drafts) in the CleanIT project? *Please provide a list of potentially interested persons together with their contact details (name, e-mail address, organisation) from the government, law enforcement authorities, the Internet industry, Internet service provider associations, the top-5 webhosting providers, national non-English language (*) social media, vendor sites, non-governmental organisations and science and research. (CleanIT would then contact these persons with a view to inviting them to participate in the project.)* *Note: This question is not to be understood as a request for an exhaustive list.* *We would just like to benefit from your personal network and ideas.* *Please do not forget to put yourself on the list, if you would like to be kept updated!* *(*) we already have contact details for persons from the most popular multinationals including Facebook, Google, Twitter and E-bay.*
Answer:

Please return this questionnaire and send any supporting documents to questionnaire@cleanitproject.eu no later than **April 1, 2012.**

If you need any further explanation, have questions or wish to comment, please send an e-mail to questionnaire@cleanitproject.eu or call **DELETED**

For more information about the project: www.cleanITproject.eu