National Coordinator for
Counterterrorism

Clean IT

Reference: HOME/2010/ISEC/FP/C2/4000001442

A project to fight online illegal activities on the internet from the Netherlands, Germany, United Kingdom, Belgium, Spain and Europol, with financial support from the Prevention of and Fight against Crime Programme of the European Union, European Commission – Directorate General Home Affairs

Agenda Kick off meeting coordination group
30 may 2011
Hotel Continental, Belgrade

13:00 Welcome coffee

13:30 Recap from previous project, and the road to this new project
Attachments:
- 1. project outline, June 17, 2010
- 2. pages 4-6 from official application form
- 3. To be distributed in hardcopy: "Exploring the Islamist extremist Web of Europe - Analysis and Preventive Approaches"

14:00 Objectives of Clean IT in relation to existing initiatives
Attachments (for your information, not for discussion):
- 4. Draft recommendations for public-private cooperation to counter the dissemination of illegal content within the European Union (DG HOME, as discussed in the "Public Private Dialogue to fight online activities")
- 5. Draft Elements for a Framework of General Principles of Internet Governance (Discussion paper Ad-hoc Advisory Group on Cross-border Internet, Council of Europe)
- 6. Discussion paper for next conference CT coordinators and Heads of fusion centres.

14:30 Project strategy and planning
Attachment:
- 7. Project planning (will be distributed in hardcopy)

15:00 Logistics and Finance
Attachments:
- 8. Initial budget Clean IT
- 9. Lettre from Commission from March 17th
- 10. Lettre (repons) from mr Akerboom
- 11. Reimbursement claim for kick off meeting Clean IT

15:30 Wrap up, next steps

16:00 Closing, and join EuroDIG conference and social evening event
Attachment:
- 12. Programme EurDIG
- 13. Article in Digital Magazine

The Clean IT Project

Fighting the illegal use of internet

Minutes Kick off Meeting Coordination Group
30 May 2011, Belgrade, Serbia

Participants:

[redacted]

Absent: Europol: [redacted]

1. Opening and introduction

Partners of the Clean IT project are Germany, United Kingdom, Spain, The Netherlands, Belgium and EUROPOL. Germany will participate with representatives of BMI and the Joint Internet Centre (GIZ). The UK is represented by home office OSCT. Mr. Klaasen will establish a small project team within the NCTb in The Netherlands; ms [redacted] will be the first member of that team. [redacted] is reassigned to the national cyber security strategy implementation taskforce and will not participate in this project.
Unfortunately, [redacted] from Europol and [redacted] from Belgium /OCAD were not able to join this kick off meeting. Mr. Klaasen will consult them separately and convey the results of this meeting.

2. Objectives of clean IT in relation to existing initiatives

The first step within the project will be to identify new and existing initiatives that could be of interest to the Clean IT project. This overview will be provided by the project team and is foreseen for fall 2011.

Two existing projects were already discussed: the European Commission's Public Private Dialogue on countering illegal online content, and the Council of Europe's draft elements of a framework for internet governance.

Concerning the EC initiative, stakeholders from the private sector (IT industry) had some reservations about the draft recommendations. Current state of play is that the way to go forward is still under discussion by the Commission. In addition, the EC initiative is of a broader scope (e. g. including child abuse). Clean IT should therefore not be inextricably bound up with the PP dialogue.

The Clean IT project will clearly put the private sector partners in the first lead, and focus on Al Qaida inspired terrorism. This is because it is seen as the most significant terrorist threat at the moment. The IT industry could be enabled to consider their own interest in keeping their presence on the Internet clean from violent extremist content, which could, e.g., create a negative environment for advertisements.

The project does not exclude other terrorist phenomenons. The project outline, dated June 17th 2010, will be updated in this sense.

The EU National CT coordinators and Heads of Fusion Centres will meet end of June in The Hague. They will be asked to function as a soundboard, so we can brief them on the progress of Clean IT during their meetings. We will appreciate involvement from other Member States with Clean IT.

3. Project strategy and planning

The way we involve the private sector will be crucial for the success of this project. Private sector must be in the first lead. Before we engage with industry, we must however have a clear picture of our own agenda. We should be able to present the problem of online terrorist activities in the way that a nonprofessional will understand. All team members are asked to present some use-cases for our next event, which can be shared with private parties. The next step will be to identify the interest / agenda of the private partners. Three relationships will be central

1 Law enforcement – industry
2 User- law enforcement
3 User – industry

Our approach must be based on mutual benefit/ interest, pragmatism and self-regulation (not legalistic). The Youtube flagging system for terrorist content is mentioned as an example for a good practice.

4. Logistics and planning

The final budget is still being negotiated with the EC; still pending are staff costs, which are currently not covered. The official grant agreement is therefore not yet signed. Nevertheless, the EC has agreed to start the project allready.

The EC will finance 80% of the final budget, project partners are asked to contribute the remaining 20%. This will mean an estimated € 10.000-20.000 per partner (not Europol). The team members are asked kindly if their organisation could contribute to the project and report on this in our next meeting. As there is a special bank account for the entire duration of the project, project partners are free to decide at what point during the project they would like to transfer these funds.
Should partners not be able to provide the requested funding, contributions in kind (e.g. by hosting workshops and meetings) could also be considered.

A draft planning for the workshops and conferences will be sent to the project partners for approval.
Germany and Spain will check if the first two events could take place in Berlin and Madrid respectively.

5. Wrap up and closing

Mr. Klaasen announces that he will mention the start of Clean IT the next day in the plenary Cybersecurity meeting at the EuroDIG conference; and he thanks all team members for their contribution to this meeting and support for the project.

The Clean IT Project

Fighting the illegal use of internet

Agenda meeting Coordination Group

October 24, 2011
10.00 – 12.00h, Amsterdam

1. Opening of the meeting

2. Discuss minutes Belgrade meeting

3. Confidentiality of the meetings

4. Generating publicity about the project

5. Target groups
    a. Different circles of participants
    b. How do we deal with new (associated) partners?

6. Closing of the meeting

October 25, 2011
13.30 – 14.30h, Amsterdam

1. Opening of the meeting

2. What did we think about the workshop?

3. Who should be a part of the Editorial Board?

4. Planning of next activities
    a. Workshop 2: January 18 and 19, 2012 in Madrid
    b. Workshop 3: March 21 and 22, 2012 in Brussels
    c. Conference 1: May 23, 24 and 25, 2012 in Berlin
    d. Workshop 4: September 13 and 14, 2012 in London
    e. Conference 2: November 1,2 and 3, 2012 in Brussels
    f. Final presentation: January 22, 2013 in Brussels

5. Closing of the meeting

Annexes:

1. Minutes meeting Belgrade
2. Confidentiality form
3. Press statement about the project
4. Target groups; different circles

The Clean IT Project

Fighting the illegal use of internet

Workshop 1
Industrieele Groote Club, Amsterdam

October 24, 2011

Time	Session	Speaker
10.00 – 12.00	Meeting Coordination Group	But Klaasen
12.00 – 13.00	Opening lunch	
13.00 – 13.15	Introduction	[redacted]
13.15 – 16.00		
• 13.15 – 13.45	[redacted]	[redacted]
• 13.45 – 14.15	Spain	[redacted]
• 14.15 – 14.30	Brainstorm: Challenges	[redacted]
• 14.30 – 15.00	Break	
• 15.00 – 15.30	Belgium	[redacted]
• 15.30 – 16.00	Deep web	[redacted]
• 16.00 – 16.15	Brainstorm: Actors	[redacted]
16.15 – 16.30	End of day 1	[redacted]
19.00 – 21.30	Dinner	

October 25, 2011

Time	Session	Speaker
09.00 – 12.00		
• 09.00 – 09.30	United Kingdom	[redacted]
• 09.30 – 10.00	Netherlands	[redacted]
• 10.00 – 10.15	Brainstorm: Principles	[redacted]
• 10.15 – 10.45	Break	
• 10.45 – 11.15	Germany	[redacted]
• 11.15 – 11.30	Brainstorm: Solutions	[redacted]
• 11.30 – 12.30	Discussion about next steps	[redacted]
12.30 – 13.30	Closing lunch	
13.30 – 14.30	Meeting Coordination Group	But Klaasen

The Clean IT Project

Fighting the illegal use of internet

CLEAN IT
Programme Workshop 2
Madrid, 18-19 January 2012

18 January 2012

Time	**Session**
13.30 – 14.30	Lunch
Programme	
• 14.30 – 14.45	Opening remarks (But Klaasen [redacted])
• 14.45 – 15.25	Discussion draft text, with input presentation on the situation in Belgium [redacted]
• 15.25 – 15.40	Break
• 15.40 – 16.30	Discussion draft text, with input presentation [redacted]
• 16.30 - 17.45	Discussion draft text, with input presentations on the situation in Spain (Spanish police) and [redacted]
21.00 – 22.30	Dinner

19 January 2012

Time	**Session**
09.00 – 13.30	Programme
• 09.00 – 10.00	Discussion draft text, with input presentation [redacted]
• 10.00 – 10.15	Break
• 10.15 – 11.15	Discussion draft text, with input presentation [redacted]
• 11.15 – 11.30	Break
• 11.30 – 12.50	Discussion draft text, with input presentation [redacted] and [redacted]
• 12.50 - 13.00	Concluding remarks
13.00 – 14.00	Closing lunch
14.00 – 15.30	Meeting Coordination Group

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Contact
[redacted]
Project officer
[redacted]

Date
8 February 2012

Project
Clean IT

Minutes

Meeting coordination group

Date and time 19 January 2012, 14.00h
Location Ministry of the Interior, Madrid
Present [redacted]
But Klaasen
[redacted]
Absent

General announcements:

- [redacted] is joining the coordination group since she is actively involved in writing the draft document.
- European Commission wanted to join this second Clean IT workshop, but they were unable to attend because of other meetings.
- The Clean IT project was presented in the EU Working Group Counter Terrorism. Denmark was very enthusiastic; they may want to join the project.
- EUROPOL did not attend three times in a row. There were some questions about the role that EUROPOL can play as they are part of the Commission, but this is clarified. Hopefully they will be able to send a representative during the next meeting.
- There has been some publicity about the project. Enclosed you will find a couple of links towards these articles. There were both neutral and negative articles. We reacted to a blog Bits of Freedom and the Commission reacted to Italian article. The basis of criticism was the lack of focus and the suggested restriction of internet freedom.
- The NCTV will make a small press release stating that our second workshop took place in Madrid, we had good participants and a new draft document will be developed. We will share this press release before publishing.

Evaluation and moving forward

There was very good and active participation from both public and private organizations and the NGO's. It is important that we were able to address the issue of the scope of the project.

We need to start by communicating an end goal. During the workshop the concept of a two pager was mentioned. This seems like a good idea for the end product. The end product can be general principles with best practices attached to them. The status of the document is more important. We need a document that is owned by the industry and be put into practice. It doesn't necessarily need to be signed, but it should be handed over to the Commission in public.

The real work needs to be done after the document is complete and the project ended. A permanent public private platform has often been mentioned during the workshop. This permanent platform can officially start when we hand over the document with general principles and best practices. The document needs to remain a living document that can be adapted within the permanent platform to adjust to changing circumstances. There is enough consensus to start communicating on this idea. We should also look into the legal entity of such a platform. We will have to make sure that this is a feasible idea, especially since there might be costs involved.

Another idea to keep the project moving is to introduce a Clean IT mark. This will indicate that the companies that publish this mark will have adopted and implemented (many of the) the general principles and best practices mentioned in the draft document. This way it can become a PR necessity to participate.

Focus

Extremism/terrorism

During the workshop the discussion focused on the difference between terrorism and extremism and the difficulty of judging legal and illegal content. We should not make a very clear cut between extremism and terrorism. Extremism can be an important prerequisite for terrorism. What we can do depends on the mandate of our organizations. Preferably we remain focused on terrorism and radicalizing content (ideological material that can lead to terrorism). Al Qaeda inspired terrorism was originally the starting point of this project. We should claim that our task is to diminish the chance of an attack by terrorists that use the internet. This is our primary mandate. The use of the internet itself is legal and beneficial for its users; therefore we have to thoroughly analyze the problems we want to tackle to not interfere with this principle.

There has to be a clear justification of what we are doing. This justification will have to be short and something we can fall back on when the project is progressing. A kind of mission statement will be drafted to serve this purpose.

Legality/illegality

There are three categories of content; illegal, possibly illegal and not illegal. These categories will have to be dealt with accordingly. However, within this project we will not discuss what is legal and illegal, the EU definition of terrorism is the point of departure. Nevertheless, a lack of harmonization of legislation across Member States might still exist.

Internet companies might not want people glorifying attacks etc on their website. The companies might want to do more than just countering the illegal side. The document should be public-private or just private, with the private parties stating what they want.

Upcoming workshops

The upcoming workshop is in Brussels on March 21 and 22, 2012. [redacted] will assist us with the preparations.

After the workshop in Brussels, we will have our first conference on June 4, 5 and 6 in Berlin. [redacted] will help us with the preparations.

Date
8 februari 2012

For the next workshop and conference we will prepare a new draft document. This document will exist of a part that is agreed upon, and one part that is still in discussion in the group.

Editorial board
Some workshop participants had noticeable good input during the workshop and might at some time be consulted directly during the drafting process.

The Clean IT Project

Fighting the illegal use of internet

Agenda meeting Coordination Group

March 22, 2012
13.30 – 15.00h
Wetstraat 22, Brussels

1. Opening of the meeting

2. Discuss minutes Madrid meeting

3. Evaluation of the workshop

4. Use of the website and consequences for the project

5. Questionnaire

6. Letter Dutch Minister to EU colleagues about partnerships

7. Berlin conference

8. Closing of the meeting

Annexes:

- Minutes Madrid meeting
- Letter Dutch Minister to EU colleagues about partnerships (concept)

The Clean IT Project

Fighting the illegal use of internet

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.

Clean IT
Programme, workshop 3
Wetstraat 22/Rue de la Loi 22, Brussels

March 21, 2012

Time	Session
12.00 – 13.00	Lunch
13.00 – 13.30	Opening remarks and participants introduction
13.30 – 14.50	Plenary discussion draft document (section 'Preamble'), with input presentations on government policies ([redacted]) and terrorist recruitment ([redacted])
14.50 – 15.00	Break
15.00 – 16.00	Small group discussion about discussion paper (items in section 'Best Practices') • Awareness, information and education (chair: [redacted]) • Improvement in legislation and regulation (chair: [redacted]) • Business conditions/acceptable use policies (chair: [redacted])
16.00 – 16.15	Break
16.15 - 17.15	Small group discussion about discussion paper (items in section 'Best Practices') • End user controlled filters (chair: [redacted]) • Flagging/report button systems (chair: [redacted]) • Notice and take down (chair: [redacted])
17.15 – 17.30	Closing
19.30 – 22.00	Dinner

March 22, 2012

Time	Session
09.00 – 10.00	Plenary discussion draft document (section 'General Principles'), with input presentation on abuse information exchange ([redacted]) and abuse policies and enforcement ([redacted])
10.00 – 10.15	Break
10.15 – 11.30	Plenary discussion and presentations of results from small group discussions about the discussion paper • Awareness, information and education • Improvement in legislation and regulation • Business conditions/acceptable use policies • End user controlled filters • Flagging/report button systems • Notice and take down
11.30 – 12.15	Plenary discussion about discussion paper (section 'Permanent Dialogue')
12.15 – 12.30	Concluding remarks
12.30 – 13.30	Closing lunch
13.30 – 15.00	Meeting Coordination Group

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Contact
[redacted]
Project officer
[redacted]

Date
28 March 2012

Project
Clean IT

CONFIDENTIAL / NOT FOR PUBLICATION

Minutes

Meeting coordination group

Date and time	22 March 2012, 13.30h
Location	OCAD, Brussels
Present	[redacted] But Klaasen [redacted]

1. Opening of the meeting
The meeting was opened by Mr Klaasen.

2. Discuss minutes Madrid meeting
The minutes of the meeting are approved.

3. Evaluation of the workshop
The composition of participants was good and both the public and private participants were actively contributing to the workshop. The group discussions were a success and we will continue this during the Berlin conference. A lot of progress was made. We now have a lot of input, but we have to use this to adapt the draft document. We have to identify gaps and try to fill them during the Berlin conference. For the next conference in Berlin we would like to see more countries represented, more social media and browser companies participating.

We are gaining support from the European Internet Society and we will present the project for the RIPE NCC working group. Some countries (for example France) want to have separate, national Clean IT meetings.

We want to expand the group that is working on the draft by organizing a writing session. All discussion group leaders will provide a new text for their best practice. This will be used to adapt the draft document. The changes will be discussed during the writing session.

Date
8 februari 2012

4. Use of the website and consequences for the project

The project team changed the communication about the project. From a fully open and transparent process, we now changed to a more confidential process. Therefore the website is not used as often as it was before. We might use the CIRCABC platform that was mentioned during the meeting, but it is not clear if we can use this platform to communicate with civil society and the private sector.

We should emphasize that the names of participants are confidential. The list of participants will only be sent to the coordination group. A print out will be distributed during the meeting. In the program there will be no names mentioned.

5. Questionnaire

The deadline to respond to the questionnaire is April 1st, but so far we only received three responses. The results of this track might be disappointing.

6. Letter Dutch Minister to EU colleagues about partnerships

Several private parties indicated that we can add weight to the project by adding more member states as participants. That is why our Minister will send a letter to all his colleagues to ask them to participate in the project.

There is also something happening concerning fusion centers. [redacted] will look into this. This might be a good opportunity to reach all member states and ask them to participate.

We will e-mail the letter to the coordination group so they can brief their superiors.

Europol is not included in the letter because they cannot participate actively due to budget restraints. We will ask them to speak at the Berlin conference.

7. Berlin conference

The conference in Berlin will be a two day event. It will start on June 4th in the afternoon and end on June 5th in the late afternoon. [redacted] will ask his DG to speak at the conference. This seems to be the appropriate level for speakers.

[redacted] is interested in how Germany counters online extremism in their youth protection program. This might be a good option for a presentation during the conference.

During the Berlin conference we should provide the participants with some real life examples of what is legal and what its illegal. The Joint Internet Center in Germany can prepare this.

[redacted] will try to arrange one large room (60 people) and three smaller rooms, so we can have both plenary sessions and group discussions.

8. Closing of the meeting

Mr Klaasen closed the meeting.

The Clean IT Project

Fighting the illegal use of internet

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.

Clean IT
Programme, conference 1

Bundeshaus, Bundesallee 216, Berlin

June 4, 2012

Time	**Session**
12.00 – 13.00	Lunch
13.00 – 13.10	Welcome
13.10 – 13.30	Opening remarks and introductory round
13.30 – 14.45	Plenary discussion 'draft document' (section 'Preamble'), with input presentations on historical development and recruitment
14.45 - 15.00	Break
15.00 – 16.15	Plenary discussion 'draft document' (section 'General principles'), with input presentations on a real case and Youth Protection
16.15– 16.30	Break
16.30 – 17.15	Plenary discussion 'draft document' (section 'Best Practices')
17.15 – 17.30	Closing
19.30 – 22.00	Dinner Solar, Stresemannstrasse 76, Berlin

June 5, 2012

Time	**Session**
09.00 – 09.15	Plenary Presentation Results of Questionnaire
09.15 – 10.30	Plenary discussion 'discussion document' (section 'Best Practices), with input presentations [redacted] policies and terrorist training
10.30 – 10.45	Break
10.45 – 12.00	Working groups a. Legislation b. End-user controlled filters c. Service/business conditions and unacceptable use policies d. Flagging/report button systems
12.00 – 13.15	Lunch
13.15 – 14.30	Working group discussions a. Government policies b. Notice and take down c. Exchange abuse information d. Awareness, education and information
14.30 – 14.45	Break

14.45 – 16.00	Working group discussions a. Neutral foundation b. Referral units c. Cooperation in investigations d. Points of Contact System
16.00 – 17.15	Plenary discussion ‘discussion paper’ (section ‘Permanent Dialogue’)
17.45 – 18.00	Evaluation and Concluding remarks
18.00 – 19.00	Meeting Coordination Group

The Clean IT Project

Fighting the illegal use of internet

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.

Clean IT
Programme, Workshop 4

Beatrixbuilding, Jaarbeursplein 6, Utrecht

Wednesday September 12, 2012

Time	**Session**
12.00 – 13.00	Lunch
13.00 – 13.30	Opening remarks and introductory round
13.30 – 14.30	Plenary discussion draft document, Section General Principles, with input presentation on ´Terrorist use of the Internet´
15.00 - 15.15	Break
15.15 – 16.15	Plenary discussion draft document, Section Best Practices, nrs 18 - 22, with input presentation on ´Browser Based Reporting Tool´
16.15 – 18.00	Plenary discussion of the draft document, Section Permanent Dialogue, and of the Roadmap and Detailed Recommendations document, Section Implementation
19.30 – 22.00	Dinner Huize Molenaar, Korte Nieuwstraat 6, Utrecht

Thursday September 13, 2012

Time	**Session**
09.00 – 10.30	Plenary discussion draft document, Section Best Practices, nrs 23 - 27
10.30 – 10.45	Break
10.45 – 11.30	Working groups a. Police social media patrolling b. Referral units/hotlines c. Government policies d. Real identity policies
11.30 – 12.15	Working groups a. Semi-automated detection b. Legal framework c. Notice and take action d. Browser based reporting tool
12.30 – 14.00	Working Lunch Plenary discussion draft document, Section Best Practices, nrs 28 - 33
14.30 – 15.30	Meeting Coordination Group

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Contact
[redacted]
Project officer
[redacted]

Date
13 September 2012

Project
Clean IT

CONFIDENTIAL / NOT FOR PUBLICATION

Minutes

Meeting coordination group

Date and time	13 September 2012, 14.30h
Location	Utrecht
Present	[redacted] But Klaasen [redacted]

1. Opening of the meeting
The meeting was opened by Mr Klaasen.

2. Minutes Brussels meeting
The minutes of the meeting are approved.

3. Draft document
There is still a lot of work to be done on the draft document. Different people need to be involved in the drafting process. The project team will make a new text which incorporates the comments from this workshop. When this text is ready, we will have an electronic writing session where members of the coordination group can participate. This session will take place on October 7 or 8, 2012. After this writing session we will publish the draft and use it for the meeting in Vienna.

4. Conference in Vienna

The conference in Vienna will take place on 5 and 6 November, 2012. The OECD and UNOCD will be invited to the conference. It will be especially interesting if UNODC can present their latest paper.

Date
13 September 2012

There is some discussion about opening the conference up to the general public. It might add a lot of value to the discussion, but it might also pose difficulties regarding media attention. Participants of the meeting need to feel free to talk. The decision has been made to stick with a controlled environment, invitation only.

The twitter account of the project will be activated to communicate actively and be more transparent about the project.

5. Accreditation

We will ask for political instead of formal commitment. Governments and companies will be asked to express their commitment in writing (eg by a letter) instead of formally signing the document.

6. Final presentation

The final presentation will take place in January or February 2013. We will invite high level representatives from private, public and NGO sector. We will have a short presentation of the document. The participants will hand the end product over to the European Commission (or another suitable body).

There has to be a good incentive for the high level representatives to attend this meeting. It would be helpful if we can pick a moment when they are in Brussels already.

6. Legislative review

There should be some kind of literature and legislative review about the project. There will be a questionnaire as well. For high response rates, the government partners will be asked to assist. ULB will arrange this with the partners from the UK.

7. Closing of the meeting

Mr Klaasen closed the meeting.

Procedure amendements
Meeting Clean IT Vienna
November 5 and 6, 2012

The Clean IT meeting in Vienna will be used to generate a final version of the draft document we have been producing over the last months. The version that has been sent to you today is the pre-final version where all comments we have had so far have been processed.

During the meeting in Vienna we will work with amendments to make the final changes to the text. The procedure will be as follows.

1. Drafting and collecting amendments
During the first day of the conference there will be the opportunity to work on amendments on the text. This will be concrete text changes. At the end of the day all amendments will be collected by the project team.

2. Discussion of amendments
During the second day of the conference all amendments will be discussed. The person that drafted the amendment will be asked to explain the amendment shortly. After this, there will be a discussion with the audience.

3. Accepting or declining amendments
After the discussion about an amendment, the Clean IT project team will give the audience an advice on whether to accept the amendment or not. The next step is voting. Every participant will get a vote on each amendment. Amendments will be accepted if 2/3 of the audience is in favor of accepting.

4. Incorporating amendments
The amendments that have been accepted will be incorporated by the Clean IT project team in the exact way that they were proposed. After incorporating the amendments into the draft document, we have a final version.

Please send any amendments you might have to editorialboard@cleanitproject.eu or draft and submit them during the conference.

The Clean IT Project

Reducing the impact of the terrorist use of internet

Clean IT
Programme, Conference 2

Federal Ministry of the Interior
Herrengasse 7, Vienna

Monday November 5, 2012

Time	**Session**
12.00 – 13.00	Lunch
13.00 – 13.15	Welcome and opening remarks
13.15 – 14.15	Plenary presentations on terrorist use of the Internet
14.15 - 15.30	Working groups a. Legal framework and government policy b. End-user browser button c. Cooperation in investigations d. Points of contact
15.30 – 15.45	Break
15.45 – 17.00	Working groups a. No automated detection, unless… b. Business conditions c. Notice and take action procedures d. Sharing abuse information e. Research and Advisory organisation
17.00 – 18.00	Working groups a. Referral units and hotlines b. Awareness c. Flagging mechanisms d. Voluntary end-user controlled services
19.30 – 22.00	Dinner

Tuesday November 6, 2012

Time	**Session**
09.00	Deadline written amendments
09.00 – 09.30	Plenary presentation on United Nations project on terrorist use of the Internet
09.15 – 10.15	Plenary discussion General Principles
10.15 – 10.30	Break
10.30 – 10.45	Plenary presentation on right-wing terrorist use on the Internet in Germany
10.45 – 12.00	Plenary discussion of Preamble and Best Practices 1 - 6
12.00 – 13.00	Lunch

13.00 – 13.15	Plenary presentation by Internet company
13.15 – 15.00	Plenary discussion of General Principles
15.00 - 15.15	Break
15.15 - 15.30	Plenary presentation by Internet company
15.30 – 17.00	Plenary discussion of Best Practices 7 – 13
17.30 – 18.30	Meeting Coordination Group

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Contact
[redacted]
Project officer
[redacted]

Date
6 November 2012

Project
Clean IT

CONFIDENTIAL / NOT FOR PUBLICATION

Minutes

Meeting coordination group

Date and time	6 November 2012, 17.30h
Location	Vienna
Present	[redacted] But Klaasen [redacted]

1. Opening of the meeting
The meeting was opened by Mr Klaasen.

2. Minutes Utrecht meeting
The minutes of the Utrecht meeting will be sent to the participants in the coming weeks together with the minutes from the Vienna meeting.

3. Evaluation of the workshop
The meeting in Vienna was considered a successful meeting. The General Principles have been finalized and the participants are in agreement about this.

It was good to see that there was still a good turnout after all the media attention. It was clear that the participants were conscious of the media attention and acted accordingly. Where last meetings were more focused on personal expertise, this meeting had a more political focus. Some larger key players were not present during the meeting, we should try to involve them again.

Date
6 November 2012

The plenary discussions were very constructive. Discussions went into a lot of detail and were sometimes difficult to follow for participants without legal background.

4. Final version of the document
The General Principles are final now. Working group leaders will send their input and text changes to [redacted] and this will be incorporated into a new version of the document. This version will be send to all participants where there is one final round of comments before we finalize the document.

When finalizing the draft, it is important to pay a lot of attention to terminology and the consistent use of words. We should not define concepts that have been defined elsewhere. We should refer to other texts as much as possible.

Some elements of the draft have been deleted because a few participants did not agree. We can make a separate document with these elements, just to state that it has been discussed, but that there was no consensus.

5. Final meeting
The final meeting of the Clean IT project will take place on 30 January 2013. The location still has to be decided upon, but will probably be Brussels. [redacted] and [redacted] have been invited. The counterparts from the partners will be invited too, so please reserve the date in their agenda's.

During the meeting there will be a debate on the public private way the Clean IT project worked. Dilemmas, experiences and lessons learned will be discussed.

There are several opportunities to embed the results from the Clean IT project. The Vox-Pol programme is an FP7 programme against violent political extremism. They are bringing together an advisory organization. Part of the project involves research of legal frameworks. It may also be possible to connect to the UNODC track or the FP7 project Surveille.

6. Accreditation
The participants will commit to the General Principles only. We will not ask for formal commitment, we will ask for political commitment. Time will be necessary to inform the ministers and arrange for some kind of commitment.

7. Other
It may take a while before we get an official reaction from Portugal about partnering the project. They remain connected to the project through the WGT.

ULB can conduct research into the legal issues concerning the document. Our UK counterparts are in the lead here. [redacted] will contact them to ask if this is still necessary.

We will send a list of participants to the government partners. We will not include the names of individuals or companies due to the confidentiality of the project, but only state the number of participants per sector.

8. Closing of the meeting
Mr Klaasen closed the meeting.

Call for a continuation of public-private dialogue on reducing terrorist use of the Internet

The persons and organizations subscribing to this statement,

NOTING that the Internet plays a positive role in our lives and societies, but it is also used for illegal purposes, including terrorism;

STATING that we oppose the use of the Internet for terrorist purposes and that any action taken to reduce the terrorist use of the Internet, whether by governments or by private entities, must be effective, proportionate, legitimate and respectful of fundamental rights and civil liberties;

STATING that in cases of suspected terrorist use of the Internet, our actions will be guided by the general principles that are described in the final document of the Clean IT project, that was presented on January 30th 2013 in Brussels;

CONSIDERING the best practices as described in Clean IT' s final document to be useful in reducing the terrorist use of the Internet;

CALL for a continuation of a constructive public-private dialogue on reducing the terrorist use of the Internet.

NAMES / BANNERS

Statement by public and private organisations about reducing the terrorist use of the Internet.

The Internet plays a positive role in our lives and societies, but it is also used for illegal purposes, including terrorism. We oppose the use of the Internet for terrorist purposes.

We believe that any action taken to reduce the terrorist use of the Internet, whether by governments or by private entities, must be effective, proportionate, legitimate, and respect fundamental rights and civil liberties.

In cases of suspected terrorist use of the Internet, our actions will be guided by the general principles that are described in the final document of the Clean IT project, that was presented on january 30th 2013 in Brussels. We consider the best practices as described in Clean IT's final document to be useful in reducing the terrorist use of the Internet.

We call for a continuation from the structured public-private dialogue that started with the Clean IT project, to ensure that further public-private cooperation to reduce the terrorist use of the constantly evolving internet is based on mutual trust and understanding.

NAMES / BANNERS

Statement by public and private organisations about reducing the terrorist use of the Internet.

The Internet plays a positive role in our lives and societies, but it is also used for illegal purposes, including terrorism. We oppose the use of the Internet for terrorist purposes.

We believe that any action taken to reduce the terrorist use of the Internet, whether by governments or by private entities, must be effective, proportionate, legitimate, and respect fundamental rights and civil liberties.

In cases of suspected terrorist use of the Internet, our actions will be guided by the general principles that are described in the final document of the Clean IT project, that was presented on january 30th 2013 in Brussels. We consider the best practices as described in Clean IT's final document to be useful in reducing the terrorist use of the Internet.

We call for a continuation from the structured public-private dialogue that started with the Clean IT project, to ensure that further public-private cooperation to reduce the terrorist use of the constantly evolving internet is based on mutual trust and understanding.

NAMES / BANNERS

The Clean IT Project

Reducing the impact of the terrorist use of internet

Clean IT Project

Return address:
Ministry of Security and
Justice / NCTV
Oranjebuitensingel 25
2511 VE The Hague
PO box 16950
2500 BZ The Hague
www.nctv.nl

Email: info@cleanITproject.eu
URL: www.cleanITproject.eu

With the financial support from the Prevention of and Fight against Crime Programme of the European Union
European Commission – Directorate-General Justice, Freedom and Security

Date December 2012
Concerning **Invitation final symposium Clean IT project**

Dear Sir, Madam,

It is with great pleasure that we invite you to the Clean IT final symposium, which will take place in Brussels, Belgium on Wednesday 30 January 2013.

The central theme of the symposium is "the making of Clean IT". We will be reflecting on the process of public-private dialogue and the experiences we shared. A number of speakers will inspire us with their perspectives on the Clean IT subject matter, the ways in which the project efforts fit into broader internet safety and cyber security themes, and possibilities to take these forward. There will be opportunity to ask questions and a panel discussion will provide insight in the types of issues the project addressed in the one and a half years of its existence. The meeting will end with the official presentation of the Clean IT final document to Mr. Gilles de Kerchove, EU Counter-terrorism Coordinator.

We very much hope you will be able to attend! If so, please use the link below to register. We only have room for a limited number of participants and registration will close when we reach the maximum number of participants.

https://english.nctv.nl/clean-it-final-symposium/index.aspx

Hoping to see you in Brussels at the start of next year we remain,

With kind regards,

The Clean IT project team

Feel free to leak this document :-)

National Coordinator for
Counterterrorism and Security
Ministry of Security and Justice

> Return address Postbus 16950 2500 BZ The Hague

European Commission
DG Home Affairs
Crisis Management and Fight against terrorism
Mr. Olivier Luyckx
B-1049 BRUSSELS
Belgium

Strategy and Operational Management Department
NCTV

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

Contact
[redacted]
Project Officer

[redacted]

Project name
Clean IT

Appendix
Draft Programme

Our reference
339617

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

Date 10 January 2013
Concerning Invitation Clean IT final symposium DG Home

Dear Mr Luyckx,

It is with great pleasure that I invite you to the Clean IT final symposium, which will take place at the Thon Hotel EU in Brussels, Belgium on Wednesday 30 January 2013, from 12:30-17:00.

The central theme of the symposium is "the making of Clean IT". We will be reflecting on the process of public-private dialogue and the experiences we shared. A number of speakers will inspire us with their perspectives on the Clean IT subject matter, the ways in which the project efforts fit into broader internet safety and cyber security themes, and possibilities to take these forward. There will be opportunity to ask questions and a panel discussion will provide insight in the types of issues the project addressed in the one and a half years of its existence. The meeting will end with the official presentation of the Clean IT final document to Mr. Gilles de Kerchove, EU Counter-terrorism Coordinator.

The European Commission's commitment to the project was greatly appreciated and I very much hope you will be able to attend this closing session.

Hoping to see you or a representative of DG Home in Brussels at the end of January I remain,

Kind regards

Th.P.L. Bot
Deputy National Coordinator for Counterterrorism and Security

The Clean IT Project

Reducing the impact of the terrorist use of internet

It is with great pleasure that we invite you to the Clean IT final symposium on Wednesday 30 January 2013

The Internet plays a positive role in our lives and societies, but it is also used for illegal purposes, including terrorism. The Clean IT project started a dialogue between governments, industry, NGO's, law enforcement and academics on reducing the use of the Internet for terrorist purposes. In this final symposium, we will be reflecting on the experiences we shared, the results we achieved and ways to take these forward in the future.

Invitees

The symposium is open for attendance to all project participants and any other interested persons or organizations.

Time and location

The symposium will take place at the Thon Hotel EU in Brussels from 12:30 until 17:00 on Wednesday 30 January 2013.

Programme

What can you expect this afternoon? Contributions and discussions on the project's process and results. Reflections on issues such as the importance of awareness and prevention, free speech, transparency and security concerns.

Arda Gerkens (HCC), Pascal Gloor (Pirate Party Switzerland), Michael Whine (Community Security Trust), Tamara Walker (UK Home Office), Asiem El Difraoui (Institute for Media and Communication Policy) and Maura Conway (Dublin City University) will be giving their perspectives. But Klaasen (project manager) will be providing insight in the "making of" Clean IT. And Theo Bot (National Coordinator for Counterterrorism and Security) will be presenting the end results to Gilles de Kerchove (EU Counterterrorism Coordinator). The symposium will be moderated by Cyrus Farivar; radio producer, author and senior business editor at Ars Technica. In this last capacity he wrote two articles about the Clean IT project.

Participation

We very much hope you will be able to attend! If so, please register using this link https://english.nctv.nl/clean-it-final-symposium/index.aspx.

We only have room for a limited number of participants and registration will close when we reach the maximum capacity.

The Clean IT Project

Reducing the impact of the terrorist use of internet

CLEAN IT FINAL SYMPOSIUM
Wednesday 30 January 2013
Draft programme 10.01.13

12:30 Lunch

Opening remarks by Cyrus Farivar, symposium moderator

"Public Private Partnerships in counterterrorism projects" by Theo Bot, Deputy National Coordinator for Counterterrorism and Security of The Netherlands

"Inside Clean IT" by But Klaasen, projectmanager

"The making of Clean IT" – contributions, Q&A session and panel discussion

- *Arda Gerkens, Director, HCC ("Awareness")*
- *Pascal Gloor, Vice President, Pirate Party Switzerland ("Why prevention matters")*
- *Tamara Walker, Policy Advisor, Home Office, UK ("UK perspectives on Clean IT")*
- *Michael Whine, Director, Community Security Trust ("Balancing free speech considerations with European concerns – interfacing with the US social networks")*
- *Asiem El Difraoui, Senior Fellow, Institute for Media and Communication Policy ("There is no "Clean IT" – a friendly polemic")*
- *Maura Conway, Senior Lecturer in International Security, Dublin City University ("Tackling violent online political extremism: An academic perspective")*

Q&A session and panel discussion

15:45 Presentation of the Clean IT final document to Gilles de Kerchove, European Counterterrorism Coordinator

16:00 Reception

17:00 End

National Coordinator for
Counterterrorism and Security
Ministry of Security and Justice

> Return address Postbus 16950 2500 BZ The Hague

Strategy and Operational Management Department
NCTV

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

Contact
[redacted]
Project Officer

[redacted]

Project name
Clean IT

Appendix
Draft programme

Our reference
339622

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

Date 10 January 2013
Concerning Invitation Clean IT final symposium

Dear Clean IT project partner,

It is with great pleasure that I invite you to the Clean IT final symposium, which will take place at the Thon Hotel EU in Brussels, Belgium on Wednesday 30 January 2013, from 12:30-17:00.

The central theme of the symposium is "the making of Clean IT". We will be reflecting on the process of public-private dialogue and the experiences we shared. A number of speakers will inspire us with their perspectives on the Clean IT subject matter, the ways in which the project efforts fit into broader Internet safety and cyber security themes, and possibilities to take these forward. There will be opportunity to ask questions and a panel discussion will provide insight in the types of issues the project addressed in the one and a half years of its existence. The meeting will end with the official presentation of the Clean IT final document to Mr. Gilles de Kerchove, EU Counter-terrorism Coordinator, and a photo moment with the coördination group partners and Mr. De Kerchove together.

Your active cooperation in the project was greatly appreciated and I very much hope you will be able to attend this closing session.

Hoping to see you or a representative of your organization in Brussels at the end of January I remain,

Kind regards

Th.P.L. Bot
Deputy National Coordinator for Counterterrorism and Security

The Clean IT Project

Reducing the impact of the terrorist use of internet

It is with great pleasure that we invite you to the Clean IT final symposium on Wednesday 30 January 2013

The Internet plays a positive role in our lives and societies, but it is also used for illegal purposes, including terrorism. The Clean IT project started a dialogue between governments, industry, NGO's, law enforcement and academics on reducing the use of the Internet for terrorist purposes. In this final symposium, we will be reflecting on the experiences we shared, the results we achieved and ways to take these forward in the future.

Invitees
The symposium is open for attendance to all project participants and any other interested persons or organizations.

Time and location
The symposium will take place at the Thon Hotel EU in Brussels from 12:30 until 17:00 on Wednesday 30 January 2013.

Programme
What can you expect this afternoon? Contributions and discussions on the project's process and results. Reflections on issues such as the importance of awareness and prevention, free speech, transparency and security concerns.

Arda Gerkens (HCC), Pascal Gloor (Pirate Party Switzerland), Michael Whine (Community Security Trust), Tamara Walker (UK Home Office), Asiem El Difraoui (Institute for Media and Communication Policy) and Maura Conway (Dublin City University) will be giving their perspectives. But Klaasen (project manager) will be providing insight in the "making of" Clean IT. And Theo Bot (National Coordinator for Counterterrorism and Security) will be presenting the end results to Gilles de Kerchove (EU Counterterrorism Coordinator). The symposium will be moderated by Cyrus Farivar; radio producer, author and senior business editor at Ars Technica. In this last capacity he wrote two articles about the Clean IT project.

Participation
We very much hope you will be able to attend! If so, please register using this link https://english.nctv.nl/clean-it-final-symposium/index.aspx.

We only have room for a limited number of participants and registration will close when we reach the maximum capacity.

Inside Clean IT : january 30th 2013

[sheet met afbeelding ISEC programma]

Ladies and Gentlemen,

In the year 2008 I was project manager for the development of a voluntary Notice-and-Take-Down code of conduct. I brought together law enforcement agencies, ministries, interest groups and the internet industry in a complex discussion on how to handle carefully notifications of misuse of the internet. In that period, Germany was finalising its international case study on jihadism on the internet. The German project concluded that a public-private approach might be an interesting attempt to react to the fast growing terrorist use of the internet. When early 2010 the European Commission issued a call under the "Prevention of and Fight against Crime" programme, the Dutch government launched the Clean IT project proposal with Germany, the United Kingdom, Belgium and Spain. The project started in the summer of 2011, and during the project more governments joined. Upon closing, it has the support of 6 other countries: Austria, Denmark, Hungary, Romania, Greece and Portugal, making it an eleven country effort.

Now, after 21 months, we deliver exactly what we promised in 2010: a set of general principles and a list of best practices, created in a multi-stakeholder, public-private dialogue. I would like take this opportunity to illustrate how the project was actually managed, which dilemmas we faced, and what lessons we learned. But first: a brief overview of how Clean IT was made.

[sheet verdeling participants]

One of the starting points to establish a constructive dialogue, is to find the right participants:
- participants with different but relevant backgrounds,
- participants with specific expertise, and
- participants willing to have an open discussion.

In order to come to a balanced, interesting group of participants, we chose to invite people directly and notified organizations we think they could be interested in this matter. The meetings, however, were not closed. Anybody could join the discussion as long as all relevant target groups were represented at the table. We tried to include

1. Law enforcement agencies and intelligence services,
2. Ministries,
3. NGO's,
4. Academics,
5. End users,
6. Internet industry, and
7. Technology industry

And we managed quite well as you can see in this graph.

Secondly, we wanted to encourage free discussions. We wanted participants to express their opinions, without concerns for their personal reputation or their official duties. We wanted to create a setting which allowed for open discussions about good and bad ideas, about complex and controversial issues.

To do so, we used the so-called Chatham House rules. This means that participants are free to use the information discussed in the meeting, but that neither the identity nor the affiliation of any participant are to be disclosed, other than by the participant himself.

[sheet timeline 1]

The Clean IT project scheduled six meetings, with a growing number of participants. We started the first meeting with 20 participants in Amsterdam, and ended with 50 participants in Vienna. We had 110 different participants in total, and many of them came more than once. Already during the first meeting in Amsterdam, we started to draft a working document that reflected the outcome of the discussion. After each meeting the draft document was improved, checked by the participants, and published on the internet where it was open for comments. We used this new draft and the comments we received as input for the next meeting. In this way, we had a discussion not only with our meeting participants, but also with anyone else interested in the matter.

[sheet timeline 2]

Participants in the second meeting in Madrid suggested to start small working groups because they wanted to have more specialised, in-depth discussions which are difficult to have in a plenary session. We started to do this in the third meeting in Brussels. Those small groups discussions worked well, and we collected the outcome of these discussions in a second document. This document contained more detailed ideas, more controversial issues, and did not undergo the same careful editing process as the main working document. Because some information in this second document was still inaccurate, we decided not to publish it but to use it for discussion only. In our fifth meeting in Utrecht we discussed how this discussion document should be linked to the main document. One thing became clear. By the time of our final meeting in Brussels, which is here and now, we did not want to present an unfinished document. The conclusion in Utrecht was that when this project finishes, we should not have any confidential documents left. So we had to do some extra editing and participants suggested to merge both documents into one. That is what we did in preparation of the meeting in Vienna.

But then something else happened.

[sheet EDRI leak]

First, let me tell you that I personally invited Joe McNamee of the European Digital Rights Initiative to take part in our discussions. This happened right at the start of the project, in June 2011. I told him more than once that we really wanted the perspectives on protecting online freedom well-represented at our meetings. But he did not want to participate. Nevertheless we decided to keep EDRI updated all the time.

Two weeks after the meeting in Utrecht, EDRI published the second document that was confidential and for discussion purposes only. EDRI claimed that the Clean IT project wanted binding engagements from internet companies to carry out surveillance, to block and to filter the internet and to seek for new, stricter legislation from Member States. This news quickly traveled around the world and framed Clean IT as an infamous secret censorship programme. I remembered well that during one of the first meetings the idea came up to create a Facebook page about Clean IT to raise awareness and start online discussions. Now we have plenty of them, with the title "stop Clean IT". There are also websites and Twitter accounts with this name. So thanks to the EDRI publication, we caught the attention of many concerned citizens.

[sheet facebook + filmpje anonymous + sheet webbezoek]

It is interesting to see that our website was visited from all around the world, especially after this outburst in September last year. By far most visitors to the Clean IT website, 28%, came from Germany. The Netherlands and United States are second and third with both approximately 7%.

As Clean IT was a hot topic in online discussions, it also led to parliamentary questions in the Bundestag and in the European Parliament. One of the questions was if Clean IT might violate fundamental rights and individual freedoms on the internet. This is of course an interesting topic, and one that was already addressed in the first meeting in Amsterdam. After six meetings where this item was extensively discussed, the principle of online freedom is firmly rooted in the final document. But this is no guarantee for the future. Best practices can be implemented in a bad way. Therefore we asked the University of Tilburg which has a good reputation in scientific research in the area of human rights, to conduct a quick scan in order to comment on the possible impact of the Best Practices on fundamental freedoms.

[sheet rapport tilburg]

We invited the researchers to present their report this afternoon here in Brussels, but unfortunately they were not able to attend. Their report will be published on our website very soon, and I will summarise their conclusions now. But let me first underline that the best practices in the Clean IT report do not raise immediate human right concerns at this stage. In future, however, much depends on how the Best Practices are interpreted, how they are implemented in practice, and how they relate to other practices. The researchers scanned carefully for possible threats to human rights that might occur by future implementation of the best practices. The researchers conclude that some best practices should be accompanied by clear procedures and guarantees, yet that others do raise significant questions. For me, this sounds very much like "don't try this at home, always consult a professional". And I think that isgood advice, because in general: implementing security measures can probably always affect someone's online freedom. So we strongly recommend reading this report, which also describes some interesting dilemmas that we discussed in our Clean IT meetings.

Now speaking about dilemmas, we faced a lot of them during the Clean IT project. I would like to summarise four statements in this regard, also to inspire the speakers for the panel after the break.

[sheet dilemmas]

The first one is that the 'terrorist use of the Internet' is vague term, and requires extensive explanation by professionals every time. We did that during our meetings. We repeated presentations more than once to bring the basic knowledge about this complex issue for all participants to the same level.

The second dilemma is about controversial issues. On the one hand, discussions about controversial issues might reinforce a culture of fear, especially if you publish them on the internet. But on the other hand we noticed that these controversial issues were very inspiring for the participants and often led to very fruitful discussions.

Then the point of transparency. I think personally this is was a core issue for the whole project. We tried to be as open as possible, but it did not always lead to more trust. Publishing rough interim results that are open for comments, sometimes raised more questions and caused misunderstandings. We were aware of the complexity of the issues at stake, but we also wanted to be just as open and interconnected as the internet is. To my knowledge, the Clean IT project was the most open counter-terrorist project in the world. There is one thing I am sure of. If we would have chosen for a more confidential approach, the end results would not have been the same.

The last dilemma to mention is a classic one and addresses the tension between security and privacy. It should actually be expanded to openness. In my opinion, security, privacy and openness of the internet are the three basic sides of a triangle that should always be balanced.

Ladies and gentlemen,
What I just told you, is now written in a document called "the making of Clean IT". We will publish this on our website. It

describes in more detail how the project was managed, how we handled different situations, and which lessons we learned. I hope this insight is useful to anyone that would like to organise a similar public-private dialogue in future.

The Clean IT project comes to an end now. After many years of project management I feel honoured to end a long list of projects with such a thrilling issue as the terrorist use of the internet. We explored a new way of working in this field. Governments, in my observation, are not always used to cooperate with the private sector on an equal footing. Where internet governance is concerned, public and private parties need each other, and should be connected to each other. I hope that the Clean IT working method enriches both public and private partners.

Finally, let me thank our government partners that supported this project: Germany, United Kingdom, Belgium, Spain, Austria, Denmark, Hungary, Romania, Greece and Portugal. Let me also thank the members of the projec tteam that did a great job, and of course my director and his staff that always supported the direction this project took. But most of all, let me thank all the participants that attended our meetings or that contributed online to our discussions. The insights we gained, the experiences we had, the dilemmas we faced, the knowledge we acquired and the views we shared, it is all thanks to the participants. The call for continuation of this dialogue is therefore not my call, it is yours.

Thank you very much.

Inside Clean IT

The 'Making Of' the Clean IT project

With financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Justice, Freedom and Security

Inside Clean IT

The ‘Making Of’ the Clean IT project

Clean IT project team,
The Hague,
January 2013

Contents

1 **Introduction** **4**

2 **Structure of the project** **6**

2.1 Preceding Initiatives 7

2.2 Objective 7

2.3 Procedure 8

3 **Course of the project** **12**

3.1 Time Schedule 13

3.2 Activities and Developments 14

4 **Lessons Learned** **18**

4.1 Complex and Specialist Subjects Require Detailed Explanation 19

4.2 Controversial Subjects Are a Source of Inspiration 19

4.3 More Transparency Leads to More Questions 20

4.4 Security versus Freedom: An Ongoing Dilemma 21

5 **Conclusions** **22**

1 Introduction

The Internet plays a major – and predominantly positive – role in our society. Unfortunately, the Internet is also used for criminal purposes, including terrorism. The Internet is of strategic importance to Islamic extremist and terrorist networks. Since 2001, these groups have used the Internet more and more for achieving their purposes, such as propaganda, recruitment, and radicalisation, but also for preparing and planning attacks. This has been the subject of many publications by governments and scientific institutes. The use of the Internet for these purposes is punishable under European legislation.

In 2010, the European Commission called upon the Member States to submit project proposals to tackle this problem, and to include public-private cooperation in the working method. This prompted the Dutch Ministry of Security and Justice to submit the project proposal 'Fighting the illegal use of the Internet with public-private partnerships from the perspective of counter-terrorism'. The word 'illegal use' was used deliberately to exclude the possibility that the government would tackle 'undesirable content' as well, for this would mean censorship by the government. The abridged title of this project became 'Clean IT'.

The Clean IT project was an experiment. Never before had a counterterrorism project given so much room to citizens and companies to watch during the work in progress, and to take part in determining how the final product would look like. The Clean IT project team opted for an interactive process in which, during the project, increasingly more participants had to reach consensus on the problem and on appropriate solutions for this problem. Such a working method was not only new to the participants, but also to the project management.

The purpose of this publication is to provide insight into how this process proceeded, and to explain the dilemmas that were encountered in the process. Much has been learned from the experiences gained in the Clean IT project, and this insight may be of use to any following projects of comparable scope and objective.

First, a description is given of how the Clean IT project was structured and how the project actually proceeded. Subsequently, the lessons learned are discussed on the basis of dilemmas experienced by the project team. Finally, some conclusions will be drawn.

2 Structure of the project

This chapter describes several of the initiatives that preceded the Clean IT project, and determined the structure of the project. It subsequently provides a description of the project objectives as well as the working method followed, including the public-private cooperation, the aim of the meetings, and the process in which the final document was accomplished.

2.1 Preceding Initiatives

There were *three* initiatives that formed the building blocks of the Clean IT project.

The *first* building block was the EU project 'Exploring the Islamist extremist Web of Europe' (2009) conducted under the management of Germany. The partner countries were the United Kingdom, the Netherlands, and the Czech Republic. The project generated a study of radicalisation processes and Islamic extremist content on the Internet. One of the conclusions of the project was that a public-private approach could be an interesting subsequent step. This was the reason to start thinking about a follow-up project on a public-private basis.

During the implementation of the German project, several best practices emerged, including the Dutch code of conduct 'Notice-and-Take-Down'. The latter is a working method that can be used on a voluntary basis and describes how internet companies that are confronted with illegal content can best deal with this problem. There was a growing awareness that there were many more 'best practices' being implemented at a national level, whereas terrorism and the Internet are international phenomena. The *second* building block of the Clean IT project was consequently formed by identifying the best practices that were followed in the different countries and, where applicable, by promoting their use internationally.

While the Netherlands was making plans for a follow-up project, the European Commission organised a public-private dialogue to develop ways to be better able to tackle different forms of illegality, such as terrorism and child pornography. Although this dialogue met a need, this initiative was not continued after a few meetings. The need for a dialogue about these issues between public and private partners constituted the *third* building block of the Clean IT project.

The idea for the Clean IT project on the basis of these three building blocks appeared to fit in well with the call by the European Commission to submit project proposals in the area of counterterrorism by means of public-private cooperation. Germany, the United Kingdom, Belgium, and Spain joined as partners, and the Clean IT project proposal was submitted on the initiative of the Netherlands.

2.2 Objective

The Clean IT project had the following three main objectives:

1. To start a constructive public-private dialogue about terrorist use of the Internet.
2. To draft a set of 'general principles' that are supported by the participating public and private parties and that can be used as a guideline to deal with terrorist use on or through the Internet.
3. To identify 'best practices' which are considered useful in dealing with terrorist use of the Internet.

As the Clean IT project is a public-private cooperation, it cannot impose obligations as legislative projects do. As a result of this, the use of best practices and compliance with the general principles cannot be legally enforceable. Organisations may decide to follow the best practices on a voluntary basis, but this does not fall under the responsibility of the project. The general principles and the best practices are described in the final document of the Clean IT project.

2.3 Procedure

Public-private cooperation

On the one hand, the internet infrastructure is owned for the greater part by private companies, and these companies have the most knowledge of internet use and internet technology; on the other hand, public authorities have an in-depth knowledge of terrorist networks. The philosophy of the project was therefore that it was necessary to combine these different specialist areas of expertise in order to be able to get to the bottom of the problem of terrorist use of the Internet. It will not be possible to arrive at practicable and broadly-based solutions until this step has been made.

In addition, fundamental interests/freedoms as privacy and access to a free and accessible Internet should also be included in the discussions about the Internet and terrorism. Therefore, the Clean IT project team organized a structured dialogue between experts addressing all relevant interests.

Network approach

It was the intention to achieve the project objectives with broad and growing support. The project was started with a relatively small group of participants which was gradually expanded. It appeared that new participants were reached mainly by personal contact. The project team approached potentially interested persons and organisations by telephone and by e-mail. In addition, the team gave presentations, and the project's existence and progress was communicated publicly.

Selection policy for the meetings

In order to keep the discussions orderly, within the budget, and effective, the number of participants in each meeting was subject to a maximum. The participants had to be given the opportunity to contribute actively from their areas of expertise and the composition of the group had to be balanced, with representations from:

- Enforcement agencies
- Policymakers and legal experts (central government)
- Nongovernmental organisations
- Academics and scholars
- Internet industry (in particular hosting, social media, and to a lesser extent, access providers)
- Technology/software industry
- End users

In order to achieve this, the participants were approached personally. Some were invited on the basis of their specific expertise to give presentations in plenary meetings. Not a single participant was refused for reasons other than those stated above. The chairman played a major role in the preparations for the meetings, and succeeded in drafting an attractive agenda for each of the participants.

Confidentiality of the meetings

The meetings were partly confidential. It was not always possible to disclose the participants' names, as this would endanger the safety of the relevant participants (charged with counterterrorism). In addition, several participants desired protection of their privacy. A few companies, for instance, did not want their public image to be associated with counterterrorism. Therefore, the Clean IT project team never published the names of persons or organisations without prior consent, unless they had already publicised their participation themselves. Participants in the Clean IT project were, however, free to discuss the contents of the discussion outside the meetings under the so-called 'Chatham House rules'. This means that neither the identity nor the connection of the speaker(s) or that of other participants may be disclosed.

Process steps

The main activity of the Clean IT project team was to draft a text that would generate broad support. This process involved a series of 6 meetings with experts over a period of 21 months. Each meeting was held in a different country in order to achieve the maximum possible balance in the input from the participating countries. The results of the meetings were described in a draft document, so that each meeting resulted in a text that had been adapted and tightened up. In more detail, the steps were structured as follows:

1. The updated draft document was sent to all contact persons and published on the project's own website, with a general invitation to comment on the document. These comments were collected and bundled.
2. The meetings were organised with experts of public and private organisations. The entire document and the comments collected were discussed in plenary sessions during these this meeting.
3. During the meetings, there were also discussions about specific issues in small workshops. The results of the small workshops were subsequently used as an input for the plenary sessions.
4. At the end of the meeting, the project team drafted a new version of the draft document on the basis of the discussions; this document was submitted to all participants for approval.
5. The project team processed the comments of the participants into a new version of the draft document, after which the cycle started again with step 1.

This cycle was repeated around the meetings that were organised. For the purpose of modifying the draft document, the project team was expanded by an editorial board composed of several willing participants.

In addition to these steps, the project team designed a questionnaire and sent it out to experts in all EU Member States to identify additional best practices.

The project organisation

The Clean IT project was organised by a small team that was located at the Dutch Ministry of Security and Justice. The project manager bore general responsibility for the project and made the decisions necessary to implement the project properly. He monitored the process and he was the point of contact for external parties. He was assisted by a secretary who also arranged the logistics and the financial affairs. The third team member was primarily responsible for the proper course of the meetings and for drawing up the final document.

In addition to the project team, there was an international coordination group composed of officials from ministries or counterterrorism organisations from the participating countries. This group evaluated the meetings and coordinated the strategic course of the project. It was not the task of the coordination group or of the project team to determine the contents of the document. This was done by the participants in the meetings.

3 Course of the project

This chapter describes how the projected proceeded. First, the time schedule is presented with the most important milestones, followed by a description of the activities and the developments of the project.

3.1 Time Schedule

2010			
	Jan		
	Feb		
	March		
	Apr	*27 April*	*ISEC's publication call*
	May		
	Jun		
	Jul	*28 July*	*Submission of project proposal to European Commission*
	Aug		
	Sep		
	Oct		
	Nov		
	Dec		
2011			
	Jan		
	Feb		
	March		
	Apr	*2 April*	*The Dutch Minister of Security and Justice announces the intended start of the project during a cybercrime conference in Budapest*
	May	*1 May*	*European Commission gives permission to start the Clean IT project*
		31 May	*Kick-off meeting in Belgrade*
	Jun		
	Jul		
	Aug	*23 August*	*Grant agreement signed*
	Sep	*1 September*	*project team formed*
	Oct	*24-25 October*	*First meeting, Amsterdam*
	Nov		
	Dec	*16 December*	*Questionnaire sent to 23 EU Member States*
		22 December	*Publication of the first draft document on the website*
2012			
	Jan	*18-19 January*	*Second meeting, Madrid*
	Feb		
	March	*21-22 March*	*Third meeting, Brussels*
	Apr	*17 April*	*Invitation to other EU countries to become a 'Supporting Government Partner'*
	May	*22 May*	*Publication of new version of the draft document on the website*
	Jun	*4-5 June*	*Fourth meeting, Berlin*
	Jul		
	Aug	*14 August*	*Publication of new version of the draft document on the website*
	Sep	*12-13 September*	*Fifth meeting, Utrecht*
		21 September	*EDRI publishes 'leaked document'*
	Oct	*1 October*	*Members of the European Parliament ask written questions about the Clean IT project*
		24 October	*The German Minister of Home Affairs answers written questions from the 'Bundestag'*
		31 October	*Publication of new version of the draft document on the website*
	Nov	*5-6 November*	*Sixth meeting, Vienna.*
	Dec	*18 December*	*Deadline last round of written comments*
2013			
	Jan	*30 January*	*Presentation of the final document in Brussels*

3.2 Activities and Developments

Kick-off meeting

During the European Discussion on internet Governance (EuroDIG) conference, the project manager announced in a plenary session that the project had started. The EuroDIG was a source of inspiration for the Clean IT project because of the multi-stakeholder model and the transparent character of the conference. The first meeting of the coordination group was also held during the conference on 31 May 2011.

A short time later, the project team started its activities. It organised the first meeting and contacted potential participants in writing. The European Digital Rights organization (EDRI, an international non-profit association) was also approached, and the project team explained that, it was the intention in this project, with respect to the discussions, to properly safeguard the interests of the end users and internet freedom, from the very beginning. Nevertheless, EDRI was sceptical, and decided not to participate. However, EDRI received updates on the project and was still invited to give comments.

Formulation of the first draft document

The first meeting on 24-25 October 2011 was attended by approximately 20 participants. Presentations were given both on terrorist use of the Internet and on the practice of abuse of networks in general. With regard to some of the issues, the private parties and government representatives had difficulty agreeing on a shared problem analysis. The participants came to the conclusion that, in practice, it was not easy – not even for professionals – to indicate exactly when the threshold of illegality was crossed.

There was also a brainstorming session about which parties could contribute to a solution, and about how the general principles and the best practices could be formulated. This session resulted in the drafting of a rough text, which was submitted to the participants and subsequently published on the website.

Agreement on the scope of the project

It became evident from the reactions on the draft document published on the website that there were different interpretations of terms such as ‘terrorism’, ‘extremism’, and ‘illegality’. When approximately 25 participants from governments, police, internet companies, and NGOs met in Madrid on 18 and 19 January 2012 for the second Clean IT meeting, ‘terminology’ was consequently also a topic of discussion. Another important question was what the precise delineation of the project would be. In order to end the discussion, it was decided to adopt the official EU definitions of terrorism. It was also decided to include the problem analysis in a separate chapter, with the project partners being responsible for the final editing as they had most expertise in this context. This part was to become the ‘preamble.

The development of the working process

The participants expressed the wish to deal in greater depth with the subject matter, and proposed to discuss specific subjects in smaller workshops. This way of working was experimented for the first time during the third meeting in Brussels on 21 and 22 March 2012. The participants approved of this way of working and it was decided to continue this way during the next meetings.

One consequence of holding workshops in addition to plenary sessions was that the results of the meeting were from that time onwards represented in **two** documents. On the one hand there was the **draft document** that had been tightened up and adapted further after Amsterdam and Madrid. On the other hand the participants came up with new and undiscussed ideas and raised new questions. These ideas and questions were gathered in a second document for discussion during the meeting in Brussels. This second document was more detailed than the principal document. Due to the rough nature of the texts, this **discussion document** was not published and was treated confidentially. The texts in the confidential discussion document were elaborated further, or removed due to a lack of consensus in subsequent meetings. During the fifth meeting in Utrecht, the participants concluded that the discussion document had to be rewritten, and the project manager stated that at the end of the project no confidential documents would be left.

Answer to the question of what was to happen once the Clean IT project had been concluded

Since the second meeting, the participants stated to be satisfied with the quality of the discussions, the mix of expertise present, and the existing interests. This raised the question of what was actually to be the tangible result once the project had been concluded. The participants discussed how to continue after the project, and they wondered what the status of the final document would mean in practice, as it would not be legally enforceable. They drew the conclusion that, as far as the Clean IT project is concerned, it was a matter of ‘political commitment’ and not a ‘formal commitment’. Therefore, the participants would be able to support the results without the necessity to sign the document. In addition, there was a unanimous call to give this form of meetings a permanent character. From that time onwards, the text included a call to continue this dialogue.

Form of the general principles and best practices

The text of the general principles gradually took shape during the meetings. During the fourth meeting in Berlin on 4 and 5 June 2012, the approximately 50 participants made much progress, as a result of which this text developed more and more into its final form. However, the best practices still underwent a great deal of doctoring. After the best practice ‘sharing abuse data’ had been added, ‘end user browser mechanism’ was not added until the meeting in Berlin.[1] Participants in Berlin suggested that it would also be useful to include bad practices to make clear that they considered some practices **not** a good idea. Blocking and filtering, for instance, were qualified as ‘bad practices’ in Berlin. In subsequent meetings the best practices ‘real identity policies’ and ‘virtual community policing’ (Utrecht), and ‘automated detection systems’ (Vienna) were deleted completely.

[1] Some practices were renamed in the course of time.

The joining of government supporting partners

The Dutch Minister of Security and Justice requested his European colleagues in April 2012 whether they wished to become 'supporting government partner' of the Clean IT project. To various companies operating internationally the project had become more interesting as they could discuss the same issues with multiple countries at the same time. Various countries reacted positively to this request. During the meeting in Utrecht in 12 and 13 September 2012, approximately 45 participants met, including several Government Supporting Partners who attended the meeting for the first time. These countries assumed the same role as the initial project partners. The only difference was that they had joined later.

In the end, six new countries joined the project: Austria, Hungary, Denmark, Romania, Greece, and Portugal. As a result of this, the Clean IT project was supported by the ministries or security services from 11 countries.

Media attention

The publication of the draft document after each meeting sometimes attracted media attention. The nature of the reactions varied, and some media interpreted the project differently than was intended. On the one hand, the reactions were critical, in the sense that the text of the draft document was considered to pose a threat to internet freedom; on the other hand, the reactions were positive in that the initiative to enter into a public-private dialogue about this issue was appreciated.

Once the draft document developed further, several reputable IT web magazines from the United States, Australia, and France paid attention to the Clean IT project. Their articles discussed, in particular, the tension between internet freedom and counterterrorism measures. On 21 September 2012, the European Digital Rights Initiative (EDRI) published the confidential discussion document – without consultation – that had been submitted to the participants prior to the meeting in Utrecht. According to EDRI, this document had been leaked and was said to show that large-scale and undemocratic measures were being taken to monitor the Internet, and that binding measures were being proposed to have internet service providers block and filter content. This publication caused a flow of negative media coverage and also gave rise to written questions in the German and European parliaments.

Completion of the final document

The negative publicity around the project caused some potential participants to be hesitant about committing themselves to the project. Nevertheless, the meeting in Vienna on 5 and 6 November 2012 was attended by 50 participants. During this meeting, consensus had to be reached about the texts. The project team had merged the draft document and the confidential document on the basis of the discussion in Utrecht into one document, in which the remaining points of discussion had been included in the text.

During the meeting in Vienna, most time was spent on the general principles. These were dealt with meticulously. Plenary discussions were sometimes held about whether or not to include specific terms. Finally, all those present agreed to this text. A last round of written comments was held after which the text achieved its final status.

During the final meeting in Brussels on 30 January, the document was presented to the EU Counter-terrorism Coordinator. During this meeting, various speakers from public and private sectors looked back on their experiences with the Clean IT project and the result achieved.

4 Lessons Learned

This chapter describes which lessons can be learned from the dilemmas experienced during the project, and which can be useful for any follow-up projects or other comparable public-private initiatives.

4.1 Complex and Specialist Subjects Require Detailed Explanation

Problem/dilemma:
In the case of a terrorist threat, the activities are often hard to detect and may be socially disruptive once they have been performed successfully: a combination of a small risk with large consequences. In practice, manifestations of terrorist use of the Internet occur relatively less often than other forms of crime. In addition, the activities are often hard to recognise as such, and the illegality of specific content can often be assessed only in its context. In these cases, the urgency of the problem is not felt by everyone. People are, after all, rarely – if ever – confronted with it, and lack the expertise and the trained eye of the professionals who are occupied with this issue on a daily basis.

How the Clean IT project team dealt with this issue
To the Clean IT project team, this issue meant that the nature, scope, and complexity of the problem had to be explained and presented to the participants, new and old, and the public again and again. This was difficult where sensitive or confidential information was concerned, but there were still sufficient issues, whether settled or not, that could be explained in public. In the course of the project, the Clean IT project team added a page with frequently asked questions to its website, and it published various scientific and other publications on terrorism on its website.

Lesson learned
The lesson learned is that these types of complex problems that hardly appeal to outsiders require ongoing and thorough explanation. The repetition of substantive presentations will finally result in a common picture among all participants, and thereby to a qualitatively edifying discussion.

4.2 Controversial Subjects Are a Source of Inspiration

Problem/dilemma
The results of the dialogue in the Clean IT project are based on consensus. Many subjects of discussion had advantages and disadvantages that were weighed up in the process. Subjects that the group considered controversial were not included in the text. According to the participants, the preceding discussions were valuable and a source of inspiration.

How the Clean IT project team dealt with this issue
Not one subject remained undiscussed because of its controversial nature. Subjects that could not count on consensus were finally also not included in the final document.

Lesson learned

Discussions about controversial subjects have added value, even if no consensus is reached. The discussions were considered valuable and a source of inspiration, providing new insights to the participants. In the future, this may contribute to progress in the manner in which people solve comparable problems.

4.3 More Transparency Leads to More Questions

Problem/dilemma

The starting point of the Clean IT project team was to provide transparency in order to inspire confidence in the participating partners and to be consistent with the best practices of the internet community. This is a striking difference with other counterterrorism projects, as those are often conducted under a statutory regime of confidentiality. The transparency of the Clean IT project was reflected in the fact that the draft document was published periodically on a public website.

Not everything was transparent, though. If desired, names of participants could be kept confidential for privacy reasons. Rough and inaccurate texts were not published, because they would be misunderstood without their contexts and could cause misunderstandings. The meetings themselves were held under the ‘Chatham House Rules’, enabling the participants to exchange ideas freely. It gradually emerged that the information that was actually provided during the Clean IT project incited distrust, and negative and speculative reactions.

How the Clean IT project team dealt with this issue

The Clean IT project team did not only publish the interim results, but also sought publicity itself. This was done to reach more potential participants. After some time, however, the transparency appeared to turn against the project. The project team therefore changed the nature of the information provided about the Clean IT project: more information was communicated about facts and circumstances, and less information about subjects that were still being processed or discussed. The transparency also turned out to be a dilemma to many of the participants. Some participants, for instance, fully supported the project objectives and results, but did not want to be associated with counterterrorism in public publications.

Lesson learned

The question is whether transparency in controversial and complex subjects inspires confidence or rather gives rise to distrust? It is evident that if the Clean IT project had been 100% transparent, or had been conducted in full confidence, the results would have been different. In any case, it is recommended to pay much attention to public communication in a working process that is entirely or partly transparent.

The criticism directed at the project, in so far as the transparency of the process was concerned, has also been the reason for drawing up this document.

4.4 Security versus Freedom: An Ongoing Dilemma

Problem/dilemma

The discussion about the alleged restriction of internet freedom by governments has been going on for years. As a corollary, the question of whether fundamental freedoms of internet users will be restricted was also raised in the context of the Clean IT project. It will be clear that the Clean IT project itself did not affect any freedoms. The question is, however, how high the risk is that fundamental freedoms will be curtailed by organisations that wish to implement the Clean IT best practices in the future and do not sufficiently observe the general principles in the process? There is, after all, often tension between keeping our freedom and protecting our security.

How the Clean IT project team dealt with this issue

Protection of internet freedom was one of the basic principles in the design of the Clear IT project. The participants stated in the very first meeting that the interests of internet freedom and the fundamental rights of the end users required protection. This is currently stated explicitly in the general principles that must be met by all best practices.

This is, however, not a guarantee that fundamental freedoms could not be curtailed in the future. In theory, each sound proposal or practice could be executed poorly. For this reason, the project team requested Tilburg University, which has proven expertise in this area, to review the best practices formulated during the Clean IT project for any potential violations of fundamental freedoms. The result of this quick scan was that none of the best practices, as currently formulated, carry a great risk. Much will, however, depend on how the best practices will be interpreted and implemented, and how they will interrelate. From that perspective, a number of best practices raised serious questions that are essential to the endeavour of protecting fundamental freedoms in any subsequent steps to be taken. The report has therefore been published on the Clean IT website and is highly recommended to anyone who is considering putting the Clean IT best practices into practice.

Lesson learned

Experts in the area of the protection of fundamental freedoms are seldom experts in the area of counterterrorism. Both areas of expertise are, however, required to arrive at good solutions. The multi-stakeholder approach adopted by the Clean IT project team is therefore a precondition to ensure that the discussions about this issue are kept in balance. Discussions about counterterrorism and fundamental freedoms are, however, extremely complex and consequently will also require the opinion of professionals. It is therefore essential that these professionals continue to be involved.

5 Conclusions

With the Clean IT project, a new working method was introduced to deal with an extremely complex subject. It was not possible to assess in advance whether this working method would produce better results than those obtained with, for instance, a traditional legislative procedure. The assumption underlying the Clean IT project was that it was possible to make progress in counterterrorism on or through the Internet without regulating the Internet itself.

The first conclusion is that this can be achieved by such a working method, but that it takes much time and energy, and that progress is made little by little. A public-private cooperation for this subject should consequently be limited to a dialogue. The Clean IT project was not a tool to privatise enforcement tasks or to make formal decisions about concrete measures. This should continue to be reserved at all times for the competent authorities.

A second conclusion ensued from the positive experiences of the participants in the Clean IT project. It turned out that drawing up an interesting agenda together with a mixed, competent, and balanced group of participants proves fruitful. In this way, the advantages and disadvantages of – in particular – controversial subjects can be held against the light systematically. This is valuable, and a source of inspiration. The participants have indicated that they wish to continue the dialogue, and this desire is supported wholeheartedly by the project team.

Finally, the project team is of the opinion that in terms of contents an interesting document has been created, whereby the interests of security, privacy, and openness of the Internet are in balance. Various participants will be able to take advantage of this. We trust that this will contribute to a cleaner Internet, while retaining all the good things provided by the Internet.

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

Februari 2013 | Publicatienr: J-17106

National Coordinator for
Counterterrorism and Security
Ministry of Security and Justice

> Return address Postbus 16950 2500 BZ The Hague

Coordination and Crises Management Department

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

Contact
H.M. Klaasen
Programme manager
[redacted]

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.

Date 17 January 2012
Concerning Questionnaire

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 the 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.

Coordination and Crises Management Department

Date
17 January 2012

Our reference
www.cleanitproject.eu

New project: Clean IT

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.

Coordination and Crises Management Department

Date
17 January 2012

Our reference
www.cleanitproject.eu

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 [redacted]

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 you to send 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,

H.M. Klaasen
Programme manager

National Coordinator for
Counterterrorism and Security
Ministry of Security and Justice

> Return address Postbus 16950 2500 BZ The Hague

Coordination and Crises Management Department

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

Contact
H.M. Klaasen
Programma manager
[redacted]

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.

Members Counter Terrorist Working Group

Date 16 December 2011
Concerning Questionnaire

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.

Coordination and Crises Management Department

Date
16 December 2011

Our reference
www.cleanitproject.eu

New project: Clean IT

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.

Coordination and Crises Management Department

Date
16 December 2011

Our reference
www.cleanitproject.eu

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 [redacted]

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,

H.M. Klaasen
Programme manager

Questionnaire to identify practices to limit the use of the internet by terrorists and extremists

With practices are meant measures like internet monitoring, filter mechanisms, subsidising non-governmental organisations, notice-and-take down agreements with internet industry, flagging tools, real name policies, research, education or awareness programmes.

QUESTIONS

1. **How is the use of the internet by terrorists or extremists limited in practice in your country? If there is no general policy, are you aware of any best practices in this field?**

Please list practises applied or planned in your country, if possible include a hyperlink where we can find more information on the web. Please describe each practice (actors, actions, governance, costs, effects) in some detail. If possible, please include for each practice which person can be contacted for receiving more information (name, emailadres, mobile phone number).

Answer:

2. **Which kinds of internet use by terrorists and extremists is seen as a problem in your country?**

Please give examples of cases in which practical measures could help limiting internet use by extremists and terrorists.

Answer:

3. **Who in your country would be interested in participating (receiving emails with updates, invitations for meetings and commenting on drafts) in the CleanIT project?**

Please provide a list of persons (name, emailadres, organisation) from government, internet industry, association of internet service providers, top-5 webhosting providers, national / non-english (*) social media, vendor sites, law enforcement, non-governmental organisations, science and researchers, who you think would be interested. (CleanIT will send them an email inviting them to participate.)

Note: this question is not meant as a demand 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 like to be kept updated!

(*) we have allready contact persons from most populair multinationals like Facebook, Google, Twitter, Ebay.

Answer:

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

If you need any explanation, have questions or want to comment: please send an email to questionnaire@cleanitproject.eu or call [redacted]

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

The Clean IT Project

Fighting the illegal use of internet

Report on Clean IT Questionnaire

The Hague,

February 2013.

FOR PUBLICATION

This document is for publication. The recipient may share this document freely with others.

Content

Introduction 3

Recognition of the problem 6

Instruments to reduce terrorism on the Internet 11

Two additional best practices 14

Introduction

The Clean IT project

The Internet plays a central role and is of great strategic importance to terrorists and extremists. It is a critical tool for generating funds, recruits, support, propaganda, communication, coordination of activities and planning of operations. Those phenomena were studied during the European Union project “Exploring the Islamist extremist Web of Europe - Analysis and Preventive Approaches”, that was finalized 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 the Internet. The 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. The project, however, did conclude that prevention of Internet crime is of common interest to governments, security authorities, the Internet sector and Internet users. Prevention should consist of a wide range of approaches and include a number of partners. Traditional law enforcement approaches are not always effective when dealing with terrorism and extremism in the virtual world. 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. The industry has much more knowledge and capacity to keep the Internet ‘clean’ than public organizations do. Solutions can be found in direct cooperation between Member States and the Internet industry.

The Netherlands (National Coordinator for Counterterrorism and Security) has therefore submitted a project proposal in partnership with Germany (Federal Ministry of the Interior), the United Kingdom (Office for Security and Counter Terrorism), Belgium (Coordination Unit for Threat Analysis), and Spain (Centro Nacional de Coordinación Antiterrorista). The project was named Clean IT and started in the summer of 2011, partially funded by the European Commission. The Clean IT project (www.cleanitproject.eu) organizes open discussions in a trusted environment (by means of workshops and conferences) between the Internet industry, government, law enforcement, non-governmental organizations and user organizations. These workshops focus on reducing the terrorist use of the Internet. The objective of the project is to identify general principles, best practices and methods for permanent dialogue that can reduce the terrorist and extremist use of the Internet. These general principles, best practices and methods for permanent dialogue will be written down in a draft document.

Questionnaire

A separate track of the Clean IT project aims to identify practices to reduce terrorist and extremist use of the Internet in all European Union Member States by means of a questionnaire. The practices that were identified in the questionnaire will be used as input for the draft document. Best practices can be related to Internet monitoring, end user controlled filtering mechanisms, subsidizing non-governmental organizations, notice-and-take down agreements with the Internet industry, flagging tools, real name policies, research, education and awareness programmes.

In December 2011, a questionnaire was sent to the members of the European Union Counter Terrorism Working Group to gather information on best practices that reduce the terrorist use of the Internet, and to establish contact with experts in both public and private organizations that would be interested in participating in the Clean IT project and possible follow-up projects. The questionnaire was also sent to 23 countries and 8 Internet Service Provider Associations (ISPAs).

In the questionnaire three questions were posed:

- How is the use of the Internet by terrorists reduced in practice in your country? If there is no general policy, are you aware of any best practices in this field?
- Which kinds of Internet use by terrorists is seen as a problem in your country?
- Who in your country would be interested in participating (receiving emails with updates, invitations for meetings and commenting on drafts) in the Clean IT project?

Respondents were asked to answer the questions according to their own knowledge and insight. They were suggested to contact a couple of other experts if needed, but no detailed and thorough study was required.

The deadline for returning the questionnaire was set at April 1,2012. The main findings of the questionnaire were presented during the Clean IT conference in Berlin, June 4 and 5, 2012.[1] At the end of June 2012 a draft report based on the questionnaires was sent to all respondents for comments to be returned before the end of July 2012. The final version was send to the members of the Working Group by e-mail at the end of August and presented at the Clean IT Workshop in Utrecht in September 2012. This document is a public version of the report: all names of Member States and ISPAs have been anonymized or deleted.

Return of the questionnaire
Out of the total of 31 questionnaires being sent, 12 were returned: a reasonable 39% response rate. The questionnaires were returned by 11 countries and 1 ISPA. Two national ISPAs replied they would like the European ISPA to handle these types of issues and contacts.

While a couple of questionnaires being returned were only one page long, most were 2 to 5 pages, the longest covering 8 pages. In general, answers were rather to-the-point and provided a clear picture of the issue in the responding countries. Except for two, all questionnaires answered all three questions. In reply to the third question, a total of 45 persons were mentioned that might be interested in the Clean IT project. Most of these people worked for the public sector; government, law enforcement agencies and intelligence. Some respondents provided only one suggestion, most provided 3-5, while the maximum was 9. The persons that were named in the answers of the questionnaire were contacted by e-mail by the Clean IT project team to ask if they would be interested to be kept up-to-date on the projects progress. From these initial contacts a number of other connections were made. The project currently has a database including about 60 organizations or persons in the countries responding to the questionnaire, making clear how valuable including this ‘networking’ question in the questionnaire was.

This report
In this report the answers provided by the respondents to the questionnaire are summarized and analysed. Most importantly, they will provide input to the other tracks of the Clean IT project.

[1] A number of instruments to reduce terrorist use of the Internet that were mentioned in the questionnaires and were new to the Clean IT meetings, have been discussed by participants during the conference in Berlin and included in a new version of the Clean IT draft document.

In the following chapter (chapter 2), we analyse whether and how the threat of terrorist and extremist use of the Internet is experienced in these European Union Member States. These results are compared to the scope of the Clean IT project.

In the third chapter the instruments to reduce terrorist use of the Internet that were mentioned by the respondents are compared to the ones that have been identified in the Clean IT meetings.

In the final chapter (4) the instruments that have not been identified in the Clean IT meetings at all, are discussed in more detail, to describe how these could contribute to reduce terrorist use of the Internet.

Recognition of the problem

This chapter focusses on the second question in the Clean IT questionnaire: 'which kinds of Internet use by terrorists are seen as a problem'? In the first part of this chapter, the answers that were provided by the countries and ISPA are summarized. In the sub conclusions, these summaries are added up to provide an overall impression of the characteristics of the terrorist use of the Internet in these Member States. In the sub conclusions, this is compared to the scope of the Clean IT project.

Summaries

Member State 1

The answer to this question received from Member State 1 was that in the recent past, especially right wing extremist websites were of great interest to its security services. Member State 1 security authorities were able to stop the servicing/regular updating of a right-wing extremist website in the year of 2011. In the course of the investigations, security authorities were specifically challenged with the circumstance that the server of the website was based abroad. Although an actual deactivation of the website was not possible, at least a change of the domain could be achieved by several initiatives. In addition, Member State 1 security services are aware of the growing threat of Islamist terrorists using the Internet as a tool (e.g. for spreading propaganda) but also as a weapon (e.g. possibility of cyber-attacks).

Member State 2

Authorities of Member State 2 answered that until now on the country has not faced any incidents of Internet use by terrorists or extremists. The use of the Internet by terrorists or extremists is recognized as a cause of concern to the authorities, however.

Member State 3

Terrorists and extremists are perceived generally as the most significant potential intruders of Cyber Security in the Member State 3. Security authorities at this time do not have any information about terroristic or extremist groups using Cyber Space as a tool for achieving their goals. In recent years, Member State 3 faced mostly right and left wing extremism. Extremist groups use the Internet mainly for dissemination of their propaganda. In the past, some extremist activities were detected, like the distribution of instructions on how to organize illegal actions, instructions on how to eliminate or evade police and intelligence measures during monitoring activities, manuals on how to make explosives and the spreading of information concerning combat training.

Member State 4

In Member State 4 groups like Anonymous are a matter of great concern when it comes to hacking and the disruption of government networks and attacks against critical infrastructure and national economy. The increasing use of Internet as a tool for radicalization is also a matter of concern.

Member State 5

Member State 5 authorities are concerned by the Internet being used for incitement to commit acts of terrorism, for the distribution of terrorist or extremist material, recruitment and radicalization, and for practical, operational advice, for example, on how to build an explosive. In addition, the Internet and its forums are used to promote extremist views and hate speech. Authorities expect the use of the Internet for both an operational and propaganda purposes (radicalization and recruitment) will continue to increase in the future. Internet has had a crucial role in globalizing the extremist ideology and in the future it will continue to have a significant impact for extremists, especially for the manufacturing and dissemination of propaganda material. Due to the technical and multinational structure of the Internet, it makes it hard for the national authorities to efficiently reduce the use of the Internet for terrorist purposes. The increasing technical capabilities of extremists, the advanced and in many cases free security technology (e.g. anonymity, encryption) and communication makes it easier to communicate, disseminate material and use the Internet as an operational tool.

<u>ISPA</u>

According to the ISPA, the ISPA hotline and national authorities mostly deal with Jihadist propaganda websites and forums, that are rarely hosted in this Member State. Here they find different kinds of online extremism and do-it-yourself bomb making techniques. The solution is usually provided through carefully monitoring of such platforms by specialised law enforcement agents and if necessary starting a notice-and-take-action procedure, even though in some cases it is difficult to identify and therefore notify the hosting provider, especially when the content is located in the United States. One specific ISP hosts quite some jihadist propaganda, but the hosted content in itself is not illegal under this Member States' law for it is mostly historic speeches of Al-Qaeda leaders and other influential figures of the Jihad community, videos which were previously broadcasted on international news channels. The Member State authorities do however keep a close lookout for comments posted in reaction to these videos and are constantly gathering intelligence on the individuals behind the publications.

<u>Member State 6</u>

In Member State 6, no use of Internet by terrorists has been established. Nevertheless, people that are active in an anti-authoritarian – environment do use the Internet for communication, dissemination of views, instructions for actions (by using social networking websites, Voice over Internet, chat boxes and e-mails) and for propaganda by means of videos that are uploaded to websites with to attract new followers. Moreover, leading members that are active in the anarchist environment influence other members by means of meetings and discussions, with the goal of having them adopt extreme positions and/or recruit other individuals. In addition, they use the same websites to publish to claim responsibility for their actions and for tracking down information concerning possible targets. For training, at times practical instructions appear on the Internet, regarding the manufacturing of explosive materials, improvised explosives – incendiary devices, Molotov bombs, etc. Moreover, instructions are given on the implementation of communication rules and on what someone should avoid doing in case he/she is arrested by the police.

<u>Member State 7</u>

Authorities answered that extremist activity is noticeable in social networks in Member State 7. Extremists spread their views (against ethnical, sexual minorities etc.) to attract more people to join them. In general, authorities assume that the dissemination of terrorist or extremist ideologies or information related with the preparation and conducting of terrorist acts, are the most threatening types of Internet use by terrorists and extremists. The biggest challenge for national authorities is to identify authors of terrorist or extremist material. In most cases the authors this material are related to terrorist or extremist circles and are out of reach for national authorities, as they are based abroad or are using foreign servers. Sometimes it takes too much time for successful investigation to get information from foreign countries, or it is even impossible to receive information because of national restrictions.

Member State 8

Authorities from Member State 8 state that the Internet is a haven for radicalization for all sorts of ideologies. Thus, the fact that individuals can become involved in self-radicalization without attracting the attention of authorities is regarded as problematic. The wide variety of available instructions and documentation on the Internet are subject to misuse by terrorists and extremists for their purposes and aims.

Member State 9

Member State 9 answered that to date its Police had no investigations involving the use of the Internet by terrorists or extremists. However, online recruitment and radicalization, along with the growing availability of extremist propaganda in online popular social networks and services, presents a major source of concern for the Intelligence Service. As extremist content becomes more and more available at these social networks and services, it becomes inevitable that, even without actively searching for this content, users are confronted with it. A user can also easily come into contact with active online radicalizers and recruiters. These people can, even if they are not formally associated with a terrorist organization, play a part in the radicalization, recruitment and eventually directing a susceptible user towards violent action in his home country or abroad. Online violent radicalization and recruitment, although often associated with lone actors, can and has been demonstrated to occur within groups. Simultaneously, these platforms also provide the tools and framework for discrete and secure communications between radicalizers/recruiters and their subjects. Furthermore, intelligence is aware of a trend of growing awareness of the need for security (“securitization”) among Internet jihadists, particularly in social networks and services. This awareness places great emphasis on the “clean-up” of extremists profiles, advising against posting or using extremist content in profile pictures, user’s galleries, etc. and instead opting for neutral content.

Member State 10

According to the authorities, Member State 10 has not been faced with systematic terrorist propaganda, conceived or disseminated on its national territory, or targeting the country itself. The use of the Internet by extremist/terrorist entities or for extremist/terrorist purposes is currently not a phenomena in Member State 10. The activities that are carried out by potential extremists and terrorists are not programmatic, systematic or specifically guided by foreign extremist/terrorist entities. Authorities note, however, there was a significant global growth in the degree and complexity of Internet and information networks that were used by terrorist entities in the last years. This is due to the ever-growing spectrum of activities dedicated to terrorist propaganda, intelligence gathering, target choice, resources (financial, logistical, and human) that can be used for extremist/terrorist purposes, enhancing self-radicalization, recruiting, encouraging and training of new followers, communications and coordinating terrorist activities. Taking advantage of the benefits provided by the Internet has become a common practice for terrorist entities internationally. Given the features of the Internet (easy to be accessed, large audience, the anonymous character of those who post and access various websites), it has become an ideal place for propaganda. These same features of the Internet also facilitate conversion and the risk of self-radicalization of lone wolves. The international developments in this field are a cause of concern to the competent authorities.

Member State 11

Member State 11 authorities indicated that the Internet is a good breeding ground for a variety of terrorist and extremist groups (racist, xenophobic, neo-Nazis, anti-gypsies), and is used to support terrorism and extremism. Through the Internet individuals and groups advertise their thoughts, ideas and messages to communicate, recruit new members and expand their network. It also gives them the ability to very effectively organize their activities, marches, demonstrations and meetings, on a global scale. There is a number of websites that promote these groups and on which their members place documents, photos, videos of their events, organize the exchange of objects and literature. This trend of publishing in electronic formats instead of using classical forms is becoming more apparent. There is a noticeable increase in the numbers of such websites, but also in the numbers of posts on forums with racist content. Most of these websites were published with a free web hosting service, either in Member State 11 or abroad. If such websites are hosted in Member State 11, the managers of these websites will be noticed to it. Problems occur when the pages with content that is illegal by law in Member State 11, are located on servers outside the country. Especially, if the content is on a server in the United States, where publication of similar material is not a criminal offence. In the United States some hosting facilities are dedicated solely to providing space for right-wing groups. In addition, numerous websites and Internet chat discussions where people openly support the idea of spreading racism, neo-Nazi and anti-Semitism, and websites promoting terrorism exist.

Sub conclusion

In all countries that responded the use of the Internet by terrorists or extremists is recognized as a cause of concern to authorities. More forms of extremism are mentioned than forms of terrorism. Right-wing ideological activities on the Internet are regarded as posing more of a threat than jihadi activities. The most common terrorist/extremist activities on the Internet seem to be propaganda, incitement, radicalization, training, learning, preparation and recruitment. Countries mentioned websites, web forums, social networks, Voice over Internet Protocol, chat and e-mail as parts of the Internet (services) that are used by terrorists and extremists.

Comparing this summary-of-summaries with the scope of the Clean IT project, that was developed in cooperation with Belgium, Germany, the Netherlands, Spain and the United Kingdom, the conclusion must be drawn that the project addresses the concerns of other

European Union Member States. There are no large differences in the views of the responding countries and the views of the partners of the project. One minor difference is that the project addresses more types of Internet services.[2]

[2] The Clean IT *Discussion paper* version 0.53 states that the role of role of access providers, browsers, chat boxes, certificates, domain registration, e-mail services, end-user control filters, exchange points, hosting, messaging systems, search engines, social networks, e-commerce sites, Voice-over Internet protocol and web forums have been considered during the projects meetings.

Instruments to reduce terrorism on the Internet

This chapter lists the instruments to reduce terrorist use of the Internet that were mentioned in the questionnaire, and compares these with the best practices that currently have been identified in the Clean IT meetings. From this comparison will be recommended which instruments should be included in the discussions and decision making of the Clean IT meetings and draft document with general principles, best practices and permanent dialogue.

Instruments mentioned as answers

A number of instruments that were mentioned as answers in the questionnaires that have been returned to the project team, unfortunately, fall outside the current scope of the discussions in the Clean IT meetings. (The scope of the project limits itself to terrorist incitement/propaganda, radicalization, recruitment and training/learning using the Internet). The answers that fall outside the scope are: monitoring government networks for attacks by extremist groups and establishing Computer Security Incident Response Teams or Computer Emergency Response Teams.

Fourteen practices were mentioned by one or more countries or the ISPA and are inside the scope of the project:

1. Having various legal basis that deal with or that can be applied against the misuse of the Internet by extremists or terrorists;

2. Enhancing cooperation between security services and the private sector, including networking, meetings and information exchange, with the aim of reducing terrorist use of the Internet together or be more effective when acting individually;

3. Security services can monitor the Internet and/or specific websites of an extremist or terrorist nature on a regular basis with the aim of identifying trends, new (kinds of) actors or tactics, and assist in developing government policy;

4. Government and law enforcement participation in other international projects or exchanges of best practices regarding the use of the Internet by terrorists or extremists, in order to develop technology, policy, tactics etc. by learning from each other and experts from private companies and research organizations;

5. Public organizations purchasing and applying technology for filtering or detecting access to illegal websites for civil servants at ministries and other public services;

6. Governments implementing a Cyber Security Strategy, Action Plan and National Centre For Cyber Security, that includes cyber terrorism and specifically mentioning the goal of reducing terrorism on the Internet;

7. Performing intelligence on the web by intelligence service that is directed at detecting, following and in ending terrorist actors' propaganda, radicalization and recruitment

attempts, as well as developing plans for physical or virtual attacks and disseminating the knowledge to prepare and execute attacks;

8. Police officers that ‘patrol’ visibly on social media (which will be discussed more extensively in the last chapter of this report);

9. Police reporting button (“blue button”) added by Internet companies to their web pages (which will be discussed more extensively in the last chapter of this report);

10. Creating a specific unit or division (cyber police), which is responsible for criminal investigations and background research in the field of terrorism, including specifically propaganda, radicalization, recruitment and learning processes of terrorists and extremists through the Internet. During the pre-trial investigation the necessary control measures on the content and persons involved can be sanctioned by a judge;

11. Awareness, counselling and communication programmes by government, civil and not for profit organizations, with the aim of improving both quantity and quality of reporting and other activities by the general public and professionals that would help in reducing terrorist and extremist use of the Internet;

12. Establishing hotlines by law enforcement (together with Internet companies) to allow the public to report terrorist content and have law enforcement (together with Internet companies) take action against terrorist or extremist propaganda, radicalization, recruitment and ‘training’ through the Internet;

13. Establishing helplines by law enforcement, not for profit organizations, Internet industry or governments, providing Internet users and (less informed) professionals a portal to find information on a web site or to ask questions via e-mail or by phone, on the phenomenon and options to report cases of (possible) terrorist use of the Internet;

14. Academic and private research organisations, on request of governments, law enforcement, not for profit organizations or Internet industry, to perform scientific research, on the threat posed by cyber terrorism and to develop new tactics or technologies to reduce terrorist use of the Internet, including propaganda, radicalization, recruitment and learning.

Comparison with Clean IT meetings

Comparing this list of fourteen instruments that were mentioned in the questionnaires with the best practices that are currently identified in the Clean IT meetings,[3] three conclusions can be drawn.

[3] The Clean IT *Discussion paper* version 0.53 lists: legislation, government policies, end-user controlled filters, flagging/report button systems, service/business conditions and unacceptable use policies, notice and take down, investigations, awareness/education/information, points of contact, advisory foundation, real identity policies, share abuse information, and referral units.

First, four instruments that were mentioned in the questionnaires have been identified in the Clean IT meetings as well. The fact that these practices are suggested by other European Union Member States is not insignificant, however, because this indicates that the best practices that are developed during the Clean IT meetings will probably find support in other European Union Member States. This is the case for the following instruments:

- Legal basis (instrument number 1);
- Cooperation between security services and the private sector (instrument number 2);
- Awareness and communication programmes (instrument number 11);
- Scientific research and developing new technologies (instrument number 14).

Second, half of the instruments that were mentioned in the questionnaires do not have the same level of abstraction as the best practices identified during the Clean IT meetings. These instruments could easily be added to the Clean IT draft document or discussion paper with more detailed recommendations. This applies to:

- Monitoring the Internet, participation in other international projects, filtering for civil servants, Cyber Security Strategy, Web intelligence (instrument numbers 3-7); and creating a specific cyber police unit (instrument number 10) could be included in the Clean IT best practice of ‘government policies’;
- Establishing hotlines with Internet companies (instrument number 12) could be included in ‘referral units’.
- Establishing helplines (13) could be included in ‘awareness/information/education’.

Third, some of the instruments that were mentioned in the questionnaires have not been identified during the Clean IT meetings at all (although the project team has come across them in doing research and discussing with various organizations in between meetings). These could be included into discussions and decision making on the Clean IT draft document, too. It might take more effort to explore and develop their background, precise workings and the benefits they could bring, as well as to decide whether these instruments should be promoted as best practices and to develop more detailed recommendations on implementing them. This is the case for:

- Police officers that ‘patrol’ on social media (instrument number 8);
- Police “blue button” added by Internet companies (instrument number 9).

Sub conclusions

From the analysis above follows that more than half of the instruments that were mentioned in the questionnaire have not been identified during the Clean IT meetings. It would be valuable to include these in the draft document of Clean IT as well as discussion and decision making on finalising this text. Including the majority of these in the draft document is possible without major effort. Only two best practices, which are new to the Clean IT meetings, will require more effort. These are the subject of the final chapter of this report.

Two additional best practices

In this chapter two specific instruments mentioned in the questionnaires will be discussed. As these are new to the Clean IT project and could be (very) valuable to add to the best practices that have been identified before, the two instruments have been explored with police experts and are described below in more detail.

Police ‘patrol’ on the social media.
Problem: Far less than in the physical world, Internet users realize their behaviour must be within laws and social norms. On the Internet users are hardly ever confronted with or reminded of the presence of law enforcement agencies (LEAs), signalling abusive behaviour might have consequences. On social media platforms, where there is lots of social interaction, currently terrorists and extremists too feel secure and unobserved, to unrestrictedly spread their propaganda and recruit.
Goal: LEAs will be visible and active on most relevant social media platforms to deter and react to terrorist and extremist activity.
Benefits: Police patrolling on social media will limit terrorist incitement and recruitment.
Detailed recommendations:

1. Police patrolling must be used to find and connect to persons in danger to get radicalized.
2. To reduce terrorist use of the Internet police officers should (also) be active on those social media platforms known for terrorist or radicalizing activity.
3. Police patrolling on social media 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. 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. 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. Police patrolling of social media 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.

Police reporting button.

Problem: While social media platforms can offer 'flagging' opportunities, hosted websites often lack such a mechanism. There is not one (national) and user friendly reporting mechanism available to all Internet users, irrespective of which part of the Internet they are using at the moment they notice terrorist use of the Internet.

Goal: National LEA will develop and offer Internet companies a reporting button to be put on their platforms, allowing any user to report terrorist use of the Internet.

Benefits: This best practice will increase the number of notices on (possible) terrorist use of the Internet, resulting in more terrorist content on hosted websites that is dealt with.

Detailed recommendations:

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.