Thank you very much,

The internet is a wonderful medium that is beneficial for our society, but infortunately it is also used for illegal purposes. The internet is used as a weapon for example. A weapon to attack critical infrastructures, to carry out criminal actions, or for espionage. This is the core-field of cybersecurity. The internet can also be a target itself, however I think it is not easy to hit the internet beacuse it is such a strong and redundant medium. There is a third way how the internet can be used for illegal purposes, and that is as a resource. At this moment, when we speak about the terrorist use of the internet, which is more precise than the term cyber-terrorism, this is the most common way that terrorist groups like Al Qaida use the internet.

As you might know, the terrorist threat level in Belgium has just been raised from level 2 to level 3 after last weeks stabbing on two police officers on the Brussels metro. Now this week, the french extremist that was arrested, Brahim Bahrir, explained in a Belgium newspaper why he did it.

I quote:
My personal live was a mess, I was unemployed and divorced. I started a spiritual search and came accross extremist webistes like Shariah4-Belgium. I became addicted to this site and it confused me. I started thinking like a zombie, and the range of extremist thoughts fascinated me. I could not think clear anymore. Compare it with the followers of Adolf Hitler, it was like they were all hypnotised."
Unquote

Now I tell you this, because I think that probably no one in this audience is familiar with this webiste Sharia4 Belgium. And this is not the only website that contains extremist content and a call for violance. Many countries in Europe have these kind of websites, which are at least partly illegal. A characteristic of these websites, is that the owners are not willing to cooperate with authorities. I see, when analysing the terrorist use of the internet, three layers on the internet. This one is the middle one, I will also describe the two other layers.

The first layer, that is the one we all know. It is the easy accessible part of internet, where we van find the social media we all use. I asked a group of experts two weeks ago how many friends Al Qaida has on Facebook. Off course they did not know because Al Qaida doesn t have a facebook page. But if you look at the Facebook activities from the

French terrorist that was killed in Toulouse a few weeks ago, it is amazing to see how many support he received for his acts in just a few days.

So, the first layer is the easy accessible one where we find the social media, in the second one we find the ideological websites, partly illegal and more difficult to find. The third layer is very difficult to find and even more difficult to acces. This is the online inner circle of terrorist groups that meet in these dark place on the internet, in hidden chatrooms and encrypted peer to peer channels.

I described these three layers to show how terrorists make use of the internet. Considering these three layers, you will find two processes that take place. The first is bottom-up, the proces of propaganda that is prepared in the deepest part of the internet, in the hidden inner circle, is explained on the ideological websites in the second layer, and is sometimes dissiminated and spread to the public with our well known social media. The second process goes top-down. This is the recruitment and radicalization process. With the use of social media terrorist groups look for new recruits, those who are interested are directed to the ideological sites and if they reach the proper mindset they are directed to the hidden discussion rooms where violance is glorified and deadly attacks are planned.

Those two processes, the propaganda going up, and the radicalization and recruitment going down, this is the terrorist use of the internet that we discuss in the Clean IT project. And let me be very clear that it is not the use of the medium and the existance of those three layers that I described that is illegal, it is the purpose for which it is used. And that is why it is so difficult for Law Enforcement to take action against it. It is often difficult to evaluate if certain specific content is illegal or not, because it often depends on the context where it is presented. Does it contribute to one of the two processes I described? At a certain moment the online activities cross the threshold of illegality, and it is not easy to point out where this exactly begins.

And this, this is the main reason the Clean IT project started. We think that this problem is too compex to be solved only by governments. It is the industry that owns the internet, and has the knowledge about how it works. And as a government, we need private interest groups to remind us about privacy issues and the importance of internet freedom. In the Clean IT project these three parties (governments, industry and internet freedom) meet together to find practicals solution to reduce the impact of the terrorist use of the internet. Examples and possible solutions we discuss are flagging mechanism, referral units, exchange of information on known illegal material, notice-and-takedown procedures, and so on. We created a kind of trusted environment to discuss the technical and legal consequences for these solutions in a multi stakeholder environment. And I consciously use the term ‘multi stakeholder’ because this is what I appreciate so much from the EuroDIG conference. So to be honest, I copied that idea from you into our project.

If you would like to see the progress we made until now, please visit the website cleanITproject.eu.

Now I will make a final statement. And this is not restricted to the terrorist use of the internet, because I think the public-private approach we use in this project could be adopted to other issues. The Clean IT project is now shaping its end result, which will consist of a code of conduct between the industry and governments, and attached is a list of best practices. The challenge we face, is that we do not have a formal body or committee to accept our end results. No one has really a coordinating responsible on how to fight the terrorist use of the internet. Who can make dicisions when it concerns the use of the internet? In last years EuroDIG in Belgrade I heard somebody asking which law applies on the internet. I am sure Marco will like this. For the younger generation it is very simple what is allowed and what is not on the internet. The answer was: If google allows it, you can do it. But from a legal perspective, this is a fascinating discussion.

My statement is that we need such a formal body, especially if we would like to take concrete measures in order to keep the internet a secure place. The point is, I do not know who should be this body and I am not sure about how it should work. But I suppose that is the reason we have a discussion on Internet Governance.

Thank you very much

National Coordinator for
Counterterrorism

Clean IT

Fighting the illegal use of internet with public-private partnerships from the perspective of counter-terrorism

PROJECT OUTLINE

June 17, 2010

Contact: [redacted]

1. Context and project justification

The internet plays a central role and is of great strategic importance for Islamist extremist networks. Islamist extremists know that propaganda is a critical tool for generating funding, recruits and support for their cause within Muslim communities. Historically they have used a variety of media channels, such as television, radio and publishing, in order to communicate their views. During the past decade of huge global growth in the internet, Islamist extremists have made increasing use of this medium. There is now a significant and increasing number of websites and forums, hosted across the world, that promote Islamist extremism.

This project builds on the results of 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 via the internet and to develop ways and means to preventively address Islamist extremist content in the internet. This project identified several best practices in Germany, the United Kingdom, the Czech Republic and the Netherlands.

Although some potential interesting national best practices were identified, it is not always clear how to apply them effectively on the Internet because:

- Content on the internet is difficult to localise, and is duplicated easily or automatically;
- Information on the internet criss-crosses geographical borders and therefore is not always submitted to a single legal system;
- 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". It does not regulate in concrete steps how to act in case of illegal use of the internet and does not define in wich way public and private parties can shoulder their common responsibilty to keep the Internet clean from criminal and terroristic activities;

The preceding project concluded that the internet and its fast and anonymous means can be used as contributing to individual radicalisation processes. There are concerns about the possibilities for illegal use of the internet for terrostic purposes and the misuse of legal / neutral websites. These concerns probably also apply on other forms of cybercrime or abuse, like fraud, illegal trade and sexual exploitation children. The primary focus of this project however, is combatting the misuse of internet for terroristic purposes. The project partners have a strong will to solve these problems, but they realise that current initiatives are bound to national systems and need international coordination and stimulation.

To deal with these problems in the virtual world, traditional legal approaches are not always effective. The use of internet makes it possible that unlawful activities are undertaken in one part of the world, but affect multiple places at the other side of the world, within a split second. Legal counter-actions are not always effective because they often take some time, and are limited to geographical borders.

In addition to regulatory approaches, public-private partnerships can cause a breakthrough in deadlocked talks between government and industry.Also, the internet is in most countries predominantly privately owned, and the internet knowledge is 100% privately owned. For these reasons, the solutions to these problems can be found in direct cooperation between member-states and the Internet business.

2. Overall objectives

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. Responses must be brought by a number of partners and include a wide range of approaches

To prevent the misuse of the Internet for terroristic purposes, a non-legislative approach should be developed to address most categories of illegal use of the Internet. This approach will only work if it is based on a broad public support by member states and Internet Sector.

This project should emphasise that only by working together between public and private partners, the fight against illegal use of the Internet can be successfull. This means that all participants are equal, and open and direct communication during the project is imperative. Therefore, building trust is a key factor. Building trust cannot be realised with a 'big bang strategy'. The idea is to start with a relatively small group of pioneers, and seek to broaden public and private support during the project.

3. Specific objectives of the project

For the application of preventive measures, distinction needs to be made between illegal use or content, and use or content that is harmful or potentially disturbing but not necessary illegal. For the illegal use of the internet public-private partnerships can provide quicker and faster solutions to achieve law-compliance. For potentially disturbing or harmful use of the internet, public-private partnerships can clarify conflicts of interest and create a transparant platform for democratic debate. This project will focus on the illegal use of the Internet, and will not lead to any regulation or obligation concerning harmful or disturbing content that is not illegal.

The solution to these problems lie in a kind 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 Internet. These principles should fill the gap between Member States (national) regulation and private initiatives / best practices and should be adopted by all partners.
- **Best practices** that can be implemented voluntarily in order to achieve more law-compliance on the Internet
- A **platform for dialogue** for public and private partners to strengthen the fight against illegal use of the Internet.

This project will not carry out the concrete implementation of best practices in member states. A platform for dialogue has already started under the auspicien of the European Commission (DGJLS). All activities from this project will fit smoothly into this promising initiative.

The primary **stakeholders** of the proposed projects are private partners that own the Internet infrastructure, or deliver important Internet services. Also included are interest groups or associations from religious or social target groups that can act as feedback group. The private partners will avoid excessive regulation and their responsibilities will be clarified.

The **secondary stakeholders** are the Member States in European Union (law enforcement agencies included), and involved third countries. They will establish clear procedures to cooperate with private parties that help them to achieve a higher level of law-compliance on the Internet.

The **third stakeholdres** are the end-users of the Internet. Although they are not involved in this project, they will benefit from a safer Internet.

4. Expected results

Short term

The most important deliverable for this project is a set of general principles that tells us what the responsibilities are, and which concrete steps public and private partners should take in order to fight the illegal use of the internet. These principles will at least be applicable for counter-terrorism measures on the internet. The principles will be adopted by public and private "initiators" and have the form of a declaration or code of conduct.

During the project also, the iniators of these general principles will start a permanent platform for dialogue. This platform will also make possible that futur changes (if necessary) to the general principles can be managed and adopted.

Because the general principles are co-produced by internet industry and governmental organisations, this project is likely to boost the public-private cooperation to achieve more law-compliance on the internet.

Medium and long term impact

The public-private platform will be self-supporting and growing. More companies from the internet industry and more member states or law enforcement agencies will join the coalition. This can only be achieved as result of a more or less autonomous process. In that process the cooperation between public and private partners will intensify. The aim of this process at the long term is to cover all EU member states and may be also third countries. A world wide coverage for the principles would be the ultimate goal, but outreaches the project ambitions.

5. Main activities

There are three parallel tracks in this project. The first track is about the draw up of the general principles. Therefore consensus is needed from all project partners. This will be achieved through a series of workshops, followed by an editing and fine-tuning process. The second track is about the identified best practices from the preceding project. How do they fit into the general principles, and how can these national best practices be implemented in other countries? The result of this track will be an implementation guideline, that can be attached to the general principles. The goal of the third track is to make an inventory of new best practices from member states that did not participate in the preceding project. These new best practices will be added to the second track.

6. Specific activities, timeline

To achieve good partnership between internet industry and government, it is imperative that mutual understanding is created, and a process of building trust is followed. This means that the project management will have good communication skills at its disposal and will organise various moments for interaction with experts.

Track 1
To draw up the general principles experts from government (law enforcement and policy-makers) and industry (internet services, and infrastructure) are brought together in workshops. The next points of discussion will be adressed:

- What is the scope of the general principles, which legal or technical situations should be included or excluded?
- What are the best choices or solutions to tackle the problems of the illegal use of internet?
- How will we lay down these solutions in general principles?

This will lead to a first draft of the general principles, that will be presented and discussed in a conference with a broader public.

Next, there will be a written commentary round and the possibility for bilateral meetings to work out specific solutions. This will lead to te second draft of the general principles, to be discussed in a second conference. At least, after a process of fine-tuning, the final version of the general principles will be presented, if desired, in a press conference.

The work in this track should be consistent with other activities in this field, such as the implementation of the cybercrime convention from the Council of Europe and guidelines that are developed for law enforcement agencies and internet industry.

Track 2

The main objective of the second track is to explore how national best practices (as identified in the preceding project) can be implemented at an European level. The following points of discussion will be adressed:

- Which best practices are suitable for other countries?
- How can they be implemented, do they need to be tailored to specific countries?
- Which partners can help us to implement the best practices in other countries?

These issues will also be adressed in workshops, that take place parallel or directly after the workshops from track 1.

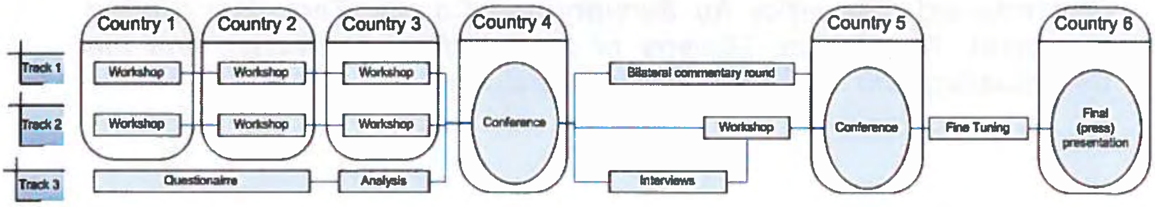
The results of the workshops are put together in a report that will be presented in the first conference. Next, only one workshop is needed to create an implementation guideline and to draw-up a “best practices partnership agreement”. A draft of this agreement is presented in a conference. If needed, the agreement can be finalised in the same fine-tuning process from track 1. At the end, it will be presented in combination with the general principles.

Track 3

As in the preceding project only four countries participated, it is to be expected that more best practices to fight terrorism-related offences on the internet can be found in other countries. Therefore a questionnaire will be developed and dispersed to member states and internet industry. The results will be analysed and also presented in the first conference. If possible, information from other projects on non-legislative initiatives in this field will be used.

If interesting new best practices are identified, interviews will be held to describe them more in detail, and to raise the same questions that were addressed in track 2. After this interview-round, the results will be brought into the workshop from track 2.

The workshops and conferences from the three tracks are outlined in the next project-chart. The estimated timeline is approximately 16 months.



The first workshop will take place approximately one month after signing the grant agreement between project partners and European Commisison.

Strategic role of the conferences

The two major conferences play an important role in the whole process of bringing public and private parties together. The workshop-results will be presented in conferences. This gives us the opportunity to get feedback from a broader audience, and to create a social/public support for the solutions that are found. Also, the conferences are a way to expand the coalition of public and private partners that want to reach agreement on the topics identified. New partners can join and participate (gradual extension). The initial coalition consists of the partners that attended the november 27th 2009 and april 23th 2010 meetings in Brussels "Public-private dialogue to fight online illegal activities".

7. Project Organisation

The Netherlands is the coordinator for this project and is responsible for the overall projectmanagement. Germany, the United Kingdom and Belgium are partners in this project. A small project team is based in The Hague, at the office of the National Coordinator for Counter Terrorism in the Netherlands.

The project partners will form a coordination group that will meet several times during the project. The coordination group will keep a close watch on the project strategy and will monitor the (interim) projectresults.

The role from the coordinator and project partners is limited, except for the managerial aspects. The input will mainly come from experts from private and public organisations who will bring in their expertise and views into this project. Representatives from Law Enforcement Agencies, Internet Industry, and intrest groups including privacy watchers will discuss technical and juridical issues in a series of 4 workshops and 2 conferences. The task form the project team is to facilitate this process. In this way, the general principles will be the result of a bottum-up process with the private sector in the lead.

A project proposal is submitted on 17/06/2010 to Directorate General Justice, Freedom and Security (unit F4), under the targetted call for proposals "illegal use of internet" (action grants 2010).

Signed by The National Coordinator for Counter Terrorism (Netherlands), The office for Security and Counter-Terrorism (United Kingdom), The Federal Ministry of the Interiour (Germany), and the Coordination Unit for Threat Analysis (Belgium).

WELCOME

Final Clean IT symposium

Brussels, 30-01-2013

The Clean IT Project

Reducing the impact of the terrorist use of internet

13:30 Opening remarks Cyrus Farivar

13: 40 Mr. Theo Bot (deputy National Coordinator for Counter Terrorism and Security in the Netherlands)

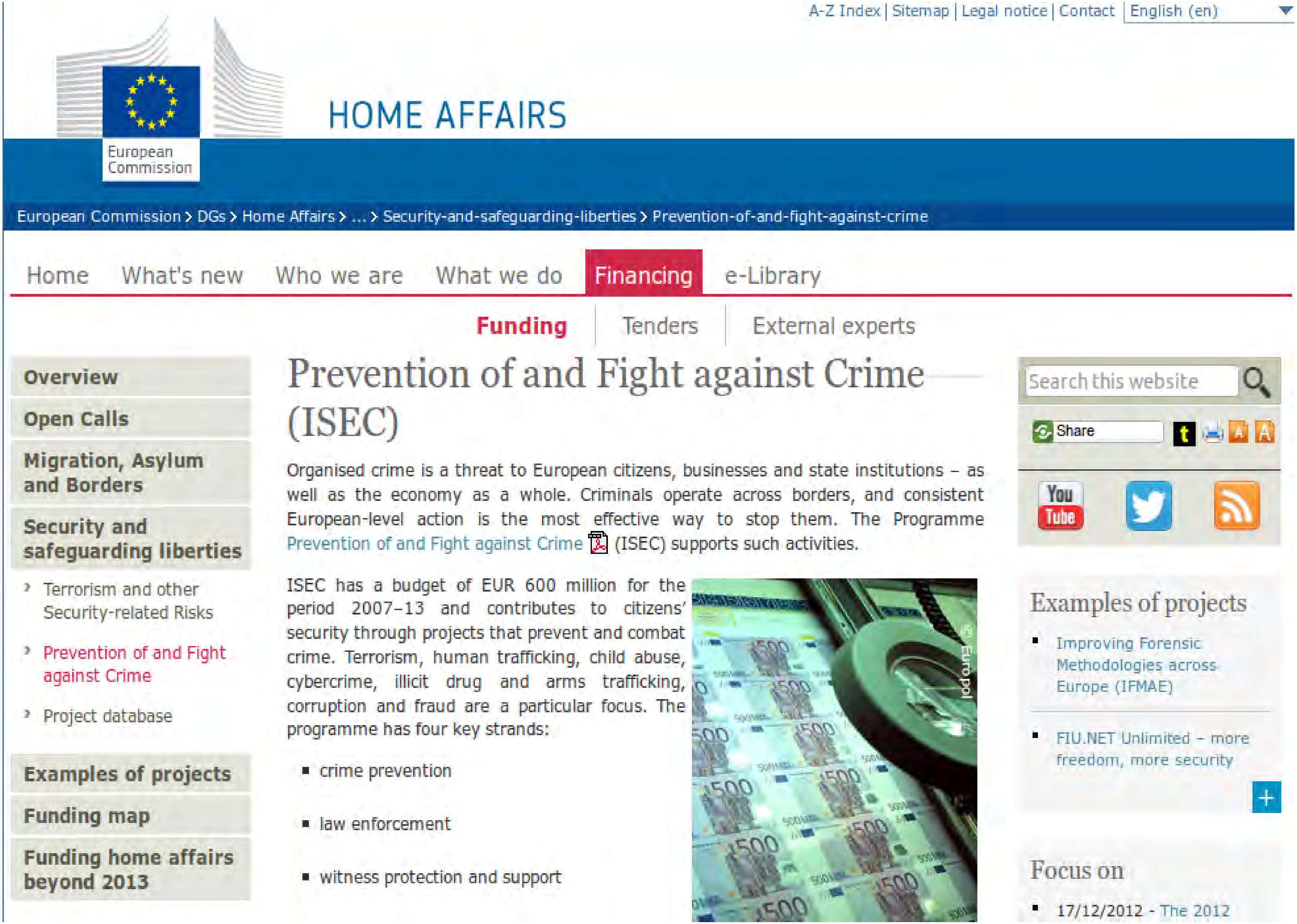
13:50 Mr. Gilles de Kerchove (European Counter Terrorisme Coordinator)

14:00 Mr. But Klaasen (Projectmanager Clean IT)

14:20 break)

14:30 Panel introduction & discussion

16:00 Reception



A-Z Index | Sitemap | Legal notice | Contact | English (en)

European Commission

HOME AFFAIRS

European Commission > DGs > Home Affairs > ... > Security-and-safeguarding-liberties > Prevention-of-and-fight-against-crime

Home
What's new
Who we are
What we do
Financing
e-Library
Funding
Tenders
External experts
Overview
Open Calls
Migration, Asylum and Borders
Security and safeguarding liberties
Terrorism and other Security-related Risks
Prevention of and Fight against Crime
Project database
Examples of projects
Funding map
Funding home affairs beyond 2013
Search this website
Share

Prevention of and Fight against Crime (ISEC)

Organised crime is a threat to European citizens, businesses and state institutions – as well as the economy as a whole. Criminals operate across borders, and consistent European-level action is the most effective way to stop them. The Programme Prevention of and Fight against Crime (ISEC) supports such activities.

ISEC has a budget of EUR 600 million for the period 2007–13 and contributes to citizens' security through projects that prevent and combat crime. Terrorism, human trafficking, child abuse, cybercrime, illicit drug and arms trafficking, corruption and fraud are a particular focus. The programme has four key strands:

- crime prevention
- law enforcement
- witness protection and support

© Europol

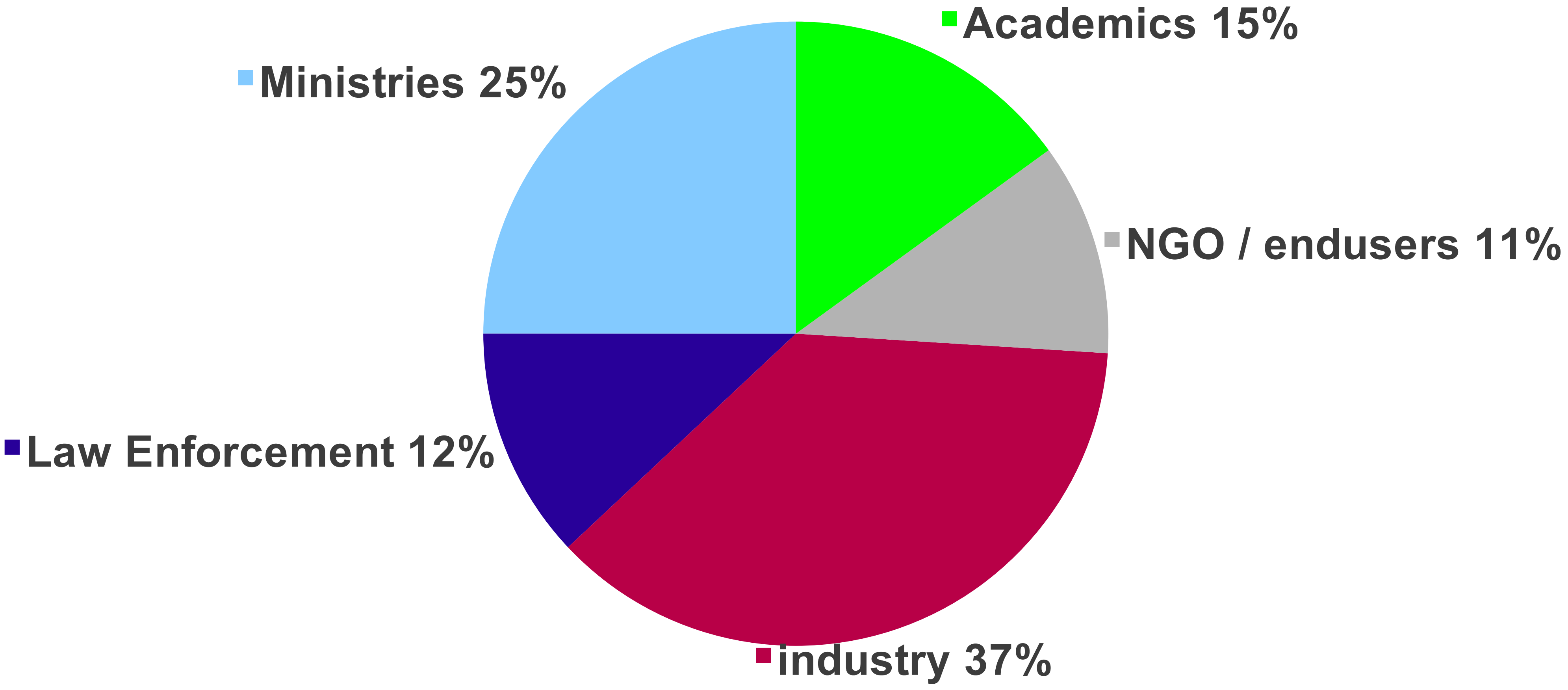
Examples of projects

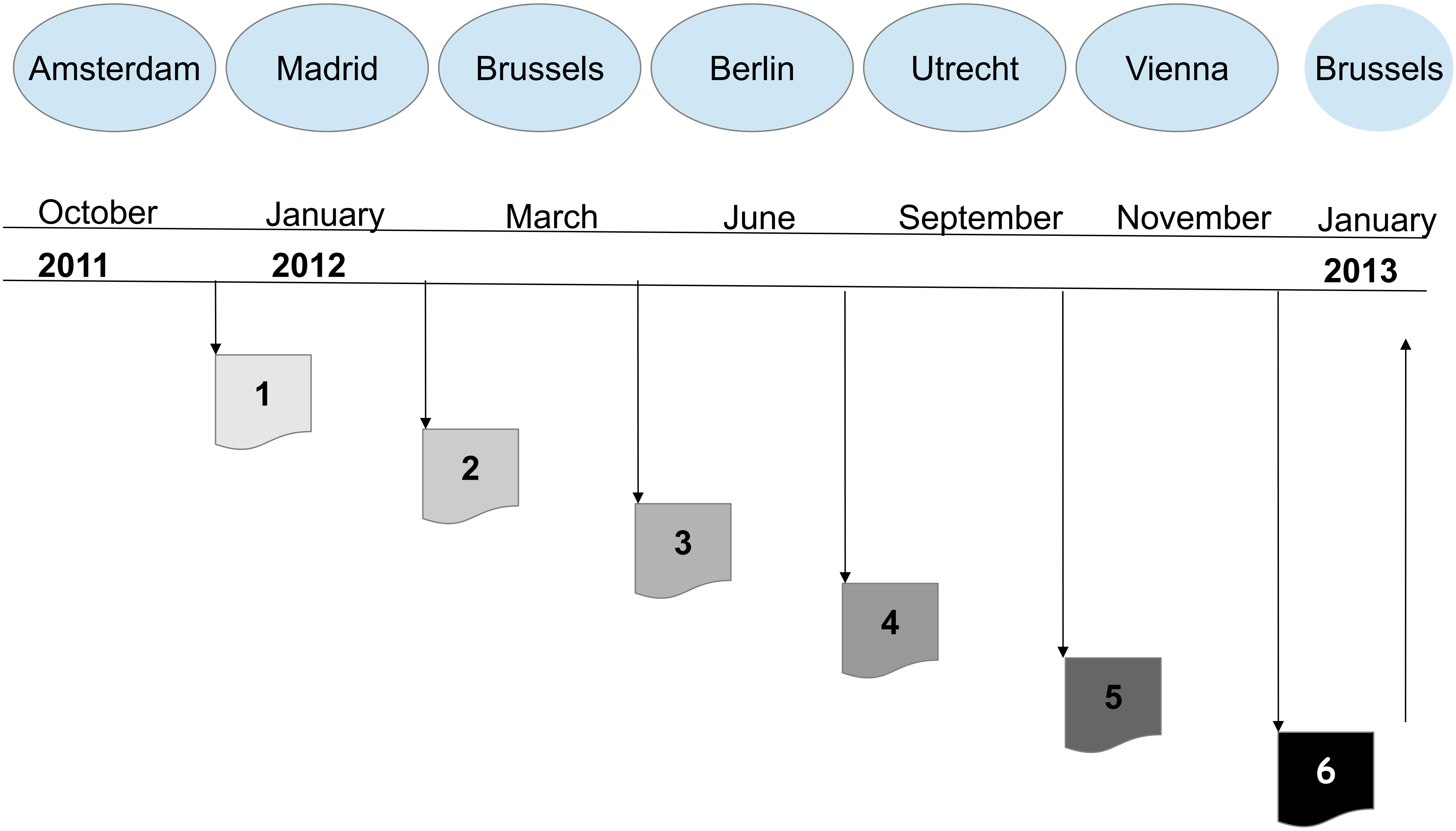
- Improving Forensic Methodologies across Europe (IFMAE)
- FIU.NET Unlimited – more freedom, more security

Focus on

- 17/12/2012 - The 2012

110 different participants from 15 countries in 6 meetings



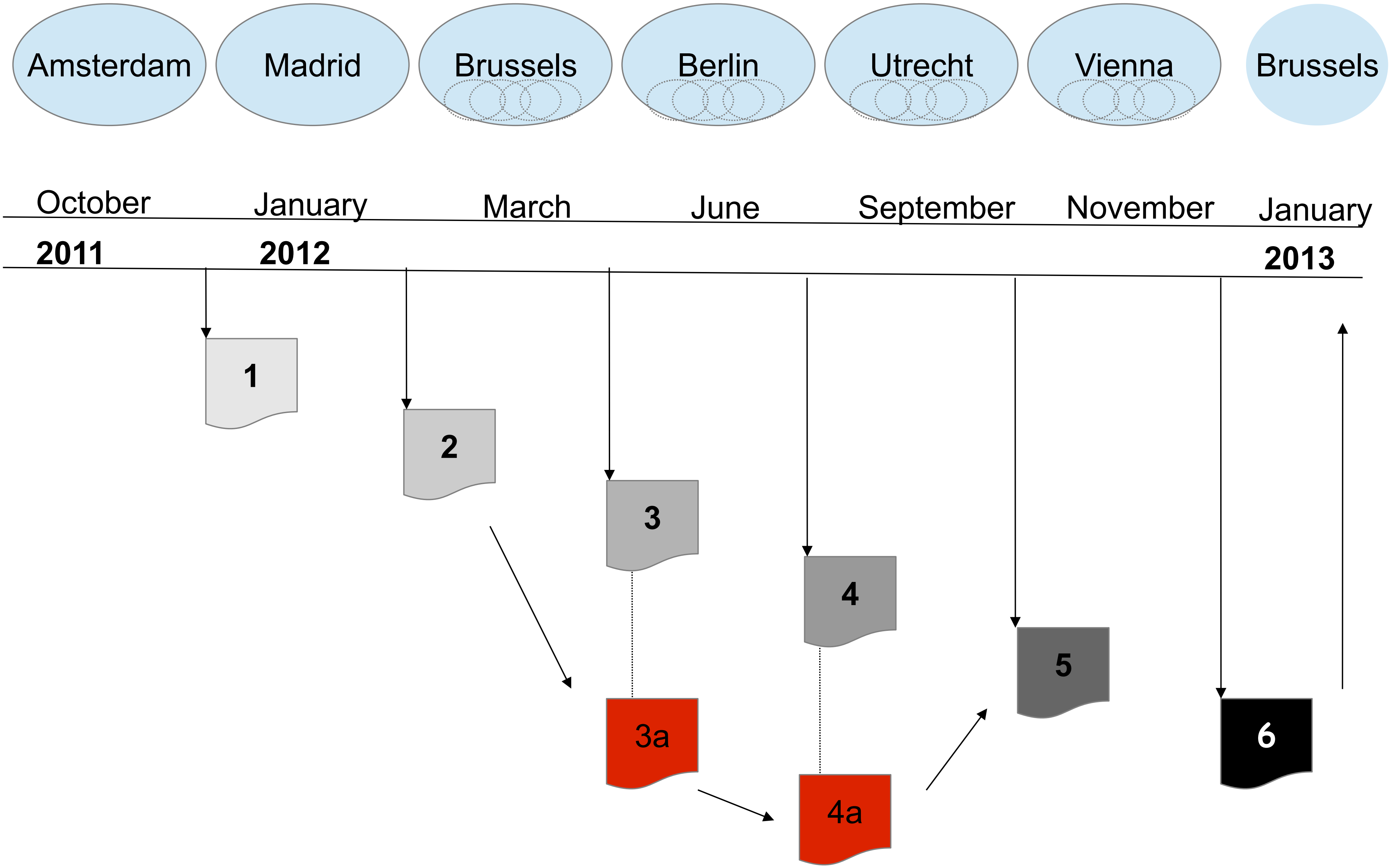


Amsterdam Madrid Brussels Berlin Utrecht Vienna Brussels

October January March June September November January

2011 2012 2013

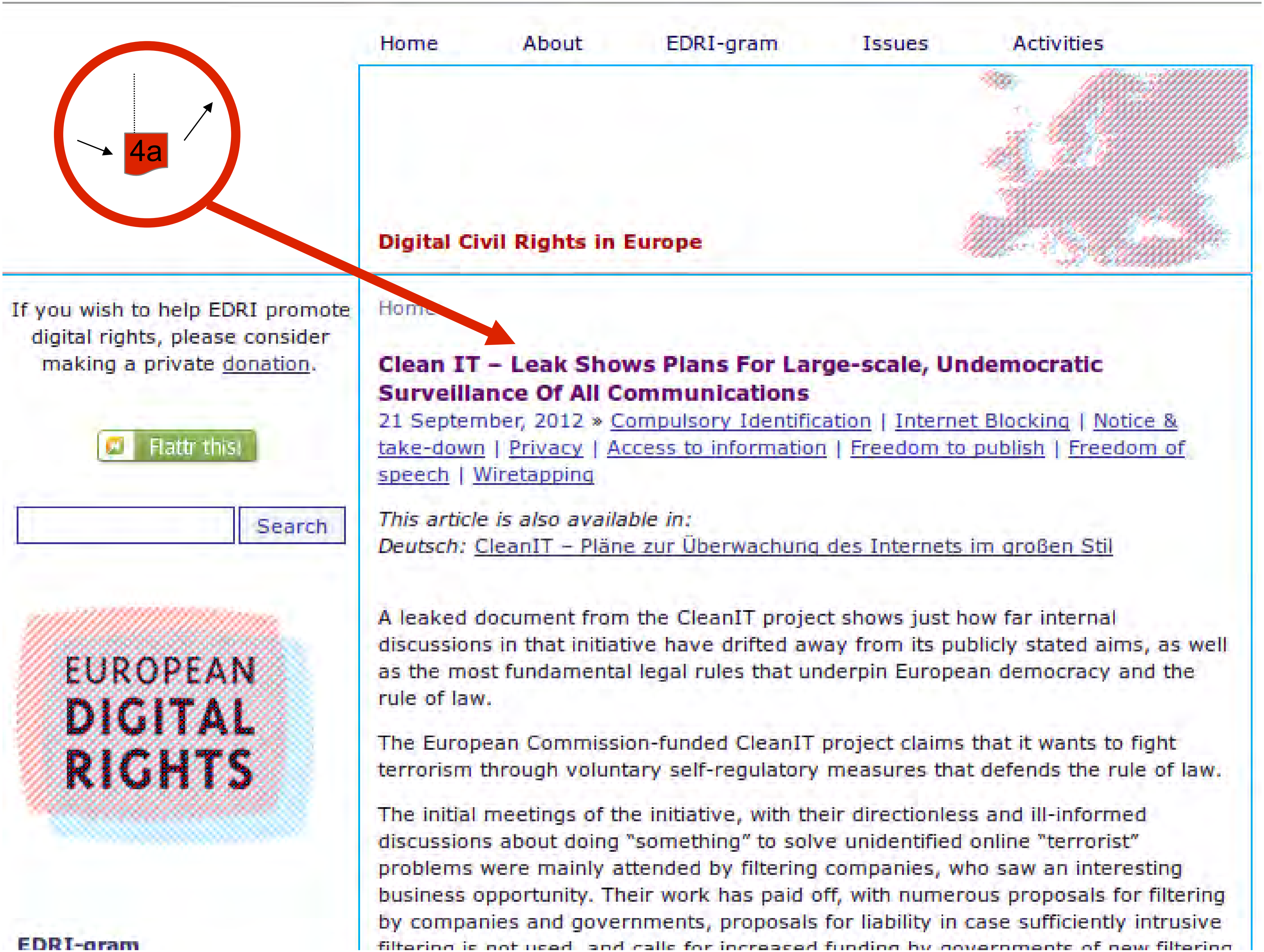
1 2 3 4 5 6



Amsterdam
Madrid
Brussels
Berlin
Utrecht
Vienna
Brussels

October
2011
January
2012
March
June
September
November
January
2013

1
2
3
3a
4
4a
5
6



Digital Civil Rights in Europe

If you wish to help EDRI promote digital rights, please consider making a private donation.

EDRI-gram

Home

Clean IT – Leak Shows Plans For Large-scale, Undemocratic Surveillance Of All Communications

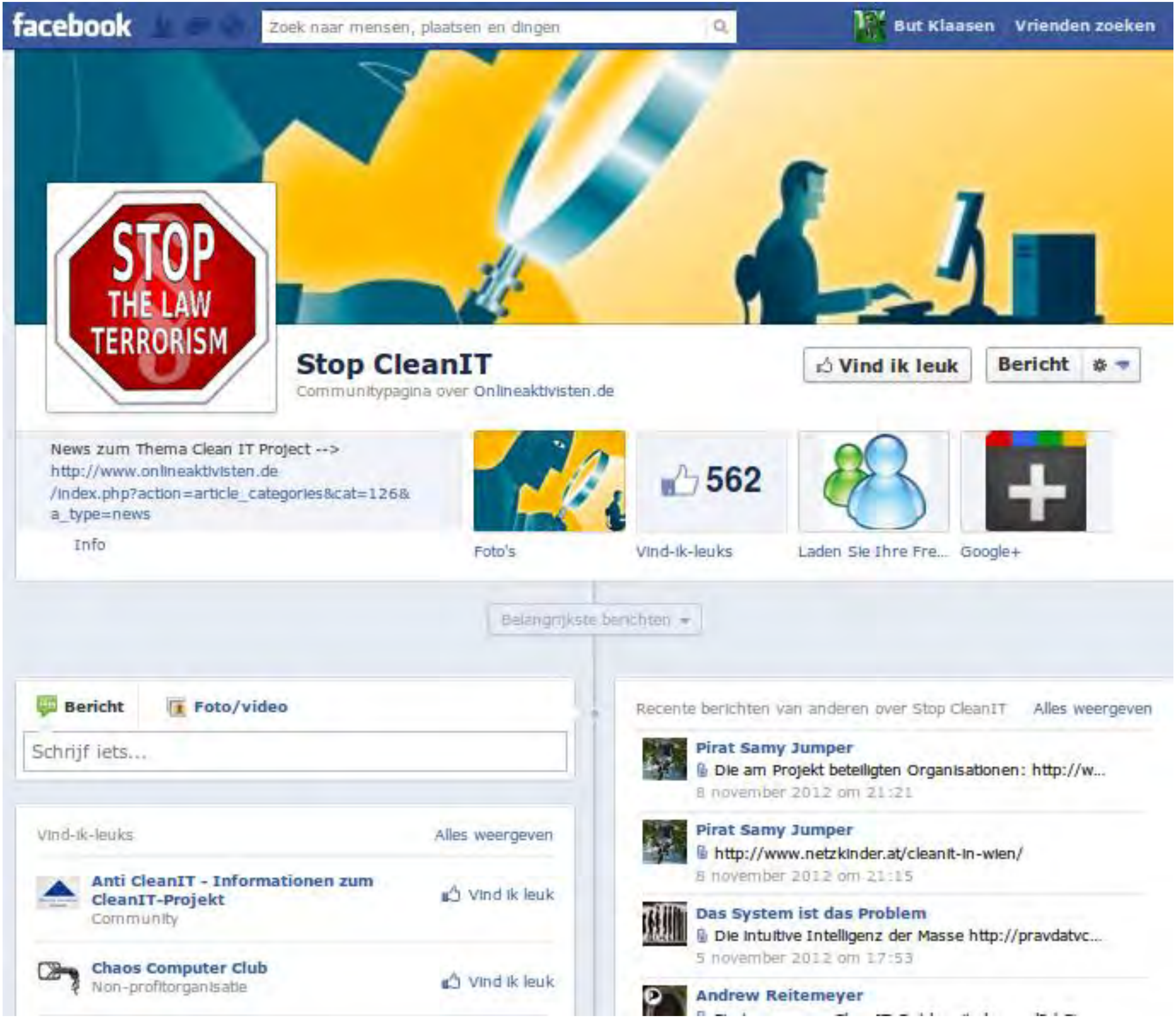
21 September, 2012 » Compulsory Identification | Internet Blocking | Notice & take-down | Privacy | Access to information | Freedom to publish | Freedom of speech | Wiretapping

This article is also available in:
Deutsch: CleanIT – Pläne zur Überwachung des Internets im großen Stil

A leaked document from the CleanIT project shows just how far internal discussions in that initiative have drifted away from its publicly stated aims, as well as the most fundamental legal rules that underpin European democracy and the rule of law.

The European Commission-funded CleanIT project claims that it wants to fight terrorism through voluntary self-regulatory measures that defends the rule of law.

The initial meetings of the initiative, with their directionless and ill-informed discussions about doing "something" to solve unidentified online "terrorist" problems were mainly attended by filtering companies, who saw an interesting business opportunity. Their work has paid off, with numerous proposals for filtering by companies and governments, proposals for liability in case sufficiently intrusive filtering is not used, and calls for increased funding by governments of new filtering



Stop CleanIT

Communitypagina over Onlineaktivisten.de

News zum Thema Clean IT Project -->
http://www.onlineaktivisten.de/index.php?action=article_categories&cat=126&a_type=news

Info

Vind-ik-leuks | Alles weergeven

Anti CleanIT - Informationen zum CleanIT-Projekt
Community
Vind ik leuk

Chaos Computer Club
Non-profitorganisatie
Vind ik leuk

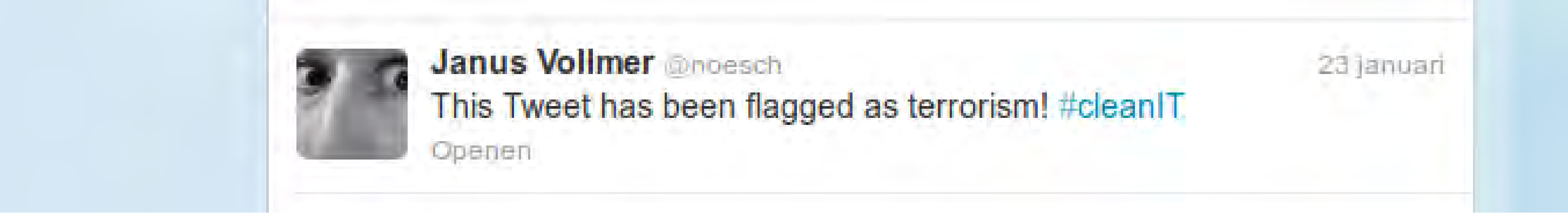
Recente berichten van anderen over Stop CleanIT | Alles weergeven

Pirat Samy Jumper
Die am Projekt beteiligten Organisationen: http://w...
8 november 2012 om 21:21

Pirat Samy Jumper
http://www.netzkinder.at/cleanit-in-wien/
8 november 2012 om 21:15

Das System ist das Problem
Die intuitive Intelligenz der Masse http://pravdatvc...
5 november 2012 om 17:53

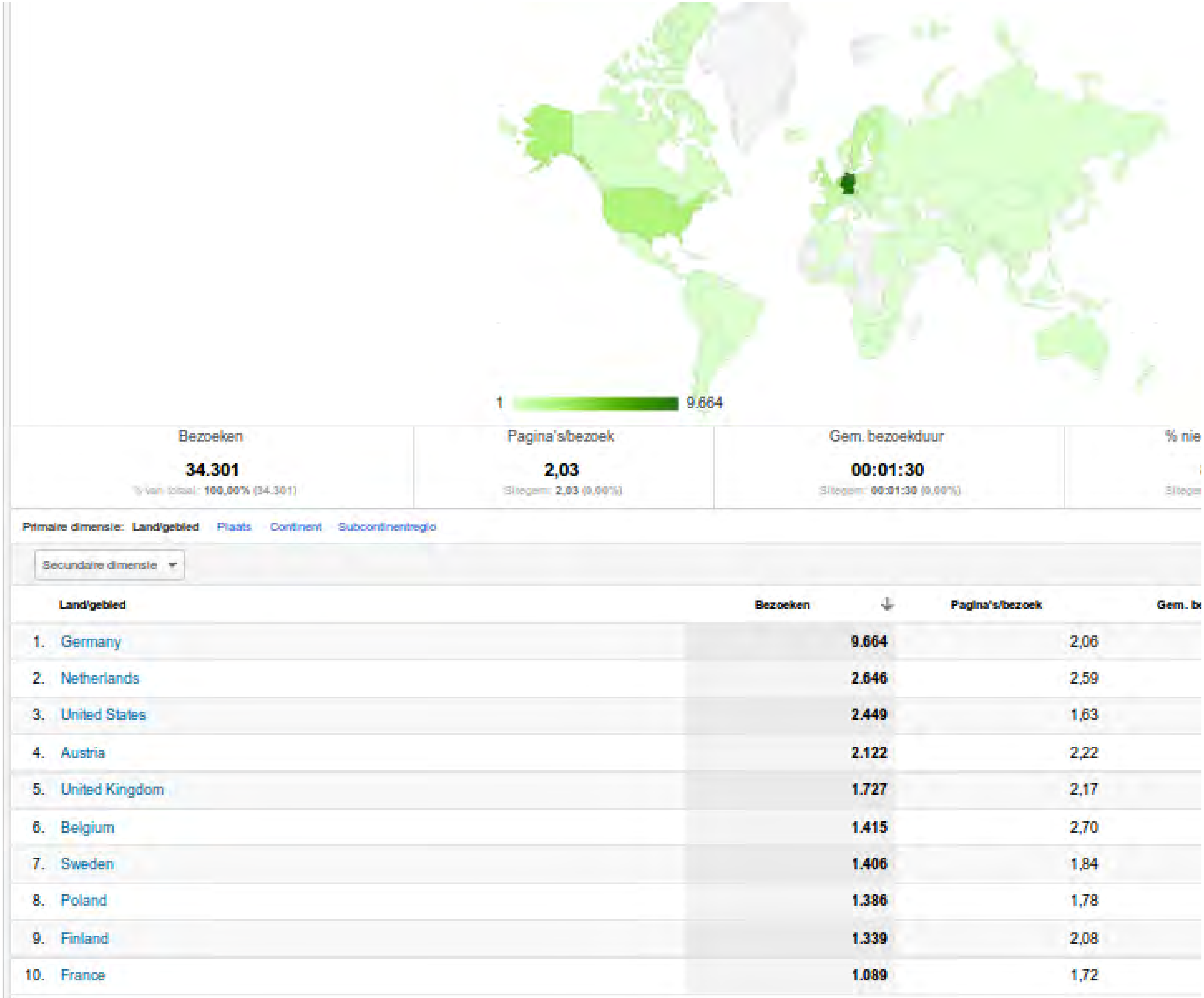
Andrew Reitemeyer



Janus Vollmer @noesch 23 januari

This Tweet has been flagged as terrorism! #cleanIT

Openen



Bezoeken	Pagina's/bezoek	Gem. bezoekduur	% nie
34.301	2,03	00:01:30	
% van totaal: 100,00% (34.301)	Sitegem: 2,03 (0,00%)	Sitegem: 00:01:30 (0,00%)	Sitege

Primaire dimensie: Land/gebied Plaats Continent Subcontinentregio

Secundaire dimensie ▾

	Land/gebied	Bezoeken ↓	Pagina's/bezoek	Gem. be
1.	Germany	9.664	2,06	
2.	Netherlands	2.646	2,59	
3.	United States	2.449	1,63	
4.	Austria	2.122	2,22	
5.	United Kingdom	1.727	2,17	
6.	Belgium	1.415	2,70	
7.	Sweden	1.406	1,84	
8.	Poland	1.386	1,78	
9.	Finland	1.339	2,08	
10.	France	1.089	1,72	

UNIVERSITEIT VAN TILBURG

Clean IT Best Practices: comments from the perspective of fundamental rights

Colette Cuijpers
Paul De Hert
Bert-Jaap Koops
Eleni Kosta
Ronald Leenes

The Clean IT Project

Reducing the impact of the terrorist use of internet

Dilemmas:

Terrorist use of the Internet is a vague term, and requires constant explanation by professionals

Controversial issues like the best practice “automated detection systems” might reinforce a culture of fear, but are an inspiring source for fruitful discussions

More transparency does not lead to more trust

Security and privacy should not be considered as separate issues

The Clean IT Project

Reducing the impact of the terrorist use of internet

13:30 Opening remarks Cyrus Farivar

13: 40 Mr. Theo Bot (deputy National Coordinator for Counter Terrorism and Security in the Netherlands)

13:50 Mr. Gilles de Kerchove (European Counter Terrorisme Coordinator)

14:00 Mr. But Klaasen (Projectmanager Clean IT)

14:20 break)

14:30 Panel introduction & discussion

16:00 Reception

The Clean IT Project

Fighting the illegal use of internet

But Klaasen

Ministry of Security and Justice
Netherlands

National Coordinator for Counter Terrorism

05/2012

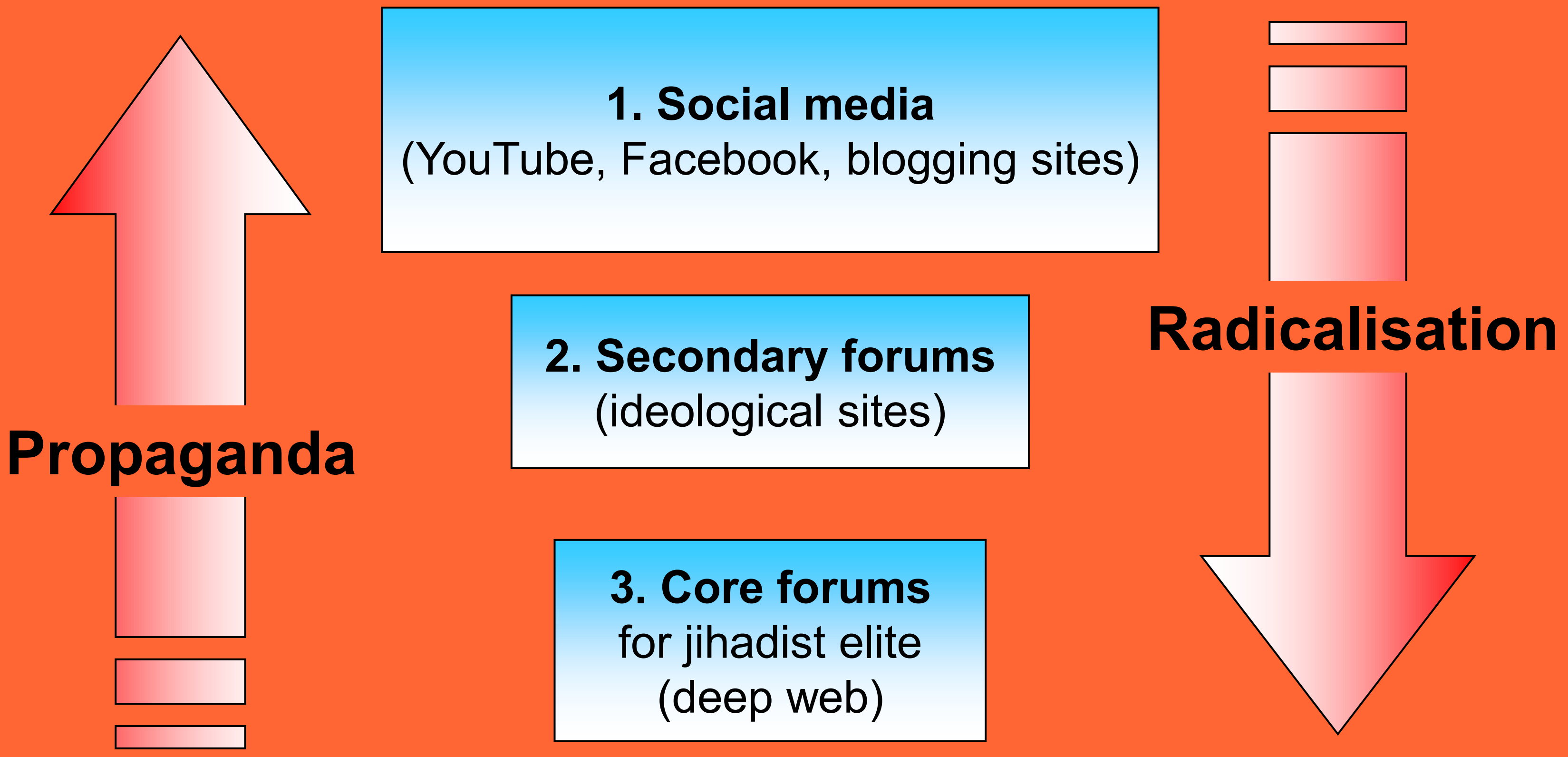
The Clean IT Project

Fighting the illegal use of internet

- What is 'terrorist use of the internet'?
  - Internet as a target
  - Internet as weapon
  - Internet as a resource
- How does the project work?
  - Public-private
  - Open dialogue
  - Trusted setting
- What challenges we face?
  - IFreedom?
  - Good and bad practices

The Clean IT Project

Fighting the illegal use of internet



1. Social media
(YouTube, Facebook, blogging sites)

2. Secondary forums
(ideological sites)

3. Core forums
for jihadist elite
(deep web)

Propaganda

Radicalisation

The Clean IT Project

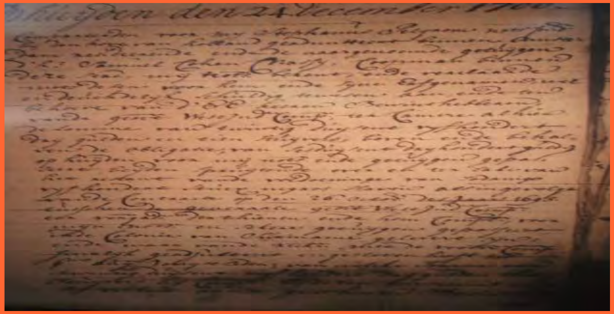
Fighting the illegal use of internet

The project, the way we work

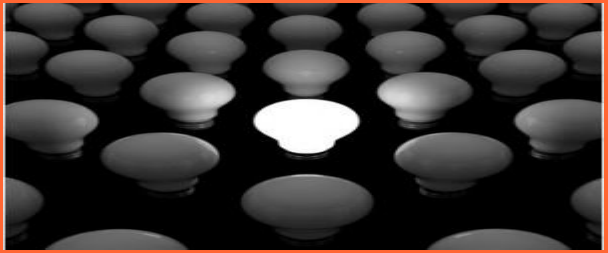
The Clean IT Project

Fighting the illegal use of internet

- GENERAL PRINPLES



- BEST PRACTICES



The Clean IT Project

Fighting the illegal use of internet

Questions...??

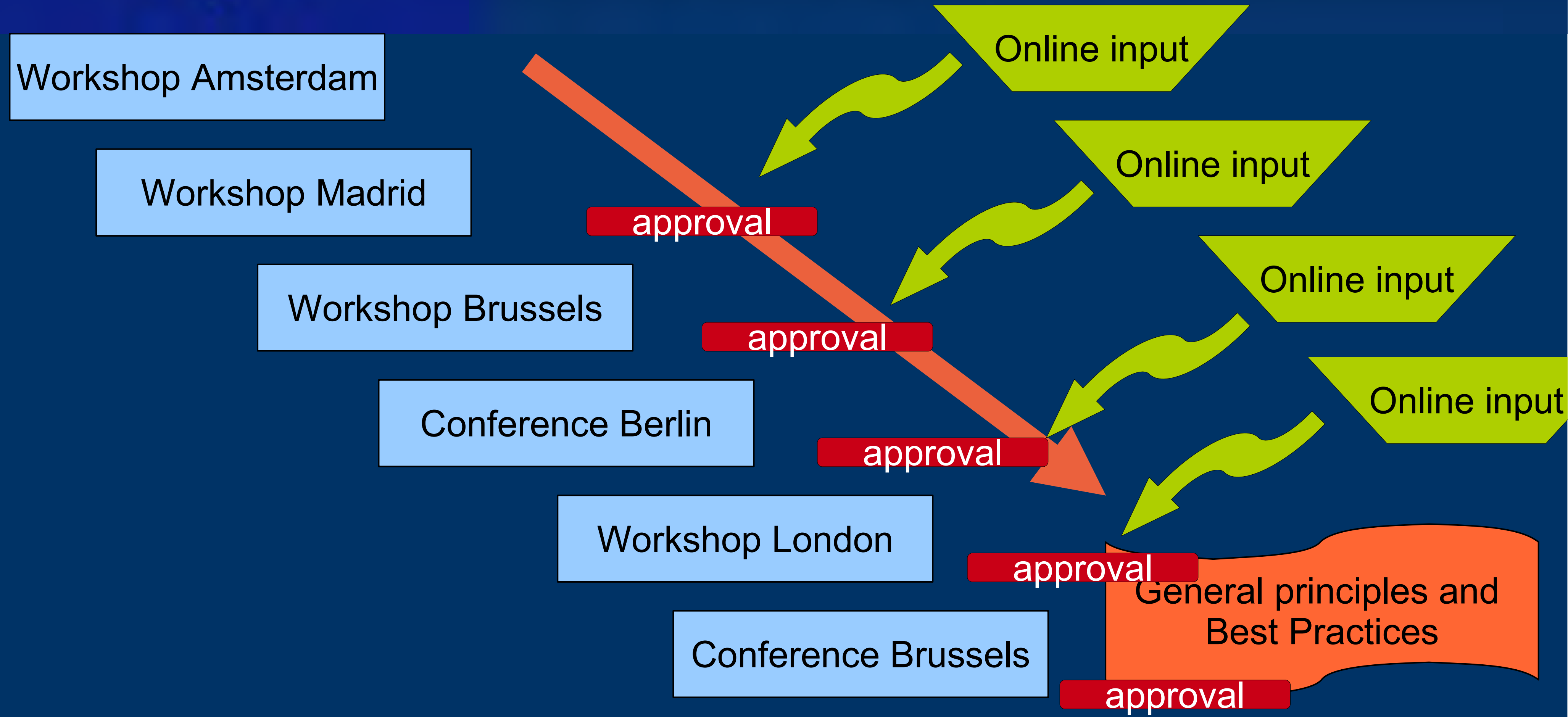
www.cleanITproject.eu

Mailings/updates: info@cleanitproject.eu

Contact me: but.klaasen@cleanITproject.eu

The Clean IT Project

Fighting the illegal use of internet



The Dutch National Cyber Security Strategy

The Netherlands have launched their national cyber security strategy on 22 February this year. Cyber security is one of the priorities of the current Dutch government and has been high on the political agenda since 2010.

The Dutch government regards safe and reliable ICT to be of fundamental importance for Dutch prosperity and well-being because it is a catalyst for (further) sustainable economic growth. After all, in Europe 50% of the growth in productivity is due to the application of ICT. The Netherlands aspires to be among the world leaders in the use and application of ICT in society and at the same time guarantee the safety of the digital society. The ambition is to grow into the Digital Gateway to Europe.

The vulnerability, dependency and complexity of ICT gives way to new threats. Skimming, identity fraud, phishing, but also targeted attacks on critical infrastructures, espionage and large scale disruptions. It is important that we direct our attention to the whole range of threats. Not only because techniques developed by criminals (often the most creative lot) may find their way to more politically motivated actors, but also because cyber incidents man made or not can have significant effects beyond the place where they first occur. A case such as the Stuxnet virus, with side effects around the globe, make this all too clear.

"We must not get carried away by alarmist stories, but the threat we face in cyberspace is real", says Rob Duiven, who as program director at the Ministry of Security and Justice is responsible for the implementation of the national cyber security strategy.

In the actual event of a cyber attack it is often difficult to determine what the cause or source is. It can be an individual, an organisation, a state or a combination of these players. Often it is not immediately clear what type of cyber threat is involved. In a cyber attack use is often made of the same techniques and methods.

The title of the Dutch Cyber Strategy translates as "Strength through collaboration'. Mr Duiven continues: " we have not chosen that title without reason: we outline an integrated approach in this strategy, all hazard and with both public bodies, private organizations and academia. ICT infrastructure, products and services are for the greater part supplied by private sectors so government cannot do this alone."

The Dutch strategy has several action lines Rob Duiven explains:

- We will set up a Cyber Security Council, in which all relevant parties (public private and academia) have a position at strategic level, and aim to provide governance for all parties involved. The installation and first meeting of this council is foreseen for June 30th . This is easily said, but it will be a challenge. But one we will face up to.
- There will also be a National Cyber Security Centre. This Centre can only function properly if supported by a thorough threat analysis which is updated regularly. This analysis must be based on information from government and private parties. International cooperation will also be key in providing a complete picture.
- We will also strengthen the defence mechanisms of critical infrastructure against IT disruptions and cyber attacks. Together with industry, the government will stimulate the use of minimum ICT security standards on the basis of good practices.

In consultation with the ICT suppliers, we also want to look for options for improving the security of hard- and software and intend to make agreements on secure hard- and software at international level.

- In the field of cyber crime, we will intensify and reinforce our investigation and prosecution efforts. We aim for more cross-border investigations with investigation departments of countries within Europe and with other international partners. In addition we will be focusing on furthering international legislation and regulations for cyber crime in which the Council of Europe’s Cyber crime convention has a central role .
- And last but not least, we will encourage scientific and applied research, and develop innovative security solutions. Our aim is to put the Netherlands in the top ten of countries with optimum cyber security.

The cross-border nature of threats makes it essential to focus on strong international cooperation. The basic principle is an international ‘level playing field’. Many measures will only be effective if they are aligned or implemented at an international level. The Netherlands supports and actively contributes to the efforts of, e.g., the EU (Digital Agenda for Europe and the Internal Security Strategy), NATO (development of cyber defence policy in the framework of the new strategic concept). The Internet Governance Forum offers an excellent opportunity for discussions between private and public parties on much needed international governance.

Clean IT

Many initiatives are already taking shape against this background. During the Ministerial cybercrime conference in Budapest last month, the Dutch minister of Security and Justice, Ivo Opstelten, announced that several European countries and Europol would strengthen their cooperation to fight online illegal activities for terroristic purposes on the internet. The project is called “Clean IT” and the Netherlands came to an agreement with Germany, United Kingdom, Belgium, Spain and Europol to give an important role to the internet industry itself in this project. Being financed partially by the European Commission, this project is based on a bottom-up, public-private approach.

It builds on the results of 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 via the internet and to develop ways and means to preventively address Islamist extremist content in the internet. This project identified several best practices in Germany, the United Kingdom, the Czech Republic and the Netherlands.

One of those best-practices was the Code of Conduct for Notice-and-Take-Down that was implemented in the Netherlands in 2008. This code of conduct does not only focus on terrorism, but for example also on child pornography and phishing. “We are seeking for these kind of best-practices, and we need to put them into practice on a voluntary base”, says But Klaasen who is the project leader from the Ministry of Security and Justice in the Netherlands, and one of the speakers in the plenary cyber-security track at the EuroDIG conference in Belgrade.

He continues: "The problem with illegal activities on the internet, is that the speed and connectivity of our ICT infrastructure, does not fit with our traditional approaches for law-enforcement. The digital society is global. Cyber attacks and disruptions cross over national borders, cultural and legal systems in the blink of an eye. It is often unclear which jurisdiction applies and it is uncertain whether applicable laws can be effectively enforced."

The objective of the project is to create basic rules of play, which are non-legislative, voluntary, and endorsed by the industry. If this will work for illegal terrorist activities on the internet, it might contribute to the creation of leading principles for a cleaner internet in general. The project partners will meet during the Eurodig Conference for their kick-off meeting. This multi-stakeholder conference in Belgrade is a unique opportunity to share thoughts and collect input from all parts of Europe. Klaasen: "That is why we welcome the opportunity to be here!"

- **Wat is de rol van Nederland in dit project? Ik zie/lees dat het projectteam bij het Nederlandse ministerie van Justitie zit, en dat Nederland het project aanvoert. Wat houdt dat in?**

  Nederland, het ministerie van Veiligheid en Justitie, is de indiener van de projectaanvraag bij de Europese Commissie en daarmee de hoofdverantwoordelijke voor de uitvoering van dit project. Het ministerie heeft hiervoor een projectleider aangesteld. Het projectteam is gehuisvest bij de Nationaal Coordinator Terrorismebestrijding en Veiligheid, en is verantwoordelijk voor de hele financiële en organisatorische / procesmatige kant van het project. De inhoudelijke koers is in dit project in de eerste plaats afhankelijk van de deelnemers aan de workshops, en wordt op hoofdlijnen afgestemd in een "coordination group" waarin deelnemers zitten van de partner-landen.

- **Heeft Nederland ook een oprichtende rol vervuld?**

  Ja, zie hierboven.
  Het project bouwt wel voort op twee eerdere initiatieven. In de eerste plaats is onder leiding van Duitsland een Europees project uitgevoerd waarin het jihadistisch gebruik van internet in een aantal landen in kaart is gebracht. Daarin is geconcludeerd dat een publiek-private aanpak en een variëteit aan oplossingen de voorkeur geniet. In de tweede plaats wordt voortgeborduurd op de totstandkoming van de Nederlandse gedragscode Notice-and-Take-Down. In dat project is een vorm van zelfregulering tot stand gekomen. Hierbij had het bedrijfsleven een prominente rol bij het ontwikkelen van oplossingen (voor de toen geldende NTD-problematiek).

- **Wat is exact het doel, de focus, van het project? En waarom is er gekozen voor de wel erg breed klinkende naam?**

  De naam van het project is "Clean IT: Fighting the illegal use of internet with public-private partnerships from the perspective of counter-terrorism".
  Dat heeft een formele achtergrond. Het project is ingediend onder het "prevention of and fight against crime" programma van Directoraat Generaal Binnenlandse Zaken van de Europese Commissie (DG HOME). In de betreffende call dient men specifiek te refereren aan onderdelen van dat programma. Dit project valt onder het kopje "illegal use of internet" en dat moest derhalve in de titel terugkomen. Taalkundig gezien valt er wat aan te merken aan die titel, want het gebruik van internet op zich is immers niet illegaal. Er is daarom een kortere 'roepnaam' bedacht (Clean IT), en een uitgebreidere formele naam die beter de lading dekt.

  Het doel van het project is om het gebruik van internet voor terroristische doeleinden tegen te gaan zonder bindende overheidsvoorschriften ("non-legislative approach"). Daarbij is gesteld dat oplossingen moeten komen uit een publiek-privaat 'bottum-up' proces, en dus niet top-down door overheden moet worden opgelegd. Dit maakt overigens dat het project een experimenteel karakter heeft, het eindproduct is immers niet exact omschreven, maar zal de uitkomst zijn van de samenwerking tussen verschillende partijen. Dat is geen open einde, want de bedoeling is uit te komen op "general principles" die door alle partijen onderschreven worden, en waaraan diverse (nationale) best practices aan verbonden kunnen worden (die internationale uitrol verdienen).

Los van het bovenstaande, is het ook steeds de bedoeling geweest om binnen deze kaders samen met de deelnemers de focus steeds scherper te stellen. Eén van deze aanscherpingen is dat het nu in eerste instantie gaat om op Al Qaïda gebaseerde vormen van terrorisme (en niet IRA, ETA, dierenextremisme, etcetera).

In de komende draft (wordt over +/- één week verwacht op de www.cleanITproject.eu website) staat een "preamble" die door de overheidspartijen is opgesteld en waar de probleemanalyse kort en krachtig is beschreven.

- **Wat wordt er precies bedoeld met "Public-private partnerships can cause a breakthrough in deadlocked talks between government and industry."? Als gesprekken tussen overheid en bedrijven vastlopen, kan samenwerking tussen overheid en bedrijven wel een doorbraak/uitkomst opleveren? Dat volg ik even niet.**

  Met deze passage wordt gerefereerd aan diverse dossiers (zonder een specifieke op het oog te hebben) waarin de overheid vanuit de positie van wetgever of opdrachtgever allerlei zaken ten aanzien van internet aan de industrie wil opleggen. De samenwerking loopt hierbij niet altijd even soepel. In dit project wordt nadrukkelijk gewerkt aan het opbouwen van vertrouwen in evenwichtig samengestelde groepen. In de Clean IT workshops worden deelnemers uitgenodigd waarbij de ideale samenstelling is 1/3 overheid, 1/3 belangengroepen, en 1/3 betrokken industrie. Bovendien beperken de overheidspartijen zich vooral tot het formuleren van het probleem en uitleggen van het fenomeen internet&terrorisme. Oplossingen worden veel meer door de industrie aangedragen en vervolgens in gezamenlijkheid besproken. Dat is dus wezenlijk een andere insteek dan bijvoorbeeld een traditioneel wetgevingstraject.

- **Welke private partners werken er mee?**

  Deze informatie geven wij (nog) niet prijs. Het is aan de private partners zelf om aan te geven of ze hier bekendheid aan willen geven. Zeker in de beginfase van het project is het natuurlijk onzeker wat de uitkomsten precies zijn of men daar hun bedrijfs-imago aan wil koppelen.
  Wel kan opgemerkt worden dat voor dit project de zogenaamde "access providers" minder relevant zijn dan bedrijven uit de hostingsector en social media. Het gaat hier immers vooral om propaganda en recruterings-activiteiten van terroristen.

- **Wat is er tot op heden gedaan/bereikt door dit project?**

  Zie de nieuwe draft die volgende week gepubliceerd wordt. Er is voor een belangrijk deel consensus bereikt over enkele 'general principles'. Maar er liggen nog vele discussiepunten open. Het is dus nog steeds work-in progress.

- **Wat voor doelen staan er (nog meer) op de planning, en hoe en voor wanneer?**

  De doelen zijn niet anders dan boven beschreven. De planning voorziet in worksop in Brussel in Maart, Berlijn in Juni, London in September en dan nog 1 of

2 bijeenkomsten in Brussel.
Er is ook een workshop-proposal ingestuurd voor de EuroDIG conferentie in Zweden half juni. De bedoeling is om daar de tussenresultaten in de open multi-stakeholder omveving van www.eurodig.org te presenteren en bediscussiëren. Of het workshop voorstel wordt gehonoreerd, is echter niet in onze handen.

EXTRA VRAAG (telefonisch) over de kosten:

Het totale projectbudget is € 407.134,55 en 80% wordt daarvan gefinancierd door de Europese Commissie. Dit is een maximum budget, de afrekening vindt plaats op basis van werkelijke gemaakte kosten. Niet meegenomen hierin zijn de kosten die betrokken ambtenaren maken vanuit hun reguliere functie.

- You write the project is partly funded by the European Commission, in particular by Prevention of and Fight against Crime Programme. It is possible to know the exact amount of this funding? It is possible to read any document proving that? I searched in the EU Commission website, but (probably for my fault) I could not find anything.

Information about ISEC projects can be found on the Commission website: http://ec.europa.eu/home-affairs/funding/isec/funding_isec_en.htm

The Clean IT budget is € 407.245,89 euro, from which 80% is financed by the European Commisison. This budget also can be found on the Commissions website: http://ec.europa.eu/home-affairs/funding/isec/2010_FPA_all_awarded.pdf

- There is a project leader? And who is he?

The Clean IT project is lead by the Netherlands, by an experienced project manager from the Ministry of Security and Justice. Our policy is that we do not publish names from project team members on the Internet for security reasons.

- With the purpose to contrast online illegal activities every EU member has its specific laws already. Member states apply measures especially against pedophilia, illegal gambling, monitoring web-sites and forum suspected to be a match-point for terrorists, etcetera. Other laws (someone says "censorship-laws") has been approved recently (ley Sinde in Spain) or are going to be approved (in Italy) to contrast copyright violations. Why do you think the CleanITProject is necessary? What are the gaps you intend to fill?

The gaps that we focus on, are not necessarily legal ones. Every country has its own responsibility to adopt laws and regulations. We focus on the way existing laws are put into practice, because it is not always clear how to apply them on the Internet. The Notice-and-Take-Down procedure in the Netherlands is an example of this approach. The law states that unequivocally unlawful material should be pulled offline if a Internet Service Provider is notified about the material. The law does not state who can notify the providers, what a notification should look like, within what timeframe content should be taken offline, or what to do if it is not "unequivocally unlawful". Filling these blanks is necessary to make the system of taking down illegal content work properly. In the Notice-and-Take-Down procedure the industry answered these questions.

- CleanITProject does not aim for new laws or regulations, neither in EU, neither in member states. You prefer "best-practices". What does "best practice" mean? I think about unofficial agreement between Police Forces and Isp. Am I right?

A code of conduct or covenant, with attached local best practices that can be implemented internationally, could indeed be the end result. But since we are in an open dialogue with the private sector, we do not know for sure what the end result will look like. This is a well-considered project strategy. We do know that the end result cannot be regulation, simply because a European legislative procedure would take too much time, and the private sector is not in the lead of such a process.

But if the outcome will not be legislation, that does not mean that it will be “unofficial”. It could result in a signed document or just a publication on the internet. This will be decided upon in a later phase of the project.

- At the moment, there are no italian Isp or Ngo or government representatives in the CleanITProject. Are you in contact with someone in Italy? Have you noticed some interest in the CleanITProject by some association or institution in Italy so far?

Many ISP’s, associations or institutions are at this moment not aware of the Clean IT project. We are not yet in the stage where ISP’s come to us spontaneously, but we see that our network is gradually expanding. Thanks to some publications and mailings we start to have more visitors to our website, also from Italy. We presented this project twice in the Counter Terrorist Working Group from the European Commission where all Member States are represented. We are now working on a questionnaire that will also be send to Italian public and private institutions. We are well aware that for a small project like ours, it is not possible to inform all relevant parties throughout Europe. This is why it is no problem for any interested organization to connect to the project. Interested persons and organizations can subscribe to newsletters through info@cleanITproject.eu and anybody is welcome to comment on interim results that are published on our website through editorialboard@cleanITproject.eu

- On the 6th of january draft document you say "project aims to limit the use of the internet for terrorist and extremist purposes including: [...] animal rights, left-wing, racist, religious, right-wing, separatist and all other terrorist and extremist organizations and individuals". I think this statement is potentially dangerous for the freedom of expression. Who decides - for example - if a separatist association in effectively "separatist"? And who decides if someone uses the internet for "terrorist purposes"? Who had to interpret the meaning of "extremis purposes"?

You are right about this. Let me underline that this document is in discussion and does not necessarily reflect the views of all the participants. It is a kind of `living document` and will be updated regularly. We will consider your questions as input for our next discussions.

To answer your question correctly, it is the law that determines if someone uses the internet for terrorist purposes. For various types of terrorism the legal basis is the Framework Decision 2002/475/JHA as amended by the FD/2008/919/JHA, in particular Article 3(1)a, b and c (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:330:0021:0023:EN:PDF)

This article outlaws: "public provocation to commit a terrorist offence", "recruitment for terrorism" and "training for terrorism" also when committed (intentionally) in the online environment, irrespective of the underlying ideology.

This will not be changed by the project. But let me underline also that this project does not aim at restricting our internet freedom. The internet has become very important to modern society and by far the most use of the internet is legal and beneficial to its users. The point is, that it is also used for terrorist purposes. That is what we want to limit. These two goals seem conflicting. The challenge is to balance them properly (openness versus security). This is exactly why we encourage NGO´s and supporters for an open and free Internet to participate in our discussions.

Prague, 10 May 2012

The Honourable

Ivo Opstelten
Minister of Security and Justice
Netherlands

<u>HAGUE</u>

Dear Minister,

I highly value your invitation to participate in the "CleanIT Project" which was initiated by the Netherlands and the other European countries.

Let me inform you that the Czech Republic has already been involved in the activities of above mentioned project via Council of the European Union. In March 2012 the Ministry of the Interior of the Czech Republic had filled in the questionnaire concerning the "CleanIT Project" and sent it to project staff.

In relation to the "CleanIT Project" the Czech Ministry of the Interior recommended to contact Czech National Security Authority which is responsible for Cyber Security in our country. Based on this the Ministry will not participate in the Project.

Yours Excellency, let me assure you of my highest considerations.

Respectfully yours,

Jan KUBICE
ministr vnitra

Praha 10. května 2012
Počet listů: 1

Vážený pane ministře,

velmi si vážím vaší nabídky účastnit se na projektu "CleanIT", který byl iniciován Nizozemskem a dalšími evropskými zeměmi.

Dovolte mi, abych Vás informoval, že Česká republika se již podílí na aktivitách vztahujících se k výše zmíněnému projektu, a to prostřednictvím Rady Evropské unie. V březnu 2012 Ministerstvo vnitra České republiky vyplnilo dotazník týkající se projektu "CleanIT" a zaslalo jej iniciátorům projektu.

V souvislosti s projektem "CleanIT" české Ministerstvo vnitra doporučilo kontaktovat český Národní bezpečnostní úřad, který je v naší zemi národní autoritou pro oblast kybernetické bezpečnosti. Na základě této skutečnosti ministerstvo nebude na projektu participovat.

Vaše excelence, dovolte mi ujistit Vás o mé nejvyšší úctě.

S pozdravem,

H.E. Ivo Opstelten
Ministr pro bezpečnost a spravedlnost

0 BD

BM/6446/3/2012.

MJ/NCTV

BELÜGYMINISZTÉRIUM

DR. PINTÉR SÁNDOR
miniszter

Ivo Opstelten úr részére
biztonsági és igazságügyi miniszter

Schedeldoekshaven 100
2511 EX, Hága
Hollandia

Tisztelt Miniszter Úr!

Szeretném megköszönni az Ön levelét illetve felkérését a „Tiszta IT" *(„Clean IT")* projektben való részvételre. Egyetértek Önnel abban, hogy a szélsőséges, az erőszak alkalmazását alátámasztó nézetek terjedését jelentősen megkönnyítik az internet adta lehetőségek. A kommunikációs technológiák komplex és gyorsan változó területén a közös fellépés az egyetlen megoldás, mely valóban nagyban fokozhatja jelenlegi erőfeszítéseink hatékonyságát.

A magyar Belügyminisztérium alárendelt szerve, a Terrorelhárítási Központ (továbbiakban: TEK) venne részt az Önök által koordinált projekt munkájában, melynek eredményei minden tagállam számára pozitív hozadékkal szolgálhatnak. Szeretném kiemelni, hogy a TEK a közeljövőben tervezi külön, internetfigyeléssel foglalkozó szakegység kialakítását, éppen ezért azt gondolom, hogy szakértőink számos, hasznos információval segíthetik mind a jövőben, mind e program keretében is egymás munkáját.
Kérésének megfelelően, a TEK szakértője [redacted] r. százados úr (Felderítési Igazgatóság [redacted] [redacted] fel fogja venni a kapcsolatot [redacted] asszonnyal a konkrét együttműködés megkezdése érdekében.

Budapest, 2012. május „ 14 "

Üdvözlettel:

Dr. Pintér Sándor

"courtesy translation"

Budapest, " " May 2012

Mr Ivo Opstelten
Minister of Security and Justice

Schedeldoekshaven 100
2511 EX The Hague
The Netherlands

Dear Minister Opstelten,

I would like to thank your letter and invitation to take part in the „Clean IT" project. I agree with you on that the internet plays an increasing role for recruits, propaganda or supporting and makes the spreading of extreme ideologies or those legitimating or even considering indispensable the use of violence easier. It is also common, that the whole area of communications technology is complex and fast-moving, and our efforts could only be successful if we act together.

Furthermore I think that the "Clean IT" project could have a positive impact for all the Member States, accordingly I support the participation of the Ministry of Interior and particularly the Counter-terrorism Centre in its tasks. The Hungarian Counter-terrorism Centre also plans to set up a special unit countering the use of the internet for terrorist purposes in the near future therefore I do believe that our colleagues could give useful contributions for each other in the future and even within the framework of this programme.

According to your letter, [redacted] the expert of the Counter-terrorism Centre (Intelligence Directorate, [redacted]) will contact [redacted] concerning the details.

Yours sincerely,

Sándor Pintér Dr.

LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJA
MINISTRY OF THE INTERIOR OF THE REPUBLIC OF LITHUANIA
Šventaragio g. 2, LT-01510 Vilnius Tel. +370 5 271 7154/+370 5 271 7178 Faks. +370 5 271 8551
2 Šventaragio st., LT-01510 Vilnius Tel. +370 5 271 7154/+370 5 271 7178 Fax +370 5 271 8551

Ministerie van Veiligheid en Justitie
Schedeldoekshaven 100
2511 EX The Hague
The Netherlands

16 July, 2012 No. 1D-4822(52)

RE: Invitation to participate in the Clean IT project

Dear Colleague,

In response to your letter of 17 April 2012, whereat you introduced the Clean IT project and invited the Ministry of Interior of the Republic of Lithuania to participate in the said project as a "supporting government partner", we would like to thank you for your kind invitation and express our support to the idea of clean IT being addressed on the governmental level.

Unfortunately, at present, due to the lack of financial and human resources, the Lithuanian Ministry of the Interior will not be able to join the Clean IT project as a "supporting government partner". Nevertheless, we hope for cooperating with your Ministry in the future.

Yours sincerely,

Artūras Melianas
Minister

MV&J/DEIA

[illegible]/29/2012 10:38 045

0 BD

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Intérieur
et à la Grande Région

Le Ministre

Luxembourg, le 18 MAI 2012

2012/13665/0905/DSI

A
Monsieur le Ministre
de la Sécurité et de la Justice
du Royaume des Pays-Bas
- Ministerie van Veiligheid en Justitie -
Schedeldoekshaven 100
NL-2511 EX The Hague

Dear Minister,

I have been sensitive to the efforts you make in introducing the "Clean IT project" inviting Luxembourg to participate as a "supporting government partner ".

I transmitted the invitation to the General Director of the Luxemburgish Police, his services being in charge of this item.

Yours faithfully,

Le Ministre de l'Intérieur
et à la Grande Région

Jean-Marie HALSDORF

MINISTÉRIO DA ADMINISTRAÇÃO INTERNA

Ministro

H.E.
Dr. Ivo Opstelten
Minister of Security and Justice of
The Neteherlands

Lisbon, 12th of July 2012

I would like to start by thanking you for your letter, dated from the 17th of April, concerning the possible participation of the Portuguese Ministry of Home Affairs in the "Fighting the illegal use of the Internet with public-private partnerships from the perspective of the counter terrorism" / "Clean IT" project, as a supporting government partner in such an interesting and relevant initiative.

After analyzing the a.m. letter, I have conclude that, under the Portuguese law, this matter falls primarily under the competencies of the Judiciary Police, and, consequently, should be handled by the Portuguese Ministry of Justice.

Henceforth, I would like to inform you, dear Colleague, that your letter has been sent to the attention of my colleague, the Minister of Justice, [redacted] so that she can respond on the matter under consideration.

On behalf of the Ministry of Home Affairs of Portugal, I would thus like to reiterate our full willingness to continue strengthening the ties of cooperation between our countries, both bilaterally and in the context of the European Union.

Please accept, dear Colleague, the assurances of my highest consideration.

Miguel Macedo

4956

EMBAIXADA DE PORTUGAL
HAIA

The Hague, 28 December 2012

His Excellency,
Mr. Ivo Opstelten
Minister of Security and Justice
of the Kingdom of the Netherlands
The Hague

Your Excellency,

I have the honor of sending herewith copy of a letter addressed to Your Excellency by Mrs. Paula Teixeira da Cruz, Minister of Justice of the Portuguese Government.

The original of the letter will be sent as soon as received from Lisbon.

Please accept, Your Excellency, the assurances of my highest consideration.

Mafalda Groba Gomes
Chargé d'Affairs a.i.

EMBAIXADA DE PORTUGAL
HAIA

Ministério da Justiça

H.E.
Dr. Ivo Opstelten
Minister of Security and Justice
of the Netherlands

Lisbon, 13 of December 2012

Thank you for your letter inviting Portugal to be part of the project “Fighting the illegal use of internet with public-private partnerships from the perspective of counter terrorism - “Clean IT”, as a supporting government.

The prevention of and the fight against all forms of serious crime, in particular terrorism and its financing, should be a matter of concern to all States, bearing in mind the adverse effects that they may cause in free, democratic societies. The use of the new technologies for recruitment purposes, for the dissemination of messages and for crime public support should also be a primary concern.

Portugal, as a Member State of the European Union, and given its participation in the framework of other international organizations, is also committed to the collective purpose of tackling terrorism. Hence, we believe that the involvement of the civil society, through public-private partnerships, may constitute an added-value in the prevention of and fight against terrorism.

Taking into account all these factors, and having heard the Criminal Police, the entity entrusted with the prevention of and fight against terrorism in its several aspects, Portugal accepts the invitation to be part of “Clean IT Project”, as a supporting government.

Yours sincerely,

A Ministra da Justiça

Paula Teixeira da Cruz

România

Serviciul Român de Informații

Director

His Excellency Ivo Opstelten
Minister of Security and Justice of the Kingdom of Netherlands

Dear Sir,

We share your views regarding the importance of the virtual space for the future of our society and the need to keep the Internet a safe place from any such entities that might attempt to use this tool for terrorist purposes.

As national authority in both cyberint and combating terrorism, the Romanian Intelligence Service (SRI) believes that the CleanIT Project has the potential to bring added value to national and European efforts to reduce cyber terrorism and we express our interest to take part in this initiative as "supporting partner".

The CleanIT Workshop we organized in Romania on the 28 of June this year was an opportunity to engage in really fruitful discussions with Dr. Michiel de Weger, the representative of the project, but also to try and find common grounds between national institutions with competencies in this field and the major Internet providers. Thus, we might say that the first step towards supporting the project was already taken and we look forward to future events under the aegis of the CleanIT project.

Sincerely yours,

Ambassador George Cristian Maior

Director of the Romanian Intelligence Service

EMBASSY OF ROMANIA
to the Kingdom of the Netherlands

Catsheuvel 55
2517 KA The Hague

Phone: 0031-70-3223613
Fax: 0031-70-3541587
roembnl@xs4all.nl
http://haga.mae.ro

No. 4364

The Hague, 10.01.2013

Excellency,

I have the honour of sending you, herewith attached, the original letter addressed to Your Excellency by the former Romanian Minister of Administration and Interior, H.E. Mr. Mircea Duşa, regarding the participation of the Romanian Ministry of Administration and Interior in the *Clean IT Project*. The letter is dated November 2012.

Please accept, Excellency, the assurances of my highest consideration.

Sincerely Yours,

Ireny Comaroschi,

Ambassador

His Excellency Mr. Ivo OPSTELTEN
Minister of Security and Justice
The Hague

ROMÂNIA
MINISTERUL ADMINISTRAŢIEI ŞI INTERNELOR

MINISTRU

NESECRET
Nr. din
Exemplar nr. 1
Număr exemplare: 2

To
Mr. Ivo Willem OPSTELTEN
Minister of Security and Justice

Ministerie van Veiligheid en Justitie
Schedeldoekshaven 100
2511 EX Den Haag

Dear Minister,

Terrorism and extremism represent two major challenges in the current European security environment, both to the citizens' rights and in term of the fundamental values of our society: freedom, rule of law and tolerance. These phenomena use the great potential of the mass communication technology to achieve their purposes, making the countering extremely difficult for the competent authorities due to the openness and fast communication flows that characterize the globalized world.

In this respect, I consider the *Clean IT project* initiated by The Netherlands as being of utmost importance. The project brings together the efforts of the competent authorities across Europe in a common endeavour to maximize the opportunities offered by the virtual space through innovation and openness, to secure the IT systems against the upcoming risks and challenges. Therefore, following the active participation of our colleagues from the Romanian Service of Intelligence, the Romanian Ministry of Administration and Interior expresses hereby its intention of becoming supporting government partner to the *Clean IT project*.

Our contribution within the project would focus on identifying the best practices models and on studying the experience of other international and regional. I would also like to emphasize the importance of setting up of a cooperation platform with rules and standards to be used in the virtual space, based on a risk analysis of the *Clean IT project*, to identify the vulnerabilities and to offer suggestions to reduce/remove them. These elements should be comprised in an information security template supported by all participants involved. The information security measures applied to the system should be based on the ISO 27000 family of standards.

Acknowledging the excellent cooperation between our institutions, please accept, dear Minister, the expression of my highest consideration.

Yours sincerely,

Mircea DUŞA

Minister of administration and interior

ROMÂNIA MINISTERUL ADMINISTRAŢIEI ŞI INTERNELOR MINISTRU

Embassy of Romania
to the Kingdom of the Netherlands
Catsheuvel 55, 2517 KA
The Hague

nr. 4364

H.E. Mr. Ivo Opstelten
Minister of Security and Justice
Postbus 20301
2500 EH Den Haag

REGERINGSKANSLIET

Ju2012/3337/PO

4 June 2012

Ministry of Justice Sweden

Division for Police Issues
Special Advisor
[redacted]
Telephone [redacted]

Minister van Veiligheid en Justitie

[redacted]
Den Haag
Netherlands

Participation in the Clean IT project

Thank you for your letter regarding the Clean IT project. We share your concern for how the internet could be used for nefarious purposes by antagonists to plan and commit terrorist acts.

The project's approach to involve the private sector in such a clear way is novel and an important step to create the long-term commitment and understanding that is needed in this area. We have found in other crime areas that involve the internet that, in order to be successful, the private sector needs to be actively included.

Unfortunately, we do not have the possibility to participate fully in the project in the capacity as a *supporting government partner* at this time. We thank you again for you proposition and will continue to follow the project and its results with interest.

With kind regards,

[redacted]

EUROPEAN COMMISSION
DIRECTORATE-GENERAL HOME AFFAIRS
Directorate A : Internal Security
Unit A4 : Financial support – Internal Security
The Head of Unit

Brussels, 19 August 2010
HOME-A4/FK/WW/D(2010)/ 13006

MS JOHANNA HEYNENS
MINISTRY OF JUSTICE
SCHEDELDOEKSHAVEN 100
2500 EH THE HAGUE
THE NETHERLANDS

Subject: Your application for funding under Call for Proposals Restricted to Framework Partners – the Programme "Prevention of and Fight against Crime 2010"

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

Dear [redacted]

This is to acknowledge receipt of the application for the project:

Clean IT: Fighting the illegal use of internet with public-private partnerships from the perspective of counter-terrorism

It has been registered under the above mentioned reference number, which should be quoted in all future correspondence. It was received within the deadline for receipt of applications and is currently under evaluation. We shall contact you again should further information be required.

Yours sincerely,

f.o. [redacted]

B

EUROPEAN COMMISSION
DIRECTORATE-GENERAL HOME AFFAIRS

Directorate A : internal Security
Unit A4 : Financial support – Internal Security
The Head of Unit

Brussels, 17 MARS 2011
HOME/A4/FK/WW D (2011)

[redacted]
MINISTRY OF JUSTICE
SCHEDELDOEKSHAVEN 100
2500 EH THE HAGUE
THE NETHERLANDS

REGISTERED MAIL and electronic mail

Subject: Your application for funding under Call for Proposals Restricted to Framework Partners – the Programme "Prevention of and Fight against Crime 2010"

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

Dear [redacted]

Following the thorough assessment of each eligible application against the selection and award criteria set out in the Call for Proposals, I am pleased to inform you that the aforementioned application has been awarded a grant. The maximum amount of the grant has therefore been set to **325.796,71 €**, the maximum co-financing rate is **80,00%**.

During the evaluation process the estimate budget submitted together with your proposal has been thoroughly verified and corrected. Expenditure was decreased or removed when assessed as non-eligible, higher than available market price or not related to the project. Following revisions have been made:

Heading A

Item A1 – daily rate automatically reduced to 450€/day in the absence of any salary slip or contract.

Item A4 – project assistant: reduction of salary rate from 484€ to 300€ per day.

Item A5 - this staff member has the same function as project leader – since neither additional justification nor offer has been given the item has been deleted.

Item A6 – costs transferred to heading F

Item A7 – since the option 1 has been chosen this cost is not eligible – set to 0€.

Heading D

Item D22 – transport cost for interpreters is not eligible – removed from the budget

Items D5, D10, D15, D19, D26, D31 – please explain difference in the speaker's fees, the basis for calculation and provide names and CVs of speakers.

Heading E

Item E2 – number of pages decreased form 7500 to 5250

Item E3 – number of units decreased from 400 to 250

Heading F. Item F2 – the cost has been removed. Tasks should be undertaken by project assistant (otherwise it's extensive presence in the project is not justified).

[redacted] will be responsible for preparation and management of your grant agreement. She is also your contact person for any financial matters you might have.

Before the Commission proceeds with the preparation of the grant agreement please provide Ms Becq (European Commission, DG HOME Unit A4 "Financial Support – Internal Security", LX-46 04/122, B-1049 Brussels, [redacted] by **31 March 2011** also with the following information:

- a new start date of the project (since the initial date was 1/12/2010; there is a need to specify a new date). You can either indicate a concrete date or chose the option when the agreement enters into force when the last party signs it.
- updated technical annex (if needed).

Failure to meet this request will result in cancellation of this grant.

In case the MINISTRY OF JUSTICE is unable to accept the above-mentioned revisions, I regret to inform you that the European Commission will not be able to proceed with the conclusion of the grant agreement and the grant will be cancelled.

Thank you in advance for your cooperation.

Yours sincerely,

[redacted]

Klaasen H.M. - BD/NCTB/DR

Van: [redacted].[redacted]
Verzonden: woensdag 11 mei 2011 15:03
Aan: Klaasen H.M. - BD/NCTB/DR
Onderwerp: FW: HOME/2010/ISEC/FP/C2/4000001442

Vriendelijke groet, / Kind regards,

[redacted]
Senior beleidsmedewerker / senior policy officer

....
Ministerie van Veiligheid en Justitie / Ministry of Security and Justice
Directie Europese en Internationale Aangelegenheden / European and International Affairs Department
Schedeldoekshaven 100 | 2511 EX | Den Haag | L 5.33
Postbus 20301 / PO Box 20301 | 2500 EH | The Hague | The Netherlands
....
[redacted]
www.rijksoverheid.nl
....
Veiligheid en Justitie. Recht raakt mensen.
....

Van: [redacted]
Verzonden: woensdag 11 mei 2011 15:02
Aan: [redacted].[redacted]
CC: [redacted]
Onderwerp: RE: HOME/2010/ISEC/FP/C2/4000001442

Dear [redacted]

Following your message I would like to inform you that the Commission has granted you permission to start the project before the grant signature. Please bear in mind however that it doesn't mean that all costs related to activities to be undertaken before the grant agreement is signed are automatically accepted as eligible.

Best regards,
[redacted]

[redacted]

Programme Manager - Prevention of and Fight against Crime
European Commission
Directorate-General Home Affairs
Directorate A: Internal Security

Unit A4: Financial support - Internal Security

[redacted]

Please consider the environment before deciding to print this e-mail.

Disclaimer:
This message represents solely the views of its author and cannot in any circumstances be regarded as the official position of the European Commission. This message is intended for the use of the addressee only and may contain information that is privileged and confidential. If you are not the intended recipient, you are notified that any dissemination of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by return of this e-mail. This communication does not constitute any formal commitment on behalf of the European Commission.

From: [redacted].[redacted]
Sent: Tuesday, May 10, 2011 4:01 PM
To: [redacted]
Subject: HOME/2010/ISEC/FP/C2/4000001442

Dear Ms Becq,

Herewith I would like to ask permission to start the project Clean-IT with reference number HOME/2010/ISEC/FP/C2/4000001442 before signing the grant agreement. It concerns the kick-off meeting which will be held in Belgrado on the 30th and 31st of May. Participants are: Germany (1), Belgium (1), Spain (1), UK (1) and The Netherlands (2). It would be really helpfull if the meeting could be scheduled before the start of the holiday season. Hoping for a positive answer,

Vriendelijke groet, / Kind regards,

[redacted]
Senior beleidsmedewerker / senior policy officer

....
Ministerie van Veiligheid en Justitie / Ministry of Security and Justice
Directie Europese en Internationale Aangelegenheden / European and International Affairs Department
Schedeldoekshaven 100 | 2511 EX | Den Haag | L 5.33
Postbus 20301 / PO Box 20301 | 2500 EH | The Hague | The Netherlands
....
[redacted]
M [redacted]
[redacted]
www.rijksoverheid.nl
....
Veiligheid en Justitie. Recht raakt mensen.
....