This document is a summary of what was discussed during the Clean IT project workshop in Amsterdam, October 24 and 25, 2011, comments on the draft by participants and various meetings, discussions and reactions via email afterwards.

This draft has been published on the CleanIT website (www.cleanitproject.eu) and subscribers to the projects email have been noticed on its publication. All reactions send to editorialboard@cleanitproject.eu (please use track changes) will be studied and can lead to changes in the draft. This document will be discussed intensively during the January 18 and 19 2012 CleanIT workshop in Madrid, and later in Brussels (March 21 and 22), Berlin (June 4 and 5).

(Main text starts here)

The participants in the CleanIT project have discussed the use of the internet by terrorists and extremists. They spoke about current obstacles in limiting terrorist and extremist use of the internet and discussed what kinds of organizations can possibly contribute to limiting this type of use. The participants discussed that:

1. 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. By and large the internet plays a positive role in our lives and societies.

2. Nevertheless, the internet is also used for illegal purposes. It is misused in many forms, including cybercrime, hate speech, discrimination, illegal software, child pornography and terrorism.

3. The internet is used by terrorists and extremists to spread violent images and propaganda material, glorify and encourage violence, radicalize and recruit individuals, spread training manuals and other knowledge on how to commit violence, and the internet is even used to plan and organize deadly attacks.

4. Even though international and European organizations, national governments, private companies and non-governmental organizations (NGOs) are currently working to limit illegal and unwanted the use of the internet by terrorists and extremists, many obstacles to solving the problem still exist. The participants pointed out that there is a lack of knowledge, resources, awareness, communication, (international) cooperation, points of contact and trust. Limiting the use of the internet by terrorists and extremists comes at high costs, while the technology to use the internet is cheap and widely available. Moreover, assessing (il)legality is difficult in many cases, there is no cross-border jurisdiction and there are international (legal) differences.

5. Limiting the illegal and unwanted use of internet by terrorists and extremists requires the participation of Internet Service Providers (ISPs), users, research and educational organizations, NGOs, policy makers and Law Enforcement Agencies (LEAs). Their European organizations can contribute, too.

6. Finding common ground by ISPs and LEAs is difficult. The LEAs involved in this project are far more focused on terrorists and extremists than the ISP´s are. (Individual) ISPs receive large numbers of complaints and notifications, but only few of the complaints focus on supposedly terrorist or extremist activities. When receiving notifications by LEAs, ISPs often lack the contextual information LEAs have about other online or physical activities by the suspects. When taking their decisions, ISPs always consider the risk to lose clients and damage their business. Some ISPs are not willing to react to informal notifications by LEAs as a matter of

principle; they are only taking action in case of court or Public Prosecutor's orders. LEAs should follow existing, prescribed procedures for notifications to ISPs as much as possible.

7. Various kinds of ISPs could contribute to limiting the use of the internet terrorists and extremists. This includes (alphabetical order) browser providers, certificate providers, cloud providers, domain registrars, e-mail service providers, exchange points, filter providers, hosting providers, hotlines, investigation companies, law firms, security consultants, search engine companies, social network sites, technology innovators, vendor sites and web forum providers. Their national and European associations can also contribute.

8. NGOs that could contribute in limiting the use of the internet by terrorists and extremists include consumer, internet user, civil rights, human rights, anti-discrimination, religious and parents organizations, at both the national and European level.

9. LEAs that could contribute in limiting the use of the internet by terrorists and extremists are i.e. local and national police, counter terrorism units, intelligence agencies, courts, Public Prosecutors and police internet referral units.

10. Last, but not least: individual users could also contribute, i.e. by notifying ISPs and LEAs about the use of the internet by terrorists and extremists.

Scope

The organizations that met in Amsterdam have suggested that the Clean IT project should to aim to limit the illegal and unwanted use of the internet by terrorist and extremist organizations

11. for propaganda, glorification, encouragement, recruitment, incitement, financing and acquiring knowledge, weapons, other materials and other kinds of support.

12. by all kinds of terrorists organizations, including lone wolf terrorists and individual extremists. Including (alphabetical) animal rights, left-wing, racist, religious, right-wing, separatist and all other terrorist and extremist organizations and individuals.

13. within in all layers and parts of the internet. This includes (in alphabetical order) audio messages posted on internet, blogs, chat rooms, documents posted, e-mail, messaging systems, payment systems, social media, static texts on websites, video messages, web forums.

14. The project also aims to limit the use of the internet by organizations or individuals inciting murder and violence, and or publishing or disseminating racist and xenophobic material, and hate speech.

General principles

The participants of the Clean IT project suggested a number of general principles for activities and cooperation to limit the use of the internet by terrorists and extremists:

15. Share an interest in clean internet. ISPs primarily focus on making profits, LEAs on enforcing the law. ISPs would benefit from a cleaner internet as well as it would protect their customers.

16. Have mutual understanding and mutual trust. To reach this LEAs have to understand ISPs procedures and needs, know whom to contact, have sufficient knowledge of laws and

regulations, and knowledge about internet technology. ISPS have to better understand the context LEAs are working in. LEAs and ISPs should act professionally and be as transparent to each other as possible. LEAs activities should be predictable, enforce the law effectively and treat all ISPs the same. In case of disagreement, LEAs and ISPs should respect each other's positions and responsibilities. Crossing of red lines, like LEAs that are putting excessive pressure on ISPs, is unacceptable and counterproductive.

17. Respect for fundamental rights and freedoms, including access to the internet, freedoms of assembly and expression, non-discrimination, privacy. Working within the limits of national and European laws and regulations.

18. Laws and regulations do provide some clarity of what terrorist and extremist illegal use of the internet is. Unequivocally unlawful content must be removed from the internet by ISPs or their clients. Unwanted content is not necessarily illegal, but by definition of an ISP's terms of business nevertheless is not wanted on its internet service.

19. While the CleanIT only aims at limiting terrorism and extremism on and via the internet as defined above, some of the partial solutions below will also limit other forms of illegal or unwanted use of the internet.

Partial solutions

The participants in the Clean IT project have suggested a number of solutions to limit the use of the internet by terrorists and extremists. They believe that a pragmatic approach will produce the best results. The participants are willing to further discuss and develop (in alphabetical order):

20. Awareness, education and information. The public and customers should be aware of terrorist and extremist content online and should know what to do about it. There is a need to increase user activity and the quality of notifications. Government campaigns can help with this. Providers can support these initiatives and publish more information on terrorism and extremism on their websites, and whom to contact in cases of potential extremist or terrorist content. NGOs have a role in awareness raising and could provide education and information.

21. Counter narratives projects.

22. Court orders.

23. End-user controlled filters. Parents and other users should be offered a regular reminder of the choice to install an end user control service blocking (among others) terrorist and extremist content. LEAs can provide blacklists through a very transparent process for these end user controlled filters. Providers could promote use of filters among their clients.

24. Exchange of knowledge by public and private experts on technical and legal issues.

25. Flagging. ISPs could offer users easy to use flagging systems as much as possible. LEAs of all countries should actively flag and encourage the use of flagging among end users as much as possible as a way of notification to the ISP that they are hosting content which might be illegal or unwanted.

26. Funding NGOs.

27. Government can email updates to ISPs. LEAs can send threat updates and general information on terrorist and extremist activity relevant to ISPs.

28. Increasing technical knowledge of the internet within government organizations.
29. International cooperation. Between European countries. Relations with countries outside the European Union. Bilateral contacts.
30. Legislation and regulation. Both at national and EU level.
31. Languages services.
32. Moderators projects.
33. Monitoring and searches.
34. Notice and take down. Clear and fast procedures by ISPs for notifications by users, NGO's or LEAs pointing at possibly unwanted or illegal activity on the internet by terrorists and extremists. LEAs should contextualize extremist content and asses whether it is breaching national legislation. Own responsibility ISPs for decision. Must reply principle. Revoking registration or security certificates.
35. Points of contact for terrorism and extremism in each organization. This includes LEAs, ISPs, user organizations and NGO´s. These points of contact should be stable; They should remain points of contact for a longer period and develop stable relations with their most important counterparts in other organizations.
36. Pop up systems.
37. Public policy. Governments and ministries need to clarify laws and regulations and their policies, and coordinate with LEAs as much as possible. LEAs could help ISPs by listing specific offences. LEAs could report back to ISPs to confirm how the information has assisted the investigation, what results have been achieved.
38. Publishing black lists.
39. Real identity policy.
40. Referral sites.
41. Terms of service/business conditions and acceptable use policies of ISPs should (also) deal with illegal and unwanted use of the internet for terrorism and extremism.
42. Specialised courts and Public Prosecutors.

Permanent dialogue

43. One European unit to administer information about LEAs, NGOs, ISPs points of contact in all organisations.