What is WhiteIT and what does it aim for?

Why you probably want to be concerned about it and similiar alliances.

Christian Rüdiger Bahls; MOGiS e.V.
christian.bahls@mogis-verein.de

28c3 Chaos Communication Congress,
Berlin, December 27th 2011

Before the talk

- My name is Christian Bahls, i represent MOGiS, a German Association of victims of sexual abuse.
- Most of the information i present here is publicly available, it just has to be pieced to together in the right way.
- First i planned to give this talk in German, but than realized the information might be useful to a larger audience.
- So please stay with me, even if you are not German. you should get some insight into what is going on.
- Especially you should listen up if you are a hosting-, service- or access-provider based or operating in Germany or the EU.
- One thing i want to make clear to not be misunderstood: I am not a fundamentalist. I am willing to cooperate with anybody who constructively works against child abuse and shows willingness to respect fundamental rights.

Why? - And why now?

- First of all i want to lead a somewhat smaller live in the future.
- Perhaps finish my first doctoral thesis before KT finishes his second. (yes, i must have been proposing this for ages :)
- So this is my chance to make you aware of what is going on hoping somebody else will take the work up.
- Actually it's a little early in the process of WhiteIT for awareness raising – but next years 29C3 would be too late.
- So going public now seems to be the best decision
- Especially in the light of recent events.

MOGiS e.V. - A Voice for Victims - A Voice for Reason

- Most of you might have come to know me as chairman of MOGiS e.V. during the German debate on Internet Blocking.
- A Few of you might be aware of my work on the EU child protection directive, (the Malmström proposal tried to introduce mandatory blocking infrastructure in all of the EU's member states)
- Together with EDRi we got the mandatory part removed and also got some judicial oversight into it.
- As MOGiS e.V. represents victims of sexual abuse, besides defending fundamental rights we are also are working on child protection issues.
- Which is one of the reasons why we got involved with WhiteIT in 2011.

How and why i got into WhiteIT

- The first time i ran into WhiteIT was in 2010 when they unveiled the „jetzt-löschen!“ (remove-now!) button. (Perhaps you remember my Reaction to it – the denunciation-button)
- Also i regularly met members of WhiteIT at hearings of the European Parliament on the Child-Exploitation-Directive (which tried to introduce blocking).
- During in a plenary discussion „CeBIT against Cybercrime“, at the CeBIT '2011, Mr Schünemann (Minister of Interior in the State of Lower Saxony) invited MOGiS to participate.
- We agreed to take part under the specific conditions that we become part of the steering committee within WhiteIT (Lenkungskreis, now Lenkungskreis+).
- Well, we did not become member of that, but a member of the newly installed Program Management Board, which for a while seemed nearly as good.

WhiteIT - So, what is it? - Structure

- WhiteIT „Bündnis gegen Kindesmissbrauch und dessen Darstellung - vor allem in der digitalen Welt“ (which translates as „alliance against child abuse and its depiction - especially in the digital world) is an alliance of more than 30 parties, from
  - Industry (Avira, Computacenter, Fujitsu, IBM, Intel, itWatch, Microsoft, Oracle, Software AG, Symantec)
  - Science (Hasso Plattner Institute, University of Hannover)
  - NGOs (Ärztekammer Niedersachsen, Auerbach Stiftung, BITKOM, eco, fsm, Initiative D21, Innocence in Danger)
  - and (of course) governmental organizations (Ministries, BKA [federal LEA] and LKA [state level LEA])
- It was founded in late 2009 (after #zensursula in Germany)
- It cooperates on projects working against the dissemination and (re-) distribution of Child Exploitation Media (CAM)
- It has a staffed office at the Lower Saxonies Ministry of Interior (WhiteIT-Geschäftstelle)
- It also has a supporting association, the WhiteIT-Supporters.

WhiteIT - So, what is it? - Structure - A deeper Look

- WhiteIT current (official) structure has three major parts
  - The steering committee (Lenkungskreis+) which determines the direction of WhiteIT
  - The program management board, managing the projects initiated by WhiteIT members
  - The White office (Geschäftsstelle) which is meant to coordinate the interaction.
- WhiteIT Supporters is an association of WhiteIT members to organize (financial) support for WhiteIT projects.
- Also there is a Bund-Länder-Projektgruppe (BLPG) „Bundesweite Hashwerte-Datenbank Kinderpornografie“ at the federal BKA (Referat SO12) feeding into WhiteIT (and also being fed back).

WhiteIT - So, what is it? - Steering Committee

Members of the WhiteIT Steering Board (Lenkungskreis+) (besides the Ministry of the Interior of Lower Saxony) are:

- Ärztekammer Niedersachsen
- Avira // Auerbach-Stiftung
- BITKOM
- Computacenter
- Fujitsu
- Initiative D21
- Microsoft
- Oracle
- Software AG
- Symantec

WhiteIT - So, what is it? - WhiteIT Supporters

- WhiteIT-Supporter e.V. has been founded in 2011 in the Lower Saxony's representation to the Federal Government in Berlin, its boards members are:
  - 1st Chairman/1. Vorsitzender: Roland Raschke, Computacenter (WhiteIT-Supporters is registered at their office address)
  - 2nd Chairman/2. Vorsitzender: Volker Klauke, MI Lower Saxony (coordination with state LKA?)
  - Treasurer/Kassenwart: Reinhard Crantz, Intern at MI Lower Saxony (a German Afghanistan veteran)
  - Secretary to the board/Schriftführer: Frank Giessen, Symantec (will talk more about Symantec later on)
  - an additional board member is Thomas Dieckmann, (CDU Lower Saxony)
- WhiteIT-Supporters' role is to enlarge the reach of WhiteIT and to be able to raise money for its Projects.
- The control by the Minister of Interior, Mr Schünemann, who also took part in the founding event, is quite apparent.

WhiteIT - So, what is it? - Its Projects - The better part

- research into the „market“ for Child Abuse Material (by the Leibnitz University of Lower Saxony)
- some preventive measures (help for (potential) abusers - „Kein Täter werden“, Charité [therapy limited to pedophiles])
- improving help for victims (esp. improved networking, by Innocence in Danger and the Auerbach-Stiftung)
- development and implementation of robust hashes for images/videos (Microsoft, IBM, LKA NDS)
- detection tools for child abuse material (CAM) for easing investigating confiscated media
- implementation and integration of databases of child abuse material and it's Meta Data(BKA, LKAs)

WhiteIT - So, what is it? - Its Projects - The scary part

- reporting integrated in client software („jetzt-löschen“-button)
- dedicated interface for processing notice-and-takedown requests, especially with regard to foreign hosting providers (coordination with INHOPE and NCMEC)
- compliance-detection and enforcement in the network and the client (Compliance-Scanner by Avira and Symantec, Scanner for graphics adaptors by itWatch)
- analysis of state and federal legislation with regard to data protection, telecommunication regulation, privacy issues and constitutional rights
- planing of new legislation (interaction with the private sector, but also: covert investigations / verdeckte Ermittlungen [§110a StPO ?V-Männer?])
- planing and guiding the political process leading to the necessary change in legislation

CAMnet - Child Abuse Media Metainformation Network

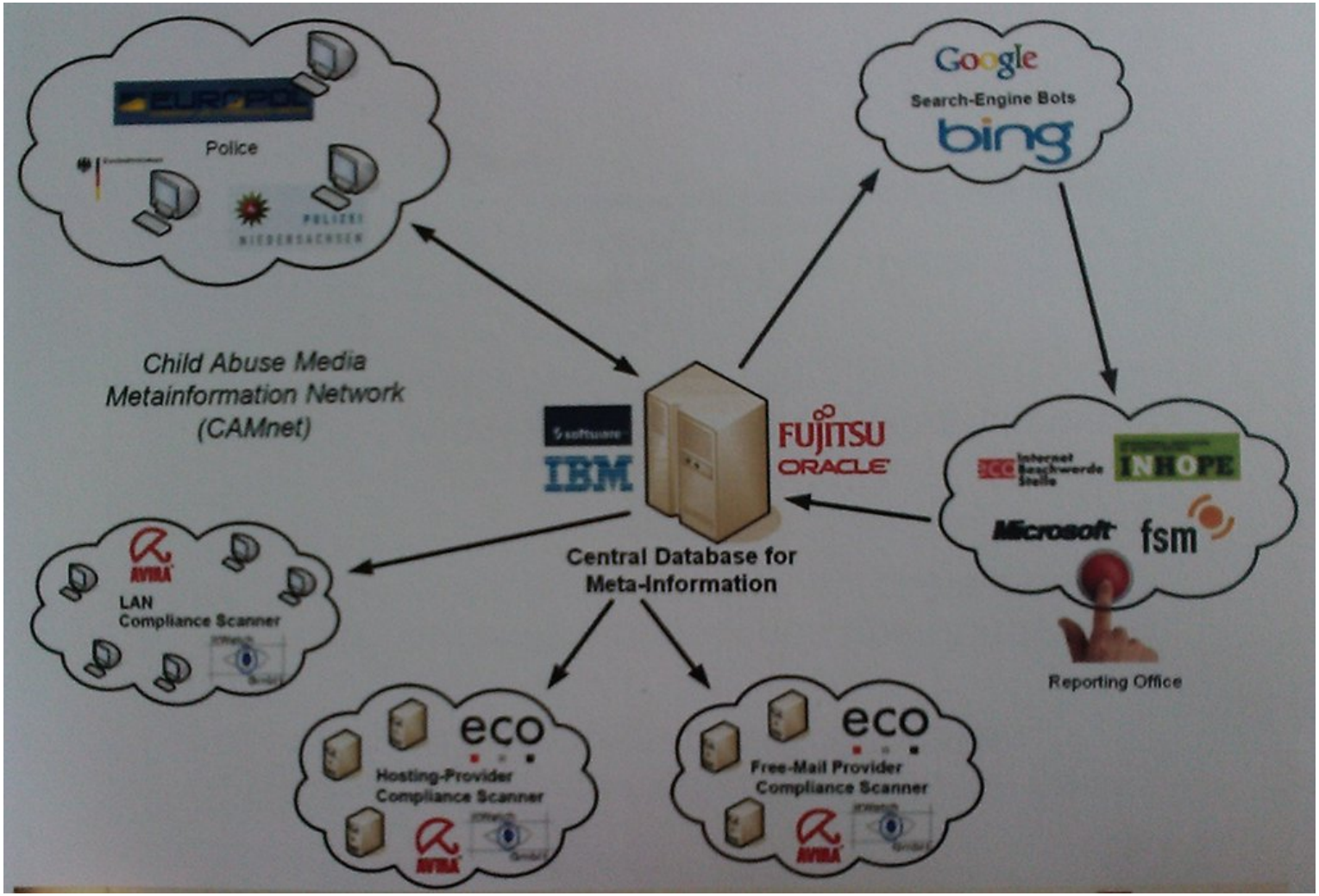

Abbildung: How CAMnet is envisioned

CAMnet - What i think is wrong with that vision

- First and foremost: i am all against throwing around images of children being sexually abused even if done by the police.
- Even more so when the data crosses jurisdictions or is being stored in international databases
- Also i become even more skeptical if metadata is involved A data leak can really compromise a victim permanently.
- Hashes might be less sensitive, though they can be used to find that content if either the database used is large enough (search engine) or one has enough clients to do the search (botnet)
- Additionally i believe it to be wrong to work on measures to scan customer data without the involvement of a larger audience in the discussion.

Spotlight: CAMnet - legal questions

Besides general questions wrt. the legal assessment of hashes and information associated with it, a legal opinion is being sought on:

- whether hashes can be exchanged with EU and non-EU LEA
- whether hashes can be disseminated to interested third parties (AV vendors and search engines for example)
- whether there is the willingness of service-providers to use scanners to search their customers data (email, hosting, cloud, etc) and how this activity by the providers is to be assessed:
  - whether the scanning by the providers violates fundamental rights (esp Art 10, 13 German constitution [Grundgesetz]),
  - and whether changing the providers terms and conditions can accommodate for this fact.
- whether and how unwilling (host-, email-, cloud) providers can be forced to cooperate
- whether and how current legislation has to be changed to accommodate for all of this.

Spotlight: Microsoft / PhotoDNA

- Microsoft has PhotoDNA which is claimed to reliably detect images even when distorted or changed otherwise.
- Facebook implements its content-filtering using PhotoDNA.
- PhotoDNA is based on Research by Digital Forensics expert Prof. Farid of the Darthmouth College.
- Unfortunately this research is under an NDA:
  - To cite Prof. Farid: „The PhotoDNA work has not been published, and we are not releasing the full technical details of this work.“
  - To cite Microsoft: „the PhotoDNA work has not been published. There is quite a bit of information available at http://www.microsoftphotodna.com.“
    (which just redirects to a press kit)

Spotlight: Microsoft / PhotoDNA #2

Not even WhiteIT could get hold of PhotoDNA for evaluation purposes (neither source code nor binary object file nor SaaS)

- Is PhotoDNA as robust as claimed? (an abstract for a poster to be found on the internet makes it look rather heuristic)
- Is Microsoft working on implementing PhotoDNA with a DPI sensor or inside a gateway/router? (as claimed by one of their marketing/sales representatives)

Spotlight: Role BSS BuCET and Arne Schönbohm

- At the 2011 WhiteIT Symposium Arne Schönbohm of German BSS BuCET shared the penal in a discussion with Minister Schünemann and Innocence in Danger.
- Arne Schönbohm (known as son of the former Minister of Interior of Brandenburg) recently came into focus when claiming that Trojan Horses (like the German Staatstrojaner) secure our prosperity and wealth. (**https://blog.fefe.de/?ts=b062f384**)
- BSS BuCET Shared Services AG's commercial focus lies on the Germany security market. It concentrates on clients that have a security-related role. (eg. governmental organizations, non-governmental organizations and companies involved with defense technology and security).

Spotlight: Role BSS BuCET and Arne Schönbohm

From the BSS BuCET web page:
„*We support all kinds of companies from the security sector in relation to increasing their market share or getting involved with security research programmes.*“
„*A further sphere of our activity is advice to various political decision-makers with regard to security strategies.*“

- What is Mr. Schönbohm role in the WhiteIT endeavour?
- Is he advising Minister Schünemann on Data retention // Vorratsdatenspeicherung [now: Mindestspeicherfrist]?
- What other Projects are BSS BuCET Shared Services AG and Mr. Schönbohm working on?

Spotlight: Symantec / Avira / itWatch

- All of these vendors are working on compliance scanners (itWatch even wants to implement it on graphics adaptors).
- On the client this will only work very limited (perhaps in a corporate setting, with limited access to the hardware).
- The situation changes if we talk about scanning customers data as planed with CAMnet (hosting provider, email provider)
- Also scanning network traffic will probably stay be something that only corporations do on there own network-
- Likely once developed this tools will also be pushed into the access providers' backbones.
- But let me single out one company: Symantec.

Spotlight: Symantec

- Symantec ows this favour to the fact that it seems to be WhiteIT's driver for Internationalization (Spain/Netherlands) and also to a talk given at the WhiteIT Symposium 2010.
- Unsing the title „Bestrebungen und technische Realisierbarkeit gegen Missbrauch der Kommunikationsstruktur“ / „efforts and technical realizability against misuse of communication infrastructure“ the lecturer (from Symantec) was asking:
  - „Ist eine technische Zensur in der Demokratie durchsetzbar?“
  - „gehen wir aktiv oder proaktiv gegen Missstände im Netz vor?“
  - „welche Maßnahmen sind im Netz heute realisierbar und wie wird darauf reagiert?“
- and than going on about how new technology is disruptive and how to adapt to it.
- It looks as if they identified social networks as a threat, their solution to it is DLP.

Spotlight: Symantec - Data Loss Prevention

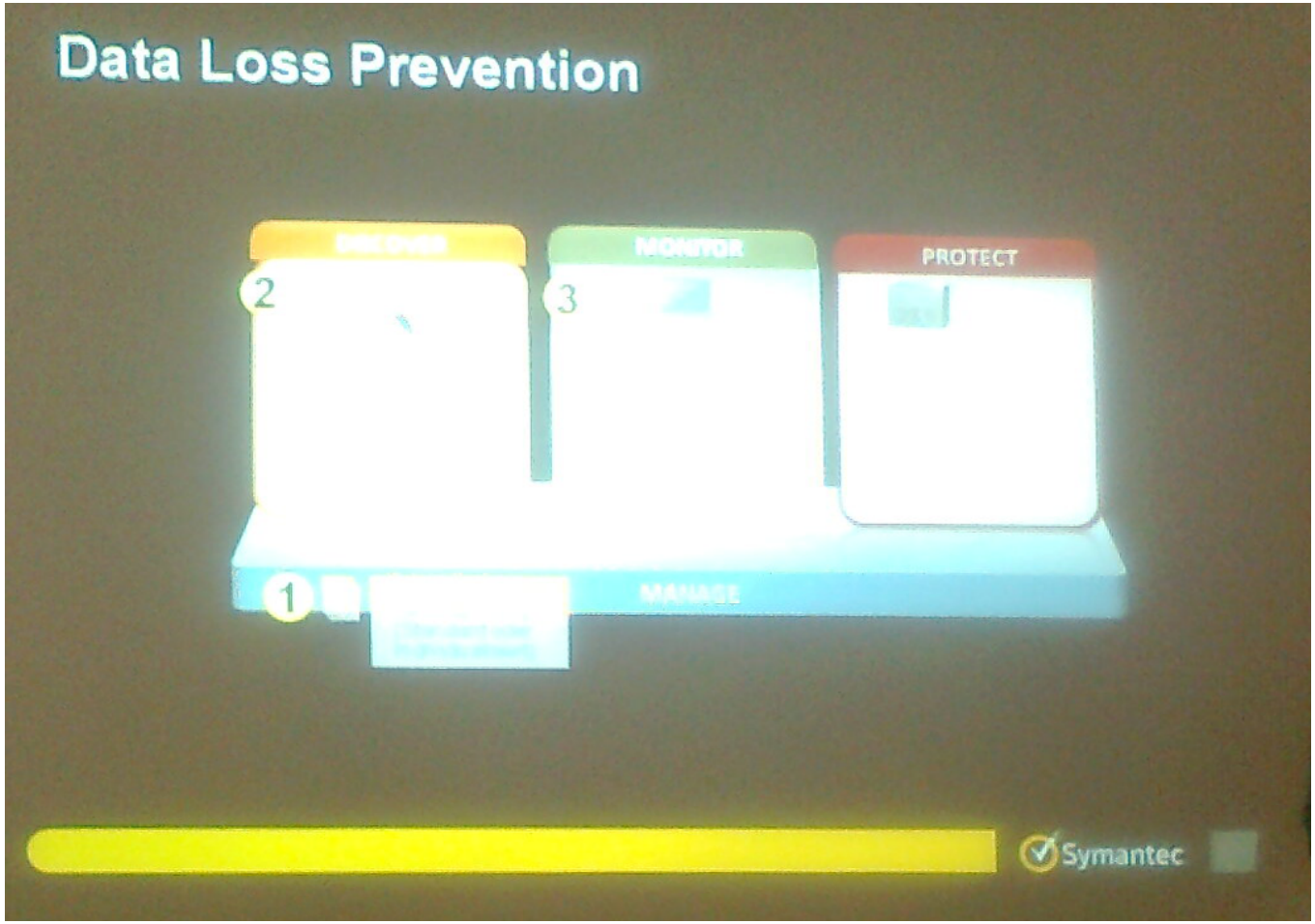

Abbildung: Symantec DLP as advertised in a workshop against the distribution of child abuse material online [Watch the Video if you want to see more :)]

Spotlight: Symantec - Global Intelligence Network

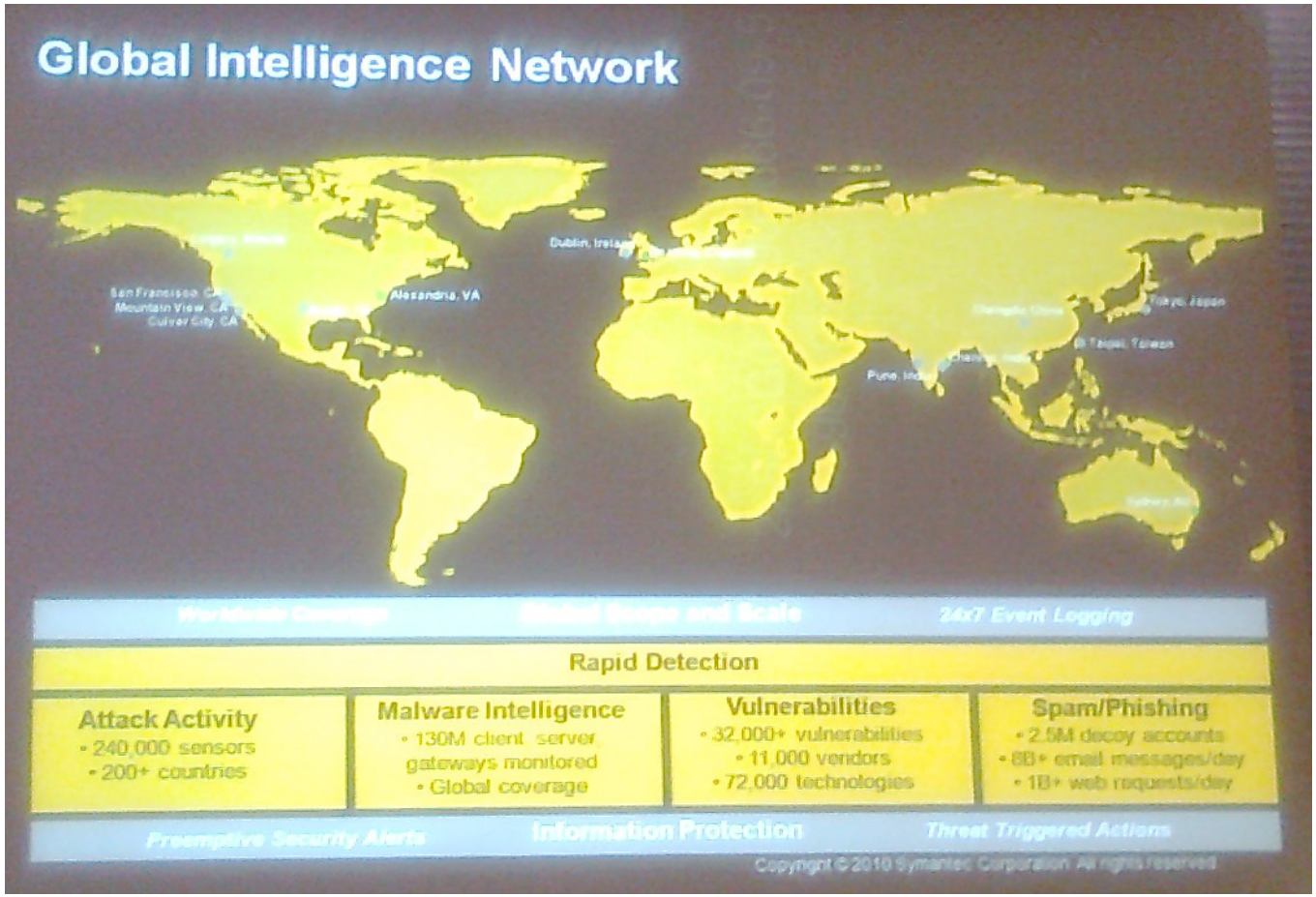

Abbildung: Symantec gets some extra points for mentioning its intelligence capabilities at the same workshop

Spotlight: Symantec - What has DLP to do with CAM?

- So the Talk explicitly refered to child abuse material online while mentioning Data Loss Prevention, Copy Prevention, Ownership Detection and Identity Management.
- But: What does DLP have to do with Child Abuse Material? Similar questions do arise for Copy Prevention, Owner Ship Detection and Identity Management.
- Either the sales representative was completely misguided or Symantec tried to enlarge its market-share by advertising it's technology to governmental organizations for law enforcement.
- I would vote for the second option, why else would the lecturer ask: „What measures are realizable? How is the reaction to them?“

Spotlight: Symantec - Questions raised

So some questions about Norton Symantec's strategy arise:

- Does Norton Symantec work on Deep Packet Inspection technology for law enforcement purposes?
- Since Verisign recently became part of Norton Symantec: Does Verisign hand out certificates to governments to enable their LEA to do active man in the middle on end users?
- Since Norton also bought PGP and GuardianEdge: Can these Software tools still be used by end users without fearing of having key escrew implemented in them?

A quick Outlook - WhiteIT

- WhiteIT tries focus on the new strategy, currently it works on getting a legal assessment on the viability of CAMnet.
- This legal opinion probably will be organized to be favorable to the measures envisioned.
- Even if not turning out to be completely in favor the measures it will point to legislative actions to be taken to allow them.
- But even apart from WhiteIT it looks as if it will get worse very fast soon.

A quick Outlook - Other alliances

At the moment the several movement to control the Internet are gaining enormous momentum.

- For example the digital agenda by commissioner Kroes (who appointed Mr zu Guttenberg as advisor on Internet Freedom) contains a plan "to make the internet a better place for kids"
- The coalition formed by the commission to support that plan has 27 founding members: Apple, BSkyB, BT, Dailymotion, Facebook, Google, Hyves, KPN, Liberty Global, LG Electronics, Mediaset, Microsoft, Netlog, Nintendo, Nokia, Opera Software, Orange, Research In Motion, RTL Group, Samsung, Sulake, Telefonica, Teliasonera, Telenor Group, Tuenti, Vivendi and (not surprisingly) Vodafone.
- Its planed actions include:
  - Easing the reporting of harmful content
  - Wider use of content classification
  - Effective takedown of child abuse material.

Call to Action

The best way
to predict the future
is to shape it!

If you want to help even after this talk

If you want to help with some open source intelligence after this the talk, visit: **http://tinyurl.com/whiteit** and follow the instructions there.

Where can you get involved with the EU's coalition?

- The EU's coalition to make the internet a better place for kids has agreed to work on 5 concrete actions:
  - Simple and robust reporting tools
  - Age appropriate privacy settings
  - Wider use of content classification
  - Wider availability and use of parental controls
  - Effective takedown of child abuse material.
- To get involved with the coalition send an email to: INFSO-SAFERINTERNETCOALITION@ec.europa.eu before the 15th of January 2012.