

## Report Workshop #172

### ***Public-private cooperation on Internet safety/ cybercrime***

#### **Internet Governance Forum 2010 Vilnius**

Wednesday 15 September 2010, 16.30 hr - 18.30 hr (day 2)

*'Public private partnerships: a holistic approach to cross border cybercrime; fighting, information sharing, cooperation and awareness raising in a multi stakeholder environment'*

#### **Provided by:**

The Dutch Ministry of Economic Affairs ,  
Dutch Registry of .nl domains SIDN,  
Dutch Independent platform for the information society ECP-EPN

In collaboration with: Wout de Natris, De Natris Consult

Moderated by: Liesyl Franz, Vice President for Information Security and Global Public Policy, TechAmerica

#### **Introduction:**

The Internet offers us many advantages, but it also has its disadvantages and the safety of the Internet is often at issue.

Cybercrime is an everyday phenomenon and is a threat to people's trust in the Internet, which is a vital condition for a successful and socially responsible implementation of ICT. Moreover, it prevents the Internet from developing worldwide to its full potential. In addition, safety measures against digital threats involves enormous costs for society as a whole. Reason enough for the organizing parties to ask more international attention for the subject of Internet safety/cybercrime. Also we want to work together on more coherence and a wider vision on cybercrime, with the ultimate goal of preventing penal and/or wrongful activities on the web.

How then can we put a stop to cybercrime?

Public-private cooperation, as well as an international approach are essential to fight cybercrime really effectively. Cooperation between policy makers and representatives of the Internet-chain is also necessary. Information sharing, notice and take down, filtering, intellectual property, and the fight against Botnets are important issues in this context. Public-private cooperation is a popular way of working together in The Netherlands. Self regulation is thereby inevitable. Also when it is about the fight against cybercrime in order to make the Internet safer for consumers.

Workshop 172 indicated the need for innovative ways of cooperation between governments and the business community in the fight against cybercrime. It listed the (im)possibilities of such a fight, in view of a series of real-life examples. During this workshop The Netherlands, United Kingdom and Georgia shared their experiences on public-private cooperation with the audience, national and international alliances showcased their method and the importance of this way of working together was illustrated.

The workshop is divided into 2 parts on public-private cooperation as an example for the fight against cybercrime:

- Information exchange between public and private parties on cybercrime threats and best practices fighting cybercrime
- Building trust and cooperation by creating national and international alliances

### The workshop:

#### Information exchange between public and private parties on cybercrime threats and best practices fighting cybercrime

In the first part of the workshop we discussed the importance of public private cooperation in the fight against cybercrime illustrated by best practices from the UK, The Netherlands, and the most recent model from Georgia.



*Alun Michael*, British Labour Co-operative politician and Member of Parliament UK, said that it is important that public and private parties work together on solutions to combat and prevent cybercrime through cooperation and self regulation, thus avoiding the need for new regulation; “laws rarely prevent what they forbid”.

In his view local and national governments should therefore be involved but the industry must be in the lead in this. But they cannot be left to do it alone and you can't leave the private sector and government to do things on their own, parliamentarians should also be involved as well as

governments, he stated. According to Alun Michael public-private partnerships can be successful in this if we get industry to accept the importance of this approach and to recognize that engagement with preventing crime is the price for avoiding the traditional approach of excessive legislation which inhibits the proper exploitation of the internet, in other words, the exploitation by the good guys not just by the criminals.

Tracking down and prosecuting cybercrime? *Annemarie Zielstra*, National Infrastructure against Cybercrime (NICC), The Netherlands, asked. She found it extremely important but not the real solution for the problem. According to her prevention is better. That is why the NICC program has brought together public and private organizations in the National Infrastructure against Cybercrime (NICC). She exemplified that the beating heart of this National Infrastructure the Cybercrime Information Exchange is. Within it, private and public organizations fight against cybercrime side by side. The experience of Annemarie Zielstra shows that starting small and learning by doing works best. Do not try to solve everything at once but see what is working and what is not.



The Georgian model was illustrated by *Rusudan Mikhelidze*, Deputy head of analytical department, Head of research and analysis unit, Ministry of Justice. Georgia just started to develop the appropriate mechanism to tackle cybercrime. Not long time ago, in spite of some experience to investigate cybercrime, constructive dialogue between the law enforcement agencies and internet service providers could not be envisaged, she tells. LEAs/ISPs cooperation is the area which still needs to be developed in Georgia. On 24th of May, 2010 LEAs and ISPs signed Memorandum of Understanding (MoU). Rusudan Mikhelidze discussed the contents of the memorandum as well as

the needs for further detailed regulations of the area and current practice.

*Building trust and cooperation by creating national and international alliances*



*Marietje Schaake*, European Parliament, illustrated in the second part of the workshop her view on the importance of cooperative fight against cybercrime. At first she sees that cybercrime is used as a need to define the problem before looking at the solutions. Is Cyber crime the sales of counterfeit medicine? Or is it is more the use of technologies to commit crimes that are specific in the ICT or digital context? Marietje sees a lack of knowledge still in mapping the problem and calls on to define cybercrime to accurately define the scope and scale of the problem. She also highlighted the need for EU wide thinking on cybercrime. Furthermore Marietje Schaake spoke about how public private partnerships relates to democratic oversight and who is finally

responsible.

*Thomas de Haan*, Ministry of Economic Affairs The Netherlands, and *Roelof Meijer*, SIDN, illustrated 'Building trust and cooperation by creating national and international Alliances' by a Dutch showcase; the creation of "Platform Internet Safety". They explained how private parties and government work together on several projects, e.g. the notice and take down Code of conduct to take down illegal or criminal sites, filtering and blocking sites (child pornography) and combating botnets.



These successful national projects were shown, but in the end this is not enough, international cooperation is needed because of the inherent cross border nature of cybercrime. A case was presented also involving international partnership to combat cybercrime, involving private partners (Microsoft, internet registries') and government agencies (law enforcement) from several countries. The Cyber Crime Working Party (CCWP) an international cooperation in the international fight against cybercrime was illustrated by *Jochem de Ruig*, CFO of RIPE NCC, *Laurent Masson*, Microsoft, *Wout de Natris*, chair CCWP,

De Natris Consult. They highlighted commitment to this initiative from the industry and registry side. They stated that no matter how committed to fighting cyber crime an organization may be, he can not solve the problem alone. It involves others and an across the board approach is inevitable.

During the dialogue, some issues were raised:

- Everyone sees the need for public private cooperation in the fight against cybercrime. But how does this public private cooperation refer to the democratic oversight? How do we deal with transparency, accountability, and democracy?
- ISPs have engaged in the fight against cybercrime, but sometimes authorities tend to stretch the definition of what is clearly illegal to what is "unwanted", a much more subjective criteria.

- It is important to all stakeholders to invest in building trust and demonstrating value in the cooperation between all parties involved: industry, government, parliament, and civil society.
- We need to move from action in isolation to action in collaboration; and we need to move from suspicion to trust.
- Challenges – knowing where to start and creating a legal framework that enabled action; not being passive but proactive; mission creep – definitional and scope issues; and measuring results.
- Need to identify the problem; find solutions in the international community, standardize information requests, and provide training for law enforcement.
- Tracking down and prosecuting is very important but not the real solution for the problem. You have to focus on prevention, including awareness.
- Key success factors of Public Private Partnership are TRUST and ADDED VALUE for all parties involved.
- When asked 'who should pay for this cooperation' it was shown that it works best when the government has a facilitating, stimulating and enhancing role. The role of the private sector is that they are responsible for taking the right measures (85% of the critical infrastructure is in hands of the private sector). They invest in the Public Private Partnership by participating and putting knowledge/expertise into the platform.

Webcasts of all workshops, including workshop #172, and plenary sessions as well as translates and transcriptions can be found at the webcast site of the IGF:  
<http://webcast.intgovforum.org/ondemand/>