EUROPOL

Director

The Hague, 19 June 2009

Mr Jerome Brown
A/g Committee Secretary
Parliament of Australia
House of Representatives
P.O. Box 6021, Parliament House
Canberra ACT 2600
Australia

Dear Mr. Brown,

I am writing in answer to the inquiry you made on behalf of the Standing Committee on Communications into Europol's perspective on cyber crime.

I will attempt to answer your questions from a law enforcement perspective in general and, more specifically, from Europol's perspective.

As you are no doubt aware, Europol's mandate is to combat against serious and organised crime, of which cyber crime is a facet.

Cyber crime, as a phenomenon, is on the rise within Member States (MS) of the EU, especially the exploitation of the internet for illegal gain. Reports from our MS show they are increasingly confronted with e-frauds such as identity theft, on-line banking attacks and auction frauds, based on more complex technical schemes which make use of malicious software and botnets. These offenses are of great interest as the organised groups of diverse origin who are believed to perpetrate these crimes, are actively taking advantage of the contradiction between the borderless internet and our clearly bordered jurisdictions.

Since the nature of these crimes is typical international, the MS expressed the need for cross-border cooperation to deal with issues of evidence gathering and jurisdiction, but also to build a better information position on cyber crime as a whole.

At this moment it is impossible to clearly define the scale of the threat cyber crime poses to our economy and communications infrastructure. With the current levels of information available it is not possible to accurately calculate the damage cyber crime groups actually cause.

It is clear that an enhanced information position is needed; Not just from the practical perspective of aiding the identification and pursuit of the criminal groups responsible for these offences; but also from a policy perspective to enable assessment of the risks to the European electronic and economic infrastructures and set priorities for their mitigation.

Due to the increasing priority MS place on cyber crime, the topic is also a prominent item on the agenda of the European Union. In the Commission communication "towards a general policy on the fight against cyber crime", the Commission already described the many new possibilities cyber crime offers criminals due to the rapid development of internet:

Raamweg 47, The Hague
Postbox 90850
NL - 2509 LW The Hague
☎ 31 (0)70 302 5000
31 (0)70 345 5896

> "a pattern of new criminal activities and attacks against the internet or related infrastructure is clearly visible and legislation and operational law enforcement have difficulties in keeping pace. The intrinsic cross-border character of this new type of crime creates a need for improved cross-border law enforcement cooperation" [1].

Europol, from within its own mandate, and in line with the EU policy to strengthen the fight against cyber crime, has taken several measures to contribute to enhancement of e-security in general and to improve cross-border law enforcement cooperation specifically.

Firstly, at the request of a majority of our MS, Europol has opened an Analysis Work File (AWF)[2] on cyber crime. The aim of this AWF is to support the MS with analysis of internet related organised crime for the purpose of financial gain. In practice the AWF will gather information from on-going investigations in the MS and use this to identify and pursue pan-European and other international groups active in this particular field. Subsequently the base of knowledge about the actual use of malware and botnet driven crime will be improved.

Secondly, Europol is working towards the implementation of the I-CROS (Internet-Crime Reporting Online System) system; a European platform for reporting offences noted on the internet. It is our intention that this work, while still in its infancy, will provide further insight into nature of crime on the internet, including the impact of malicious software, botnets and e-fraud.

We consider these measures as important steps; however they will only partially address the problems arising from cyber crime.

In order to have an effective approach towards combating cyber crime a concerted, global, cooperative effort between law enforcement, industry and other stakeholders is required.

Europol enjoys a strong relationship with our Australian colleagues and, as there are both strategic and an operational information sharing agreements in place between our organisations, I would like to suggest further exploration of the possibilities of cooperation in this area. Our Australian counterparts are welcome to become a member of the cyber crime AWF if they see an operational need to be such.

I wish you all the best with the conducted inquiries and would appreciate it if you could inform us of the outcome.

Yours sincerely,

Rob Wainwright,

Director

---

[1] EC, "The commission communication "towards a general policy on the fight against cyber crime", MEMO/07/199, Brussels, 22 May 2007

[2] An AWF is a project team performing of tasked to provide analytical support member states within a specific crime area.

Raamweg 47, The Hague
Postbox 90850
NL - 2509 LW The Hague
31 (0)70 302 5000
31 (0)70 345 5896