



INTERPOL

The role of INTERPOL in the fight against cyber crime

INTERPOL NCRP for Computer Related Crime



Kenichi TAKAO
Crime Intelligence Officer/IPSG Lyon

E mail: k.takao@interpol.int

Telephone: 0033 472 44 71 37

Fax. 0033 472 44 72 21

3rd Facilitation Meeting for WSIS Action Line C5
Geneva 23 May 2008



INTERPOL

Presentation Topics

1, What is I24/7 communication System

2, What is NCRP

3, Current Situation

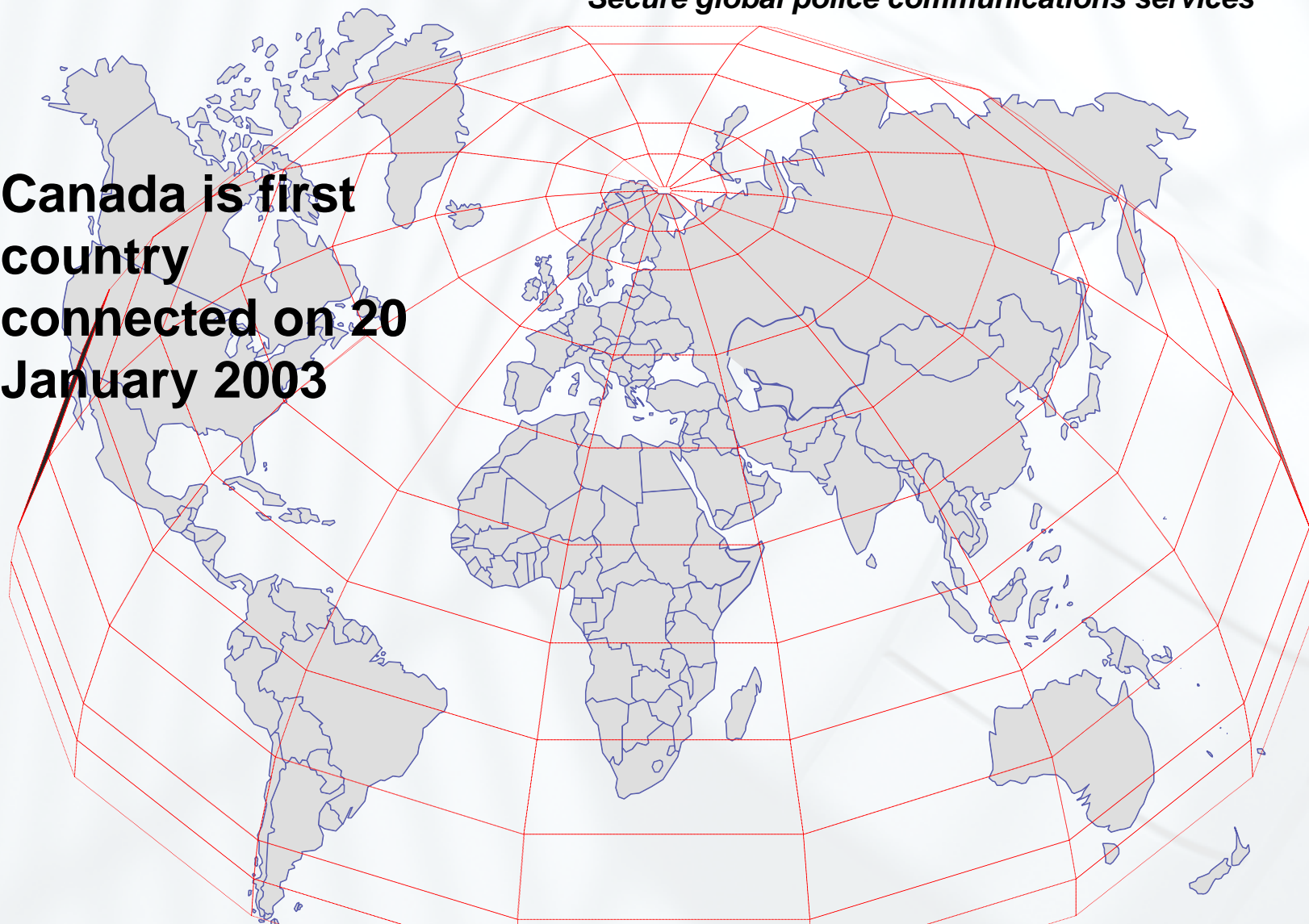
4, Usage of NCRP



1, I-24/7 communications system

Secure global police communications services

**Canada is first
country
connected on 20
January 2003**



All member countries are connected now

INTERPOL



INTERPOL

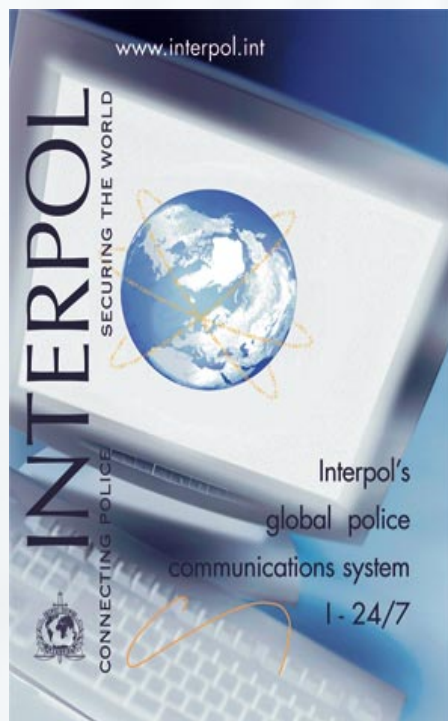
1, I-24/7 communications system

Architectures of I-24/7

Connecting police, securing the world

➤ High-security global police network

- VPN
- 3DES





INTERPOL

2, What is NCRP

NCRP

G8-24/7

Interpol National Central Reference Points for computer-related crime

Computer-related crime is gaining importance in our society: statistics indicate that there has been an enormous increase in the volume of such crime. The situation has given rise to considerable public concern because every computer user is a potential victim and the results can have extremely serious consequences, especially for commerce and industry where financial losses can be substantial. There is, therefore, a need to encourage the exchange of information within the framework of Interpol.

At the Interpol Cyber Crime Conference in Cairo in 2005 delegates requested in the conference resolution to encourage member countries to implement the Convention on Cyber Crime by the Council of Europe. At the General Assembly in Rio de Janeiro in 2006 it was also recommended that the Convention should be implemented by member countries. According to Article 35 of the Convention signature countries have to provide a 24/7 reference point with equipped and trained personnel.

To ensure that the information exchanged through the appropriate Interpol channels reaches the specialized police units with the least possible delay, a list of National Central Reference Points (NCRPs) for computer-related crime has been compiled. To date, 111 Contact Points have designated such National Central Reference Points. The list is given below.

The NCRPs are an essential prerequisite for the establishment of the early warning system. It is intended that messages will be forwarded via the appropriate National Central Bureaux. However, in order to minimize delays, the unit to be informed in each receiving country should always be specified in each message.



24-Hour Contacts for International High-Tech Crime

August 2007

A Product of the G8 Subgroup on High-Tech Crime



COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

COE

Article 35 of Cyber Crime Convention



INTERPOL

2, What is NCRP

Formal Name

INTERPOL National Central Reference Points
for Computer-Related Crime

Feature

Early warning system between IT Crime Investigation units

Purpose

To provide the secure and appropriate INTERPOL channels
To utilize for specialized IT crime investigation units
To exchange Information in minimum delays

Reminder: Principle of INTERPOL...

To Contact via **I24/7 Network** designated network of INTERPOL



INTERPOL

3, Current Situation

In a word

to ensure that the information exchange through the appropriate Interpol channels reaches the specialized police units with the least possible delay on a 24 hour 7day a week

Currently

120

reference points

On 15 March 2008



INTERPOL

The list of INTERPOL NCRP

On 15 March 2008

Available contact point (24hours/7days) **81** countries

Available 24/7 contact point (Not 24/7) **39** countries

* 185 countries/regions are connected to “I-24/7” communication system.

INDIA	
Organization/unit	Cyber Crime Investigation Cell, Central Bureau of Investigation, INDIA
Working Languages	English
Contact Person	Mr. XXXXX, SUPDT of Police Mr. XXXXX, DY SUPDT of Police
Phone No.	+91 11 2436 XXXX / +91 11 2436 XXXX
24/7 Phone No.	+91 11 2436 XXXX
Fax No.	+91 11 2436 XXXX
E-mail	xxxxxxxxxx@cbi.gov.in
Address	XXXXXXXXXXXXXXXXXXXX, Lodhi Road, New Delhi-110 003



INTERPOL

3, Current Situation: Remind

Purpose

To provide the secure and appropriate INTERPOL channels
To utilize for specialized IT crime investigation units

To ensure

NCRP is distributed **ONLY** through INTERPOL channels

To Get

Access **INTERPOL Secure Website**
Ask **FHT/HTC** directly

Data in NCRP are updated **ONLY** informed through
INTERPOL channels

To Update

Send new **DATA** to **IPSG** through **I24/7**



INTERPOL

4, Usage of NCRP

NCRP exists For Operation assistance

i.e of conversation.....

Now DDoS attack is detected by our Firewall and IDS and IP123.123.23.2 is targeted by allegedly IP 23.54.23.23. By WHOIS and nslookup it is located XX city in your country and it seems of Bot master so I Call you to contact ISP to stop the correspondence from this IP and ask them to preserve Logs of servers. For your information by Traceroot info one of its attacks depart comes from XXX so it maybe sent by Proxy therefore.....

Who can correspond ?

Only IT Crime unit

Besides,
Evidence would disappear by one click.

Ask first

formal procedure later (but definitely)



INTERPOL

INTERPOL Secure Website



<https://www.interpol.int>
<http://i247.ip>

- NCRP
- IT Crime Manual
- Project reports
- Minutes of the meetings etc.

Need ID & Password
Already extended to each NCB

Information Technology Crime



INTERPOL

Contact in charge of NCRP

Kenichi TAKAO
Crime Intelligence Officer
Interpol IPSG – FHT
(Financial and High Tech Crime Sub-Directorate)
200, quai Charles de Gaulle
F-69006 Lyon

Email: k.takao@interpol.int

Tel: +33 472447137

Fax: +33 472447221