INTERPOL

SPEECH • DISCOURS • DISCURSO • خطابات

LECTURE

by

Ronald K. NOBLE

Secretary General

D.P. KOHLI MEMORIAL LECTURE

MULTIJURISDICTIONAL INVESTIGATION: OPERATION UNMASK

30 March 2012

New Delhi, India

Mr Shri V. NARAYANASAMY, Member of Parliament and Minister of State in the Prime Minister's Office,

Mr A.P. SINGH, Director of India's Criminal Bureau of Investigation,

Dear Distinguished Former Directors of CBI,

Dear Honoured Guests

Dear Colleagues,

Ladies and gentlemen,

Namaste.

It is a great pleasure for me to be here in the magnificent city of New Delhi.

One can only be impressed when setting foot in this two millennia-old mega-city that, like its famous 'Iron Pillar', stands as a symbol of India's perennial history and glory.

I am deeply honoured to have been invited to speak at the occasion of this 13th D.P. KOHLI Memorial Lecture and to celebrate with you the 49th anniversary of India's celebrated Criminal Bureau of Investigation.

I would like to extend my gratitude to India's Criminal Bureau of Investigation more commonly known as CBI, and in particular to my dear friend, CBI Director A.P. SINGH, for having invited me to speak at this prestigious event.

I would also like to thank Indian authorities and the Indian people for the warmth and kindness that you show me during each of my visits to this great country.

D.P. KOHLI is someone whose impact lives on today in the CBI and thus in India.

While reading about him, I was struck by what he told delegates at the inauguration of the 4th Biennial Joint Conference of the CBI and State Anti-Corruption Officers.

I quote him: "The public expects the highest standard from you both in efficiency and integrity. That faith has to be sustained. The motto of the CBI — Industry, Impartiality and Integrity — these must always guide your work. Loyalty to duty must come first, everywhere at all times and in all circumstances."

With his belief in the importance of « duty, » foremost in our minds, D.P. Kohli would expect us to take a moment to pay tribute to the 12 policemen killed on Tuesday in a cold blooded Naxalite attack in the state of Maharashtra. These policemen paid the ultimate price while on duty working for the benefit of Indian citizens. Their sacrifice and commitment honours them and police around the world who each and everyday leave their homes to protect us, not knowing if they will return at the end of their work day safe and sound to be with their families.

Today, we once again honour D.P. Kohli, this great founding Director of India's CBI. His words that I just quoted must remind you that your D.P. Kohli was a true visionary and dedicated to the highest standards in terms of efficiency and integrity.

I humbly submit that were he with us today, he would continue to be proud of the CBI he helped to create. I can say in all sincerity that when police around the world speak the name CBI, they do so with the highest of esteem and respect for you and your work.

But, INTERPOL always seeks to find out a little more about the person we honour. Little details of his career that might have gone unnoticed. We discovered that it was D.P. KOHLI who took the initiative to create an INTERPOL Division within the then-Delhi Special Police Establishment prior to the creation of the CBI, and it is this former INTERPOL Division that became the INTERPOL National Central Bureau for India.

The fact that the founding Director of the CBI was also a strong promoter of international police cooperation makes it an even greater privilege for me to deliver these remarks at the 13th D.P. Kohli Memorial Lecture in honour both of his memory and the creation of the CBI.

***

Introducing “Multi-jurisdictional investigations : Operation Unmask”, which is the name given to recent cybercrime investigation conducted by several INTERPOL member countries and by INTERPOL Headquarters targeting a group of hackers operating under the name Anonymous.

Let me begin by focusing on the word « multi-jurisdictional. » As the world’s largest law enforcement organization with 190 member countries, virtually everything that we do is multi-jurisdictional. For INTERPOL the word multi-jurisdictional can be seen as an disadvantage or advantage.

Being involved in a « multi-jurisdictional » matters poses disadvantages for member countries that can only investigate or prosecute a particular case using legal documents from countries with the exact or similar legal framework. An example of this would be the European Arrest Warrant. It has no legal value outside the European Union ; so the EU can’t expect countries outside the EU to honour it. So, it is a disadvantage for EU countries to use the European Arrest Warrant to get someone arrested outside the EU.

Being a part of a multi-jurisdictional organization whose membership embraces the entire world could be seen as an advantage for EU member states. If the EU were, for example, to combine the European Arrest Warrant with an INTERPOL Red Notice or wanted person’s notice which can be issued to all of INTERPOL’s 190 member countries, then the « multi-jurisdictional » option provided by INTERPOL could be considered an advantage.

I begin with the concept of multi-jurisdictional because it reflects the real world advantages and disadvantages that INTERPOL confronts and must navigate around each and every day. INTERPOL cannot wait for the creation of an ideal and universally harmonious legal framework for international police cooperation at the global level because transnational criminals won’t wait. Their goal is to commit crimes, serious crimes, especially where gaps in legal systems or frameworks make it more difficult for law enforcement to prevent, investigate or prosecute crimes.

Helping member countries to overcome multi-jurisdictional obstacles to permit police to cooperate across borders to prevent, investigate and prosecute serious international crime is therefore really at the core of INTERPOL's work.

Many in the room know about INTERPOL from what you've seen in the movies, read about in novels or news stories or experienced in the one or two cases involving INTERPOL in which you worked on years ago?

So, let me take a few minutes to tell you about the INTERPOL of the 21st Century and to tell you what INTERPOL is not.

As I just said, INTERPOL is the world's largest police organization with 190 member countries. Using the concept of legal framework, I gave you an example to show you how INTERPOL's mission is to enhance international police cooperation — to help member countries avoid legal obstacles to police cooperation across borders.

Let me now approach the issue of multi-jurisdictional cooperation from a technical perspective. INTERPOL facilitates the widest possible mutual assistance between all criminal law enforcement authorities by providing member countries with the technical means whereby they can share or exchange information.

How ?

We ensure that police services can communicate securely with each other around the world;

We enable global access to police data and information;

We provide operational support on specific priority crime areas and;

We foster continuous improvement in the capacity of police to prevent and fight crime.

But, what are we not ?

We are not a police agency with the legal power to detain or arrest anyone.

We are not a police agency with the legal power to execute search warrants.

We are not a police agency that conducts criminal investigations in our member countries.

We are not a police agency that has armed agents who travel internationally shooting people in highly entertaining Hollywood or Bollywood gunfights.

INTERPOL is strong and essential to the safety and security of citizens around the world, not because of the powers we don't have, but because of the powers that our member countries police agencies have and because of the information that we help them access and share worldwide.

Since our strength resides in the information that we obtain and help our member countries share worldwide, it should be clear that our sovereign member countries decide what information to enter in our databases ; to leave in our databases and to exchange using INTERPOL channels.

The sovereignty of each and everyone of our member countries must be and is constantly respected by INTERPOL.

Since our sovereign member countries frequently have disputes between them, INTERPOL must remain politically neutral to survive. Our neutrality is enshrined in Article 3 of our Constitution, which does not allow us to undertake any activities of a predominantly political, military, religious or racial character.

What is more Article 2 of our Constitution recognizes the Universal Declaration of Human Rights.

With the concept of "multi-jurisdictional cooperation" explained from a legal and technical perspective, let me give you a couple of concrete examples that demonstrate how INTERPOL and its member countries work across legal and geographic borders each and every day.

I have travelled to 152 member countries as INTERPOL Secretary General, and in each and every country, they have one important concern : They don't want criminals crossing their borders to harm their citizens and they don't want criminals to escape prosecution by crossing country borders.

INTERPOL and its member countries know that criminals often cross borders using stolen or fraudulently altered passports of identity documents. We know this fact to be especially true for terrorists.

To help countries prevent this criminal conduct, INTERPOL built the world's largest database containing stolen and lost travel documents. We grew that database from a few thousand in 2003 to over 32 million as of last year.

We grew it from 12 participating countries to almost to more than 150 participating countries.

We overcame the legal obstacles of some of our member countries concerning data protection and the privacy of their citizens by designing our database in a way that does NOT include the personal data of citizens. Let me repeat — our Stolen and Lost Travel Document database contains no personal data — no names, no dates of birth, no place of birth, no photographs. No personal data !

Then, how did we make it valuable ?

We requested member countries to provide us only with the passport or identity card number and date of issue.

That is how, as a legal matter, we got 162 member countries to be able to participate by entering the numbers of 32 million travel documents while remaining in compliance with their national laws.

Then came the technical part.

Thanks to a technology designed by INTERPOL, border police and police anywhere in one of our member countries' territory can check the passport of any person wanting to cross the

border against INTERPOL's Stolen and Lost Travel Document database with a single swipe of a document through an optic reader.

In 2 to 3 seconds, the police or border control officer sees a red light signalling hit which means registered as lost or stolen in INTERPOL's database or a green light signalling that the passport number in question is unknown or not in INTERPOL's database.

It was exactly this INTERPOL technology that was used last year during the 2011 Cricket World Cup in India, Sri Lanka and Bangladesh. Just during the time of the competition, the record number of 2.8 million checks were conducted across the three countries, generating 150 red light hit alarms.

Using this INTERPOL cooperative system, India's Police as well as the police from the other host countries instantly benefited from the assistance of police from 161 countries.

This is my first concrete example of how a multi-jurisdictional sharing or exchange of police information can work legally and technically.

My second example concerns online child sexual abuse that allegedly occurred in Kerala State right here in India.

In the course of 2011, India's INTERPOL National Central Bureau here in New Delhi, which as you know is housed in the CBI and headed by my dear friend A.P. Singh, received information from the INTERPOL National Central Bureau of Luxembourg, in the heart of Europe, concerning individuals in Kerala State who were believed to be searching child sexual exploitation websites.

Under Luxembourg's national laws, it could share the information that its police uncovered such as the names, IP addresses and full postal addresses of persons believed to be from Kerala State with INTERPOL's National Central Bureau in New Delhi.

Once this information was in the databases of an Indian police agency, in this case the CBI, it could be passed on to the Cyber Police of the State of Kerala in compliance with India's sovereign laws. The police in the State of Kerala conducted an investigation over several

months and, this past October, arrested twenty individuals, who were charged with regularly frequenting child sexual exploitation websites on the Internet.

Let me commend India's Criminal Bureau of Investigation, the INTERPOL National Central Bureaus for Luxembourg and India, and the Kerala State Police for their collaboration and participation in such an important case.

At INTERPOL, we don't consider images of children being raped or sexually abused as child pornography, we consider them to be crime scene images – sex crime scene images.

Thanks to this powerful multi-jurisdictional cooperation, Indian citizens — and in particular children —, are safer and child sex offenders are where they belong …in prison.

The arrests made by the Kerala State Police were made possible because of two key factors:

First, INTERPOL's communication channels allowed the INTERPOL National Central Bureau (NCB) of Luxembourg to share solid actionable intelligence with INTERPOL NCB New Delhi.

In particular, the Luxembourg Police had mounted two operations — "Operation Hidden" and "Operation Carole" — targeting online child sexual exploitation and carefully extracted and analysed data, which they then shared with concerned authorities, including India's CBI.

Second, India had laws that enabled police to act on cases involving images of children being sexually exploited.

I can only congratulate India for having implemented one of the most advanced legislations regarding online child sexual abuse.

In India, the fact that watching online child pornography is a non-bailable offence changes the rules of the game. In most countries around the world, charges can be put against consumers of child pornography only when they are found in possession of explicit pictures.

It is this innovative legislation that allowed the Kerala State Police to act.

There is, of course, nothing revolutionary in the fact that police collaborate even across borders using the internet where their laws permit to identify, locate and apprehend sex offenders and rescue children being sexually abused.

Now, let's turn to cyber-crime where the target is digital — not human —, where the target is the Internet itself and the ability of governments, organizations or businesses to continue to stay online or to continue Internet operations.

When it comes to combating these types of cyber criminals, which include groups like Anonymous, we are at the very beginning of the road.

Few countries today have the capacity to mount such operations and to fully exploit its results.

Few countries have the power to force Internet service providers based in other countries to provide them with information or to shut them down.

Global web-based services are governed by local laws. As a result, any official request for data by foreign investigators requires the use of traditional letters rogatory that will take between six to twelve month to follow suit.

In the Kerala case, the servers, which are not based in India, containing the abuse images are still up and innocent children are still being abused.

And here it becomes very difficult.

Indeed data in cases like the Kerala State case is likely scattered around the world, fragmented in various servers in dozens of different countries with just as many sets of laws.

Not only is building a case in such circumstances extremely difficult and labour intensive, but it faces a series of legal obstacles that discourages most police services.

The current situation sees a dramatic discrepancy between the immediacy of Internet communications and the long and tenuous processes in place to fight cybercrime internationally.

With all of the above obstacles in mind, it reminds me of an image of a police officer armed with nothing more than a whistle trying to stop a speeding car.

The fight is uneven.

It is no wonder then that only an infinitely small percentage of cyber crimes actually get investigated.

To make things even worse, in more countries than we may think, cybercrime does not even legally exist! Internet-based fraud, for example, is then dealt with using standard fraud laws, which results in huge obstacles in legally obtaining and sharing such information as IP addresses and connection logs.

Police officers combatting cybercrime usually agree on one thing: inadequate legislations — with the lack of resources — is the one major obstacle that impedes their success.

Even though a real breakthrough in fighting cybercrime might only be possible when a substantial number of countries will have updated their legislation and when more countries devote the resources for police to develop greater technical expertise, INTERPOL and the world can’t wait for such an idyllic situation.

That is why INTERPOL is working with its member countries to devise innovative approaches against cybercriminals.

There won’t be any magic solution, but rather a combination of innovative tactics that will need to be backed by firm resolve from all concerned.

One good example is Operation Unmask, targeting the infamous hacker group Anonymous.

Let me quote from a recent article : « Anonymous has previously stated its intentions to shut down the Internet on Saturday, March 31st, as a form of protest. “To protest SOPA, Wallstreet, our irresponsible leaders and the beloved bankers who are starving the world for their own selfish needs out of sheer sadistic fun, on March 31, Anonymous will shut the Internet down,” the group stated last month. “Remember, this is a protest, we are not trying to ‘kill’ the Internet we are only temporarily shutting it down where it hurts the most.” Operation Global Blackout 2012 looks to shut down the Internet by disabling its core DNS servers, thus making websites inaccessible. »

Can you imagine the harm that could be caused if Anonymous succeeded in their goal ? They make these threats because they believe that they are beyond the reach of law enforcement. This is why INTERPOL launched Operation Unmask. To unmask these cyber criminals who believe that they are above the law.

Operation Unmask originated from a meeting of an INTERPOL Regional Working Group of Experts on IT Crime.

Colombia, Chile and Spain had already launched investigations against Anonymous after the group had claimed responsibility for denial of service attacks against websites of public and private entities, including the Colombian Ministry of Defence, the Colombian Presidency, the National Library of Chile, an electric company based in Chile, the Spanish Police, Spanish political parties, and a Spanish bank.

Several countries across the region showed interest, as they believed they also had been victims of attacks by Anonymous. So it was decided to organize an operational meeting, during which participants from across the region shared information on Anonymous and assessed the attacks allegedly launched by the hacker group. During the meeting, links could be made to machines and individuals located in several South American countries but also in Europe.

Then, to overcome some of the legal hurdles to a proper international investigation, we decided to directly involve the prosecutors in the concerned countries to ensure that the available proofs would be admissible in court. This allowed for the shared information to be included in the ongoing investigations.

The cases went forward and led in late February to the arrest of 25 alleged members of Anonymous, aged 17 to 40, in Argentina, Chile, Colombia and Spain,

Some 250 items of IT equipment and mobile phones were also seized during searches of 40 premises across 15 cities, as well as payment cards and cash, as part of a continuing investigation into the funding of illegal activities carried out by the suspected hackers.

A second phase of Operation Unmask was carried out this past week-end in the Dominican Republic. Six additional persons between the ages of 17 or 23 were arrested by the Dominican Police.

Overall, 31 persons have been arrested since the launch of Operation Unmask. But what has been accomplished by INTERPOL and police in the member countries involved goes well beyond those arrests.

Anonymous now knows that its members and supporters can be unmasked. And without being secure in being able to maintain their anonymity, Anonymous becomes a weakened idea and entity.

Anonymous was taken aback by the success of the operation and engaged in a massive retaliation against INTERPOL.

Calls were made on Anonymous forums to attack INTERPOL.

On 28 February, a global wave of cyber-attacks was launched on our IT systems by Anonymous and its supporters.

At its peak, the wave reached 400,000 attacks per minute, with thousands of machines mobilized around the world following an Internet posting by Anonymous. Internet users were given tools to shield their identity and told to follow the instructions in a handbook created by Anonymous. They had one and only one purpose in mind — shutting down INTERPOL's systems.

The attacks failed and at no time was the integrity of INTERPOL's databases or their content compromised, nor was our member countries' capacity to share information or access our databases via I-24/7 hindered.

Just a couple days ago, as another means of retaliation, my own parents' home address and phone number were published by Anonymous on publicly-accessible websites. This tells us in what kind of mindset are people who believe they are sheltered by the Internet's anonymity. This may only be the work of some foolish idle teenager but, as it is often the case with the Internet, the consequences in the real world might escape those who think they play some kind of game in the virtual world.

Based on their most recent threat of shutting down the Internet tomorrow, we can see that our resolve to take down Anonymous and to continue to unmask them around the world must continue. We can't allow them to continue to threaten our institutions, us or even our families. We will be waging this fight for years to come.

Despite the success in unmasking some of Anonymous' members, there were also shortcomings.

I can tell you today that, out of the several countries in Latin America who believed they had been targeted by Anonymous and wished to take part in Operation Unmask, one could not due to legal difficulties — the denial of service attacks they were facing were not actually crimes in their country.

This brings us back to the difficulties of multi-jurisdictional investigations.

INTERPOL will continue to try to find ways to fill the gaps that exist in many countries' national legislations by finding countries where those gaps do not exist, but I nonetheless believe that we must urgently take stock of the risks we incur if many countries do not bridge the legal gaps in investigating and prosecuting cyber crimes internationally.

There are approximately 2.3 billion internet users in the world today. But with the proliferation of tablets, mobile phones, connected appliances and other smart machines,

internet connectivity will grow exponentially in the years to come, and so will the threat posed by cybercrime.

This threat and risk to us all are just around the corner and, frankly, I don't think we are prepared as a world community to recognize the scope and magnitude of it.

According to a study conducted by leading internet security company Symantec, the global cost of cybercrime already reaches an enormous 388 billion USD per year — almost five times the global cocaine market —, making more than one million victim a day around the world.

A country like India, whose booming economy relies in great part on its IT infrastructure and industry, is among the countries with the highest interest in engaging the world community on this issue.

But there is even something of greater concern — cybercrime is endangering the very security of nations.

Terrorists of the cyber age can now make use of advanced technologies in the logistics of their attacks, like the Mumbai attacks' terrorists who used Blackberry encrypted communications to coordinate their attacks.

Terrorists can also directly target digital infrastructures, such as financial online infrastructures, power grids, air traffic systems and even nuclear installations, which have all already been targeted and compromised.

Dear colleagues, dear friends,

In order to face the challenges posed by cybercrime, the world needs more agencies like India's CBI and their visionary leaders, beginning with D.P. KOHLI and continuing with the current CBI Director A.P. SINGH, to lead the international law enforcement and justice communities in the fight against this threat.

The mountain may appear a steep one to climb, but INTERPOL and the global community have shown before that it could come together to address serious security threats.

It is my belief with the inspiration of D.P. Kohli behind us and the CBI and INTERPOL member countries working together, we can scale this steep mountain together in order to make the world safe from the threats of Anonymous and other cyber criminals around the world.

Thank you very much.