INTERPOL

SPEECH • DISCOURS • DISCURSO • خطابات

OPENING ADDRESS

by

Ronald K. Noble

INTERPOL Secretary General

1st INTERPOL Information Security Conference

15 September – 9:05-9:20

Hong Kong Police Headquarters

Hong Kong, China

Commissioner of Police of Hong Kong Special Administrative Region, Mr King-shing TANG,

Deputy Commissioner of Police of Hong Kong Special Administrative Region, Mr Andy TSANG,

INTERPOL Director for Information Systems and Technology, Mr Noboru NAKATANI,

Dear colleagues,

Ladies and gentlemen,

Good morning.

It is a pleasure to be here with you in the wonderful city of Hong Kong to open this 1st INTERPOL Information Security Conference.

I'm very impressed to see that nearly 300 participants from 56 countries have gathered here for this event, including law enforcement personnel, members of the public and private sectors, academia, and representatives of international organizations. I would like to thank you all for your presence at this INTERPOL conference.

I would also like to thank Hong Kong authorities for organizing and hosting this conference with the professionalism and kindness Hongkongers are known for. I have had the chance to visit Hong Kong several times and I am always amazed by the fantastic energy emanating from this place. I am convinced that it will inspire us all throughout these three days.

And what better place than a city that has built its prosperity on a technology-based knowledge economy to discuss the protection of the information and communication infrastructure that is at the very basis of modern economies?

For advanced economies like Hong Kong, but increasingly also for emerging economies all over the world, the protection of information and communication infrastructures has taken critical importance.

Our world is increasingly connected and networked and therefore also increasingly vulnerable to disruptions caused by intrusions and cyber attacks. I am not just talking about today's 2 billion internet users, but also about what we call the "internet of things", that is, the 35 billion devices that are connected to the internet and access real-time data.

And this number will only grow bigger. According to Cisco's Chief Futurist Dave Evans, there is a potential of over a trillion devices with network potential, including cars, home appliances and tags for livestock and pets. If you apply Metcalfe's Law, the value is not the 35 Billion devices, but the networked effect of those connections. Metcalfe's Law, which was established by George Gilder and Robert Metcalfe in 1993 states that the value of a network is the square of the number of connected users (n^2). That was their original Internet view: Imagine the effect of the network today with 35 billion connections squared — mind blowing numbers. For those who are math challenged, like me, that is 1.2 times 10^{21}. Clearly, that is a lot of value.

In other words, the scope of what needs to be protected, which today spans from email to mobile phones, digital cable to airplane navigation, online shopping to medical records, is likely to considerably expand in the years to come. Tomorrow's world would then become what Evans call a "thinking planet", a gigantic web of interconnected individuals and devices in which our growing dependence upon connected technology will give cyber criminals a much greater potential for high-impact attacks. Therefore, INTERPOL, NCBs and Police agencies must apply and utilize our tools and devices to increase our value in the fight against criminals.

Crimes such as identity theft and denials of service already cause significant harm to individuals and businesses. Earlier this year I attended the World Economic Forum in Davos, where McAfee's CEO revealed a study estimating that data theft and breaches from cybercrime may have cost businesses as much as $1 trillion globally in lost intellectual property and expenditures for repairing the damage for 2008 alone.

But just imagine the dramatic consequences of a successful attack on, let's say, a country's electricity grid or banking system. The value potential created by the network is exposed to an equal potential for value destruction.

And we all know this is no science fiction. You all recall the famous Titan Rain attacks against U.S. computer systems starting back in 2003, as well as the 2007 cyber attacks on Estonia, also referred to as Web War One

The magazine *The Economist* even describes cyber warfare as "the fifth domain of warfare, after land, sea, air and space". In fact, one of our partners briefed NATO on this threat as early as 2001.

But with one big difference though — because they rely not so much on technology but on expert knowledge, cyber weapons are virtually costless and can therefore be developed by any country, criminal group or terrorist organization.

Indeed, we have been lucky so far that terrorists did not — at least successfully! — launch cyber attacks. One may wonder whether this is a matter of "style" — terrorists may prefer the mass media coverage of destroyed commuter trains to the anonymous collapse of a banking system. But until when?

What is certain, though, is that cybercrime is emerging as a very concrete threat. Considering the anonymity of cyberspace, it may in fact be one of the most dangerous criminal threats ever.

As a result, countries increasingly realize that their digital infrastructure is a true strategic national asset and decide to engage significant means to protect it.

***

INTERPOL, as the world's largest international police organization, obviously has a high interest in protecting its own information systems.

Because INTERPOL handles sensitive information shared by our 188 member countries, we have the obligation to put every measure in place to ensure that no information is accessed by unauthorized personnel or by individuals outside of the Organization.

INTERPOL is a very IT-driven organization and, as a result, information security goes much beyond simply protecting the data stored in our criminal databases.

One of our strategic priorities is to provide our member countries with a secure global communication network. This system, that we call I-24/7, enables police in our 188 member countries to exchange sensitive information, including names, photos, fingerprints, and DNA, with any other country or with the INTERPOL General Secretariat 24 hours a day and 7 days a week.

This same system is also used to bring criminal data to frontline officers in the field. For example, 53 of our member countries have installed a system called MIND/FIND that enables border officers to systematically scan incoming travellers' documents against our database of stolen and lost travel documents. In a country like the UK, this system generates more than 1.3 million queries per month and plays a significant role in protecting borders.

INTERPOL also hosts a child sexual exploitation database that enables experts at the General Secretariat and in specialized police units all over the world to share, compare and analyse images of sexually abused children found on the internet.

These are just a few examples that give you a broad idea of the type of infrastructure and data INTERPOL needs to protect.

In order to do this, we constantly upgrade INTERPOL's information security management system in a constant reassessment of the risks posed to our information and communications systems.

One identified risk was the one posed by the use of USB memory sticks. Not only does INTERPOL staff use USB memory sticks inside and outside our General Secretariat, but police from our member countries visiting our headquarters in Lyon also use them to share information and make presentations. And as you all know, malicious software is often detected in removable media and can pose serious risks. The USB security standards that we now have in place, which only allows INTERPOL staff and visitors to use corporate secure USB memory sticks, protect INTERPOL's IT architecture against such attacks.

Risks also arise from the constant challenges surrounding identity verification. An organization like INTERPOL needs to be 100% sure that individuals are who they pretend to be when giving them access to buildings, facilities, networks and data.

To strengthen this aspect of our information security management system, we are currently developing, in partnership with Entrust and EDAPS, an e-Identification Card.

This e-Identification Card is an identity management tool that will provide the highest security credentials service for INTERPOL staff and law enforcement officials worldwide working on behalf of INTERPOL. Once in place it will enable these officials to identify themselves at international borders, at the INTERPOL General Secretariat or any other

INTERPOL facility, as well as to securely access INTERPOL networks and communicate from virtually any fixed or mobile location in the world.

This e-Identification Card, as Entrust CEO Bill Conner says, will “enable INTERPOL to control access to resources, prevent theft of information and comply with privacy and digital signature regulations and laws on a global basis”

But our vision doesn’t stop here. The next frontier that INTERPOL intends to lead in transformation is Identity Based Security.

Our vision is one where, one day, all law enforcement officials worldwide involved in international policing matters will be equipped with this e-Identification Card.

As I said earlier, INTERPOL provides its member countries with a secure global police communications system. Of course, not all international police communications go through INTERPOL’s system. But even when not using INTERPOL's communication channels, law enforcement needs a way to be able to know that the person on the other end of any digital communication is who he or she purports to be, and especially when communicating across borders. In other words, law enforcement worldwide needs an international identity verification system.

I strongly believe that INTERPOL, as the largest international law enforcement organization, is in an ideal position to coordinate the development of such security standards for police worldwide and that the product we are developing with Entrust and EDAPS is the first step towards that goal.

In fact, working towards the development of international standards is not new to INTERPOL. The Organization has already played a central role in developing global standards in victim identification and in fingerprint and DNA exchange, for example.

In the field of information security, INTERPOL can play a unique role in establishing electronic trust by building bridges between the police community and information security professionals from the private and public sectors worldwide while working towards the development of common standards.

We have already taken concrete steps to become closely involved with the ISO subcommittee responsible for drafting the ISO 27001 standards. And in parallel, we strongly support the wide implementation of the G8 High-Tech Crime Sub-Group’s best practices in incident response. The INTERPOL e-Identification Card, which I just discussed, spans both the ICAO global travel standards and the EITF enterprise standards to provide strong identity for our police agents both on the road and in the office for both physical and logical access.

In short, INTERPOL is ideally positioned to represent law enforcement interests in developing global information security standards, as well as to assist in the implementation of such standards across its membership, including by developing specific standards for the police community.

But as you all know, even with the best standards in place, security incidents can always happen.

Just recently INTERPOL's Information Security Incident Response Team discovered two Facebook profiles attempting to assume my identity as INTERPOL's Secretary General.

One of the impersonators was using this profile to try to obtain information on fugitives targeted during our recent Operation Infra Red. This Operation was bringing investigators from 29 member countries at the INTERPOL General Secretariat to exchange information on international fugitives and lead to more than 130 arrests in 32 countries.

This is why we constantly need to share our experience. INTERPOL's Information Security Incident Response Team is a member of the Forum of Incident Response and Security Teams — or FIRST —, which I assume most of you know. Being a member of the FIRST enables INTERPOL to learn from the experience of other members and to share our own experiences for the benefit of others. But again, it is also a way to draw bridges between the police community and information security professionals from the private and public sectors worldwide.

***

I strongly believe that building bridges and confidence in relationships between police and the public and private sectors will be crucial in facing the challenges posed to us by cybercrime globally.

Let me share an idea with you before I leave the floor.

I was reading recently an interview with Google's CEO Eric Schmidt. He was saying that the World Wide Web would have to evolve from anonymity to what he calls "true transparency" because, he said, "in a world of asynchronous threats, it is too dangerous for there not to be some way to identify you."

If some kind of a verified name service for the internet is to be created — and I believe one should be — then we will need exactly this type of bridging between police and the public and private sectors, as well as with citizens rights groups and other NGOs to be able to do it.

I think this is something we should start discussing. And here again, INTERPOL can and will play a central role as a discussion forum for law enforcement and in building bridges with all other stakeholders.

Thank you very much.