INTERPOL

SPEECH • DISCOURS • DISCURSO • خطابات

3RD INTERNATIONAL ENGAGEMENT ON CYBER CONFERENCE AT GEORGETOWN UNIVERSITY

REMARKS

BY

RONALD K. NOBLE
SECRETARY GENERAL
INTERPOL

WASHINGTON – DC, UNITED STATES
10 APRIL 2013

Ladies and Gentlemen,

This morning, cybercrime will create a victim.

The victim could be an individual, business or government entity; the crime could be fraud, identity theft, or theft of intellectual property.

Behind this crime, somewhere, there is a criminal...

Law enforcement officers across the world face this scenario every day: a criminal commits a crime that creates a victim.

Except, this is a cybercrime.

Originating in one country, aided in another, and felt in a third.

Instead of being an everyday scenario with an everyday law enforcement response, it's a complex maze, challenging to navigate even for the most specialized officers.

Looking around, they will see different laws and procedures related to cybercrime across these countries.

Different languages, cultures and bureaucracies and all matched by varying levels of capacity to fight it.

And as they investigate, they will face factors – both in the real and virtual world – which prevent them from working effectively across borders.

Exchanges between investigating officers end up taking days, weeks and sometimes without any response at all.

In the meantime, physical evidence is destroyed in one country; digital evidence is erased in another.

The investigation eventually stops, while the criminal continues to the next victim.

In other words, the opposite of what should happen.

And it's the reason why countries and their law enforcement have looked to INTERPOL.

An organization they originally established for the purpose of forging global links among each other.

Links now embodied by National Central Bureaus (NCB) in every one of our 190 country member countries.

To them and any officer, INTERPOL offers global tools and services practical **for** law enforcement, and made **by** law enforcement for the crimes they face today.

Empowering them so they can effectively react to the spectrum of global threats they face on a daily basis.

For almost a century, member countries and their law enforcement have used INTERPOL to centralize and consolidate their global response to a wide range of crime areas.

This morning, you will hear how we are doing the same in the fight against cybercrime.

How we are constructing the INTERPOL Global Complex for Innovation (IGCI) to help them coordinate, investigate and execute operations against cybercrime.

How, through IGCI, we are building tools, services and partnerships in order to maximize law enforcement capabilities.

And how their efforts will enhance cybersecurity and work towards the vision of a safe, stable and predictable cyber environment.

But the reality they, and all of us, hope to achieve is far from what we face.

Internet connectivity has become vital for any government or business that wishes to maximize its access to knowledge and growth.

And citizens worldwide are connecting to the Internet at an unprecedented pace to benefit from the information and opportunities it provides.

This applies equally to criminals, who have been so successful in using the Internet, it's becoming hard to imagine any crime that isn't in some way facilitated by it.

By abusing its global reach, however, cybercriminals have been exceptional in distancing themselves from law enforcement, who remain fixed within a physical space.

This has led to a valuable lesson: when it comes to cybercrime, we are only as strong as our weakest link.

Laws and procedures to fight it don't yet exist in some countries, while some remain more advanced than others.

These are the exact vulnerabilities that cybercriminals prey on and that local law enforcement have no control over.

Which is why, together, we must encourage all countries to develop laws and practices, while helping the ones that need our assistance.

But this must be done in a way that allows law enforcement in one country to fully cooperate with law enforcement in another country.

All law enforcement must have the training and technical expertise to act against cybercrime within this globally compatible system.

Countries know what a difference this can make in improving the effectiveness of global law enforcement action.

They know because they have seen it before – 85 years ago.

Countries then faced another global challenge: the counterfeiting of currency.

By exploiting weaknesses in production and anti-counterfeiting measures across countries, criminals were able to copy the same currency made by countries.

Starting in 1929, law enforcement from our member countries at INTERPOL organized meetings with central banks and the private sector, so together we could to better understand this shared challenge and how to confront it.

Gradually, international standards and practices were recommended to national governments, and brought into practice by them.

Many of which still exist to this day.

Concurrently, countries with greater expertise worked through INTERPOL to build capacity in countries needing assistance.

Eighty-five years ago, countries came together and made a clear statement that they would no longer give criminals the power to undermine their security and economy.

The same statement made against cybercrime three years ago when countries agreed to establish the INTERPOL Global Complex for Innovation (IGCI).

And like the response to currency counterfeiting, words will be backed up with action when the IGCI opens next year in Singapore.

Channelling our experience from the past, IGCI will focus on articulating a global cyberstrategy to harmonize the law enforcement response against cybercrime.

And like in the past, countries with greater expertise can work with INTERPOL to deliver targeted capacity building and training so that countries in need have a brighter future.

By fulfilling these objectives, we will be strengthening their weakest links, and reducing the opportunities that cybercriminals have to exploit them.

However, this is all takes time. Time that reality tells us we just don’t have.

Law enforcement officers need tools and services today, to address the real cybercrime threat of today.

Once again, countries know how tools and services that assist law enforcement can make a difference in their lives.

They know because they have seen it before with the INTERPOL Stolen and Lost Travel Documents Database (SLTD).

The start of this century saw criminals and terrorists increasingly rely on stolen and lost travel documents for international travel.

In 2002, INTERPOL member countries voted to create the SLTD database to respond, eventually deploying it to their frontlines – at border crossings, and in airports.

Anyone here arriving from abroad would have had their passport checked against it.

Ten years later, SLTD now contains 35 million records, and is searched globally 740 million times a year.

Searches that matter because any one of 61,000 hits occurring from them annually could change the course of an investigation or disrupt a terrorist network.

The evolution and diffusion of SLTD illustrates what happens when a practical solution is integrated into the everyday lives of law enforcement.

Simply put, their job becomes easier and their impact is greater.

This is what we hope to do with the INTERPOL Global Complex for Innovation (IGCI), but how will it happen?

This is the challenging part.

Law enforcement officers know how to investigate terrorism and crimes like drug trafficking, murder and theft.

These are crimes any officer can visualize and law enforcement can construct physical, visible barriers to prevent.

Officers know how to collect evidence at traditional crime scenes where fingerprints, DNA or other forms of physical evidence can be found.

Preventing, investigating and collecting evidence of cybercrime, however, is fundamentally different.

For this, they need help.

Help from other organizations and the private sector, whose expertise and reach extends to areas beyond law enforcement.

INTERPOL has already has found one such partner in Kaspersky Lab, that has extraordinary knowledge, experience and unique expertise in keeping citizens and businesses safe from cybercriminals – those intent on spreading malicious codes and viruses, and engaging in other criminal activity over the Internet.

Consider that when a cybercrime is committed, the first to know about it are not law enforcement officers – yet they need to respond as though they were.

By partnering with Kaspersky Lab, we will be able to provide first responder capability to law enforcement so they can actually be able to be the first response.

INTERPOL plans to work with Kaspersky Lab systems and analysts to create the first-ever global INTERPOL Cyber Alert, issued when malicious codes, viruses or any cyber criminal activity with a global impact is identified.

It can immediately draw the attention of law enforcement, the private sector and public to this threat, explain how it operates, and provide actionable intelligence to stop it.

And as the Cyber Alert system is being established, our goal is to make it stronger by finding other partners, such as Europol, who can assist in generating these alerts.

But what the Cyber Alert initiative, and in fact any IGCI initiative, means to each and every officer specializing in cybercrime is presence of mind.

Knowing that they are no longer alone when a cybercrime is committed, and faced with an investigative maze.

Now, INTERPOL and its partners will be standing beside them, ready to provide a map and compass.

IGCI will enable these officers to connect with each other through a global, 24/7 network in order to facilitate communication and coordination.

Instead of days, exchanges could occur within hours or even minutes.

Exchanges that could include data, information and intelligence, so that physical evidence is seized, not destroyed and digital evidence is recovered, not erased.

Investigations in this case continue, increasing the likelihood that criminals are positively identified and located.

Thanks to seconded national officers experienced in the area of cybercrime investigations and digital forensics, the Digital Forensics Lab at IGCI offers any investigator a broad spectrum of services to assist them.

And then, through the Cyber Fusion Centre platform, multi-country operations against cybercriminals can be planned and executed.

This means, next year, when a cybercrime happens one morning, law enforcement will be able to access many of the advantages already possessed by cybercriminals.

Think about it.

Cybercrime officers the world over can connect with the IGCI network to interact globally, the same way cybercriminals do on message boards and chat rooms.

They can share data, information and intelligence as seamlessly as cybercriminals carelessly share malicious programs and stolen identities.

They can tap into a global reservoir of expertise to get assistance similar to what cybercriminals have available.

And they can conduct operations like Operation Unmask, which last year saw law enforcement across four countries in Latin America, working with INTERPOL, to arrest 31 individuals tied to the hacker group Anonymous.

All of these initiatives, however, represent one side of IGCI – the reactive side.

Certainly when a cybercrime happens law enforcement must be ready to react, but preventing victimization must also be a priority.

This is why the other side of IGCI will be dedicated to innovation and outreach for the purpose of building proactive capacity.

In July, this side will begin to take shape.

Together with the French Ministry of Interior, INTERPOL will be hosting the first International Forum on Technologies for a Safer World.

An engagement where law enforcement, the public and private sectors, and academia can discuss and target technologies meant for anticipating and preventing crime.

All so that one day law enforcement will be better able to determine their future, rather than be shaped by it.

This future, however, cannot possibly materialize without these types of interactions and partnerships.

Together our individual comparative advantages can become one large collective advantage against cybercriminals.

Reminding me of the old adage: “united we stand, divided we fall”.

All partnerships start with a dialogue.

A dialogue centered on the free exchange of information and ideas in an open forum, like the one we are all participating in today.

Giving us a chance to find areas of shared interest and possible compatibilities.

And I would like to thank the organizers, particularly Catherine, for this opportunity.

The diverse range of perspectives to be shared here this morning reflects the crosscutting nature of the cybersecurity issue, of which cybercrime is apart.

We can all agree that no one benefits from cybercrime except cybercriminals.

And they way we can show them it's not tolerated is by standing united to create a more secure cyber environment.

A cyber environment where law enforcement work in tandem with all sectors, across all countries.

So that in the future, it will not be about the cybercrime that is committed this morning, but rather how we can fully prosper from the secure cyber environment we created together.

Thank you.