INTERPOL

Remarks

by

Ronald K. Noble

INTERPOL Secretary General

2nd INTERPOL-EUROPOL Cybercrime Conference

01 October 2014

Singapore

Dear Colleagues from Europol and INTERPOL
Your Excellencies,
Distinguished Guests,
Ladies and Gentlemen,

When the INTERPOL Global Complex for Innovation (IGCI) was unanimously approved by our member countries in Doha in 2010, the blueprint for the future of our fighting cybercrime and enhancing our training and capacity building was set in motion.

Thousands of miles away in Brussels, but in the very same month, the European Commission took an equally important step by announcing its intention to establish a European Cybercrime Centre - EC3.

These decisions were made by countries, for the greater security of citizens, businesses and governments worldwide. They were done with a common understanding of a threat, and the institutions needed to counter it.

Cybercrime was a transnational act that didn't respect the boundaries of space or time.

It was immediate. The perpetrators, infrastructure and victims implicated in the crimes were everywhere. No one crime was the same. It was unlike anything seen before, on a scale never seen before.

Ultimately, it fell outside the scope of our conventional thinking and action. How could we possibly expect to respond?

In order to identify, locate and prosecute perpetrators, legislation across countries needed to be compatible. The chain of evidence required to build a case was fragmented across countries, and sectors, and needed to be assembled.

Victims, particularly the general public, needed information to prevent, stop and recover from cybercrime. It wasn't that this information didn't exist, there was just too much out there, and too few vehicles to effectively share it with them.

Countries, both in the EU and globally, knew that any response if it were to work had to be inclusive: no one could be left out, and everyone had to be linked. Any gaps or weaknesses could simply be exploited by cybercriminals.

This is why they called upon Europol and INTERPOL, and we in turn, built EC3 and IGCI.

The infrastructure of these two institutions was designed purposefully.

It emphasized research and development as keys to the identification of crimes and criminals; seamless, real time and secure communication and information channels; tools, services and training needed to coordinate preparedness, prevention and action.

And underlying all this, the ability to cultivate partnerships and cooperation across countries and sectors.

To help build the first and last lines of defence, we have called upon those of you here today, representing law enforcement, governments, regional and international institutions, academia and the private sector.

These lines must be assembled and they must hold, reinforced by our experience, expertise and potential.

For example, Internet Service Providers (ISPs) and Electronic Service Providers (ESPs), like social networking platforms, can contribute crucial information about a suspect or a victim that law enforcement may not have.

The internet security industry, such as anti-virus vendors, can put to use vast knowledge and data on malware trends. This may indicate the modus operandi, the structure or the whereabouts of an organized crime group utilizing malware for criminal purposes.

CERTs can lend their ability to collect trend and intrusion information, or to detect and repel attacks as they are occurring.

Academics and researchers can contribute through methodologically rigorous research and critical analysis. Their results will help to understand the cybercrime phenomena and trends, and improve security and investigative solutions.

And internet users – individuals, families, businesses, governments – can leverage the most important capability of them all: the power of prevention.

Working together, we are hoping to realize a vision of our world where governments and critical infrastructure are protected, the integrity and continuity of businesses can be assured, and individuals and families can go online without having their personal identity or finances compromised.

This vision will certainly guide our collective action for years to come, yet we are seeing progress even in the dawn of this new era.

Six months ago, IGCI and its Digital Crime Center coordinated Operation Strikeback, focused on the growing trend of sextortion crime.

This is where an extorter misleads an individual online to obtain nude pictures or videos of them, then blackmails the victim for money to avoid the publication of the material.

The origins of Strikeback date back to last year when the sextortion trend was identified at the 1st Eurasian Working Group on Cybercrime for Heads of Units.

In response, a joint task force was created and coordinated by the Digital Crime Center, which included police agencies from three different continents and certain private entities.

In this case, an Internet trace of the perpetrators and the destination of the ransom payments pointed to the Philippines.

This intelligence was enough to initiate months of preparation for Operation Strikeback, which ultimately resulted in 58 individuals arrested in the Philippines and the seizure of more than 250 computers and electronic equipment.

Strikeback was repeated a few months later, which saw the arrest of eight additional persons including the mastermind, a 42-year-old female who was coined as 'Sextortion Queen'.

While the results from Strikeback are promising, the process of the operation is potentially more instructive because it suggests a model for our collaboration.

Through INTERPOL, different actors from different sectors and countries were able to put the pieces together to bridge the full spectrum of a cybercrime investigation, from the origins of the crime phenomenon to the prosecution of the offenders.

Replicating this outcome should certainly be one of our goals, and this is in large part the focus of this conference.
Yet, in parallel, we should also be ensuring that these types of operations and investigations never have to be initiated in the first place.

Cybercrimes are expensive, complex and time consuming to investigate and prosecute. Moreover, it is simply not possible to handle each one, especially if there are more than 1 million victims a day.

This is why we must reduce the likelihood an individual or entity becomes a victim.

Prevention will not only reduce costs downstream for investigations and prosecutions, but upstream by saving potential victim losses.

Yet, for it to work, governments, businesses and citizens need accurate, real-time intelligence, and to be empowered with relevant know-how. They also needed a global platform through which this information can be conveyed to them in their language.

This platform is what INTERPOL envisioned when it created the Turn Back Crime campaign.

The goal is to generate a level of awareness and preparedness among potential victims of cybercrime, so that victimization rates ultimately go down.

Sextortion and Operation Strikeback provide the perfect examples of where Turn Back Crime could come in to play.

The campaign allowed us in this case to relay to the public the modus operandi of a new type of Internet crime, information on what they can do in the event they are being victimized, and who they could contact.

To prove the viability of Turn Back Crime, however, we should look at it as an economy of scale.

Currently, the price tag of cybercrime is in the billions, and increasing year by year.

Establishing an effective campaign like Turn Back Crime has been done at relatively low fixed cost, and with it now in place, we are taking three actions that are reducing total costs:

1. We are establishing effective channels of information creation, developed through collaboration between INTERPOL, EC3, the private sector, academia and the general public;
2. We are growing the network and reach of the Turn Back Crime campaign, and sharing the information we create together via social media like Twitter and Facebook, and the Turn Back Crime website;
3. We are encouraging the use of this information on a day-to-day basis by those part of this network, such as through celebrity endorsement.

The output from these actions, which is awareness and preparedness, ultimately reduces victimization rates.

And because we are all working together in the information technology age, the three actions that create this output come at little or no cost.

The more output, the fewer the victims, the lower overall price tag of cybercrime.

Dear colleagues,

If we are able to pair an effective prevention campaign alongside a robust law enforcement response, we will see our vision come closer and closer into reach.

Both of these approaches take time to develop, and we have been diligent in developing them. We have strategically assembled the infrastructure by building institutions like EC3 and IGCI, and have started to see shades of our potential through Operation Strikeback and the Turn Back Crime campaign.

We are now at the next stage of growing and capitalizing on that potential. And everyone in this room – and even those outside it – are responsible, because only together can we build a safer world.

Thank you.