INTERPOL

Speech

by

MENG Hongwei

INTERPOL President

Countering Cyber and Financial Crimes: A High-level Dialogue for a New Governance Architecture

12 July 2017

Lyon, France

Members of the Executive Committee;
Secretary General Mr Stock;
Chiefs of Police and Head of INTERPOL's National Central Bureaus;
Representatives of international and regional organizations;
Partners, representatives from banks, financial institutions, Internet service providers and telecom operators;
Distinguished guests;
Ladies and gentlemen,

Good morning, I am delighted to be here today to deliver the opening address for the very first High-Level Dialogue for countering cyber and financial crimes.

First of all, on behalf of INTERPOL, I sincerely welcome you to this important event, and I would also like to express my appreciation of your strategic view to participate in the high-level dialogue which is of historic significance here in Lyon the host city to INTERPOL's General Secretariat headquarters.

This High-level dialogue is the first initiative at the global level to unite the efforts of law enforcement agencies and private institutions to counter cybercrime on such a scale. The dialogue is also one of the most substantive attempts by the international community to prevent and combat cybercrime since the creation of the Internet. I believe 'actions speak louder than words' and 'a good beginning is half the success'. I therefore welcome all of you to the starting line against global cybercrime.

The serious threat posed by cybercrime to the international community is self-evident. The convergence of cyber and financial crimes worldwide has become a major challenge that law enforcement agencies and global organizations have to respond effectively to. Telecommunications fraud is a major problem in Asia and becoming increasingly widespread across all continents, with criminals targeting massive numbers of innocent victims. It is impossible for any individual organization to address the global threat posed by cyber and financial crime, and the situation is deteriorating.

Nevertheless, the law enforcement agencies, banks, financial institutions, Internet service providers and telecom operators are facing many difficulties in countering these threats, in particular the constraints relating to information sharing, data privacy laws, multi-jurisdiction issues and a lack of resources.
Previously, when a company or a law enforcement agency had sufficient resources, they were able to prevent and detect crimes within their own areas of responsibility.

Today, as we face the unprecedented complexity and mobility of cyber-enabled financial crimes, telecommunication and social engineering frauds, no single entity is able to rely on their efforts alone to combat these crimes. Internet crimes can be described as 'flood' spreading everywhere. The mentality of 'minding one's own business' is no longer applicable if we are to protect ourselves from this danger. We must unite and construct a dam to protect us from this flooding, to make sure that the Internet is working for the sake of society's well-being.

Cybercrime is one of the three focal projects of the 'INTERPOL Strategic Framework 2017-2020', along with counter-terrorism and organized and emerging crime.

In recent years, INTERPOL has developed significant expertise in coordinating regional operations to combat cybercrime. We also have a database containing information on criminals around the world, accessible to our 190 member countries. As INTERPOL is the leading international organization in policing, we assume the responsibility to take the lead in fighting these battles. We advocate the use of INTERPOL as a working platform, and develop a partnership approach between law enforcement

agencies, banking and financial institutions, as well as with Internet service providers and telecom operators. This partnership aims to achieve three goals.

Firstly, the partnership should be able to facilitate information sharing as widely and as quickly as possible, it is a pre-requisite in combating crime. Undoubtedly differences in data privacy legislation between countries, information sensitivity, trade secrets and technological constraints may be barriers to information sharing, but this does not mean that we should maintain the status quo. We have to move forward and discuss what more can be done within existing legal frameworks and current limitations.

To encourage effective information sharing, this partnership should clearly identify the rights and obligations of each party in the information sharing process.

Secondly, the partnership should formulate a 'prevention strategy' in order to curb cyber-enabled financial crimes, telecommunication and social engineering frauds.

It is always better to adopt a proactive approach to prevent a crime from occurring in the first place, instead of responding once the damage has been done. In fact, apart from very sophisticated frauds, many criminal syndicates simply repeat their modus operandi time and again.

We need a strong coalition to raise awareness across vulnerable sectors and amongst the general public about email scams and social engineering frauds. This type of awareness raising should not be limited to our own target sectors. Awareness campaigns across all spectrum can help spread the message and encourage all areas of society to have a better understanding about crime trends and the importance of security.

Thirdly, we need to develop a 'quick response mechanism' to provide assistance to any party which comes under attack which at the same time creates a strong base for an investigation. This is to ensure prompt action is taken to avoid further spread of the attack and minimize the potential damage to other parties.

Ladies and gentlemen, nothing is easy at the beginning. Cross-agency cooperation is bound to face many obstacles, especially in the current situation where the threat of cybercrime is growing. We have to take action before it becomes too late to avoid a disaster. This is a battle related to the fate of mankind, human freedom, development, peace and legal systems. It is a priority for every stakeholder participating in this High-level Dialogue to find a common way forward.

Following this High-level Dialogue, national law enforcement agencies will build on the agreements by carrying out a two-month global operation to combat financial crime. I would ask you to fully support this operation. At the same time, I appeal for your joint efforts to build a long-term cooperation mechanism or platform, which can put forward our consensus to develop effective action, and to form up a united global line to counter the transnational cybercrime.

Thank you.