米田長官スピーチ（案）

―サイバー犯罪対策―

President Ballestrazzi, Secretary General Noble, Members of the Executive Committee, Your Excellencies, Chiefs of Police, Director of NCB (National Central Bureau), distinguished guests, Good afternoon; I am Tsuyoshi Yoneda, the Commissioner General of the National Police Agency of Japan.

Commemorating the 100th anniversary of international police cooperation this year, it is a great honor to be able to meet you all here today.

I would also like to extend my respect and appreciation to the Principality of Monaco, the host for this Assembly.

Today I will speak about the threat of cybercrime and what we shall do about it. Needless to say, the threat of cybercrime is serious and imminent for each and every country including Japan.

Cyberspace, along with the real world, has now become a new realm in which police bears responsibility to secure safety. The Japanese police, with the cooperation of the private sector, is working hard to effectively arrest and prevent cybercrime while constantly enhancing its countermeasures and capability.

However, since borders have no meaning in cyberspace, one nation cannot alone tackle with the crimes therein. It is vital for law enforcement agencies around the world to strengthen mutual cooperation and enhance their respective counter-cybercrime capabilities.

So within the time given to me today, I would like to touch upon the cybercrime-countermeasures of the Japanese police and share my thoughts on the importance of international cooperation. With regard to the latter, I would also like to introduce some of the contributions made by the Japanese police in the area of international capacity building.

First, I would like to talk about the measures taken by the Japanese police in dealing with cyber intelligence and cyber terrorism.

Recently in our country, growing number of cyber intelligence cases are being detected. In these cases, attempts are made to steal confidential information from governments, private enterprises, and other organizations. Throughout the world, there has also been a rash of cyber terrorism targeting the core systems of governments and critical infrastructures. These kinds of attacks pose serious threats to the security and economy of each nation.

In order to prevent or swiftly detect and minimize the damages caused by these cyber attacks, the police must closely work with the private sector. Accordingly, the Japanese police established a Counter Cyber Espionage Information-sharing Network with approximately 6,500 high-tech companies nationwide. Through this network, the police receive reports of cyber attacks from the member companies. The accumulated reports will be analyzed by the police and the result will be fed back to the member companies.

With regard to cyber terrorism, every prefectural police has established Cyber Terrorism Countermeasure Councils with the local critical infrastructure related companies. Through this framework the police helps the participating companies enhance their counter-cyber terrorism capabilities by, for example, periodically carrying out joint cyber terrorism drills.

The strong point of the Japanese way of cooperating with the private sector is that the police personnel who would actually take charge in cases of cyber attacks frequently visit the private companies and hold face-to-face meetings with the executives and the engineers. In this way, the police develop a close and trusting relationship with the private sector which, in my belief, facilitates our efforts in detecting, preventing and minimizing the damage caused by cyber attacks.

Next, I would like to talk about the measures taken by the Japanese police against Internet banking fraud.

The number of Internet users in Japan exceeded 100 million as of end of 2013, which is 82.8% of the population. A study report shows that the usage rate of Internet banking in Japan was as high as 65.2% in 2012.

On the other hand, in recent years, illegal money transfers related to Internet banking fraud are surging, causing a serious situation.

In particular, the amount of damage last year rose sharply to approximately 14.6 million U.S. dollars, marking a record high. Even more, the amount of damage for the first half of this year was approximately 18.5 million U.S. dollars, already exceeding the whole

amount of last year.

In response to this, the Japanese police is not only making investigations but also putting much effort in taking down the Botnets and heightening public awareness, thus preventing and minimizing the damage caused by Internet banking fraud. We are also working closely with the financial institutions and urging them to take higher security measures such as one-time password system and lowering transaction limits.

However, we strongly feel that our efforts alone are far from enough, since Internet banking fraud is notably becoming a global crime. Unauthorized access to Internet banking systems are often made from abroad and the criminal proceeds also frequently end up outside the country.

In order to deal effectively with such crimes, the police across the borders must work even more closely, sharing information and experiences in a timely manner.

I have, so far, touched on cybercrime countermeasures of the Japanese police. Lastly, I would like to talk about the cross border cooperation among police forces and the contribution of the Japanese police to it.

As I mentioned before, in cyberspace there are no borders dividing the nations. Also in this arena, traces of crimes disappear by the minute, thus making most of the tools we use in the real world to detect and seize crimes meaningless.

In order to achieve effective investigation under these circumstances, each country must not only enhance its own counter-cybercrime capability but also work together to

improve the transnational investigative cooperation mechanism. For instance, under the Convention on Cybercrime, a party state, upon request from another party state, shall order expeditious preservation of necessary data stored in a computer system located in its territory. This kind of cooperation mechanism is essential for cybercrime investigation and we together must accelerate our efforts to expand and improve it.

The responsibility to enhance counter-cybercrime capability lies first and foremost in each country. However, we must not forget to help one another and exchange information in the process.

The Japanese police contribute widely to the capacity building of countries around the world by hosting seminars and offering training programs in various fields such as countermeasures against cybercrime, international organized crime and international terrorism. In the field of cybercrime countermeasures, Japan will host a symposium this December which will be participated by law enforcement agencies of the Asia-Pacific region. The participants are expected to share their respective experiences and knowledge in the field of digital forensic and cybercrime investigation. Another seminar will be held in January next year targeting fifteen ODA recipient countries to enhance their counter-cybercrime capacities.

In addition, Japan actively supports ICPO's capacity building efforts by sending experts to its conferences, training programs and so on.

April of next year, the IGCI will be launched in full-scale. As threats in cyberspace intensify, the Japanese police strongly support ICPO's efforts to focus on the cyber field and secure a foothold in Asia. We expect that the IGCI will come to play an essential role in the international counter-cybercrime efforts.

Japanese police has sent Executive Director Nakatani and several other personnel to the IGCI. I am confident that these personnel will contribute to the operations of ICPO as well as to the enhancement of each country's capabilities to deal with cybercrimes.

As has been the case in countering international organized crime and terrorism, it is certain that the role of ICPO will become more and more important in the counter-cybercrime arena.

Japan will be hosting the Tokyo Olympic and Paralympic Games in 2020. As various threats including cybercrimes can be expected, we resolve to exert every effort to make the event a successful one. I understand that Japan cannot alone achieve this and would like to take this opportunity to ask all of you for your cooperation. Needless to say, Japan is also ready to contribute in any way possible to the efforts of police agencies around the world in their fight against threats in cyberspace.

Thank you.