UNODC
United Nations Office on Drugs and Crime

# Responding to the security threat posed by Cybercrime in East Asia and the Pacific

## Keynote speech for the Asia-Pacific Regional Workshop on Fighting Cybercrime

**by**

**Gary Lewis**

**UNODC Regional Representative**

**for East Asia and the Pacific**

**Seoul, Republic of Korea**

**21 September 12011**

Your Excellency – Mr.Han – Prosecutor General of the Republic of Korea
Your Excellency – Dr. Kim – President of the KIC
Your Excellency – Mr. Sir (Suh) – President of KISA
My colleague – Dr. Kim – Regional Director of the ITU

Distinguished Participants,
Ladies and Gentlemen,

I would like to join my colleagues in again warmly welcoming you all to Seoul – particularly at this beautiful time of year. Many of you have taken connecting flights – covering great distances – to be with us today. We are so pleased that you could join us.

A special welcome to the:

- <u>Operational law enforcement and IT public officials</u>:
    - 20 prosecutors from ASEAN Member States and IT-related public officials from across the Asia-Pacific region.
- <u>Our expert presenters</u>:
    - Legal
    - Cybercrime
    - Transnational organized crime
    - Technology

In the following 10 minutes I shall try to give an outline of latest trends which we need to worry about. I will also speak of the key elements of our response.

## 1. CURRENT DIMENSIONS

Ladies and Gentlemen,

In fewer than two decades, the Internet has grown from a curiosity to an essential element of the modern life of billions of people. But, as with other aspects of globalization, its rapid expansion has far exceeded our capacity to regulate it. In the absence of authority, many abuses have occurred. Perhaps the most dangerous of these is **cybercrime**.

Our workshop will cover a lot of ground. But it will focus mainly on **identity-related offences**. That is because these are among the most common forms of cybercrime.

It is the main goal of the cybercriminals to **collect huge volumes of protected information** and either use it or sell it – typically via dedicated bulletin boards – to criminal groups who then specialize in what we call “cashing out”.

Criminals can use identity-related information for various purposes. And the fact that the UN Secretary-General’s Global Counter-**Terrorism** Strategy addresses identity-related crime underlines the importance of that dark linkage.

## 2.  FUTURE THREATS

Now, why do I say that we should be worried?  Well, there are a number of reasons why cybercrime in general – and organized cybercrime in particular – is likely to increase and pose a greater threat to us in the near future.

I offer FOUR reasons.

(a) MORE ACCESSIBLE TECHNOLOGY.
First reason – more accessible technology.  The technology underpinning cybercrime has become more accessible.  Software tools are available online – right now – which allow the user to locate ports that are vulnerable – or password protection which can be overcome.  These tools allow a much wider range of people to become offenders – in other words not just those with a special gift for computing.

(b) AUTOMATED ATTACKS.
Second reason – automated attacks.  At present, each new offender can exponentially increase the number of attacks he makes through the use of automation.  We've all seen examples of the many millions of unsolicited bulk spam messages sent out daily.  These are sent out by automation within a very short timeframe.

(c) BIOMETRICS.
Third reason – biometrics.  The Internet now places ever-greater emphasis on associating people with bits of data.  These bits of data are not only codes, passwords and personal identification numbers – but, increasingly, they include BIOMETRIC indicators – even our body data, our emotions and senses.  It will soon be possible for this information to be streamed through one, individual and embedded device.  This ought to give us reason to worry.

(d) CLOUD COMPUTING.
Fourth reason – cloud computing.  As you all know, this is where data and programs cease to be stored on desktops.  Instead it is stored remotely on a cloud of web servers.  These clouds expand or contract depending on the amount of computing power required by users.  More and more of us like the idea of cloud computing.  Why shouldn't we?  It allows us to access applications and data from anywhere in the world where we happen to be.  But look at it from the law enforcement perspective.  Our current law enforcement approach is premised on the assumption that data is stored on a computer system.  This problem has been pointed out by many, including my colleague John Lawler of the Australian Crime Commission.  *"With cloud computing"*, he asks, *"where is the computer system?  Where is the data?  How do we gain access?  How do we deal with cross-jurisdictional issues? Where is the victim?  Where were they when the crime occurred?"*

## 3.  WHAT IS TO BE DONE? – ELEMENTS OF A RESPONSE

Ladies and Gentlemen,

This is the current situation.  Let's now turn to the elements of a response.  Here I see four main areas.

(a) DATA ANALYSIS.
First, knowing the problem.  If organized crime is seizing the opportunities provided by technology, so too must we.  And we must share this information with other law enforcement agencies which need it.

(b) TECHNICAL CAPACITY.
Second, we must sharpen our technical ability to respond.  We must think afresh.  We must act anew.  We must develop mechanisms that help us work more creatively, more speedily, more efficiently and more cost-effectively at the national level.

(c) REGIONAL COOPERATION.
Third, we must cooperate better across – and between – regions.  The fight against cybercrime is not something we can win alone.  For example, the EU/ITU project (ICB4PAC) that deals with cybercrime in 15 Pacific countries is one excellent example of strengthening regional cooperation.  Mr. Marco Obiso from ITU is present here and will provide more details about this regional approach during the course of this workshop.

(d) INTERNATIONAL NORMS.
Finally we must continue to strengthen the framework of norms and standards through which we cooperate.  My colleague who has travelled from Vienna to be with us here today – Ms. Gillian Muray (who heads cybercrime in our Organized Crime and Illicit Trafficking Branch) – will provide detail on the latest developments on international norms.

## 4.  HOW CAN THE UNITED NATIONS HELP?

As regards UNODC's role, I shall confine myself, in these opening remarks, to simply saying that UNODC – as the guardian of the **UN Transnational Organized Crime Convention –** has been given mandates to fight cybercrime through various **UN General Assembly** and **ECOSOC** and **Crime Commission** resolutions.

But the UN's response does not come only from UNODC.

I am particularly pleased therefore that we are co-sponsoring this workshop with the **International Telecommunication Union** with whom we very recently signed an MOU to fight cybercrime.  I think this is a good example of how the UN is taking global action to fight this major threat to human security.  You may also be happy to hear that this meeting today is – in fact – our very first joint activity since the MOU was signed.  In this sense, we are making history.

## 5.  EXPECTED OUTCOMES

As part of our effort to promote regional cooperation against TOC, UNODC has established – in East and SE Asia – the **Towards AsiaJust programme**. This is headed by Mr. Keebong Paek who is with us on deputation from the SPO. One of this project's main aims is to build the capacity of prosecutors, who are in charge of investigations into – and prosecutions of – TOC groups. Our TAJ programme is also very much focusing on sharing expertise between prosecutors and IT experts. Hence the reason for this conference.

You will hear a lot about current approaches in Asia-Pacific as well as other regions. This will allow us to build upon what was already achieved and develop it further instead of reinventing the wheel. I am particularly looking forward hearing your views on what we can do with regard to capacity-building, information sharing and regional / international cooperation.

## 6. THANK YOUS

Before I end these introductory remarks, I would like to take a few moments to acknowledge the immense work of a small number of people who made this workshop possible.

**The Republic of Korea's Supreme Prosecutors Office (SPO)**

- SPO has historically provided strongly support to our work in UNODC, particularly by providing public prosecutors – on deputation – to serve in our offices in both Bangkok, and Vienna.
- Last year, UNODC held a High-Level Prosecutors' Meeting of ASEAN states and the Republic of Korea here in this very room. In the Closing Declaration, the Participants affirmed the commitment of each country's prosecutorial agency to work together against TOC.
- They called for the formation of a Regional Operational Network of Prosecutors to facilitate operational work.
- Following that successful Meeting – which was sponsored by our Towards AsiaJust programme – the SPO continued its support us by generously agreeing to provide this venue, the equipment, support staff and hosting a lunch as well.
- UNODC looks forward to continuing its strong partnership with SPO.
- And I take this opportunity to thank the Prosecutor General for gracing us with his presence today.

**Korean Institute of Criminology (KIC)**

- As the donor of the Toward AsiaJust Programme – and as a UNPNI Member Institution – the KIC has shown its commitment to fostering regional cooperation to counter crime.
- For this cybercrime workshop, KIC has willingly provided an expert, as well as assistants and has also hosted a lunch for participants.
- We look forward to continuing our close cooperation with them.

- I would specifically like to thank the esteemed Dr. Il-Su Kim, President of KIC, for joining us today.

**KISA**

- KISA is the leading government agency for cyber-security in Korea.  It promotes internet services and explores international cooperation with other countries as well.
- KISA kindly provided experts for the workshop and also hosted a lunch for participants.
- We anticipate further collaboration with KISA on cybercrime.
- I would like to express my sincere gratitude to the honourable Mr. Jongryeol Suh, President of KISA, for joining us here.

**ITU**

- As you know, the ITU is the UN specialized agency responsible for information and communication technology.  In this capacity, ITU will provide technical and practical knowledge for the participants.
- I would like to sincerely thank my colleague Dr. Eun-Ju Kim, Regional Director, ITU Regional Office for Asia and the Pacific – and her hard-working team for all their support to get us to where we are this morning.
- I would also like to extend a personal welcome to Mr. Marco Obiso, cyber security coordinator of ITU Headquarters.

**UNODC**

- Within UNODC, I am privileged to manage a small, dedicated team which has been working flat-out to make everything fall into place by this morning.
- You know who you are.
- And I thank you.

## 7.  CLOSING

So, ladies and gentlemen, to conclude:

From the law enforcement perspective, here are some of the questions we should be seeking answers for at this workshop:

- What kind of partnerships can we forge between law enforcement and the financial services industry?
- What kind of information sharing arrangements need to be in place – among ourselves – to promote better cooperation?
- Remember the points I made about the future possible scenarios?  Well, what sort of technology model best allows us to anticipate these trends?
- Finally, let us ask ourselves what sort of investigators we need – and how can we empower these new leaders in the fight against cybercrime?

The future environment for cybercrime will be more fragmented.  It will be more difficult.  But we make a mistake – indeed we do our citizens a disservice – if we think that organized crime is too big and too complex to tackle.

Let us not forget that in fighting this network, we ourselves also constitute a network. And it takes a network to defeat a network.

I wish you every success in the coming days.