INTERPOL

SUMMARY

GLOBAL CYBERCRIME STRATEGY

INTRODUCTION

Cybercrime is one of the fastest growing forms of transnational crime faced by INTERPOL's member countries. While rapid growth in Internet and computer technology has enabled economic and social growth, an increasing reliance on the Internet has created more risks and vulnerabilities, and opened up new possibilities for criminal activity.

The borderless nature of cybercrime means that law enforcement agencies face challenges in responding effectively due to the limits of cross-border investigation, legal challenges and diversity in capabilities across the globe.

Different from other investigations, in many cybercrime cases, digital evidence sits mainly with the private sector, which operates and maintains many parts of the Internet infrastructure; therefore, a multi-stakeholder collaboration is essential to tackle modern cyber threats.

SCOPE

The *Global Cybercrime Strategy* outlines INTERPOL's plan to support member country efforts to combat cybercrime by coordinating and delivering specialized policing capabilities from 2016 to 2020. It will be reviewed periodically to ensure it remains relevant, continues to respond to emerging threats in the dynamic environment it operates in, and responds to member countries' expectations.

The primary scope of INTERPOL's Cybercrime Programme is to target "pure cybercrime", crimes against computers and information systems where the aim is to gain unauthorized access to a device or deny access to a legitimate user (typically thorough the use of malicious software).

However, INTERPOL recognizes the importance of fighting cyber-enabled crimes, where the use of computers and information systems amplifies crime such as financial fraud and terrorist use of social media. Additionally, there is an increasing demand for digital forensic capabilities to support the fight against many types of crimes.

MAKE CYBERSPACE SAFER FOR EVERYONE, BY HELPING COUNTRIES TO IDENTIFY CYBERATTACKS AND THEIR PERPETRATORS.

ACTION STREAMS

The strategy comprises five action streams, with the common goal of helping member countries to identify cyberattacks and their perpetrators:

1. Threat assessment and analysis, trends monitoring
Detection and positive identification of cybercrime, cybercriminals and cybercrime groups through threat assessments, analysis and trends monitoring.

2. Access to and exploitation of raw digital data
Facilitate access to data linked to cyberattacks, and the relevant tools and partners to consolidate the collection of data and enhance its exploitation.

3. e-Evidence management process
Manage digital evidence processing for the purpose of investigation and prosecution: lawful collection of digital clues, preserving the evidence, making it intelligible and acceptable for the court system.

4. Correlation of cyber and physical information
Bridge the gap between digital traces and physical identification so as to identify the location of possible perpetrators.

5. Harmonization and interoperability
Improve operational interoperability and global coordination, and encourage legislative harmonization.

CAPABILITIES AND DELIVERY

The Cybercrime Programme is run from the INTERPOL Global Complex for Innovation in Singapore, which is equipped with a multi-stakeholder Cyber Fusion Centre, a Digital Forensics Laboratory and an Innovation Centre.

These action streams will be delivered using INTERPOL's range of policing capabilities, and are aligned to the Organization's two other Global Programmes (Counter-terrorism, Organized and Emerging Crime) to ensure a coherent and effective approach to fight all forms of transnational crime.

INTERPOL'S OPERATING MODEL

Today's crimes are increasingly complex. They are interconnected and global, and they take place on both physical and virtual levels. More than ever, there is a need for multilateral police cooperation to address the security challenges affecting societies.

With its 190 member countries, INTERPOL is ideally placed to work with law enforcement agencies around the globe to strengthen their ability to prevent crime and identify and arrest criminals. Partnerships with other regional and international organizations strengthen the combined approach to tackle common challenges.

INTERPOL's activities are centered around three global crime programmes: Counter-terrorism, Organized and Emerging Crime, and Cybercrime, each of which has a 2016-2020 strategy. These strategies, and the initiatives within them, will evolve to reflect the dynamic natures of the operating environment.

These programmes are all supported by a set of policing capabilities that the Organization provides member countries. These are police data management, criminal analysis, forensic support, fugitive investigate support, a Command and Coordination Centre, capacity building and training, innovation and special projects.

INTERPOL General Secretariat - 200, quai Charles de Gaulle - 69006 Lyon - France - www.interpol.int

February 2017