



INTERPOL

National Cyber Review



The Internet has eroded physical borders, providing unprecedented opportunities for countries and individuals. This increasing reliance upon the Internet has also created a large number of vulnerabilities, allowing criminal networks operating anywhere in the world to coordinate complex attacks in a matter of minutes. Cybercrime investigations are different from traditional police investigations, requiring high-level technical expertise and cross-jurisdictional cooperation, which many countries do not yet have the capabilities to conduct alone.

A significant activity for the INTERPOL Global Complex for Innovation (IGCI) is therefore to enhance member countries' capability to fight digital crime. Many opportunities exist for INTERPOL to work with partner agencies and organizations to deliver targeted training programmes to member countries.

In addition, a broad range of other intergovernmental organizations are also involved in delivering cybercrime investigation and digital forensics training.

Combating cybercrimes, which are multi-jurisdictional in nature, requires a high degree of interoperability amongst different jurisdictions. However, vast differences in operational capabilities, legal systems, rules and procedures pose challenges to efforts to combat cybercrime. To address these concerns, INTERPOL has created the National Cyber Review (NCR) tool to assess and learn from the different methods of combating cybercrime and ultimately move towards a more harmonized global outlook. ►

NATIONAL CYBER REVIEW

CYBER REVIEW

An NCR is a comprehensive assessment of all components of a country's cyber apparatus, and will be conducted at the request of a member country. The NCR includes observations and recommendations for enhancing the existing institutional, operational, legal and technical frameworks for dealing with cybercrime.

This service will also look at the consistency of operational and legal perspective with respect to international norms. An NCR will aim to help member countries understand their strengths and weakness, as well as identify gaps in their overall capacity to combat cybercrime effectively.

The existing frameworks to combat cybercrime in the requesting member country will be reviewed in the context of global best practices, to assist the requesting member country in identifying opportunities for improvement. This will ultimately raise the overall ability of law enforcement agencies to enforce cyber laws globally and prevent cybercriminals from exploiting weakness in the legal framework of any one country.

The NCR will also help in identifying the specific training needs of the law enforcement agencies in the requesting member countries. Further to the review, INTERPOL can also assist a member country in setting up a cybercrime investigation or digital forensics unit.

ASSESSING CYBERTHREATS

Reports based on the National Cyber Reviews will be drafted by INTERPOL in coordination with external experts from partners in the private sector and academia, based on a broad range of research, including in-country interviews, focusing on:

- Governance;
- Capacity of the law enforcement agency to prevent and investigate cybercrimes;
- Moving towards global harmonization of operating procedures, rules and legal frameworks;
- Threat and vulnerability assessment.

NCRs will aim to assess the entire spectrum of cyberthreats faced by the requesting country. This will involve looking at the historical data along with reviewing new technological advances and how these can be exploited by cybercriminals, paying special attention to the unique circumstances of the country in question.



INTERPOL

► **CONTACT INFORMATION:**
Global Complex for Innovation
Cyber Directorate
18 Napier Road
Singapore 258510

Tel: +65 6550 3505
Email: EDGCI-CD@interpol.int

- Twitter: @INTERPOL_HQ
- YouTube: INTERPOLHQ
- WWW.INTERPOL.INT

