Cyber Innovation and Outreach
Preparing for future threats

The digital age has radically changed every aspect of our daily lives and at the same time brought about new global threats, which require a holistic approach to tackle them.

These global threats cover a wide spectrum of crimes and every day their number and their impact on society increase. Such crimes could include attacks against computer data and systems, identity theft, the online distribution of child sexual abuse images, attacks against online financial services or critical infrastructures, e-mail scams and the deployment of malware.

While effective law enforcement action is a crucial element in fighting these cyberthreats, we are also aware of the importance of engaging all stakeholders, especially those belonging to the technology sector, to improve global digital security.

To more effectively fight cybercrime, we must leverage the strength and expertise of our member countries and create strategic partnerships with regional and international entities, the private sector and academia in the area of research and innovation.

The research and innovation functions of the INTERPOL Global Complex for Innovation (IGCI) will principally focus on studying emerging technological developments, proactively detecting future threats and strengthening cyber capacity through the standardization of training.

An Adobe breach compromised an estimated 150 million accounts in September 2013.

Trend Micro Security Predictions for 2014 and Beyond

Organizations experienced an average of 122 successful cyberattacks per week.

The Impact of Cybercrime, InfoSec Institute 2013
**DIGITAL SECURITY RESEARCH**

Research and innovation will lead in-depth digital crime research on new and emerging threats, extrapolating future cybercrime modus operandi and their impact. It will also consolidate existing research conducted by research institutes, academic circles and the private sector. In this way, the IGCI will seek to identify new tools and research coming from private companies and academia that could innovate the way in which police conduct cybercrime investigations.

**DEVELOPMENT OF INVESTIGATIVE BEST PRACTICES**

This function will play a crucial role in the development of INTERPOL’s research and innovation strategy, with a focus on digital innovation for law enforcement. The strategy will drive, initiate and coordinate collaborative research projects with the view of developing best practices for police to maximize their preparedness for future cyber-incidents. The IGCI will consequently disseminate proactively developed standard operating procedures and guidelines for cybercrime investigations and digital forensics among its member countries to empower their investigations.

**DEVELOPMENT OF DIGITAL SECURITY TOOLS**

Building upon the research conducted on cybercrime and the subsequently developed best practices, research and innovation will enhance the coordination of collaborative research projects with a view to developing innovative IT solutions and digital forensic tools. Through this, we aim to improve digital crime investigation capacity and promote cooperation among all stakeholders in the field. This innovation will draw upon open source intelligence, strategic partnerships with leaders in the field of innovation and strong cooperation with the INTERPOL Digital Crime Centre, where future tools will be tested before being shared with member countries.

---

**Contact**

INTERPOL General Secretariat  
Global Complex for Innovation  
200 quai Charles de Gaulle  
69006 Lyon  
France  
Tel: +33 4 72 44 70 00  
Fax: +33 4 72 44 71 63  
www.interpol.int