Europol-INTERPOL Cybercrime Conference examined latest cyber threats, trends and strategies
More than 400 experts from law enforcement, the private sector, and academia have gathered this week at Europol’s headquarters in The Hague for what is one of the world’s biggest platforms of exchange on cybercrime.

Under the theme of ‘Law enforcement in a connected future’, the 7th Europol-INTERPOL Cybercrime Conference looked at ways how to effectively combine the expertise, resources and insights of law enforcement, the private sector and academia to make the internet a more secure environment, especially in a society, which is becoming increasingly dependent on digital capabilities.

Over the course of three days (9-11 October), 50 experts elaborated on the most pressing cyber threats of today and tomorrow. Key themes included the benefits and challenges of Artificial Intelligence for police; the potential impacts of 5G technology; cross-border access to electronic evidence; obstacles to international cooperation on cybercrime investigations; the importance of cyber capacity building; cryptocurrency trends and challenges; the use of open-source intelligence and privacy considerations.

This year, speakers included the Executive Assistant Director of the FBI’s Criminal, Cyber, Response and Services Branch, Ms. Amy S. HESS and the General Manager of Microsoft’s Digital Crimes Unit, Ms. Amy HOGAN-BURNEY, both of whom delivered keynote speeches on the threats perceived by their respective communities. Another international speaker was Mr Cyrus Roberts VANCE Jr., the incumbent District Attorney of New York County, who spoke on the impact of encryption on criminal investigations.
As highlighted in Europol’s 2019 Internet Organised Crime Threat Assessment (IOCTA) presented at this conference, cybercriminals continue to become more audacious, shifting their approach away from scattered to more focused, carefully crafted attacks against larger, more profitable targets with the potential for ominously greater damage and major disruptions.

This year’s conference saw the participation of over 100 organisations and more than 70 different law enforcement agencies engaging in fruitful and solution-oriented discussions on how to tackle the challenges at hand head-on in a collective manner.

Conclusions emphasised a need for an even closer cooperation in the areas of:

- **Business Email Compromise (BEC):** while BEC is not new, it is evolving, causing increasing economic damage. BEC exploits the way corporations do business, taking advantage of segregated corporate structures, and internal gaps in payment verification processes.

- **Dark web:** as the dark web evolves, it has become a threat in its own right, and not only as a medium for the sale of illicit commodities such as drugs, firearms or compromised data. The impact of law enforcement action in this arena is palpable as the environment remains in a state of flux.

- **Research & Development:** Technology develops at an ever increasing pace, creating new challenges and opportunities for law enforcement. Adding to this the data volume challenge, legal challenges and a constantly expanding threat surface, there is a need for research and development to develop solutions addressing the needs of law enforcement in an efficient and agile way.

- **Innovation:** The incorporation of innovation, as part of an effective crime response, is not exclusively a private sector affair. Europol and INTERPOL already cooperate with industry partners and academia to identify challenges and opportunities for law enforcement arising from new and emerging technologies, such as 5G.

Mr Steven WILSON, Head of Europol’s European Cybercrime Centre (EC3), said: “Three days of conference with partners from law enforcement, industry and academia have shown what we can achieve when we work closely together to tackle the global issue of cybercrime. We must make progress in prevention, legislation, enforcement, and prosecution. All of these elements are necessary in order to disrupt organised crime activity and reduce the online threat to businesses, governments, and, above all, EU citizens. I look forward to building on our trusted relationships to deliver an improved international response to this ever-increasing challenge.”

With cybercriminals constantly evolving and transforming their tactics, INTERPOL’s Director of...
Cybercrime Craig JONES said the traditional model of policing is ‘being challenged like never before’. “The cybercriminal world is agile and adapting, connecting and cooperating in ways we never imagined even just a few years ago,” said Mr JONES. “Law enforcement must adapt to this ever-changing criminal environment in order to effectively protect our communities in the cyber domain,” he concluded.

On the occasion of this conference, Europol also launched CRYPTOPOL, Europol’s first-ever cryptocurrency-tracing training game, developed and co-created in close cooperation with CENTRIC (Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research). CRYPTOPOL is a simulator of a cryptocurrency investigation with an emphasis on hands-on practice using real-life situations. CRYPTOPOL is accessible to all law enforcement cryptocurrency investigators around the world who can contact Europol to request access to the game. As the game contains information about tracing techniques used by law enforcement there is no intention of making it publicly available.

The Europol-INTERPOL Cybercrime Conference is a joint initiative launched in 2013. Held annually, it is hosted in alternate years by Europol and INTERPOL.