International Police Co-Operation on Cybercrime: The Experience of the Russian Ministry of Interior
The Variety of Encryption and Anonymization Tools

- VPN
- Dark Net
- TOR
- Cryptocurrencies
- Cloud based technologies
The Legal Basis of International Police Co-Operation

Interpol channels

Bilateral and multilateral agreements, including in criminal matters

Liaison officers
Global Interpol Sponsored Cybercrime Operations

SIMDA

DORKBOT

GHOSTDEVIL
WHAT IS BUSINESS EMAIL COMPROMISE?

ILLEGAL ACCESS
Criminals gain entry to a victim’s devices or systems – through hacking, phishing websites, malware – then deceive the victim into transferring money into their bank account.

SOCIAL ENGINEERING
Criminals can target their victims based on information they share on social media platforms.

URGENT REQUEST
The criminal impersonates a supplier requesting an urgent payment or change to banking details, or a senior employee in the company with authority to authorize payments.

#BECareful
INTERPOL
Regional Treaties on Cybercrime

The Council of Europe Convention on Cybercrime (Budapest, November 23, 2001)

Limited application (regional act, not global one)
It does not take into account the current cybercrime trends
It is not fully convenient for developing countries
Lack of holistic approach
Intervention in the internal affairs of States can take place
The priority is given to States providing infrastructure
The number of ratifications (only 65 States during 19 years)
The UN Convention on Cooperation in Combating Cybercrime is a key to success

«Human beings are members of a whole, in creation of one essence and soul. If one member is afflicted with pain, other members uneasy will remain. If you have no sympathy for human pain, the name of human you cannot retain».

Saadi