ECONOMIC CRIME AND CORRUPTION IN CYBERSPACE: NEW CHALLENGES FOR THE INTERNATIONAL COMMUNITY

Dr. Eduard Ivanov, IACA

IACA INTERNATIONAL ANTI-CORRUPTION ACADEMY

Empowering Professionals.

THE USE OF CYBERSPACE FOR CRIMINAL PURPOSES

Economic Crime and Corruption in Cyberspace

- The use of new opportunities to facilitate criminal activities

- Cyberattacks

FACILITATION OF CRIMINAL ACTIVITIES

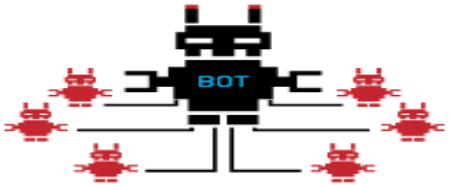
Economic Crime and Corruption in Cyberspace

- Use of new payment methods and e-carrencies for payments in the framework of criminal financial schemes
- Conducting multiple transactions between physical persons for purposes of terrorist financing, drug business, smuggling
- Collecting “charitable donations” for the financing of terrorism
- Use of front persons in ML/TF schemes
- Groups of professional criminal services providers

AIMS OF VARIOUS TYPES OF CYBERATTACKS

- Access to computers and information. The final goals of attacks can be destruction, gathering or manipulation of computer data or causing financial damage (Use of hacking techniques)

- Loss of availability of web-sites (Use of bot – nets)



- Manipulation of IT – systems, responsible for administration and control of objects of physical infrastructure (airports. railway transport, subway etc.)

CORRUPTION AND CYBERSPACE

Economic Crime and Corruption in Cyberspace

- Use of new technologies for payments for corruption services
- Corruption contributes to cybercrime by facilitating access to information about cybersecurity measures

- Corruption can be a prerequisite for non-cooperation in combating crime in cyberspace

NEW CHALLENGES FOR THE INTERNATIONAL COMMUNITY

IACA INTERNATIONAL ANTI-CORRUPTION ACADEMY

Economic Crime and Corruption in Cyberspace

- Use of global cyberspace for criminal purposes
- Use of IT infrastructure in various countries
- Level of legal regulation of the relationship on the Internet is not sufficient
- Identification of the Internet users
- Limited time for requesting cooperation

EU LAWS AND REGULATIONS

Economic Crime and Corruption in Cyberspace

- Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions
- Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market
- Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing
- Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds
- Payment services providers are obliged to take measures to prevent money laundering and financing of terrorism

CHALLENGES FOR PAYMENT SERVICES PROVIDERS

Economic Crime and Corruption in Cyberspace

- Opening an account or providing services without presence of customer at the same place (various thresholds in national AML/CFT laws)
- Defining acceptable level of due diligence
- Mitigating legal and reputational risks

OPENING AN ACCOUNT OR PROVIDING SERVICES

- Directive (EU) 2015/849. Threshold for simplified identification and due diligence – 250 -500 Euro

- Czech Republic – 250 euros, or 500 euros in case of electronic money usable only for domestic payment transactions, or in case of a rechargeable medium, should there be an annual limit of 2,500 euros, with the exception of cases when the holder of electronic money converts back more than 1,000 euros in a calendar year (Selected measures against legitimization of proceeds of crime and financing of terrorism (AML/CFT Act), Act 235/2008 Coll. of 2008)

- Estonia - An electronic money institution may take simplified due diligence measures if an electronic money device does not allow for reloading and the amount saved in one electronic money device does not exceed 250 euros

- Estonia – identification on the basis of a document issued by the Republic of Estonia for digital identification in particular cases (Money Laundering and Terrorist Financing Prevention Act of 2007)

PROBLEMS RELATED TO CYBERATTACKS

Economic Crime and Corruption in Cyberspace

- Definition of cyberterritory of state
- Attribution of cyberattacks
- Assessment of potential damage from cyberattack to apply proportional measures
- Limited time for requesting cooperation in the situation of on-going cyberattack
- Applicable measures in the situation of threat of cyberattack
- Use of intelligence information as an evidence in international judicial procedure

POSSIBLE SOLUTIONS

Economic Crime and Corruption in Cyberspace

- Defining the critical infrastructure and special protection measures (Project of the Global Commission on the Stability in Cyberspace)
- Developing international standards for identification of the Internet – users
- Establishing special international on-line procedures for information exchange and requesting for assistance in cases of on-going or threatening cyberattacks in the circumstances of limited time
- Developing guidance for private sector on cybersecurity measures and related anti-corruption measures
- Developing legal rules which will allow the use of intelligence information in international courts

Thank you for your attention!