C-PROC Cybercrime Webinars

Impact of COVID-19 on Financial Crimes

The GLACY+ Perspective

Matteo Lucchetti

Programme Manager at the Cybercrime Programme Office
of the Council of Europe (C-PROC) in Bucharest, Romania

matteo.lucchetti@coe.int

GLACY+ Project

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

To strengthen the capacities of States worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area.

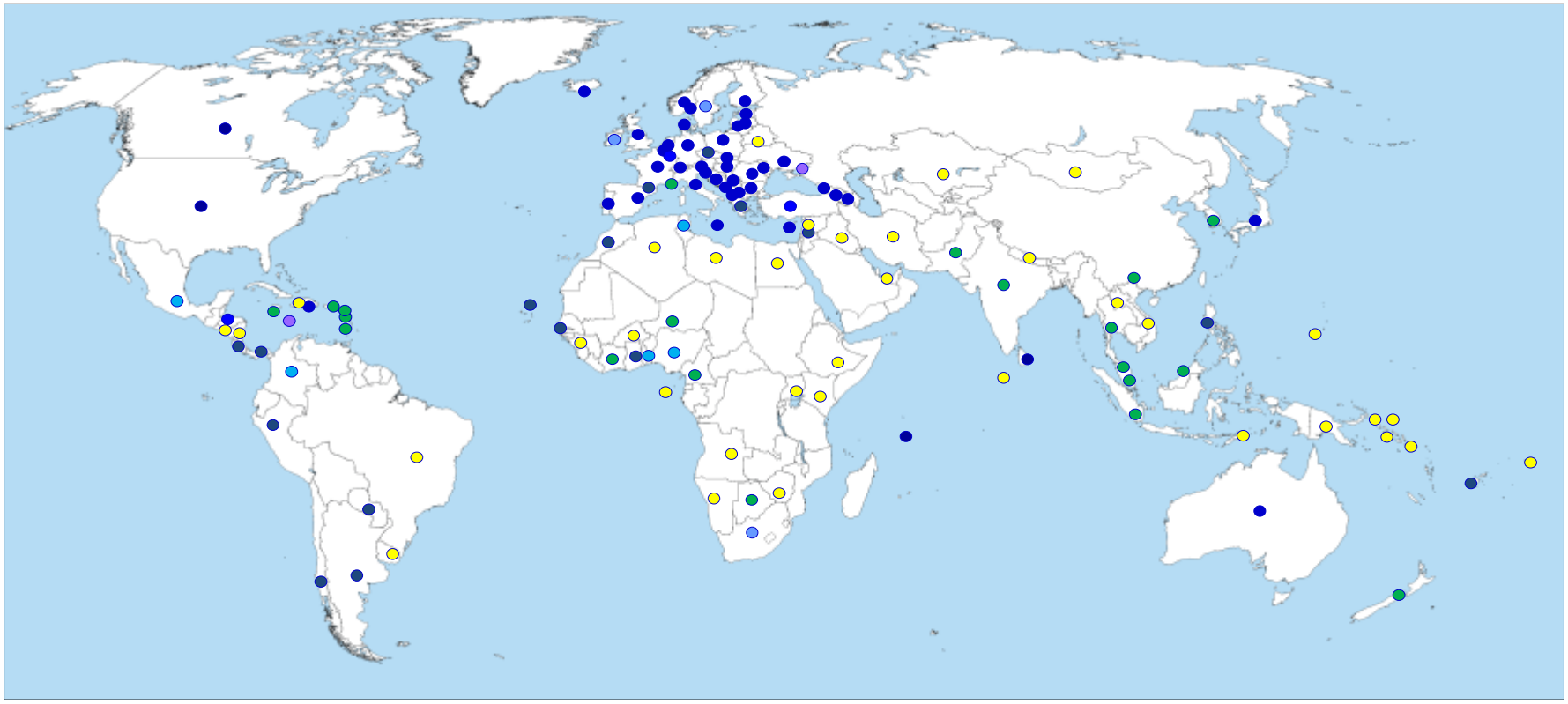
CYBERCRIME LEGISLATION, POLICIES AND STRATEGIES

POLICE AUTHORITIES AND INVESTIGATION CAPACITIES

CRIMINAL JUSTICE AND INTERNATIONAL COOPERATION

Duration	**96 months (Mar 2016 – Feb 2024)**
Budget	**EUR 18.89 million**
Funding	European Union (Instrument Contributing to Peace and Stability) and Council of Europe
GLACY+ Priority and Hub Countries	• Benin • Burkina Faso • Cape Verde • Chile • Costa Rica • Dominican Republic • Ghana • Morocco • Mauritius • Nigeria • Paraguay • Philippines • Senegal • Sri Lanka • Tonga

Reach of the Budapest Convention



Budapest Convention

Ratified/acceded: 65

Signed: 3

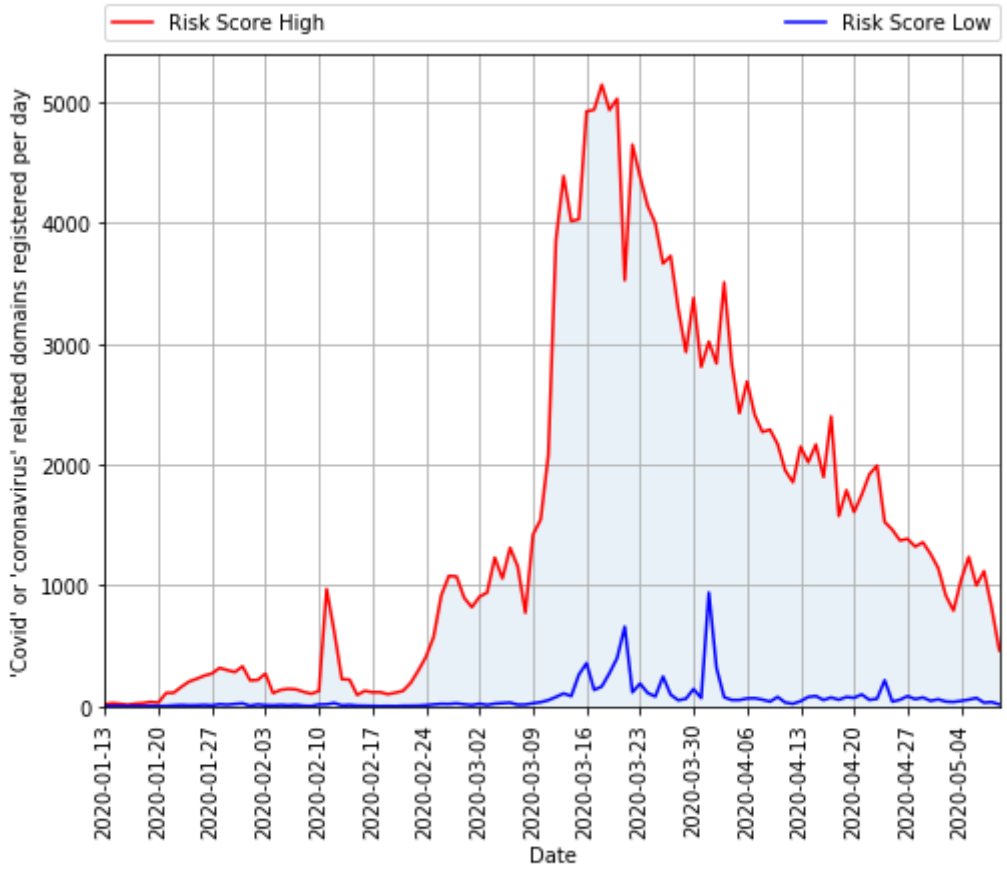
Invited to accede: 8

Other States with laws/draft laws largely in line with Budapest Convention = 20

Further States drawing on Budapest Convention for legislation = 45+

COVID-19 related on-line threats

- **After an initial spike, COVID-19 related domains registered per day are constantly decreasing**



(Source: DomainTools)

COVID-19 related on-line threats

- **After an initial spike, COVID-19 related domains registered per day are constantly decreasing**
- **COVID-19 related spam also decreasing, but still high → Phishing and other social engineering frauds**

COVID-19 related on-line threats

- **After an initial spike, COVID-19 related domains registered per day are constantly decreasing**
- **COVID-19 related spam also decreasing, but still high → Phishing and other social engineering frauds**
- **Targeted ransomware attacks against healthcare/ pharmaceuticals/ research**

06 Europe's Largest Private Hospital Operator Fresenius Hit by Ransomware

MAY 20

Fresenius, Europe's largest private hospital operator and a major provider of dialysis products and services that are in such high demand thanks to the **COVID-19** pandemic, has been hit in a ransomware cyber attack on its technology systems. The company said the incident has limited some of its operations, but that patient care continues.

Based in Germany, the Fresenius Group includes four independent businesses: **Fresenius Medical Care**, a leading provider of care to those suffering from kidney failure; **Fresenius Helios**, Europe's largest private hospital operator (according to the company's Web site); **Fresenius Kabi**, which supplies pharmaceutical drugs and medical devices; and **Fresenius Vamed**, which manages healthcare facilities.

Krebs On Security, 6 May 2020

COVID-19 related on-line threats

- **After an initial spike, COVID-19 related domains registered per day are constantly decreasing**
- **COVID-19 related spam also decreasing, but still high → Phishing and other social engineering frauds**
- **Targeted ransomware attacks against healthcare/ pharmaceuticals/ research**
- **COVID-19 themed Business E-mail Compromise attacks are increasing**

ComputerWeekly.com

SilverTerrier cyber crime group targets Covid-19 key workers

Organisations on the front line in the fight against coronavirus are under attack from Nigeria's SilverTerrier criminal gang

By **Alex Scroxton,** Security Editor

Published: **07 May 2020 15:57**

Organisations in critical sectors such as government, healthcare, insurance, medical research and publishing, and utilities, are being extensively targeted by business email compromise (BEC) campaigns originating from Nigeria's SilverTerrier cyber crime group, according to Palo Alto Networks' Unit 42 threat intelligence team.

COVID-19 related on-line threats

- **After an initial spike, COVID-19 related domains registered per day are constantly decreasing**
- **COVID-19 related spam also decreasing, but still high → Phishing and other social engineering frauds**
- **Targeted ransomware attacks against healthcare/ pharmaceuticals/ research**
- **COVID-19 themed Business E-mail Compromise attacks are increasing**

- **Not new threats**
- **Impact**
- **Targeted attacks**

COVID-19 related on-line threats and the Budapest Convention

- **After an initial spike, COVID-19 related domains registered per day are constantly decreasing**
- **COVID-19 related spam also decreasing, but still high → Phishing and other social engineering frauds**
- **Targeted ransomware attacks against healthcare/ pharmaceuticals/ research**
- **COVID-19 themed Business E-mail Compromise attacks are increasing**

Budapest Convention Guidance Notes

- Identity Theft, perpetrated through social engineering techniques that leverage on the COVID-19 crisis
- Critical infrastructure attacks, with reference to the increased attacks to national health systems and hospitals, but possibly also other critical infrastructures, e.g. through the use of ransomware campaigns themed on COVID-19 issues
- Malware, mostly related to the spread of malicious email/ drive-by-download websites/ other, themed on COVID-19 issues
- Spam, for phishing/ spreading of false information re coronavirus

COVID-19 emergency induced cybercrime threats

Huge increase of reported cases of online child sexual exploitation

- The National Center for Missing and Exploited Children (NCMEC) has received 4.2 million reports in April. That's up 2 million from March 2020 and nearly 3 million from April 2019. (Forbes, 9 May 2020)

Huge increase of COVID-19 related false information/ disinformation campaigns

Increased traffic and bandwidth strain → Increased challenges for providers → Increase in successful DDoS attacks (+17%)

Uncertain employment context → Increase in attempts to recruit online money mules

Increased attacks to remote working environments → Organizations are more vulnerable

COVID-19 related cybercrimes
Impact on the criminal justice sector

- **Emergency laws** that also include aspects on cybercrime investigation and related fields
- International cooperation with **heterogeneous legal frameworks**
- **Collaboration with multi-national service providers** jeopardized in some regions
- Effective **coordination of cross-border investigations**
- **Limited reporting** (1% Problem)
- LE officers, and in some case prosecutors too, being reassigned to enforce the quarantine → **Reduction of staff**
- **Courts functioning with a limited capacity** and a greater workload
- **Capacity building**

Cooperation is key

- **Criminal justice authorities need to make full use of the available tools and engage in full cooperation with each other** to detect, investigate, attribute and prosecute offences and bring to justice those that exploit the COVID-19 pandemic for criminal purposes.

- The ***Budapest Convention on Cybercrime*** a framework for effective cooperation with the necessary rule of law safeguards is available to now **65 state parties**.

- As a result of **capacity building** programmes generated by its implementation with the support of the European Union and the Council of Europe through its Cybercrime Programme Office, many states should be able to act.

- **Additional solutions** are required to address future crises. Capacity building for criminal justice authorities must be further enhanced. And the ***2nd Additional Protocol to the Budapest Convention***, which is currently being negotiated, will be crucial to permit **instant cooperation in urgent and emergency situations**.

Resources and useful links

Dedicated webpage on the Council of Europe website

- Strengthening criminal justice response
- Prevention and protection against cybercrime
- Respecting fundamental rights and the rule of law
- Responses from countries
- **https://www.coe.int/en/web/cybercrime/cybercrime-and-covid-19**

C-PROC Cybercrime Digest

- **https://www.coe.int/en/web/cybercrime/cyber-digests-and-updates**

Cross-sector threat intelligence information sharing

- The COVID19 Cyber Threat Coalition has 3,600+ members
- Indicators of compromise/ vetted blocklists, Web threats, E-Mail threats, Malicious domains, etc.

Thank you

Matteo Lucchetti

Programme Manager at the Cybercrime Programme Office
of the Council of Europe (C-PROC) in Bucharest, Romania

matteo.lucchetti@coe.int

The approach of Council of Europe

1 Common standards: Budapest Convention on Cybercrime and relates standards

2 Follow up and assessments: Cybercrime Convention Committee (T-CY)

3 Capacity building: C-PROC ▶ Technical cooperation programmes

Council of Europe's Convention on Cybercrime – The Budapest Convention

- **Negotiated by Council of Europe (47 members), Canada, Japan, South Africa and USA**
- **Opened for signature on 23 November 2001 in Budapest**
- **Protocol on Xenophobia and Racism via computer systems (2003)**
- **Followed by Cybercrime Convention Committee (T-CY)** – Guidance Notes, Interpretation, Monitoring
- **Open for accession by any State – 65 Accessions/ Ratifications**
- **2nd Additional Protocol under negotiation**
- **As of today, the only international Treaty on cybercrime and electronic evidence**

Budapest Convention: scope

Criminalising conduct

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

Procedural tools

- Expedited preservation
- Search and seizure
- Production order
- Interception of computer data

- **Conditions, safeguards**

+

International cooperation

- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Harmonisation

Procedural powers and international cooperation for ANY CRIMINAL OFFENCE involving evidence on a computer system!

Additional Protocol to the Budapest Convention on Cybercrime

A. Provisions for more efficient MLA

- **Emergency MLA**
- **Joint investigations**
- **Video conferencing**
- **Language of requests**
- **Etc.**

B. Provisions for direct cooperation with providers in other jurisdictions

C. Framework and safeguards for existing practices of extending searches transborder

D. Safeguards/data protection

Terms of reference approved in June 2017.

Negotiations: Sep 2017 – Dec 2020

Joining the Budapest Convention

Treaty open for accession (article 37)

Phase 1:

- A country with legislation in place or advanced stage
- Letter from Government to CoE expressing interest in accession
- Consultations (CoE/Parties) in view of decision to invite
- Invitation to accede

Phase 2:

- Domestic procedure (e.g. decision by national Parliament)
- Deposit of the instrument of accession