

International cooperation on cybercrime

The criminal justice perspective


Matteo Lucchetti


Direttore Operativo

Cyber 4.0 – National Cyber Security Competence Center

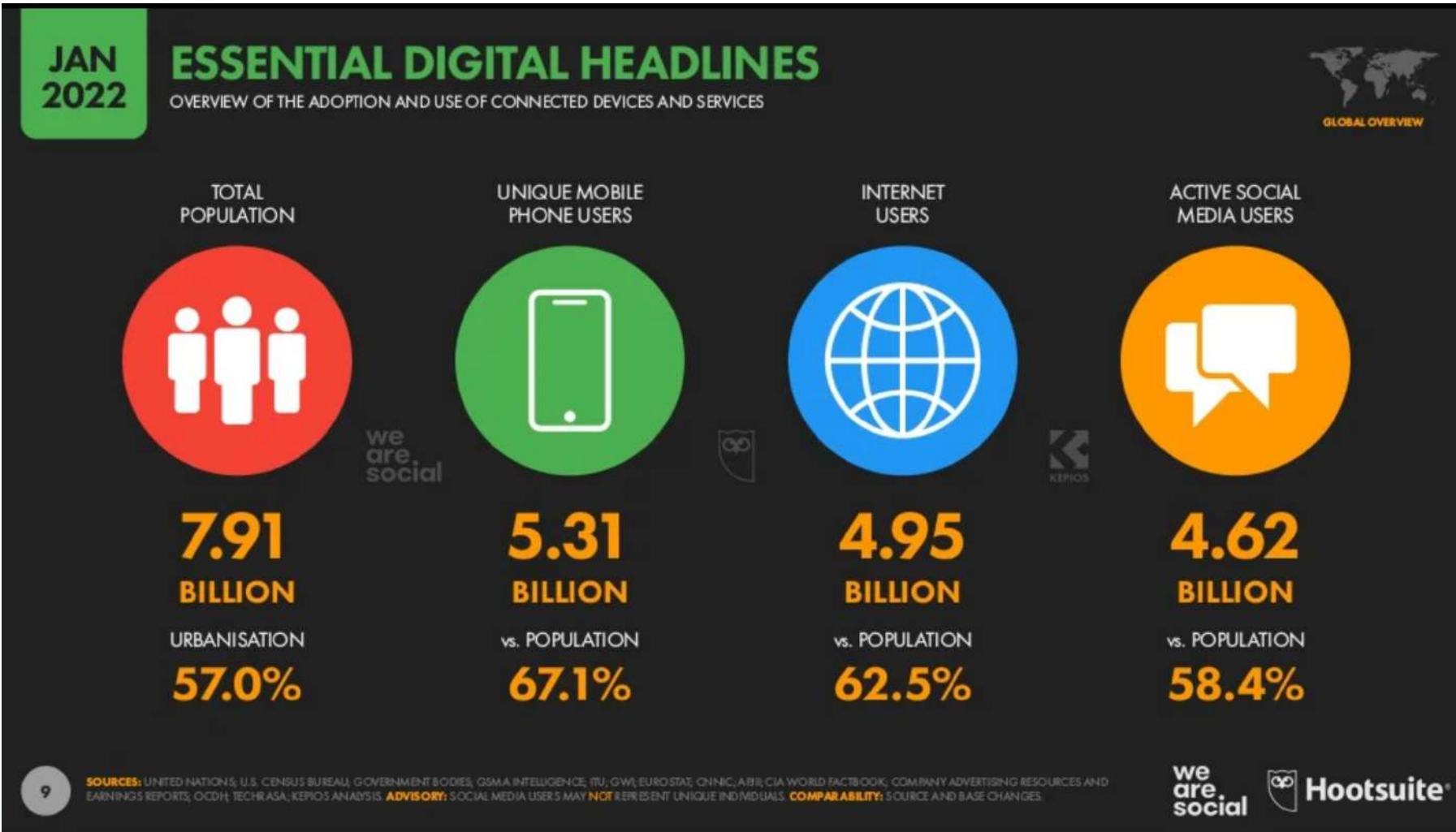
Matteo.Lucchetti@cyber40.it



- The cybercrime landscape
 - Criminal justice issues
 - International cooperation: The Budapest Convention
 - The way ahead
- 

- **The cybercrime landscape**
 - Criminal justice issues
 - International cooperation: The Budapest Convention
 - The way ahead
- 

The information society – A snapshot



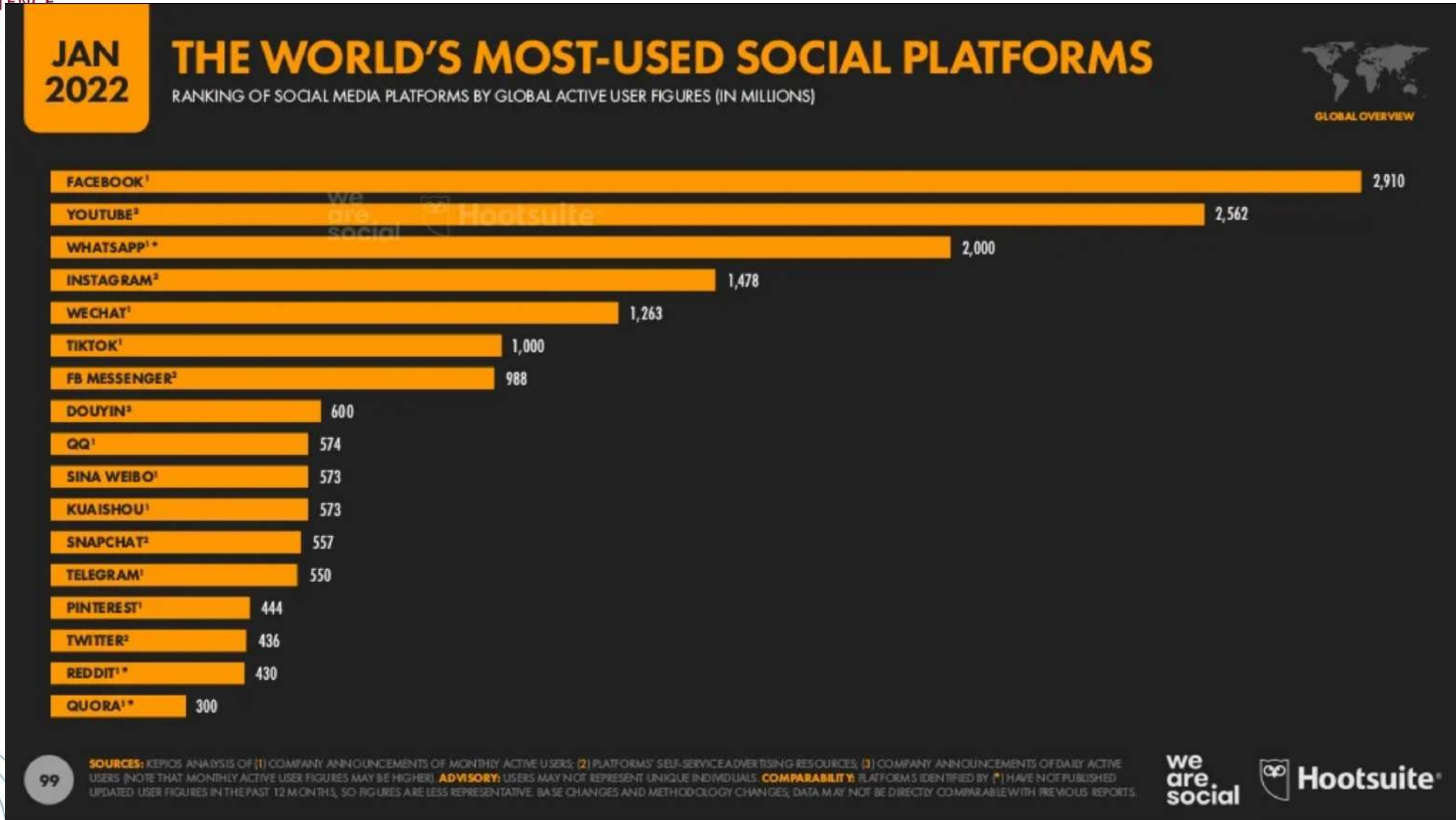
+ 7.3%
2021 vs. 2020
Internet users

+ 4.0%
2022 vs. 2021
Internet users

+ 13.2%
2021 vs. 2020
Social Media active users

+ 10.0%
2022 vs. 2021
Social Media active users

The use of social networks



How much information?

(a useful reminder: mega → giga → tera → peta → exa → zetta..)

- The amount of data in the world was estimated to be **44 zettabytes** at the dawn of 2020.
- In 2020, about **1.7 megabytes of new information was created every second for every human being** on the planet.
- By 2025, the amount of data generated **each day** is expected to reach **463 exabytes** globally.
- Google, Facebook, Microsoft, and Amazon store at least **1,200 petabytes** of information.
- By 2025, there would be **75 billion** Internet-of-Things (IoT) devices in the world
- By 2030, **nine out of every ten people** aged six and above would be **digitally active**.

Technology and crime

<p>TECHNOLOGY AS A VICTIM</p>	<p>Traditionally considered to be true “computer crime” and involves such offences as hacking, denial of service attacks and the distribution of viruses.</p>
<p>TECHNOLOGY AS AN AID TO CRIME</p>	<p>Computers and other devices are used to assist in the commission of traditional crimes, for example, to produce forged documents, to send death threats or blackmail demands or to create and distribute illegal material such as images of child abuse.</p>
<p>TECHNOLOGY AS A COMMUNICATION TOOL</p>	<p>Criminals use technology to communicate with each other in ways which reduce the chances of detection, for example by the use of encryption technology</p>
<p>TECHNOLOGY AS A STORAGE DEVICE</p>	<p>Intentional or unintentional storage of information on devices used in any of the other categories and typically involves the data held on computer systems of victims, witnesses or suspects</p>
<p>TECHNOLOGY AS A WITNESS TO CRIME</p>	<p>Evidence contained in IT devices can be used to support evidence to which it is not obviously related, for example to prove or disprove an alibi given by a suspect or a claim made by a witness.</p>

Cybercrime global trends 2021/2022

- **Cyber-dependent crime**
 - Ransomware-as-a-Service and double extortion
 - Malware
 - DDoS
- **Online child sexual exploitation**
- **COVID-19 demonstrating criminal opportunism**
- **Cybercrime and the war**
- **Cyber espionage**
 - State-sponsored
 - Competition in the private sector
 - Journalists, NGOs
- **Election interference**
- **Use of cyber to support terrorism**
- **AI and Deepfake, Impersonation**
- **Disinformation, misinformation**
- **Computer-related payment frauds**
 - Business Email Compromise
 - Card Not Present frauds and terminal attacks
- **Criminal abuse of Darknets**
 - On-line criminal markets
 - CaaS – Cybercrime as a Service
- **Intellectual property and Internet piracy**

Ransomware-as-a-Service REvil and Colonial Pipeline, May 2021

- Colonial Pipeline is one of the largest pipeline operators in the United States and provides roughly 45% of the East Coast's fuel, including gasoline, diesel, home heating oil, jet fuel, and military supplies.
- The company says that it transports over 100 million gallons of fuel daily across an area spanning Texas to New York.



Colonial Pipeline, May 2021

```
sophos_READ [REDACTED].TXT - Notepad
File Edit Format View Help
----- [ Welcome to DarkSide ] ----->

What happend?
-----
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.
Follow our instructions below and you will recover all your data.

Data leak
-----
First of all we have uploaded more then 140GB data.

These files include:
- Accounting
- Research & Development

Your personal leak page: http://darkside[REDACTED]
On the page you will find examples of files that have been stolen.
The data is preloaded and will be automatically published if you do not pay.
After publication, your data will be available for at least 6 months on our tor cdn servers.

We are ready:
- To provide you the evidence of stolen data
- To delete all the stolen data.

What guarantees?
-----
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
We guarantee to decrypt one file for free. Go to the site and contact us.

How to get access on website?
-----
Using a TOR browser:
1) Download and install TOR browser from this site: https://torproject.org/
2) Open our website: http://darkside[REDACTED]

When you open our website, put the following data in the input form:
Key:
```



Patrick De Haan
@GasBuddyGuy

GASOLINE OUTAGES as of 11pm CT... percent of all stations in state without gasoline:

- GA 10.4%
- AL 1.1%
- TN 1.0%
- SC 8.3%
- NC 16.0%
- FL 3.4%
- VA 10.2%
- MD 1.6%

5:12 AM · May 12, 2021 · TweetDeck





Colonial Pipeline, May 2021

- During the attack, over 100GB in corporate data was stolen in just two hours.
- On May 13, Bloomberg reported that **the company paid a ransom demand of close to \$5 million in return for a decryption key.**
- On 13 May, US President Biden signed an executive order to improve federal cybersecurity, noting that **agencies need to «lead by example»**:
 - a shift to *multi-factor authentication*
 - *data encryption* both at rest and in transit
 - a *zero-trust security model*,
 - improvements in *endpoint protection* and *incident response*
 - A **Cybersecurity Safety Review Board** will also be established.

Revil/ DarkSide ransomware, double extortion

- DarkSide is a [Ransomware-as-a-Service \(RaaS\) group](#) that offers its own brand of malware to customers on a subscription basis.
- A decryptor for DarkSide malware on Windows machines was released by [Bitdefender in January](#) 2021. In response, the group said the decryptor was based on a key previously purchased and may no longer work as "this problem has been fixed."
- DarkSide has already created a leak website used in **double-extortion campaigns, in which victim companies are not only locked out of their systems, but also have their information stolen.**
- **If these organizations refuse to pay up, stolen data may be published on the platform and made available to the public, or used to work with competitors or investors before leaks are published.**

REvil arrests by US, support by Conti, takedown by Russia

REvil Ransom Arrest, \$6M Seizure, and \$10M Reward

“ANNOUNCEMENT. REVILIVES.”

Nov 14

Own opinion.

The ransom has e in cry to \$1 affilia

As a team, we always look at the world from a perspective of data security, information systems, and support them in their hardships. Therefore, we would like to commend the law enforcement about the attack on the

We want to remark the following:

First, an attack against some servers is a reminder of what we all know: the United States in world affairs.

However, the fact that it became a national issue is a bone from bankers or politicians, without conscience, as well as anonymity, which "allied" governments are afraid of saying.

With all the endless talks in your meetings, the biggest ransomware group of all time was the REvil attack. First, because REvil has been arrested, the United States government acted as

At Request of U.S., Russia Rounds Up 14 REvil Ransomware Affiliates

January 14, 2022

54 Comments



The Russian government said today it arrested 14 people accused of working for “REvil,” a particularly aggressive ransomware group that has extorted hundreds of millions of dollars from victim organizations. The Russian Federal Security Service (FSB) said the actions were taken in response to a request from U.S. officials, but many experts believe the crackdown is part of an effort to reduce

tensions over Russian President Vladimir Putin’s decision to station 100,000 troops along the nation’s border with Ukraine.

The Conti ransomware gang's support to Russia

“WARNING”

The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructures of an enemy.

2/25/2022

“WA
As a response
warmongering and
use cyber warfare
Russian Federation
officially announcin
full capacity to deliv
measures in case t
warmongers attem
infrastructure in Ru
speaking region of
ally with any govern
condemn the ongo
since the West is k
primarily by targetin
our resources in or
well being and safety of peaceful citizens
will be at stake due to American cyber
aggression.

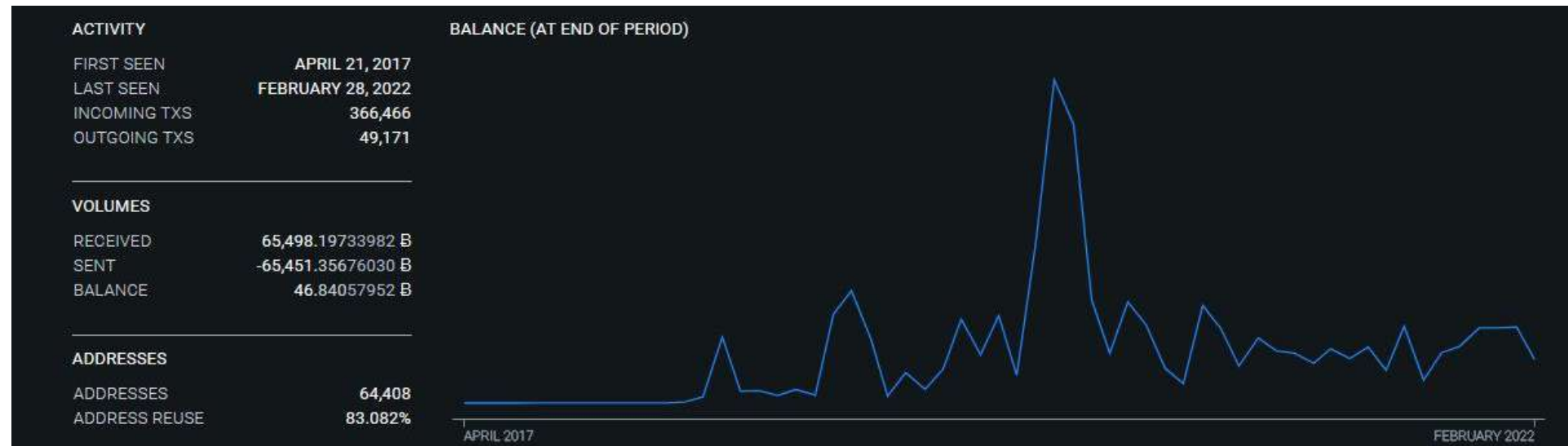
Conti ransomware gang's internal chats leaked online after declaring support for Russian invasion


Zack Whittaker @zackwhittaker / 5:35 PM GMT+1 • February 28, 2022

Comment

The Conti ransomware gang

- Through Contileaks the primary Bitcoin address of the Conti ransomware gang has been revealed
- From 21 April 2017 to 28 February 2022 the address received 65.498,197 BTC. That's **2.707.466.220,29** USD
- Conti was first detected in 2020
→ the address had been used already for three years, likely in the name of other gangs



- The cybercrime landscape
 - **Criminal justice issues**
 - International cooperation: The Budapest Convention
 - The way ahead
- 

Cybercrime is a threat to fundamental rights

- Affects the **right to private life** of hundreds of millions of individuals whose personal data are stolen
- Can be an **attack against the dignity and the integrity of individuals**, in particular sexual exploitation and abuse of children
- Is a **threat to the freedom of expression** when attacks are carried out against media, civil society organizations, etc.
- **Threatens public security and services**, such as governments, parliaments and other public institutions and critical infrastructures
- Is a **threat to democratic stability**, when ICT is used for xenophobia and racism, or radicalization and serve terrorism
- **Undermines trust in democratic institutions**, such as in interfering with the electoral processes



**CRIMINAL
JUSTICE
RESPONSE**

NEWS Home > Security > Hacking

Less than 1% of computer hacking offences resulted in prosecution in 2019

Of the 17,600 offences recorded in the UK, just 57 were able to be tried under the Computer Misuse Act, report finds

by: [Bobby Hellard](#) 1 Oct 2020



- “Not only is the current wave of **cybercrime** largely unseen, but the **chances of being successfully investigated and prosecuted for a cyber attack in the US** are now estimated at **0.05%**.”
- **For violent crime** the equivalent chance is **46%**.

(World Economic Forum, 2018)

Electronic evidence and International criminal justice cooperation

In 2018 the European Commission estimated that

- **85% of all criminal investigations require e-evidence** and of that percentage, two thirds (65%) are said to involve a cross-border request to a service provider.
- **55% of total investigations include a request to cross-border access to e-evidence** or in other words more than half of all investigations include a cross-border request to access e-evidence

Challenges for criminal justice authorities

- **Scale and quantity** of criminal conducts online, data, devices, users and victims
- **Under-reporting** and the <1% problem
- **Heterogeneous legal frameworks**, international standards
- Identification, collection and use of **electronic evidence and admissibility issues**
- **Direct collaboration with Service Providers**
- **International cooperation with foreign jurisdictions** and effective coordination of cross-border investigations
- **Cloud computing, territoriality and jurisdiction**

Challenges for criminal justice authorities – cont'd

- Increased need of **capacity building vs. available resources**
- **Technical challenges**
 - **Detection** (e.g. botnet detection) and predictive analysis of data
 - Identity/ **Attribution** (e.g. CGN)
 - **Broad use of anonymity techniques** (darknets and virtual currencies)
 - **Availability and use of information vs. need to protect personal data** (e.g. data retention, WHOIS)
 - **Protected data and encryption vs. right to not incriminate oneself**
 - **Increasing use of AI for criminal purposes** (e.g. deepfake)

Obama says hello



Deepfake and cyber operations

Forbes

Sep 3, 2019, 04:42pm EDT | 47,443 views

A Voice Deepfake Was To Scam A CEO Out Of \$243,000



Jesse Damiani Contributor 

Consumer Tech

I cover the human side of VR/AR, Blockchain, AI, Startups, Media.



TLP:WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

10 March 2021

PIN Number

210310-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Field Office**.

Local Field Offices:
www.fbi.gov/contact-us/field-offices

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS-CISA.

This PIN has been released **TLP:WHITE**: Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber and Foreign Influence Operations

AI and the war Russia-Ukraine



NEWS

Deepfake video of Zelensky telling Ukrainians to surrender removed from social platforms

By Joshua Rhett Miller

March 17, 2022 | 12:20pm | Updated



TECHNOLOGY


Ukraine is scanning faces of dead Russians, then contacting the mothers

Ukrainian officials say the use of facial recognition software could help end the brutal war. But some experts call it 'classic psychological warfare' that sets a gruesome precedent.



By [Drew Harwell](#)

April 15, 2022 at 5:00 a.m. EDT

- The cybercrime landscape
 - Criminal justice issues
 - **International cooperation: The Budapest Convention**
 - The way ahead
- 

The Council of Europe approach

1. Common standards: Budapest Convention on Cybercrime and related standards

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



3. Capacity building:
C-PROC ► Technical cooperation programmes

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 to be opened for ratifications on 12 May 2022**
- ▶ **As of today, the only international Treaty on cybercrime and electronic evidence**

The 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**

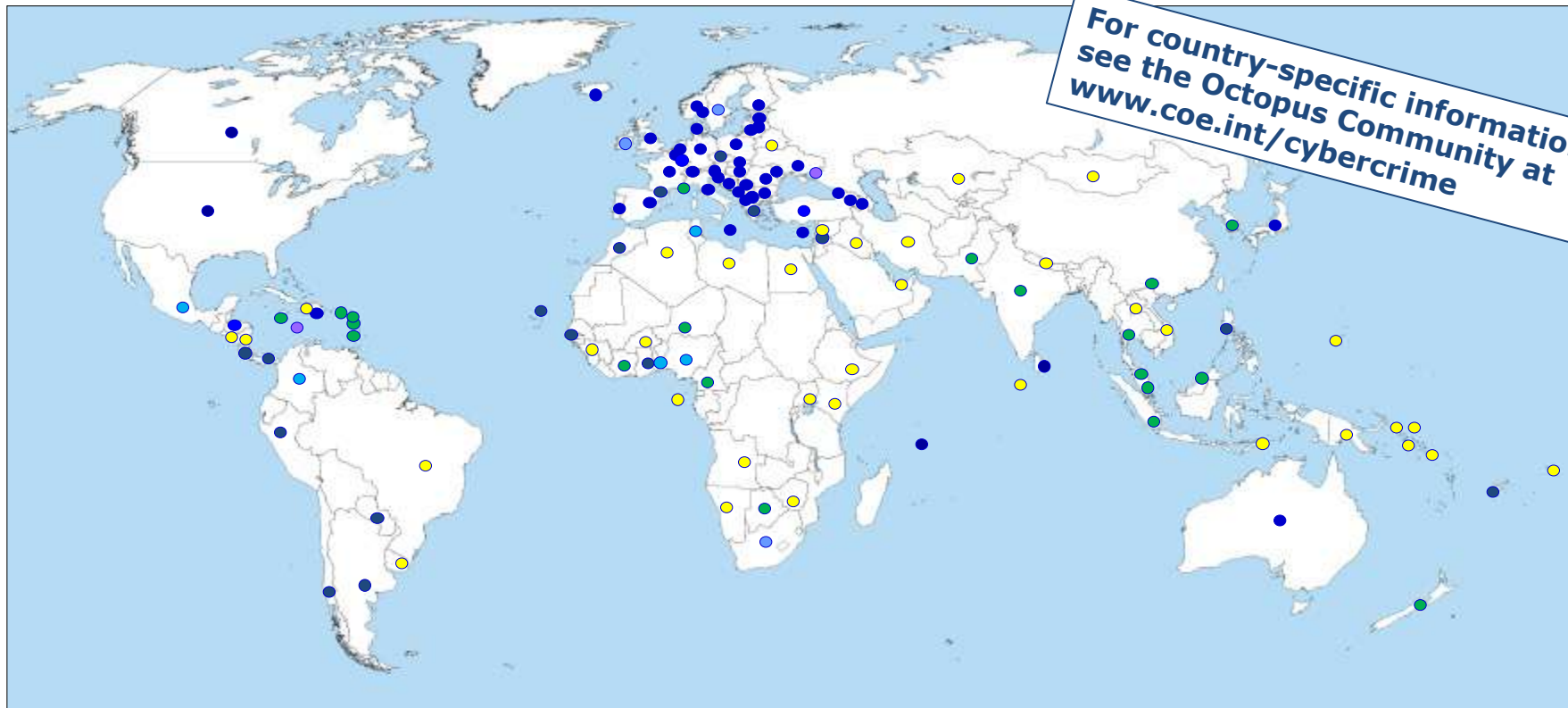
+

International cooperation

- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- Trans-border Access to Data
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

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

Reach of the Budapest Convention



For country-specific information
see the Octopus Community at
www.coe.int/cybercrime

Budapest Convention

Ratified/acceded: 66

Signed: 2

Invited to accede: 10

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

**Further States drawing
on Budapest
Convention for
legislation = 45+**



Links to the Budapest Convention

	Party, signatory or invited to accede to Budapest Convention					
	States	By January 2013			By March 2022	
All Africa	54	3	6%	11	20%	
All Americas	35	8	23%	13	37%	
All Asia	42	2	5%	4	10%	
All Europe	48	43	90%	46	96%	
All Oceania	14	1	7%	5	36%	
All	193	57	30%	79	41%	

- **128 States with substantive law in line with the Budapest Convention**
- **93 States with procedural law in line with the Budapest Convention**

The 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
- Trans-border Access to Data
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

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

Offences against the confidentiality, integrity and availability of computer data and systems (1/2)


- **Illegal Access** (Art. 2)

- To access to the whole or any part of a computer system
- **Intentionally and without right**

- **Illegal Interception** (Art. 3)

- Intentionally, and without right
- To intercept, by technical means, non-public transmissions of computer data
- To, from or within a computer system

- **Data Interference** (Art. 4)

- Damaging, deletion, deterioration, alteration or suppression of computer data
 - Intentionally, without right
- 

Offences against the confidentiality, integrity and availability of computer data and systems (2/2)

- **System Interference** (Art. 5)

- The serious hindering of the functioning of a computer system
- By inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data
- Intentionally, without right

- **Misuse of devices** (Art. 6)

- Intentionally, without right
- To produce, sale, procure for use, import, distribute or otherwise make available
 - **A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2 – 5;**
 - **a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed** with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5
- To possess an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5.

Computer-Related Offences

- **Computer-related Forgery** (Art. 7)

- Input, alteration deletion, or suppression of computer data, resulting in **inauthentic data**
- With the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible
- Intentionally, without right

- **Computer-related fraud** (Art. 8)

- Intentionally, without right
- The causing of **a loss of property to another** by:
 - (a) any **input, alteration, deletion or suppression of computer data,**
 - (b) any **interference with the functioning of a computer or system,**with the intent of procuring, without right, an economic benefit for oneself or for another

Content-Related Offences

- **Child Pornography (Art. 9)**

- Intentionally, without right

- (a) producing child pornography for the purpose of its distribution through a computer system;
- (b) offering or making available child pornography through a computer system;
- (c) distributing or transmitting child pornography through a computer system;
- (d) procuring child pornography through a computer system for oneself or for another;
- (e) possessing child pornography in a computer system or on a computer-data storage medium.

- Includes pornographic material that **visually depicts**

- (a) a minor engaged in sexually explicit conduct;
- (b) a person appearing to be a minor engaged in sexually explicit conduct;
- (c) realistic images representing a minor engaged in sexually explicit conduct.

- “minor” shall include all persons under 18 years of age

Content-Related Offences

- **Intellectual Property Rights – IPR (Art. 10)**

- Doesn't create a new regulation on the subject, purpose is to apply previous rules on copyright, extending relevant provisions to the on-line reality
- Infringements of copyright on-line, or committed by the means of a computer system, must be punished as if it was committed in the real world
- References to existing international treaties
 - Paris Agreement (24 July 1971)
 - Bern Convention
 - WIPO Treaties

- **Ancillary liability and sanctions**

- Aiding and abetting (Art. 11)
- Criminal responsibility of legal entities (Art.12)

Online defamation in Thailand

Man jailed for 35 years in Thailand for insulting monarchy on Facebook

Bangkok military court convicts 34-year-old in one of harshest sentences handed down for draconian royal defamation law



A Thai man has been jailed for 35 years for **Facebook** posts deemed insulting to the royal family, a watchdog said, in one of the harshest sentences handed down for a crime that insulates Thailand's ultra-rich monarchy from criticism.

A Bangkok military court convicted him of 10 counts of lese-majesty for posting photos and videos of the royal family on a Facebook account that purported to belong to a different user.

Wichai, 34, whose last name was withheld to protect his relatives from ostracism, was accused of using the account to slander a former friend, said iLaw, a group that tracks royal defamation cases.

“The court punished him with seven years per count. Altogether he was given 70 years, but it was reduced in half because he confessed,” said Yingcheep Atchanont from iLaw.

Thailand's lèse-majesté laws

Strict lèse-majesté laws make it a crime to criticise, defame or insult members of the royal family.

In practice, this means open discussion or critical reporting about the royal family is considered illegal.

The military junta, which seized power in 2014, has been criticised for using the law - which can see people jailed for up to 15 years on each count - to stifle opposition.


In 2015, a man was jailed for 30 years over six Facebook posts and the local printer of the New York Times refused to publish an edition with a story on the king.

Online defamation in USA

14 Jan 2022

Reuters ✓
16 h · 🌐

President Joe Biden announced his administration's plans to spend \$27 billion to fix thousands of U.S. bridges, the latest roll-out associated with the \$1 trillion infrastructure bill
<https://reut.rs/3GLoKp7>



👍👎❤️ 235 Commenti: 101 Condivisioni: 31

[Redacted]



Mi piace · Rispondi · 14 h 👍 3

[Redacted]

You're a joke pal, you need to be in a nursing home being spoon fed apple sauce you senile POS! 😏

Mi piace · Rispondi · 43 m

[Redacted]

#BABBLING #BIDEN==#BUFFOON with Dementia.

Mi piace · Rispondi · 16 h 😏 1

Over-criminalization issue

► **Cybercrime laws used to prosecute speech/ Content-related crimes**

- The protection of national security and public order is a legitimate ground for restricting freedom of expression where that restriction is
 - prescribed by law
 - necessary in a democratic society
 - proportionate
- Broad, vaguely defined provisions do not meet these requirements
 - “use of computers to create chaos in order to weaken the trust of the electronic system of the state or provoke or promote armed disobedience, provoke religious or sectarian strife, disturb public order, or harm the reputation of the country ... ”
 - “creation of sites with a view to disseminating ideas contrary to public order or morality”
- **Problematic trend ► Discredits legitimate action on cybercrime ► violates fundamental rights**

► **Need to adopt international standards → Budapest Convention**

The 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
- Trans-border Access to Data
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

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

The 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
- Trans-border Access to Data
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

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

International cybercrime investigations and data requests

International cooperation: Types of requests and data needed

Types of data requested:

- 1. Subscriber information**
(80+%?)
- 2. Traffic data**
- 3. Content data**

Underlying offences

- 1. Fraud and other financial crimes**
- 2. Violent and serious crime** (murder, assault, trafficking, child abuse etc.)
- 3. Offences against computer systems**

International cooperation – Art. 26

Spontaneous Information (Art. 26)

- The authorities from a Party, within an internal investigation, **discover that some of the information they obtained must be forwarded to the authorities of other Party**
- It can be done if the information seems to be useful or necessary to the beginning or the developing of an investigation respecting to a criminal offence in the framework of the Convention
- **Confidentiality**
- **Collection of information from another jurisdiction without using MLA treaties**

Expedited Preservation (Art. 29)

- Expedited preservation of data stored in a computer system
- Parallel framework to the internal provision, it allows one contracting **Party to require from other Party the expedited preservation of data**, if at the same time expresses its **intention of sending a formal request of assistance** for a search, or a seizure, or any similar measure
- The requested party must act as necessary, with all the due diligence, to preserve the requested data, according to its own national law

Expedited Disclosure of Preserved Traffic Data (Art. 30)

- International equivalent of domestic power established under Article 17
- Requested state observes that preserved traffic data reveals that transmission of the communication was routed through a service provider in (i) a third state; or (ii) the requesting state itself, it must **expeditiously disclose such preserved traffic data**
- Disclosure must be of sufficient amount of data to identify service provider(s) involved and path of communication
- Grounds for refusal

Mutual assistance regarding accessing of stored computer data (Art. 31)

Request to **another State** to **search** [or similarly access] or **seize** [or similarly secure] **and disclose** data stored by means of a computer system

- Located within the territory of the requested State
- Including data that has been preserved pursuant to Article 29

International cooperation – Art. 32

Transborder Access to Stored Computer Data with Consent or Where Publicly Available (Art. 32)

- Possibility given to law enforcement from a Party **to obtain evidence stored in a computer physically located in other Party's territory**
- Without any request of international cooperation if, during a concrete investigation, the officers in charge
 - a) need to obtain open source information from a computer located in a foreign country ; or
 - b) **access data with the lawful and voluntary consent of the lawfully authorised person**
- Does not require mutual assistance between Parties. Does not require notification to the other party. Does not exclude notification
- **Article 32b**
 - **Explicit consent required**
 - **Person who has the lawful authority to disclose the data depends on circumstances, laws and regulations**

Mutual Assistance Regarding Real Time Collection of Traffic Data (Art. 33)

- Key traffic data often deleted automatically by service providers before it can be preserved; thus real-time power required
- Enables a Party to request another Party **to exercise its domestic power equivalent to Article 20**
- States may limit the range of offences for which mutual assistance may be provided under this article. Range of offences covered cannot be more narrow than range of offences available in equivalent domestic case

Mutual assistance regarding the interception of content data (Art. 34)

- Mutual assistance in the real-time collection or recording of content data of specified communications transmitted by means of a computer system **to the extent permitted under their applicable treaties and domestic laws.**
- International **equivalent of domestic procedural power under Article 21**

24/7 Network (Art. 35)

- Obligation to create a permanently available contact point, 24/7
- General objectives of these contact points to facilitate international co-operation
 - giving **technical advisory** to other contact points
 - activating the proper mechanism to **expedited preservation of data**
 - urgently **collecting evidence**
 - identifying and discovering suspects
- Operational network of experts on high-tech criminality to provide quick help and cooperation even if a formal cooperation request must follow this informal way
- Immediate preservation of traffic data and other stored data worldwide

- The cybercrime landscape: criminal justice issues
- International cooperation: The Budapest Convention
- **The way ahead**



Mutual Legal Assistance and the Cloud Evidence

- Mutual legal assistance remains a primary means to obtain electronic evidence for criminal justice purposes
- **MLA needs to be made more efficient**
- Often subscriber information or traffic data needed first to substantiate or address an MLA request
- The issues of the **evidence in the cloud**
 - MLA often not feasible to secure volatile evidence in unknown or multiple jurisdictions
 - Loss of location: to whom to send an MLA request?

Direct cooperation with providers across jurisdictions

- **Example: Voluntary disclosure [of subscriber information] by service providers**
- **Current practices:**
 - **More than 170,000 requests/year by BC Parties/Observers to major US providers**
 - **Disclosure of subscriber information (ca. 64%)**
 - **Providers decide whether to respond to lawful requests and to notify customers**
 - **Provider policies/practices volatile**
 - **Data protection concerns**
 - **No disclosure by European providers**
 - **No admissibility of data received in some States**
- **► Clearer / more stable framework required**

Second Additional Protocol to the Budapest Convention on Cybercrime

A. Provisions for more efficient MLA

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

B. Provisions for direct cooperation with providers in other jurisdictions

- **Subscriber information**
- **WHOIS**

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

D. Safeguards/data protection

Negotiations:
Sep 2017 to May 2021

Adopted: November 2021

Will be opened for signature
on **12 May 2022**

A new UN Treaty?

August 13, 2021 12:55PM EDT

Cybercrime is Dangerous, But a New UN Treaty Could Do Worse for Rights

The hypocrisy of Russia's push for a new global cybercrime treaty

MERCEDES PAGE

The same Russia in the middle of invading a neighbour is preaching respect for state sovereignty online.

Russia has suggesting draft departing framework inconsistent international

restrictions on international... around further fragmentation of the global efforts to tackle cybercrime.

Joyce Hakmeh



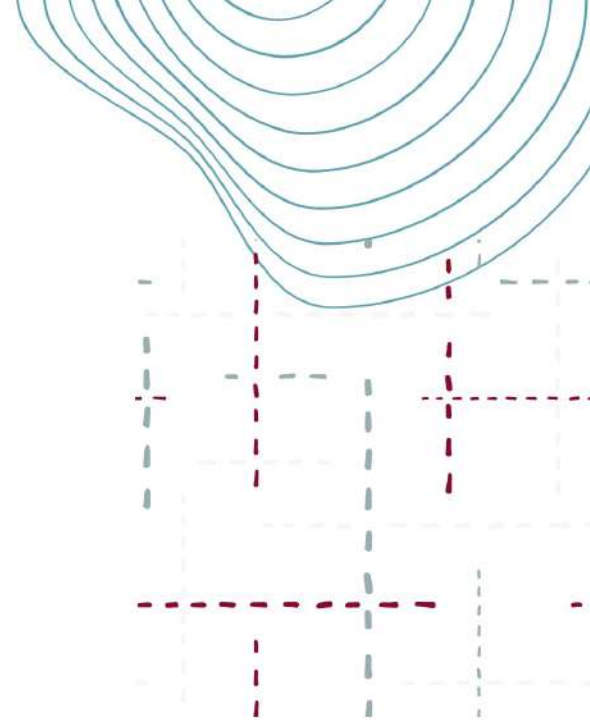
Thank you

Matteo Lucchetti

Director

Cyber 4.0 – National Cyber Security Competence Center

Matteo.Lucchetti@cyber40.it



Back-up

Matteo Lucchetti

Director

Cyber 4.0 – National Cyber Security Competence Center

Matteo.Lucchetti@cyber40.it

Investigating cybercrimes

Service providers and data

- **Cybercrime Convention: 'service providers'**

- "any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
- any other entity that processes or stores computer data on behalf of such communication service or users of such service."

- **Service Provider data**

- Content data
- Traffic data
 - "indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."
- Subscriber information



Procedural Powers Scope (Art. 14)

Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

- the **criminal offences established in accordance with Articles 2 through 11** of this Convention;
- **other criminal offences committed by means of a computer system;** and
- **the collection of evidence in electronic form of a criminal offence.**

Article 15 – Conditions and safeguards

- Establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law,
 - which shall provide for the **adequate protection of human rights and liberties**, including rights arising pursuant to obligations it has undertaken under international conventions
 - and which shall incorporate the **principle of proportionality**
- Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include
 - **judicial or other independent supervision,**
 - **grounds justifying application, and**
 - **limitation of the scope and the duration of such power or procedure.**

Procedural powers – Expedited preservation, Artt. 16/ 17

Expedited preservation of stored computer data

- Expeditious preservation of specified computer data, including traffic data
- To oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days,
- To oblige the custodian or other person who is to preserve the computer data to **keep confidential the undertaking** of such procedures for the period of time provided for by its domestic law.

Expedited Preservation and Partial Disclosure of Traffic Data

- in respect of traffic data that is to be preserved under Article 16
 - Available **regardless of whether one or more service providers were involved** in the transmission
 - Disclosure of **a sufficient amount of traffic data** to enable the Party to identify the service providers and the path through which the communication was transmitted

Procedural powers – Art. 18

Production Order (Art. 18)

- To empower law enforcement authorities to order:
 - a) a person in its territory to submit specified computer data in that person's possession or control; and**
 - b) a service provider offering its services in the territory of the Party** to submit subscriber information relating to such services.
- Order to provide
 - data stored in a computer system under their responsibilities
 - subscriber information

Procedural powers – Art. 19

Search and seizure of Stored Computer Data (Art. 19)

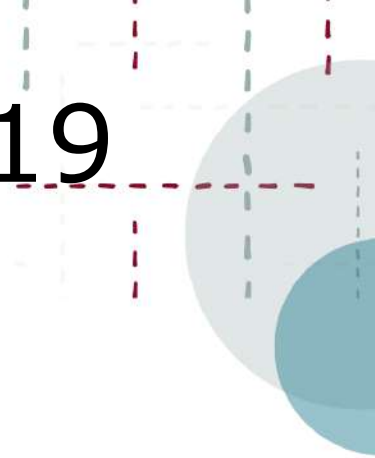
To empower its competent authorities to **search or similarly access:**

- **a computer system or part of it** and computer data stored therein; and
- **a computer-data storage medium** in which computer data are stored in its territory

Power to **expeditiously extend the search to connected systems**

Power to:

- **seize or similarly secure** a computer system or part of it or a computer-data storage medium;
- **make and retain a copy;**
- **maintain the integrity; render inaccessible** or remove computer data in the accessed computer system.



Procedural powers – Art. 20

Real-time Collection of Traffic Data (Art. 20)

To empower its competent authorities to:

- a) collect or record through the application of technical means on the territory of that Party, and
- b) compel a service provider, within its existing technical capability:
 - a) to collect or record through the application of technical means on the territory of that Party; or
 - b) to co-operate and assist the competent authorities in the collection or recording of, **traffic data**, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

To oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

Procedural powers – Art. 21

Interception of Content Data (Art. 21)

To empower its competent authorities to:

a) collect or record through the application of technical means on the territory of that Party, and

b) compel a service provider, within its existing technical capability:

a) to collect or record through the application of technical means on the territory of that Party; or

b) to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

- **General or indiscriminate surveillance or collection of large amounts of content data not permitted**