CYBERCRIME AND INTERNATIONAL COOPERATION

Current Scenario and Future Perspectives

Matteo Lucchetti

Direttore Operativo

Cyber 4.0 – National Cyber Security Competence Center

Matteo.Lucchetti@cyber40.it

Agenda

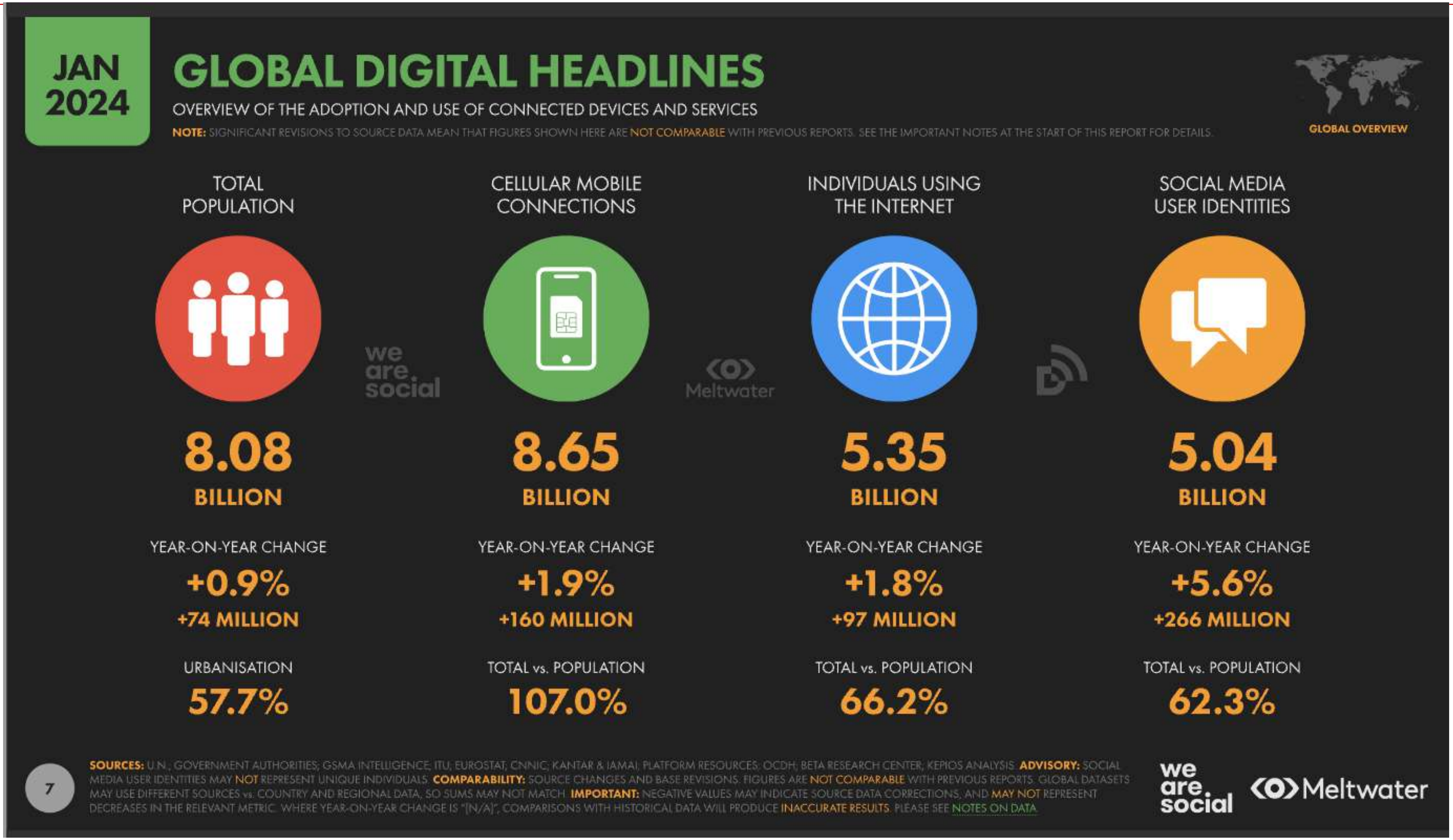
- The cybercrime global landscape
- Criminal justice international cooperation
- The way ahead

Agenda

- **The cybercrime global landscape**
- Criminal justice international cooperation
- The way ahead

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

The information society – A snapshot



JAN 2024

GLOBAL DIGITAL HEADLINES

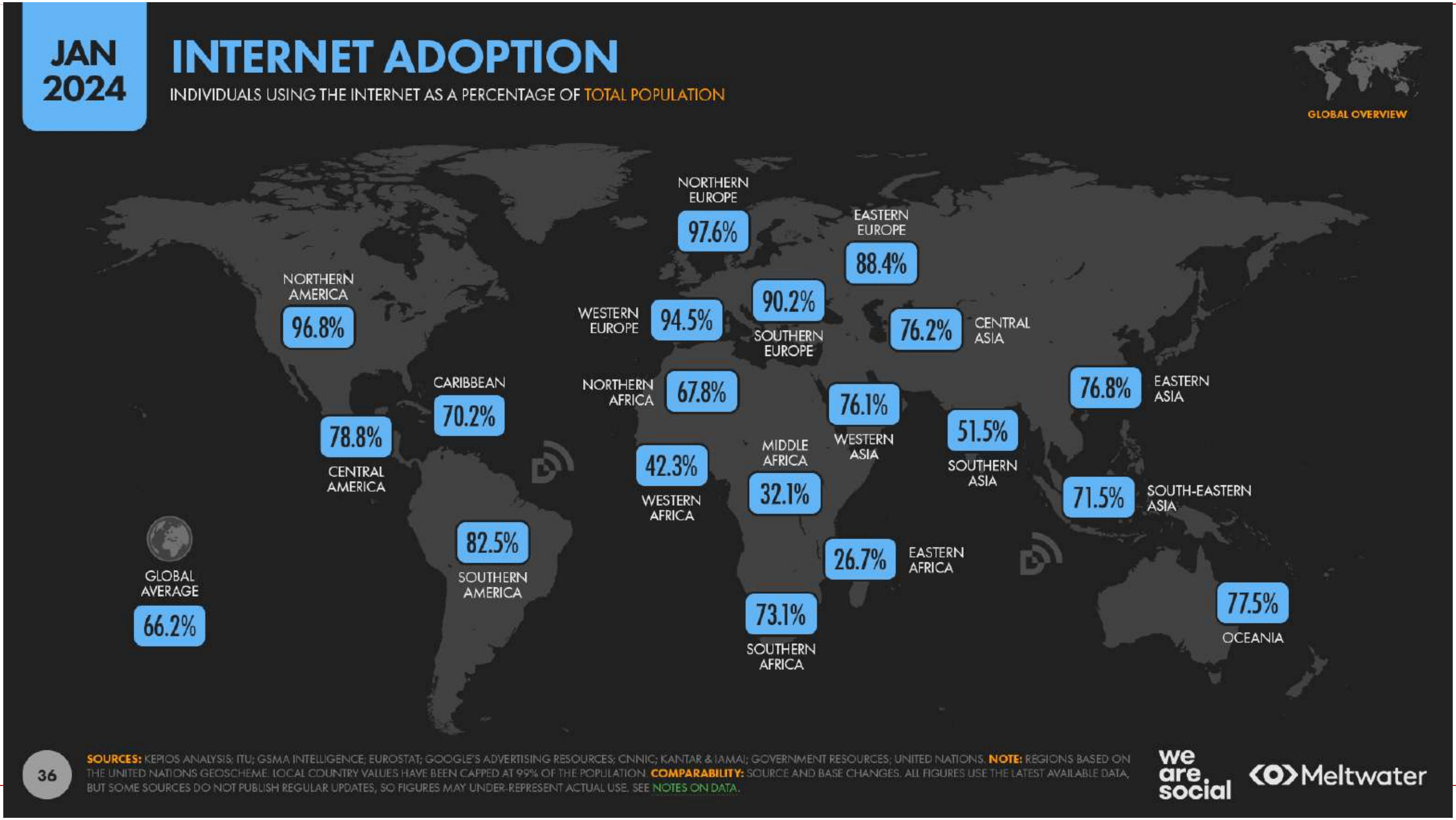
OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES

NOTE: SIGNIFICANT REVISIONS TO SOURCE DATA MEAN THAT FIGURES SHOWN HERE ARE NOT COMPARABLE WITH PREVIOUS REPORTS. SEE THE IMPORTANT NOTES AT THE START OF THIS REPORT FOR DETAILS.

TOTAL POPULATION	CELLULAR MOBILE CONNECTIONS	INDIVIDUALS USING THE INTERNET	SOCIAL MEDIA USER IDENTITIES
8.08 BILLION	8.65 BILLION	5.35 BILLION	5.04 BILLION
YEAR-ON-YEAR CHANGE	YEAR-ON-YEAR CHANGE	YEAR-ON-YEAR CHANGE	YEAR-ON-YEAR CHANGE
+0.9%	+1.9%	+1.8%	+5.6%
+74 MILLION	+160 MILLION	+97 MILLION	+266 MILLION
URBANISATION	TOTAL vs. POPULATION	TOTAL vs. POPULATION	TOTAL vs. POPULATION
57.7%	107.0%	66.2%	62.3%

SOURCES: U.N., GOVERNMENT AUTHORITIES; GSMA INTELLIGENCE; ITU; EUROSTAT; CNNIC; KANTAR & IAMAI; PLATFORM RESOURCES; OCDH; BETA RESEARCH CENTER; KEPIOS ANALYSIS. **ADVISORY:** SOCIAL MEDIA USER IDENTITIES MAY NOT REPRESENT UNIQUE INDIVIDUALS. **COMPARABILITY:** SOURCE CHANGES AND BASE REVISIONS. FIGURES ARE NOT COMPARABLE WITH PREVIOUS REPORTS. GLOBAL DATASETS MAY USE DIFFERENT SOURCES vs. COUNTRY AND REGIONAL DATA, SO SUMS MAY NOT MATCH. **IMPORTANT:** NEGATIVE VALUES MAY INDICATE SOURCE DATA CORRECTIONS, AND MAY NOT REPRESENT DECREASES IN THE RELEVANT METRIC. WHERE YEAR-ON-YEAR CHANGE IS "[N/A]", COMPARISONS WITH HISTORICAL DATA WILL PRODUCE INACCURATE RESULTS. PLEASE SEE NOTES ON DATA.

Internet adoption



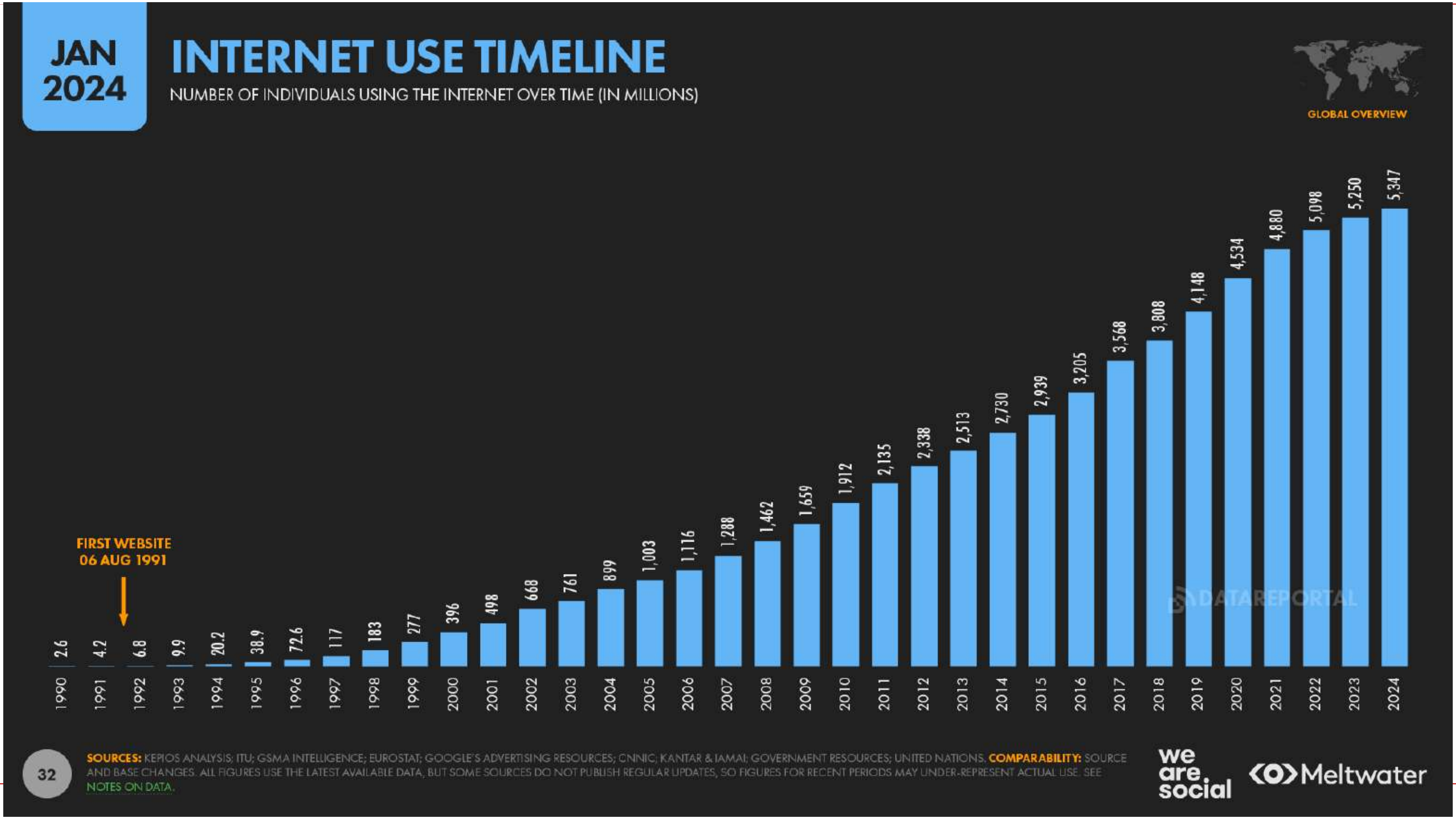
JAN 2024

INTERNET ADOPTION

INDIVIDUALS USING THE INTERNET AS A PERCENTAGE OF TOTAL POPULATION

SOURCES: KEPIOS ANALYSIS; ITU; GSMA INTELLIGENCE; EUROSTAT; GOOGLE'S ADVERTISING RESOURCES; CNNIC; KANTAR & IAMAI; GOVERNMENT RESOURCES; UNITED NATIONS. NOTE: REGIONS BASED ON THE UNITED NATIONS GEOSCHEME. LOCAL COUNTRY VALUES HAVE BEEN CAPPED AT 99% OF THE POPULATION. COMPARABILITY: SOURCE AND BASE CHANGES. ALL FIGURES USE THE LATEST AVAILABLE DATA, BUT SOME SOURCES DO NOT PUBLISH REGULAR UPDATES, SO FIGURES MAY UNDER-REPRESENT ACTUAL USE. SEE NOTES ON DATA.

Internet users over time



JAN 2024

INTERNET USE TIMELINE

NUMBER OF INDIVIDUALS USING THE INTERNET OVER TIME (IN MILLIONS)

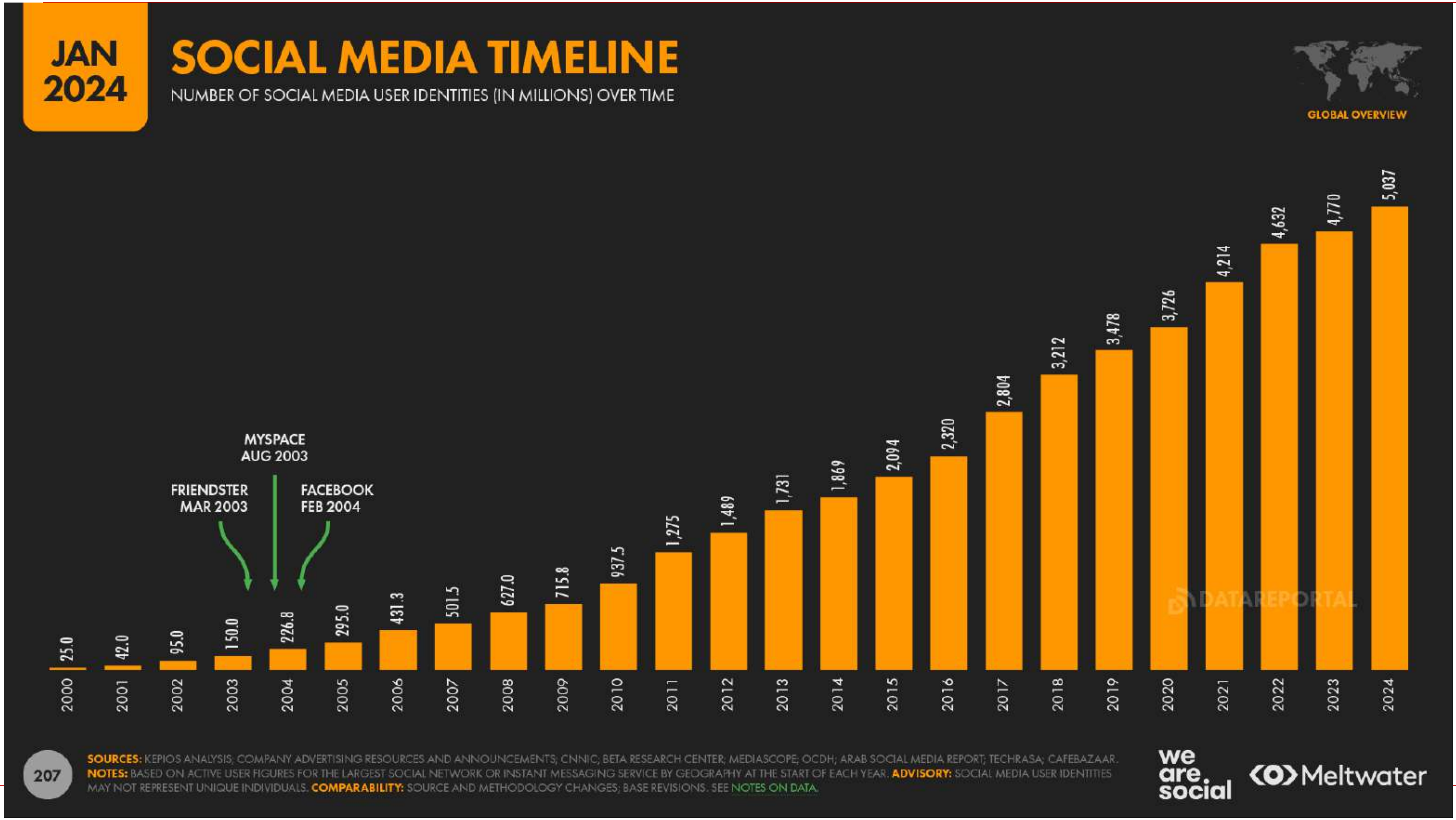
32

SOURCES: KEPIOS ANALYSIS; ITU; GSMA INTELLIGENCE; EUROSTAT; GOOGLE'S ADVERTISING RESOURCES; CNNIC; KANTAR & IAMAI; GOVERNMENT RESOURCES; UNITED NATIONS. **COMPARABILITY:** SOURCE AND BASE CHANGES. ALL FIGURES USE THE LATEST AVAILABLE DATA, BUT SOME SOURCES DO NOT PUBLISH REGULAR UPDATES, SO FIGURES FOR RECENT PERIODS MAY UNDER-REPRESENT ACTUAL USE. SEE NOTES ON DATA.

we are social

Meltwater

Social media timeline



JAN 2024

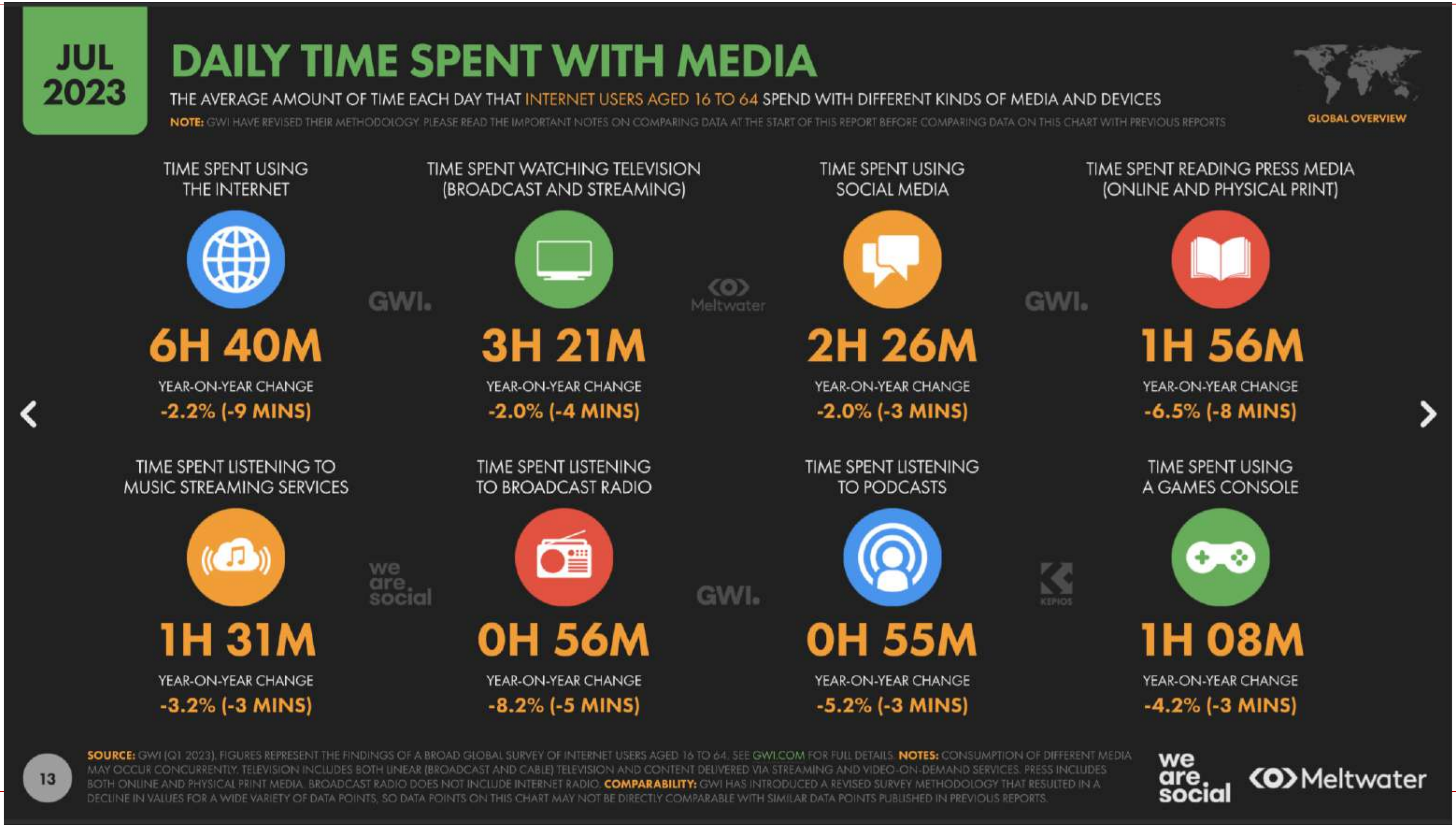
SOCIAL MEDIA TIMELINE

NUMBER OF SOCIAL MEDIA USER IDENTITIES (IN MILLIONS) OVER TIME

207

SOURCES: KEPIOS ANALYSIS; COMPANY ADVERTISING RESOURCES AND ANNOUNCEMENTS; CNNIC; BETA RESEARCH CENTER; MEDIASCOPE; OCDH; ARAB SOCIAL MEDIA REPORT; TECHRASA; CAFEBAZAAR. **NOTES:** BASED ON ACTIVE USER FIGURES FOR THE LARGEST SOCIAL NETWORK OR INSTANT MESSAGING SERVICE BY GEOGRAPHY AT THE START OF EACH YEAR. **ADVISORY:** SOCIAL MEDIA USER IDENTITIES MAY NOT REPRESENT UNIQUE INDIVIDUALS. **COMPARABILITY:** SOURCE AND METHODOLOGY CHANGES; BASE REVISIONS. SEE NOTES ON DATA.

Daily time spent connected



JUL 2023

DAILY TIME SPENT WITH MEDIA

THE AVERAGE AMOUNT OF TIME EACH DAY THAT INTERNET USERS AGED 16 TO 64 SPEND WITH DIFFERENT KINDS OF MEDIA AND DEVICES

NOTE: GWI HAVE REVISED THEIR METHODOLOGY. PLEASE READ THE IMPORTANT NOTES ON COMPARING DATA AT THE START OF THIS REPORT BEFORE COMPARING DATA ON THIS CHART WITH PREVIOUS REPORTS

GLOBAL OVERVIEW

TIME SPENT USING THE INTERNET	TIME SPENT WATCHING TELEVISION (BROADCAST AND STREAMING)	TIME SPENT USING SOCIAL MEDIA	TIME SPENT READING PRESS MEDIA (ONLINE AND PHYSICAL PRINT)
6H 40M	3H 21M	2H 26M	1H 56M
YEAR-ON-YEAR CHANGE -2.2% (-9 MINS)	YEAR-ON-YEAR CHANGE -2.0% (-4 MINS)	YEAR-ON-YEAR CHANGE -2.0% (-3 MINS)	YEAR-ON-YEAR CHANGE -6.5% (-8 MINS)

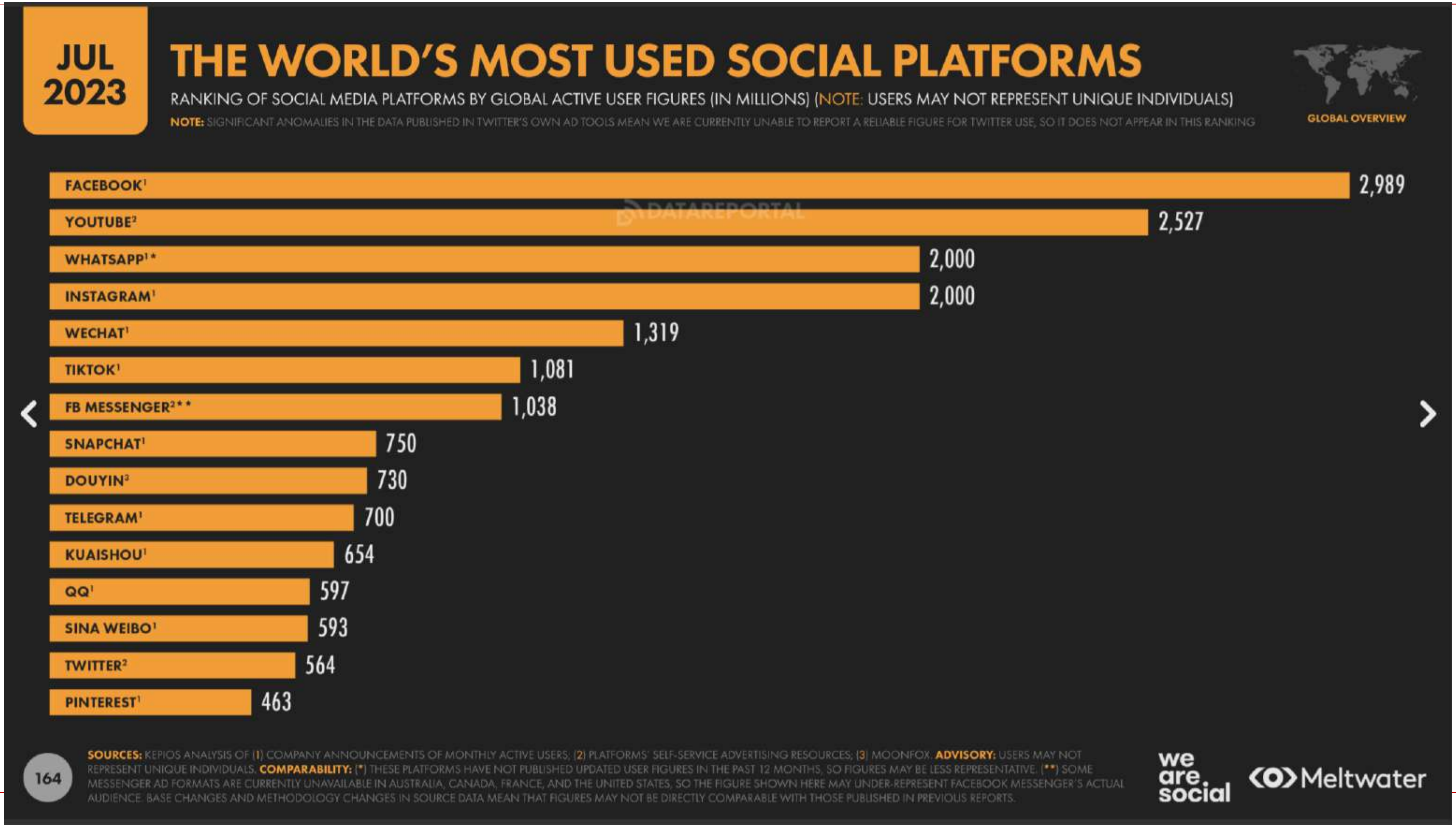
TIME SPENT LISTENING TO MUSIC STREAMING SERVICES	TIME SPENT LISTENING TO BROADCAST RADIO	TIME SPENT LISTENING TO PODCASTS	TIME SPENT USING A GAMES CONSOLE
1H 31M	0H 56M	0H 55M	1H 08M
YEAR-ON-YEAR CHANGE -3.2% (-3 MINS)	YEAR-ON-YEAR CHANGE -8.2% (-5 MINS)	YEAR-ON-YEAR CHANGE -5.2% (-3 MINS)	YEAR-ON-YEAR CHANGE -4.2% (-3 MINS)

SOURCE: GWI (Q1 2023). FIGURES REPRESENT THE FINDINGS OF A BROAD GLOBAL SURVEY OF INTERNET USERS AGED 16 TO 64. SEE GWI.COM FOR FULL DETAILS. **NOTES:** CONSUMPTION OF DIFFERENT MEDIA MAY OCCUR CONCURRENTLY. TELEVISION INCLUDES BOTH LINEAR (BROADCAST AND CABLE) TELEVISION AND CONTENT DELIVERED VIA STREAMING AND VIDEO-ON-DEMAND SERVICES. PRESS INCLUDES BOTH ONLINE AND PHYSICAL PRINT MEDIA. BROADCAST RADIO DOES NOT INCLUDE INTERNET RADIO. **COMPARABILITY:** GWI HAS INTRODUCED A REVISED SURVEY METHODOLOGY THAT RESULTED IN A DECLINE IN VALUES FOR A WIDE VARIETY OF DATA POINTS, SO DATA POINTS ON THIS CHART MAY NOT BE DIRECTLY COMPARABLE WITH SIMILAR DATA POINTS PUBLISHED IN PREVIOUS REPORTS.

13

we are social Meltwater

The world’s most used social media



JUL 2023

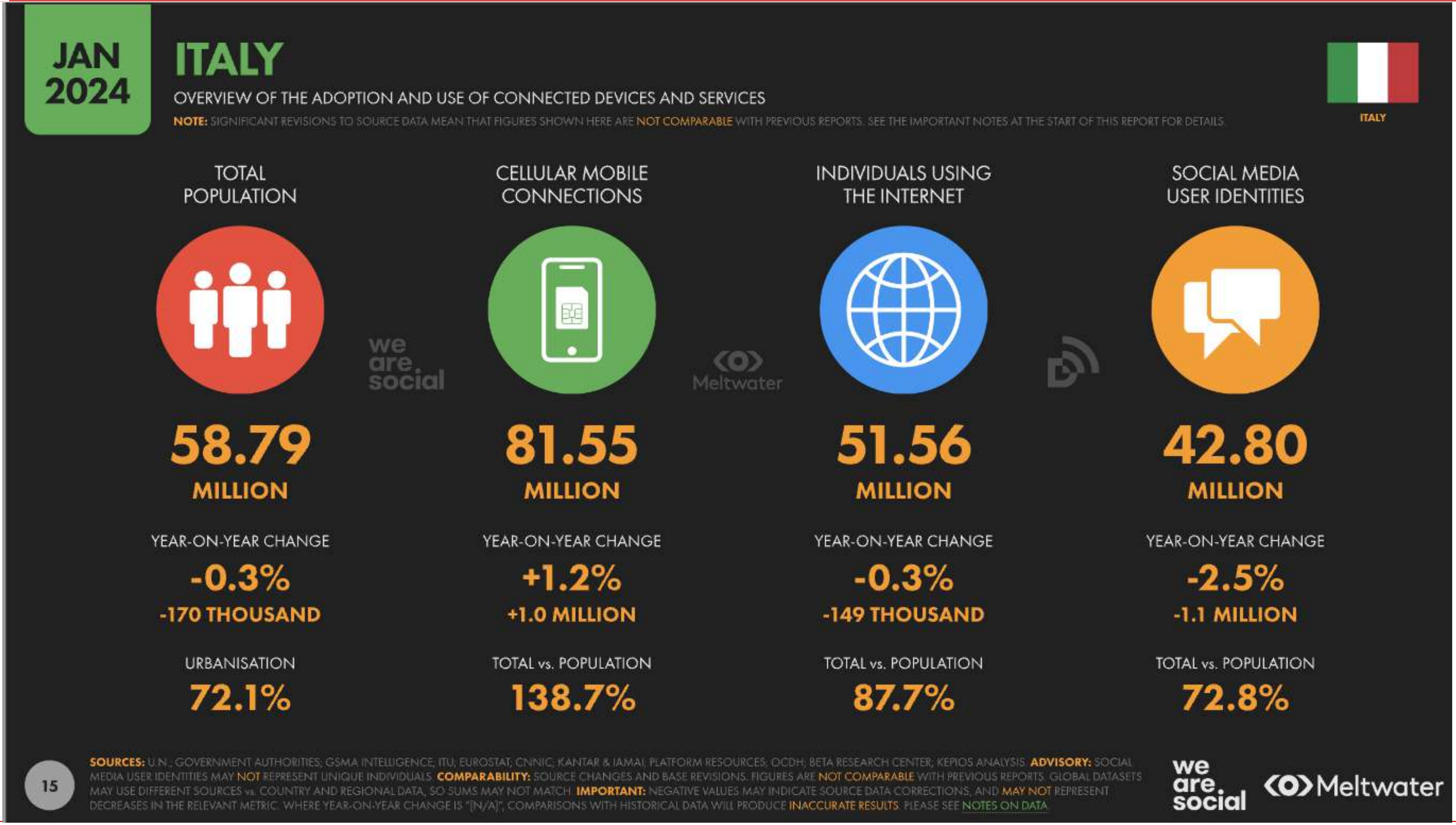
THE WORLD’S MOST USED SOCIAL PLATFORMS

RANKING OF SOCIAL MEDIA PLATFORMS BY GLOBAL ACTIVE USER FIGURES (IN MILLIONS) (NOTE: USERS MAY NOT REPRESENT UNIQUE INDIVIDUALS)

NOTE: SIGNIFICANT ANOMALIES IN THE DATA PUBLISHED IN TWITTER’S OWN AD TOOLS MEAN WE ARE CURRENTLY UNABLE TO REPORT A RELIABLE FIGURE FOR TWITTER USE, SO IT DOES NOT APPEAR IN THIS RANKING

SOURCES: KEPIOS ANALYSIS OF (1) COMPANY ANNOUNCEMENTS OF MONTHLY ACTIVE USERS; (2) PLATFORMS’ SELF-SERVICE ADVERTISING RESOURCES; (3) MOONFOX. ADVISORY: USERS MAY NOT REPRESENT UNIQUE INDIVIDUALS. COMPARABILITY: (*) THESE PLATFORMS HAVE NOT PUBLISHED UPDATED USER FIGURES IN THE PAST 12 MONTHS, SO FIGURES MAY BE LESS REPRESENTATIVE. (**) SOME MESSENGER AD FORMATS ARE CURRENTLY UNAVAILABLE IN AUSTRALIA, CANADA, FRANCE, AND THE UNITED STATES, SO THE FIGURE SHOWN HERE MAY UNDER-REPRESENT FACEBOOK MESSENGER’S ACTUAL AUDIENCE. BASE CHANGES AND METHODOLOGY CHANGES IN SOURCE DATA MEAN THAT FIGURES MAY NOT BE DIRECTLY COMPARABLE WITH THOSE PUBLISHED IN PREVIOUS REPORTS.

The situation in Italy



JAN 2024

ITALY

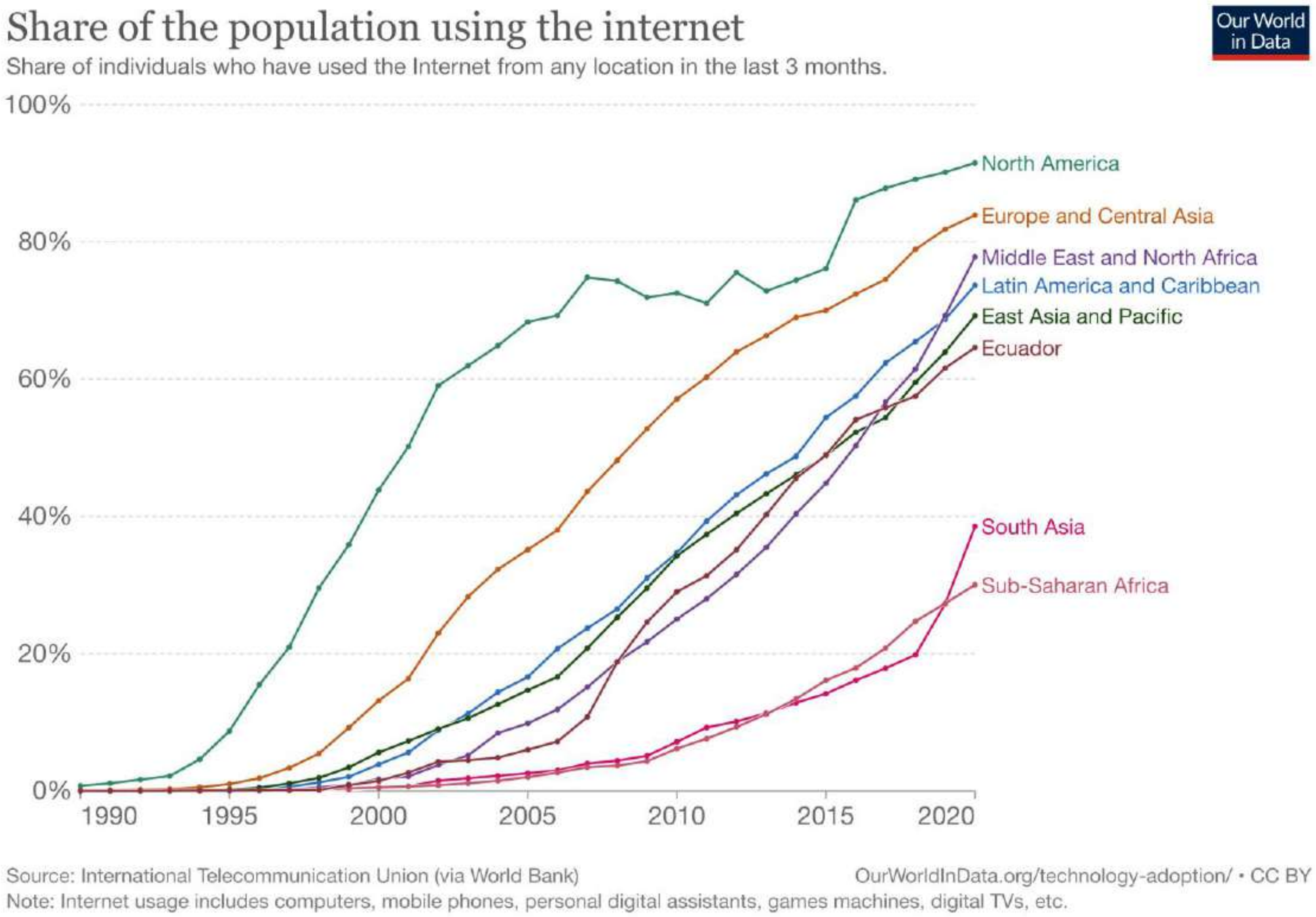
OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES

NOTE: SIGNIFICANT REVISIONS TO SOURCE DATA MEAN THAT FIGURES SHOWN HERE ARE NOT COMPARABLE WITH PREVIOUS REPORTS. SEE THE IMPORTANT NOTES AT THE START OF THIS REPORT FOR DETAILS.

TOTAL POPULATION	CELLULAR MOBILE CONNECTIONS	INDIVIDUALS USING THE INTERNET	SOCIAL MEDIA USER IDENTITIES
58.79 MILLION	81.55 MILLION	51.56 MILLION	42.80 MILLION
YEAR-ON-YEAR CHANGE	YEAR-ON-YEAR CHANGE	YEAR-ON-YEAR CHANGE	YEAR-ON-YEAR CHANGE
-0.3%	+1.2%	-0.3%	-2.5%
-170 THOUSAND	+1.0 MILLION	-149 THOUSAND	-1.1 MILLION
URBANISATION	TOTAL vs. POPULATION	TOTAL vs. POPULATION	TOTAL vs. POPULATION
72.1%	138.7%	87.7%	72.8%

SOURCES: U.N.; GOVERNMENT AUTHORITIES; GSMA INTELLIGENCE; ITU; EUROSTAT; CNNIC; KANTAR & IAMAI; PLATFORM RESOURCES; OCDH; BETA RESEARCH CENTER; KEPIOS ANALYSIS. **ADVISORY:** SOCIAL MEDIA USER IDENTITIES MAY NOT REPRESENT UNIQUE INDIVIDUALS. **COMPARABILITY:** SOURCE CHANGES AND BASE REVISIONS. FIGURES ARE NOT COMPARABLE WITH PREVIOUS REPORTS. GLOBAL DATASETS MAY USE DIFFERENT SOURCES vs. COUNTRY AND REGIONAL DATA, SO SUMS MAY NOT MATCH. **IMPORTANT:** NEGATIVE VALUES MAY INDICATE SOURCE DATA CORRECTIONS, AND MAY NOT REPRESENT DECREASES IN THE RELEVANT METRIC. WHERE YEAR-ON-YEAR CHANGE IS "[N/A]", COMPARISONS WITH HISTORICAL DATA WILL PRODUCE INACCURATE RESULTS. PLEASE SEE NOTES ON DATA

Internet and the Society



Share of the population using the internet

Share of individuals who have used the Internet from any location in the last 3 months.

Source: International Telecommunication Union (via World Bank) OurWorldInData.org/technology-adoption/ • CC BY

Note: Internet usage includes computers, mobile phones, personal digital assistants, games machines, digital TVs, etc.

- A part of the daily life of the citizens (workplace, home, leisure)
- No physical distance between different places in the world
- Political frontiers are indifferent
- Information is open and available to everybody
- No States **sovereignty** (?)
- Any person can **express** himself (?)
- Cyberspace is independent, anarchic and **ungovernable** (?)

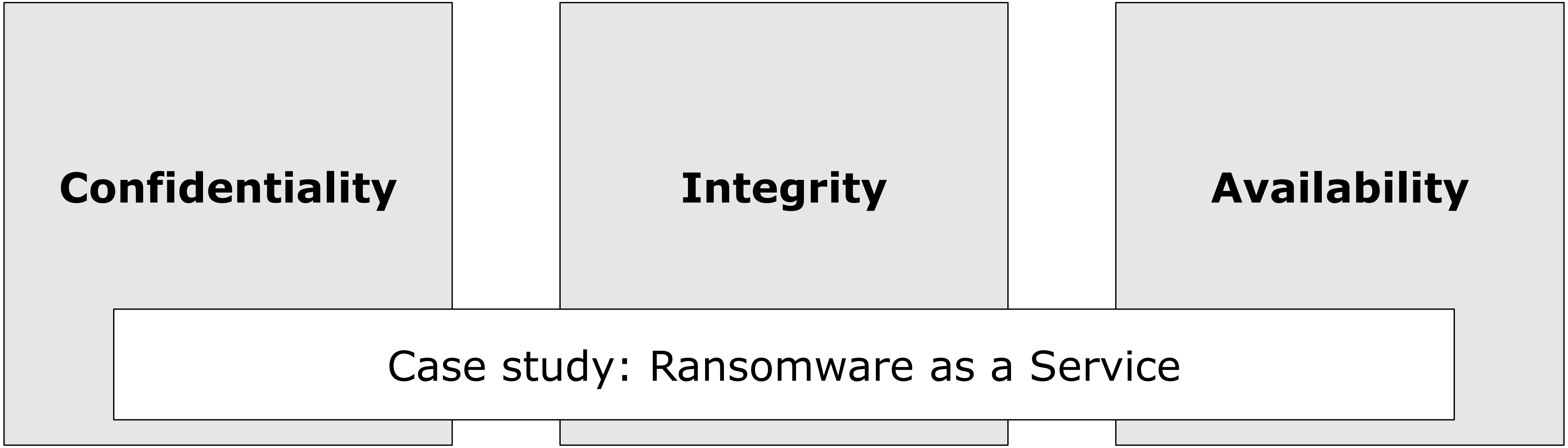
Different forms of cybercrimes, common elements

- **Cyber-dependent crimes**
  - Crimes that arose with technology and cannot exist outside the digital world
- **Cyber-related crimes**
  - The process of digitalization has facilitated the commission of these crimes
- **Cyber-assisted crimes**
  - Traditional crimes, in which the use of the computer is not essential, but rather incidental

ELECTRONIC

EVIDENCE!!

Cyber-dependent crimes



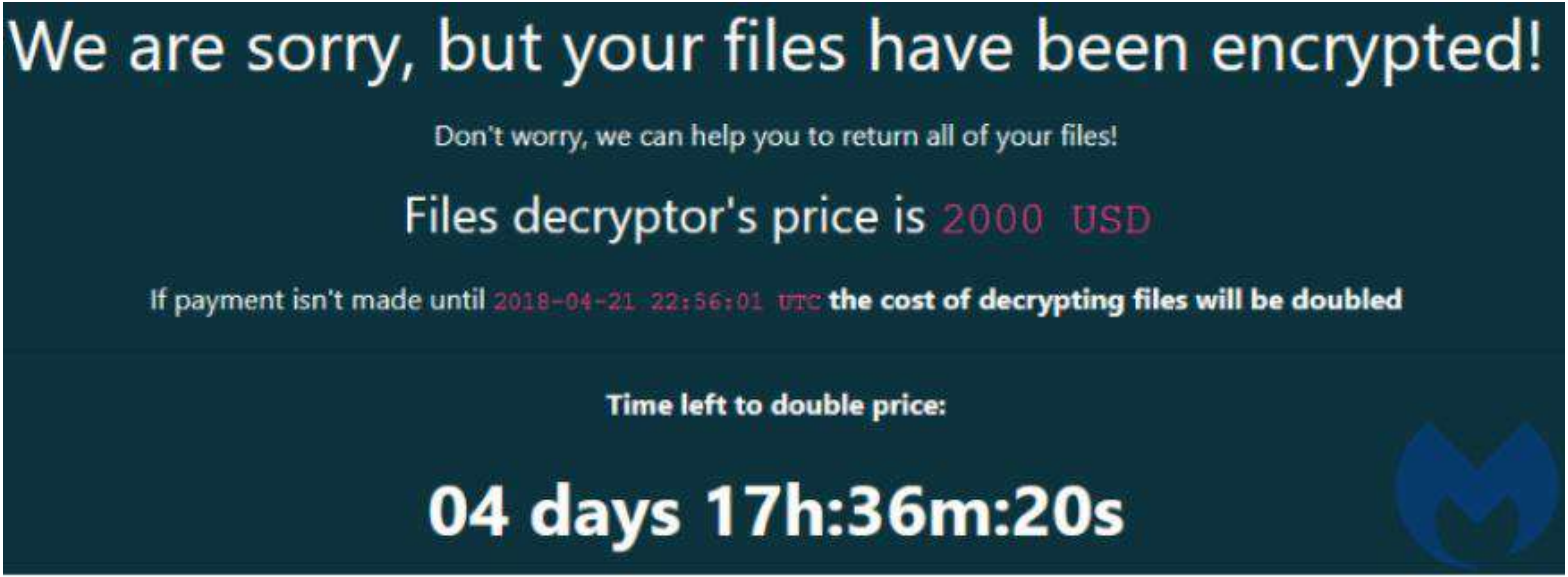
Confidentiality

Integrity

Availability

Case study: Ransomware as a Service

Ransomware



We are sorry, but your files have been encrypted!

Don't worry, we can help you to return all of your files!

Files decryptor's price is 2000 USD

If payment isn't made until 2018-04-21 22:56:01 UTC **the cost of decrypting files will be doubled**

Time left to double price:

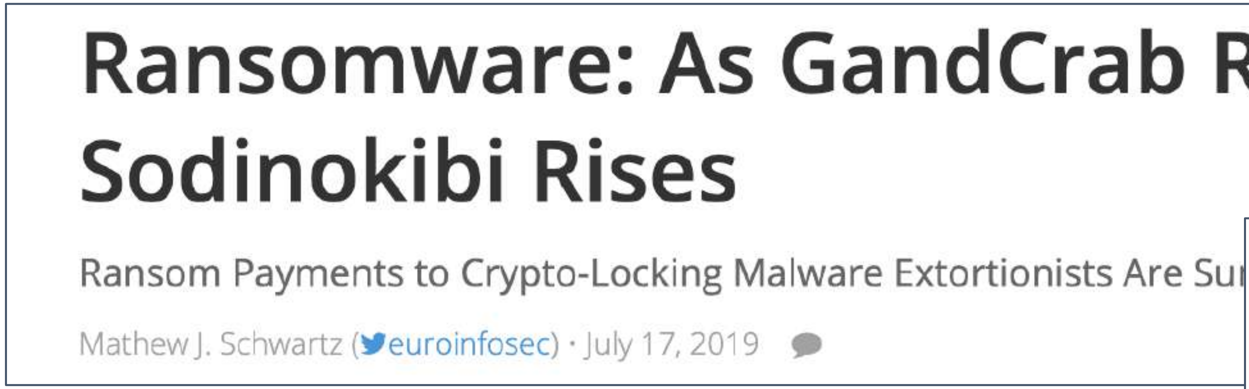
04 days 17h:36m:20s

GandCrab

- GandCrab ceased operations on 31 May 2019. It was estimated that by that time, GandCrab accounted for up to **half of the global ransomware market**.

- "In one year, **people who worked with us have earned over US $2 billion**. Our name became a generic term for ransomware in the underground. **The average weekly income of the project was equal to US $2.5 million**."
- "We ourselves have earned **over US $150 million in one year**. This money has been **successfully cashed out and invested in various legal projects**, both online and offline ones. It has been a pleasure to work with you. But, like we said, all things come to an end. We are getting a well-deserved retirement. **We are a living proof that you can do evil and get off scot-free**. We have proved that one can make **a lifetime of money in one year**. We have proved that you can become number one by general admission, not in your own conceit."

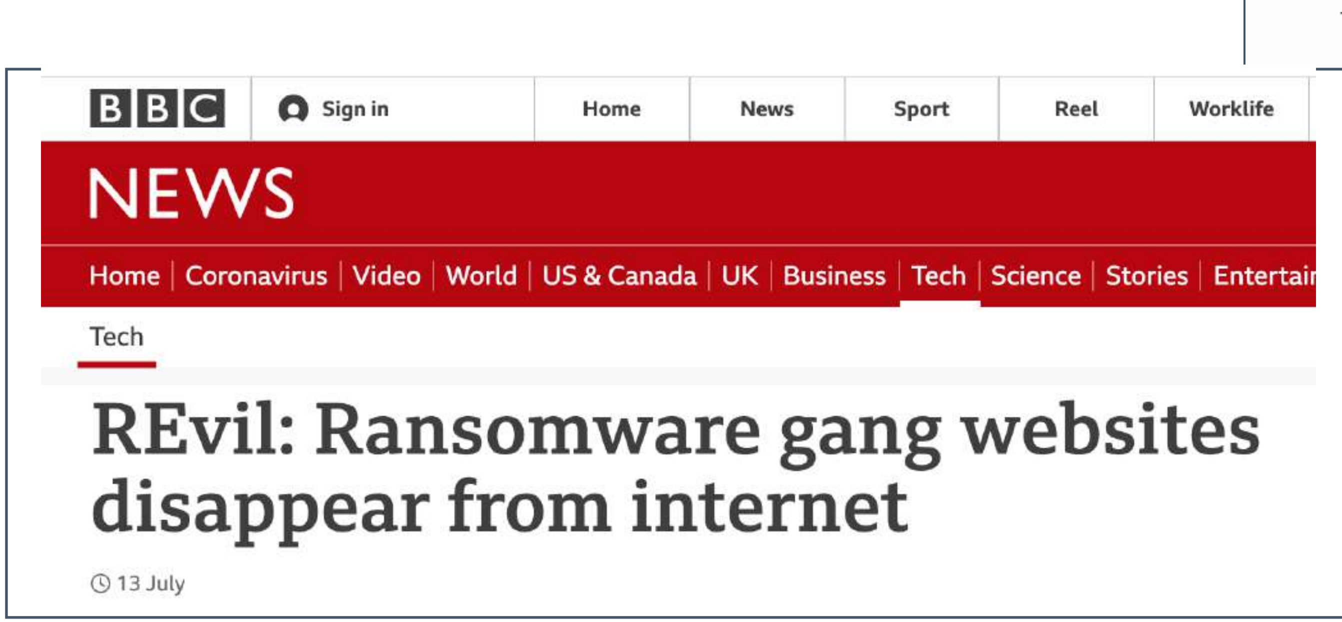
From Gandcrab to Sodinokibi/ REvil



Ransomware: As GandCrab Retires, Sodinokibi Rises

Ransom Payments to Crypto-Locking Malware Extortionists Are Su

Mathew J. Schwartz (euroinfosec) · July 17, 2019



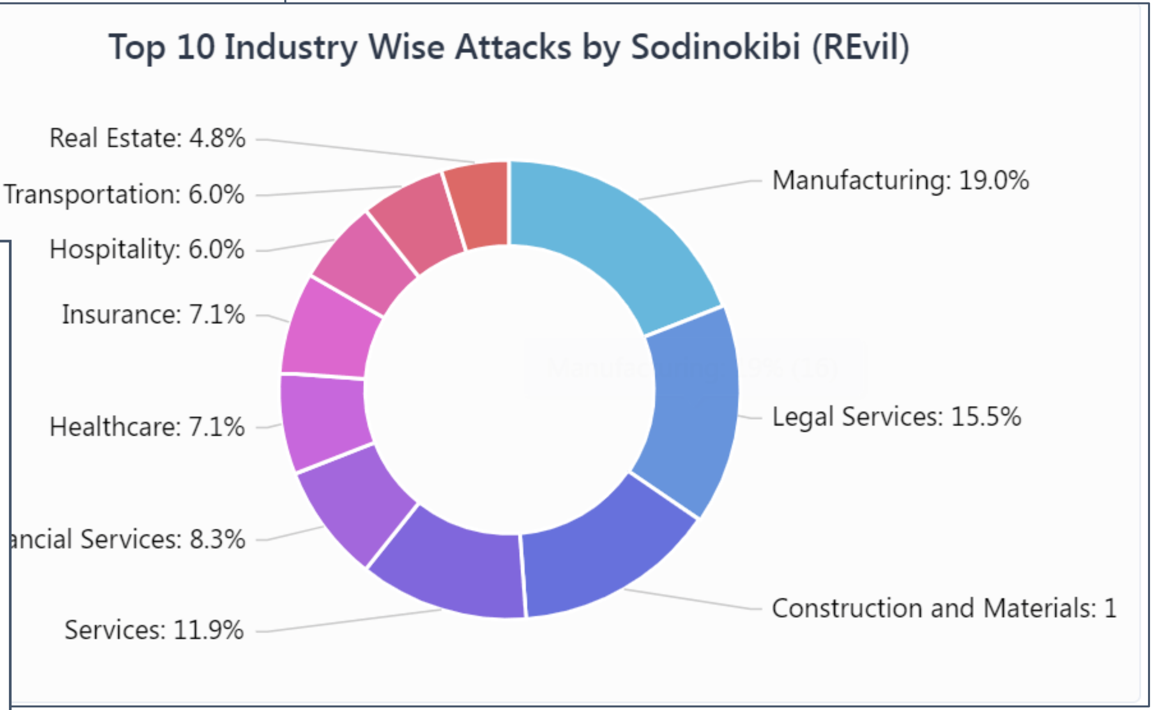
BBC
Sign in
Home
News
Sport
Reel
Worklife
NEWS
Home | Coronavirus | Video | World | US & Canada | UK | Business | Tech | Science | Stories | Entertai
Tech

REvil: Ransomware gang websites disappear from internet

13 July

Operated until 2021,

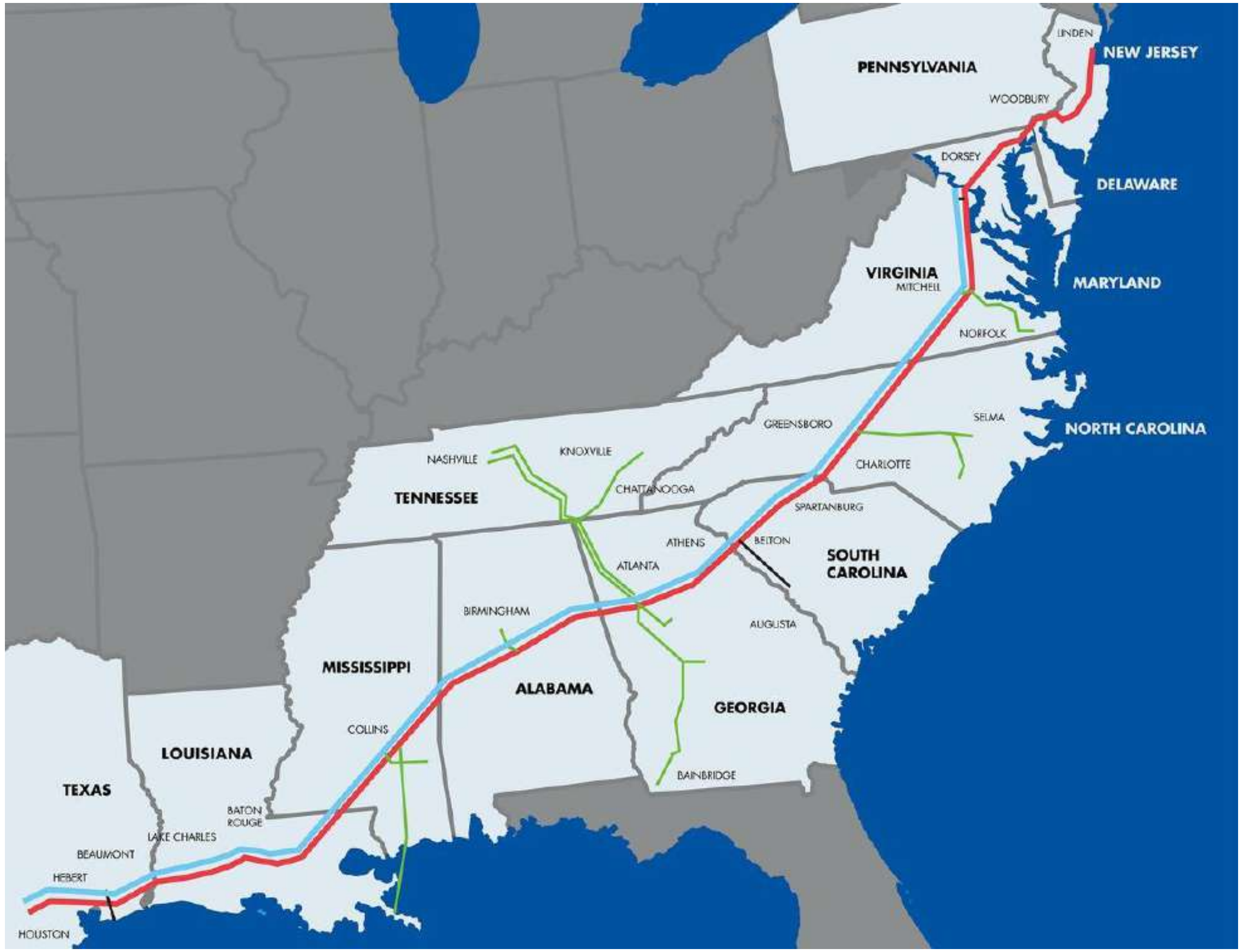
making $ 100 Mil per year



Top 10 Industry Wise Attacks by Sodinokibi (REvil)

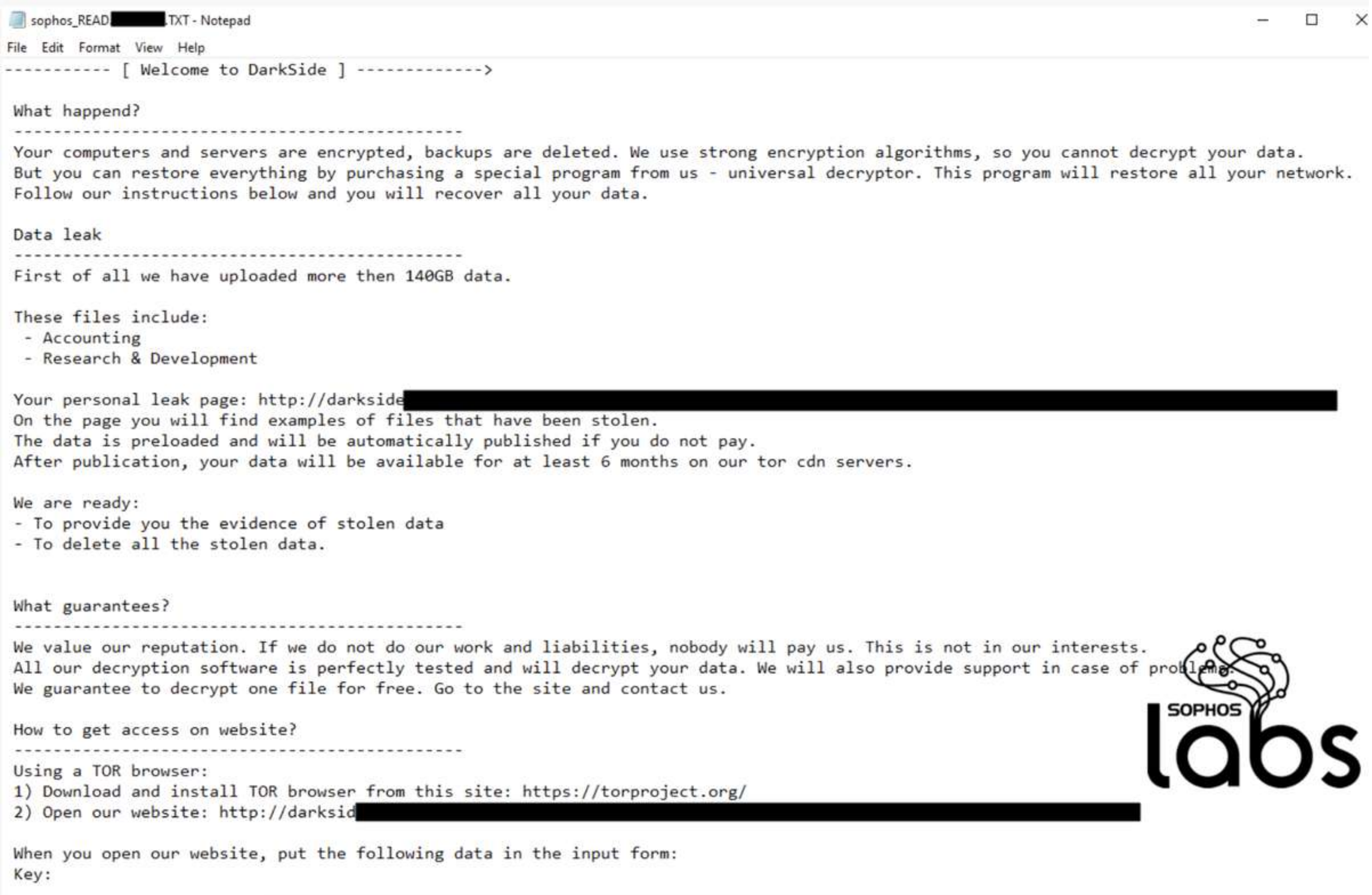
REvil in action – Colonial Pipeline, 7 May 2021

- Colonial Pipeline è uno dei maggiori operatori di trasporto del carburante negli Stati Uniti, responsabile per circa il 45% dei distributori della East Coast, inclusi benzina, diesel, riscaldamento, rifornimento degli aerei, e forniture militari.
- Oltre 100 milioni di galloni trasportati ogni giornosu un’area che va dal Texas a New York.



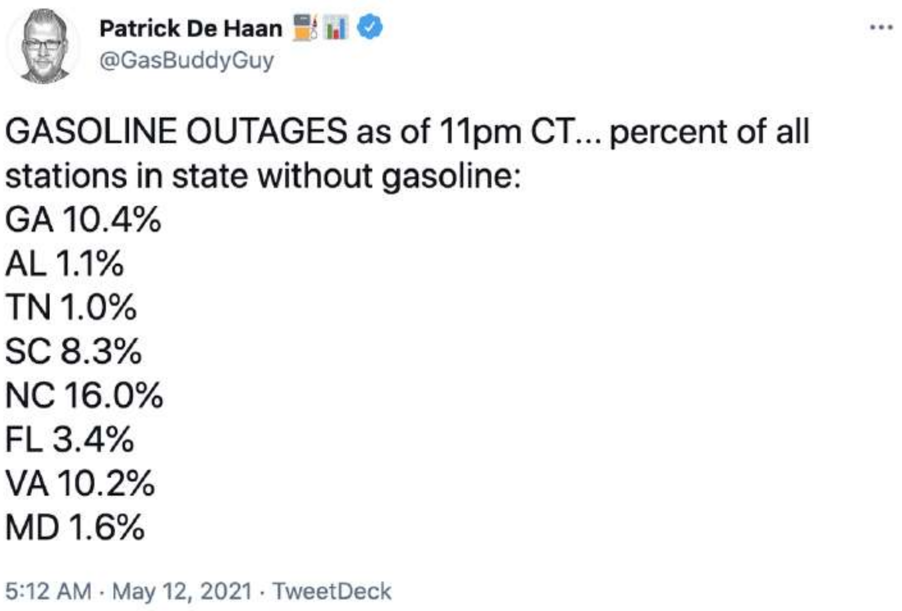
Source: ZDNet, https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/, 13 May 2021

Colonial Pipeline, 7-12 May 2021



sophos_READ[redacted].TXT - Notepad
File Edit Format View Help
SOPHOS
labs

```
----------- [ 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://darksid[redacted]

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



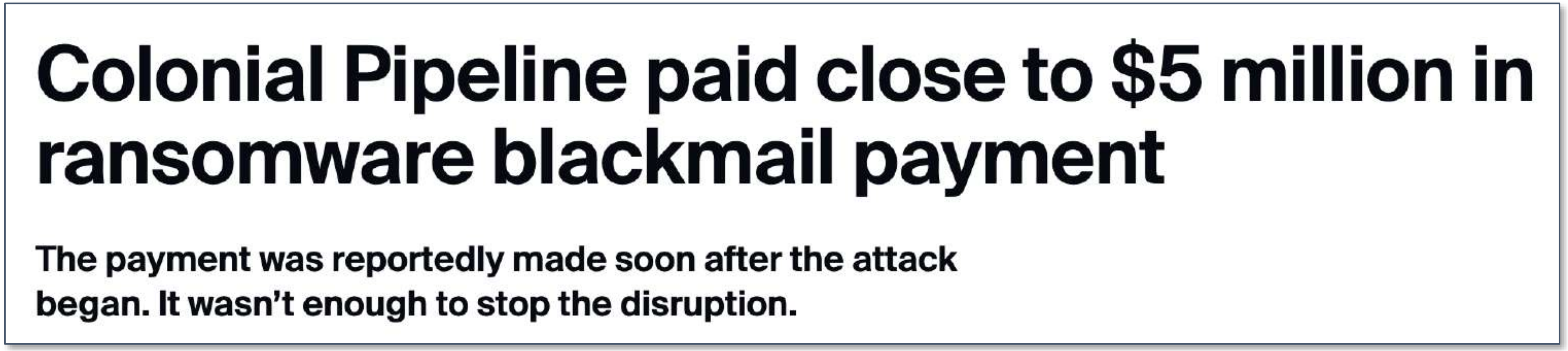
Patrick De Haan ⛽📊 ✓
@GasBuddyGuy

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

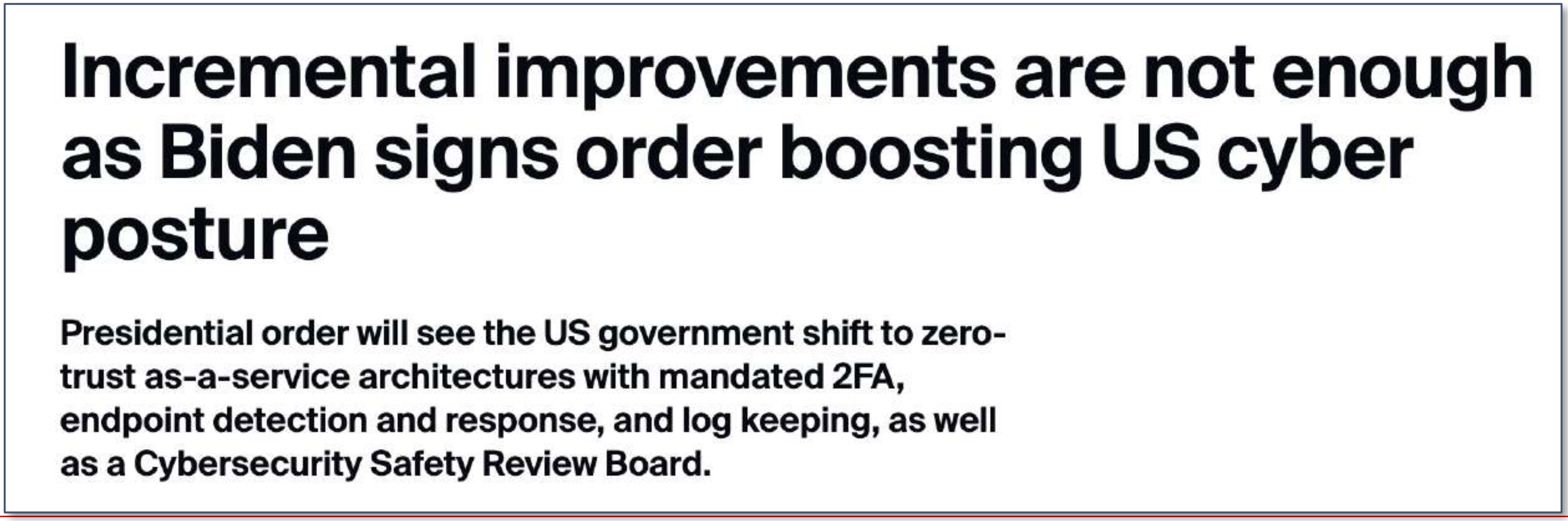
Source: ZDNet, https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/, 13 May 2021

Colonial Pipeline, 13 May 2021


Colonial Pipeline paid close to $5 million in ransomware blackmail payment

The payment was reportedly made soon after the attack began. It wasn't enough to stop the disruption.

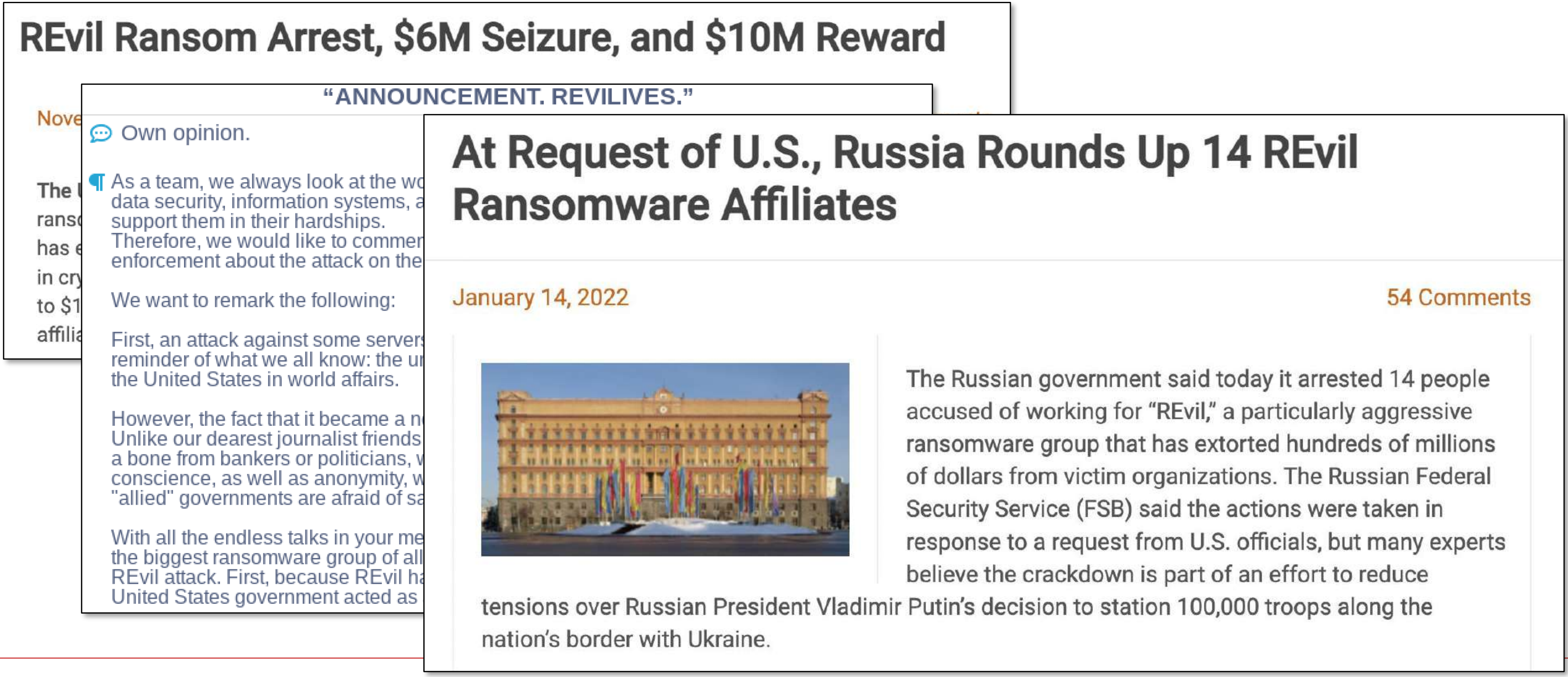
- On 13 May, US President Biden signed an executive order to improve federal cybersecurity, noting that **agencies need to «lead by example»**


Incremental improvements are not enough as Biden signs order boosting US cyber posture

Presidential order will see the US government shift to zero-trust as-a-service architectures with mandated 2FA, endpoint detection and response, and log keeping, as well as a Cybersecurity Safety Review Board.

Source: ZDNet, https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/, 13 May 2021

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



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

Nove

The
rans
has e
in cry
to $1
affilia

“ANNOUNCEMENT. REVILIVES.”

💬 Own opinion.

¶ As a team, we always look at the wo
data security, information systems, a
support them in their hardships.
Therefore, we would like to commen
enforcement about the attack on the

We want to remark the following:

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

However, the fact that it became a n
Unlike our dearest journalist friends
a bone from bankers or politicians, w
conscience, as well as anonymity, w
"allied" governments are afraid of sa

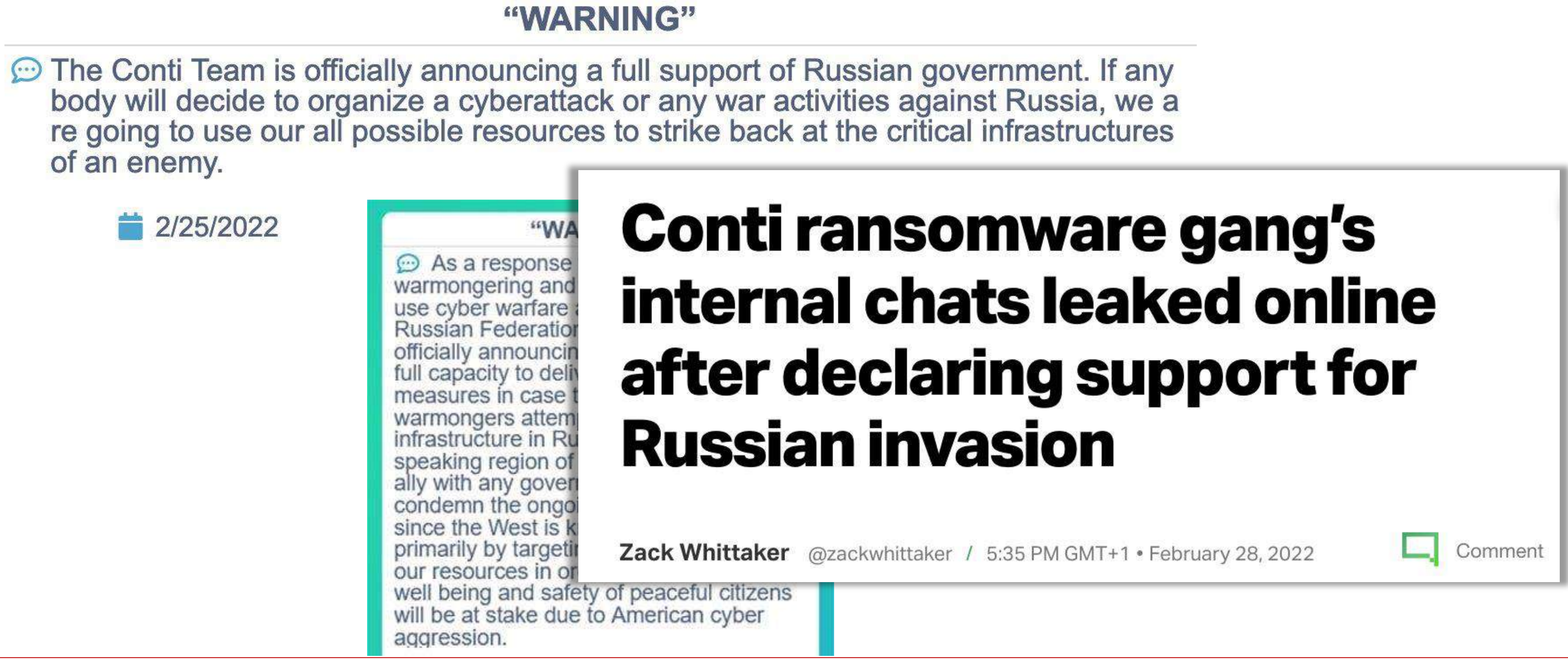
With all the endless talks in your me
the biggest ransomware group of all
REvil attack. First, because REvil ha
United States government acted as

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 a re 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 Federatior
officially announcin
full capacity to deli
measures in case t
warmongers attem
infrastructure in Ru
speaking region of
ally with any gover
condemn the ongo
since the West is k
primarily by targeti
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

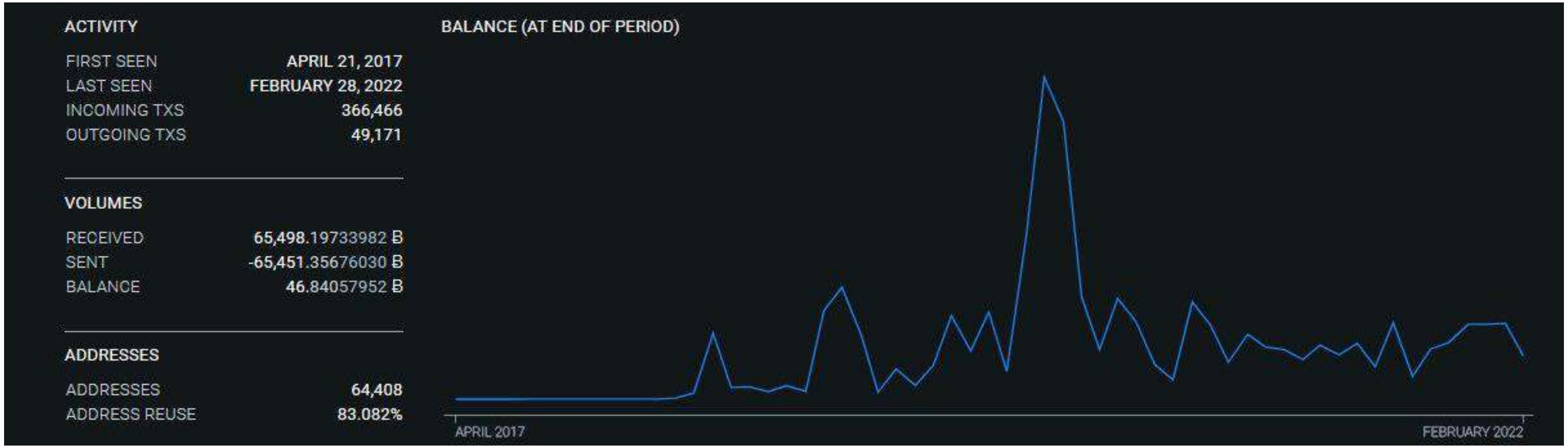
Zack Whittaker @zackwhittaker / 5:35 PM GMT+1 • February 28, 2022

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

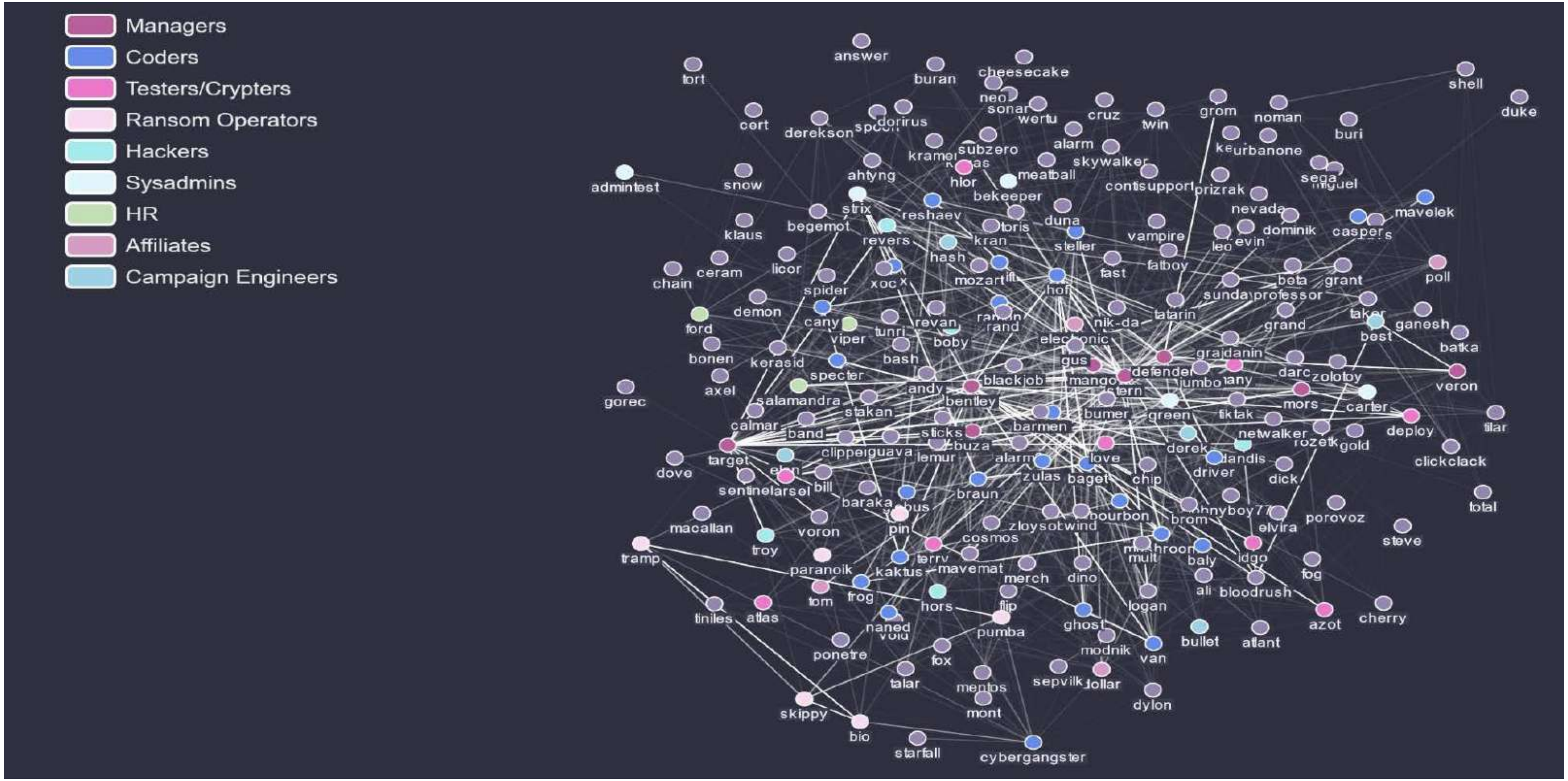


ACTIVITY	
FIRST SEEN	APRIL 21, 2017
LAST SEEN	FEBRUARY 28, 2022
INCOMING TXS	366,466
OUTGOING TXS	49,171

VOLUMES	
RECEIVED	65,498.19733982 Ƀ
SENT	-65,451.35676030 Ƀ
BALANCE	46.84057952 Ƀ

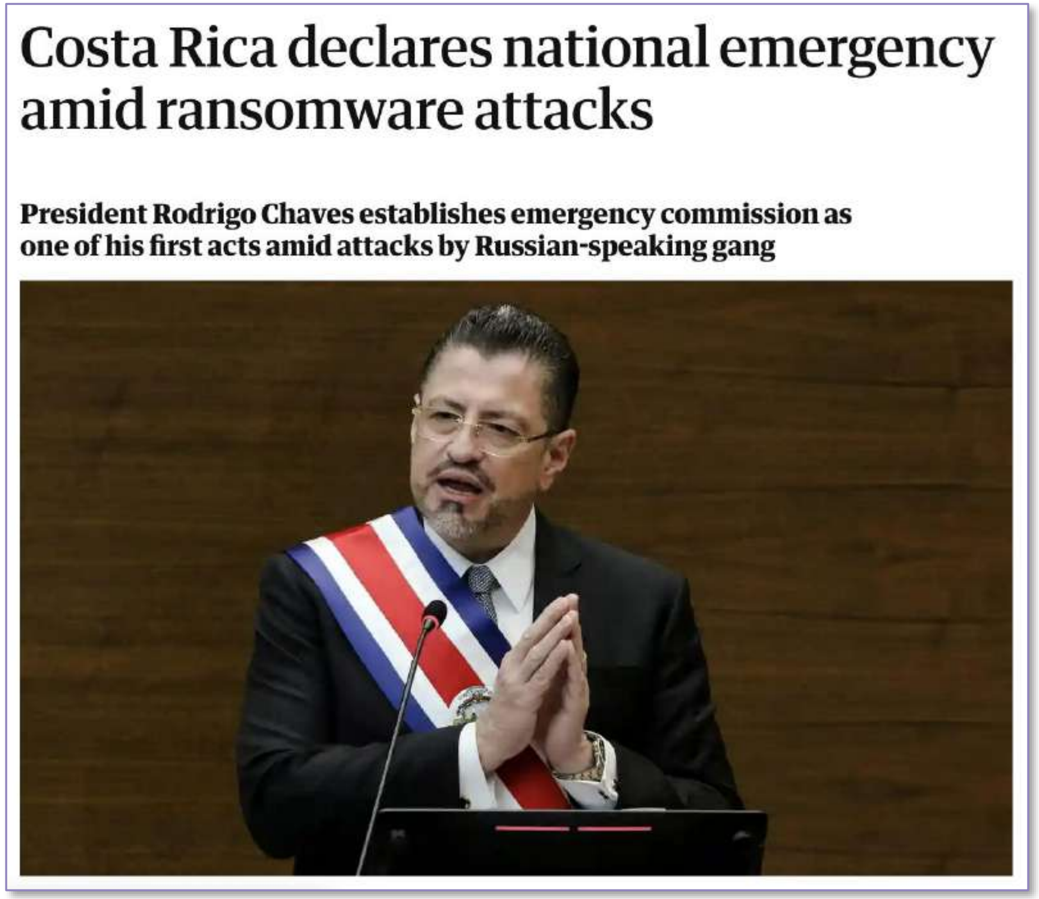
ADDRESSES	
ADDRESSES	64,408
ADDRESS REUSE	83.082%

The Conti network



https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/

Ransomware in 2022 – The case of Costa Rica



Costa Rica declares national emergency amid ransomware attacks

President Rodrigo Chaves establishes emergency commission as one of his first acts amid attacks by Russian-speaking gang

In April, Costa Rica declared a national state of emergency after 30 of its government institutions suffered ransomware attacks over the space of a few weeks.

Conti, a Russian ransomware group claimed the attack which e**ncrypted hundreds of gigabytes of sensitive information**.

Requested 30 Million USD as a ransom

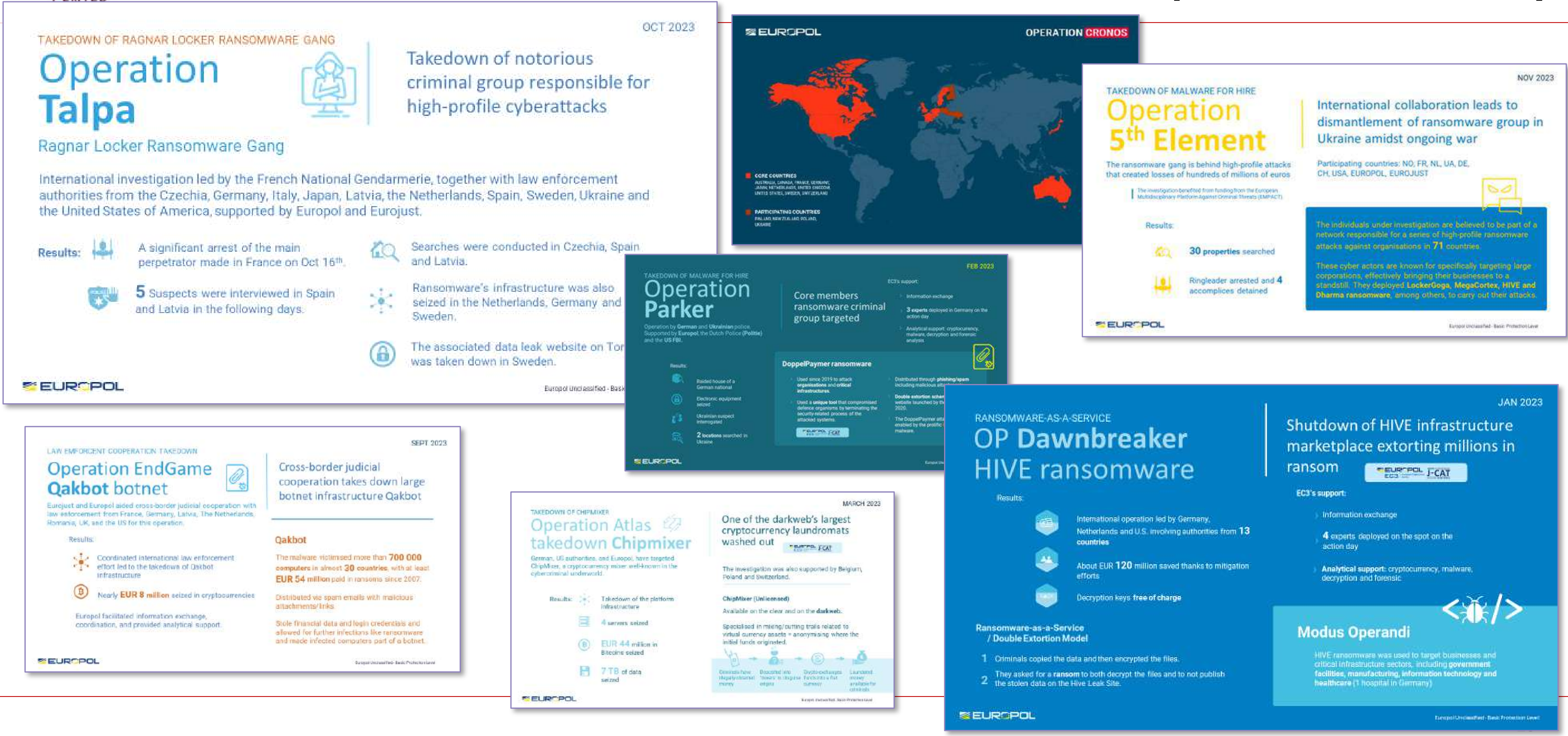
As well as the threat of leaking the data, it also resulted in **widespread disruption in the country’s foreign trade, tax and customs systems and civil servant payroll**.

Many reasons have been suggested as to why Costa Rica became a target such as it siding with Ukraine in the war with Russia, it’s recent presidential election or even spying going on within the Costa Rican government.

In any case, **it has raised concerns for other smaller nations** that do not have the level of security that nations in Europe or the USA have.

In the end, **Costa Rica refused to pay the ransom** which resulted in **50% of the encrypted data to be released to the public**.

Anti- ransomware operations in 2023 – Europol summary



OCT 2023

TAKEDOWN OF RAGNAR LOCKER RANSOMWARE GANG

Operation Talpa

Ragnar Locker Ransomware Gang

Takedown of notorious criminal group responsible for high-profile cyberattacks

International investigation led by the French National Gendarmerie, together with law enforcement authorities from the Czechia, Germany, Italy, Japan, Latvia, the Netherlands, Spain, Sweden, Ukraine and the United States of America, supported by Europol and Eurojust.

Results:

- A significant arrest of the main perpetrator made in France on Oct 16th.
- 5 Suspects were interviewed in Spain and Latvia in the following days.
- Searches were conducted in Czechia, Spain and Latvia.
- Ransomware's infrastructure was also seized in the Netherlands, Germany and Sweden.
- The associated data leak website on Tor was taken down in Sweden.

EUROPOL

Europol Unclassified - Bask

EUROPOL

OPERATION CRONOS

CORE COUNTRIES
AUSTRALIA, CANADA, FRANCE, GERMANY, JAPAN, NETHERLANDS, UNITED KINGDOM, UNITED STATES, SWEDEN, SWITZERLAND

PARTICIPATING COUNTRIES
FINLAND, NEW ZEALAND, POLAND, UKRAINE

NOV 2023

TAKEDOWN OF MALWARE FOR HIRE

Operation 5th Element

The ransomware gang is behind high-profile attacks that created losses of hundreds of millions of euros

The investigation benefited from funding from the European Multidisciplinary Platform Against Criminal Threats (EMPACT)

International collaboration leads to dismantlement of ransomware group in Ukraine amidst ongoing war

Participating countries: NO, FR, NL, UA, DE, CH, USA, EUROPOL, EUROJUST

Results:

- **30 properties** searched
- Ringleader arrested and **4** accomplices detained

The individuals under investigation are believed to be part of a network responsible for a series of high-profile ransomware attacks against organisations in **71** countries.

These cyber actors are known for specifically targeting large corporations, effectively bringing their businesses to a standstill. They deployed **LockerGoga, MegaCortex, HIVE and Dharma ransomware**, among others, to carry out their attacks.

EUROPOL

Europol Unclassified - Basic Protection Level

FEB 2023

TAKEDOWN OF MALWARE FOR HIRE

Operation Parker

Operation by **German** and **Ukrainian** police. Supported by **Europol**, the Dutch Police **(Politie)** and the **US FBI**.

Core members ransomware criminal group targeted

EC3's support:

- Information exchange
- **3 experts** deployed in Germany on the action day
- Analytical support: cryptocurrency, malware, decryption and forensic analysis

Results:

- Raided house of a German national
- Electronic equipment seized
- Ukrainian suspect interrogated
- **2 locations** searched in Ukraine

DoppelPaymer ransomware

- Used since 2019 to attack **organisations** and **critical infrastructures**.
- Used a **unique tool** that compromised defence organisms by terminating the security-related process of the attacked systems.
- Distributed through **phishing/spam** including malicious att
- **Double extortion schem** website launched by th 2020.
- The DoppelPaymer atta enabled by the prolific malware.

EUROPOL J-CAT

EUROPOL

Europol Unc

SEPT 2023

LAW EMFORCENT COOPERATION TAKEDOWN

Operation EndGame Qakbot botnet

Eurojust and Europol aided cross-border judicial cooperation with law enforcement from France, Germany, Latvia, The Netherlands, Romania, UK, and the US for this operation.

Cross-border judicial cooperation takes down large botnet infrastructure Qakbot

Results:

- Coordinated international law enforcement effort led to the takedown of Qakbot infrastructure
- Nearly **EUR 8 million** seized in cryptocurrencies

Europol facilitated information exchange, coordination, and provided analytical support.

Qakbot

The malware victimised more than **700 000 computers** in almost **30 countries**, with at least **EUR 54 million** paid in ransoms since 2007.

Distributed via spam emails with malicious attachments/links.

Stole financial data and login credentials and allowed for further infections like ransomware and made infected computers part of a botnet.

EUROPOL

Europol Unclassified - Basic Protection Level

MARCH 2023

TAKEDOWN OF CHIPMIXER

Operation Atlas takedown Chipmixer

German, US authorities, and Europol, have targeted ChipMixer, a cryptocurrency mixer well-known in the cybercriminal underworld.

One of the darkweb's largest cryptocurrency laundromats washed out

EUROPOL J-CAT

The investigation was also supported by Belgium, Poland and Switzerland.

Results:

- Takedown of the platform infrastructure
- 4 servers seized
- EUR 44 million in Bitcoins seized
- 7 TB of data seized

ChipMixer (Unlicensed)

Available on the clear and on the **darkweb**.

Specialised in mixing/cutting trails related to virtual currency assets = anonymising where the initial funds originated.

Criminals have illegally obtained money → Deposited into 'mixers' to disguise origins → Crypto exchanges funds into a fiat currency → Laundered money available for criminals

EUROPOL

Europol Unclassified - Basic Protection Level

JAN 2023

RANSOMWARE-AS-A-SERVICE

OP Dawnbreaker HIVE ransomware

Shutdown of HIVE infrastructure marketplace extorting millions in ransom

EUROPOL EC3 J-CAT

Results:

- International operation led by Germany, Netherlands and U.S. involving authorities from **13 countries**
- About EUR **120** million saved thanks to mitigation efforts
- Decryption keys **free of charge**

EC3's support:

- Information exchange
- **4** experts deployed on the spot on the action day
- **Analytical support:** cryptocurrency, malware, decryption and forensic

Ransomware-as-a-Service / Double Extortion Model

1 Criminals copied the data and then encrypted the files.

2 They asked for a **ransom** to both decrypt the files and to not publish the stolen data on the Hive Leak Site.

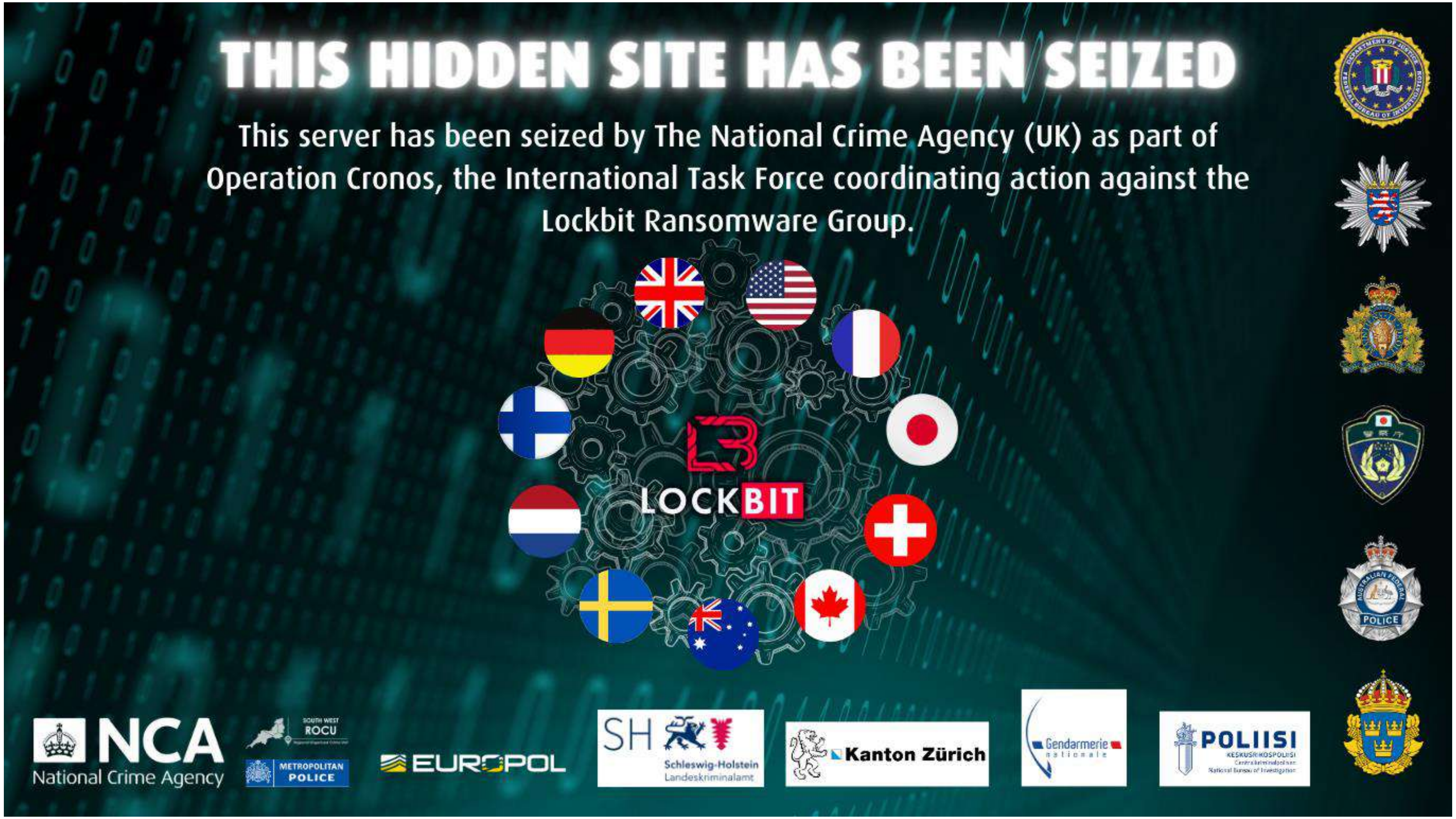
Modus Operandi

HIVE ransomware was used to target businesses and critical infrastructure sectors, including **government facilities, manufacturing, information technology and healthcare** (1 hospital in Germany)

EUROPOL

Europol Unclassified - Basic Protection Level

Operation Cronos, 2024
Taking down Lockbit



THIS HIDDEN SITE HAS BEEN SEIZED

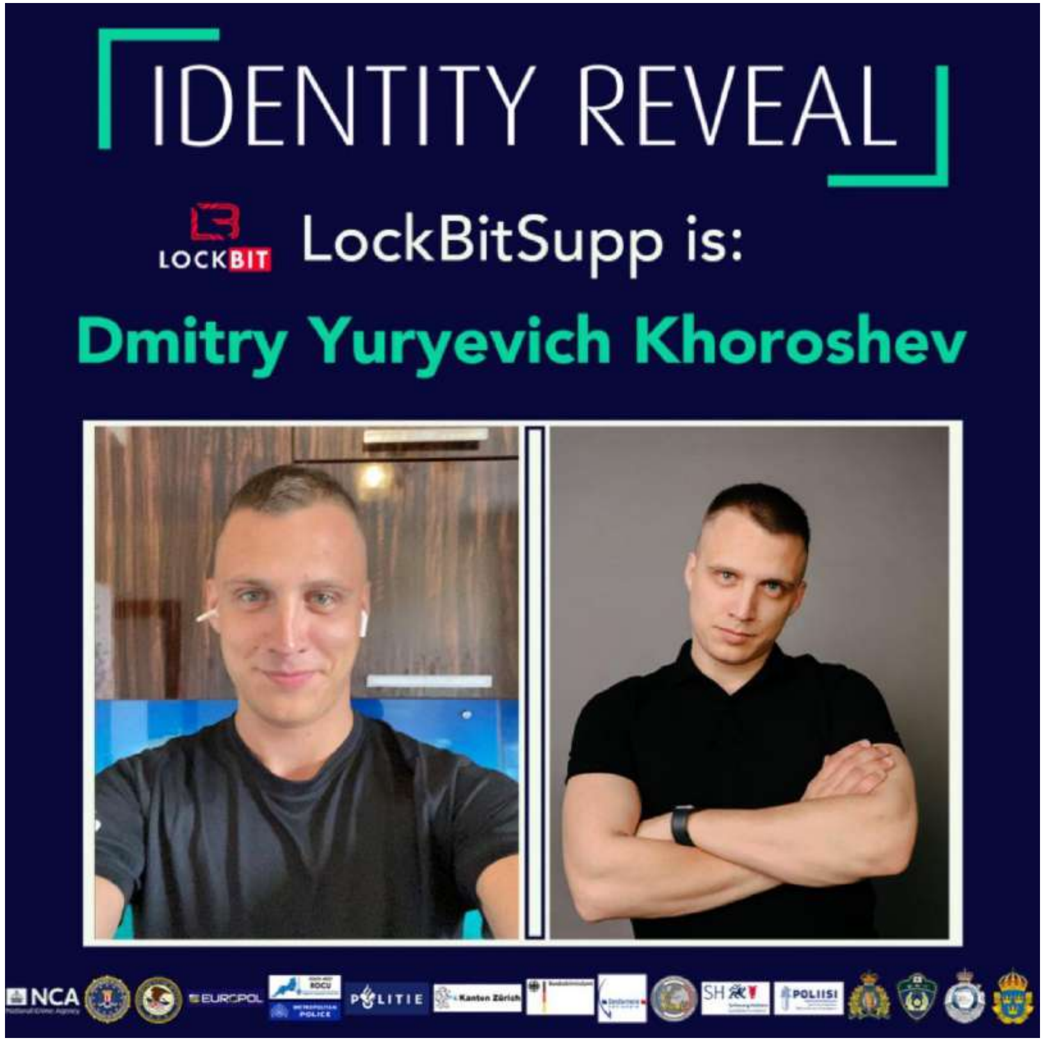
This server has been seized by The National Crime Agency (UK) as part of Operation Cronos, the International Task Force coordinating action against the Lockbit Ransomware Group.

Operation Cronos, 2024
Taking down Lockbit

International operation led by the UK involving authorities from **10 countries.**

Results:

- 2 arrests in Poland and Ukraine
  5 public indictments and 3 arrest warrants from FR and US
- Main infrastructure compromised
  34 servers disrupted
- About EUR **10** million worth in crypto frozen
  120 million on private addresses flagged and monitored
- 14 000+ accounts belonging to affiliates seized and taken down



A continuously growing threat

- Ransomware has been growing because it is **financially efficient**
- Crypto currencies are difficult – when not impossible – to trace, which makes it easy for criminals to receive payments, becoming a critical ransomware enabler.
- **Double-extortion** – If organizations refuse to pay up, stolen data may be published on the platform and made available to the public, competitors or investors

- States often provide **safe operating havens** to cybercriminal

- **Corporate practices** through specialization of skills and distributed tasks and responsibilities

Cyber-related crimes

Cyber-enabled crimes related to economy

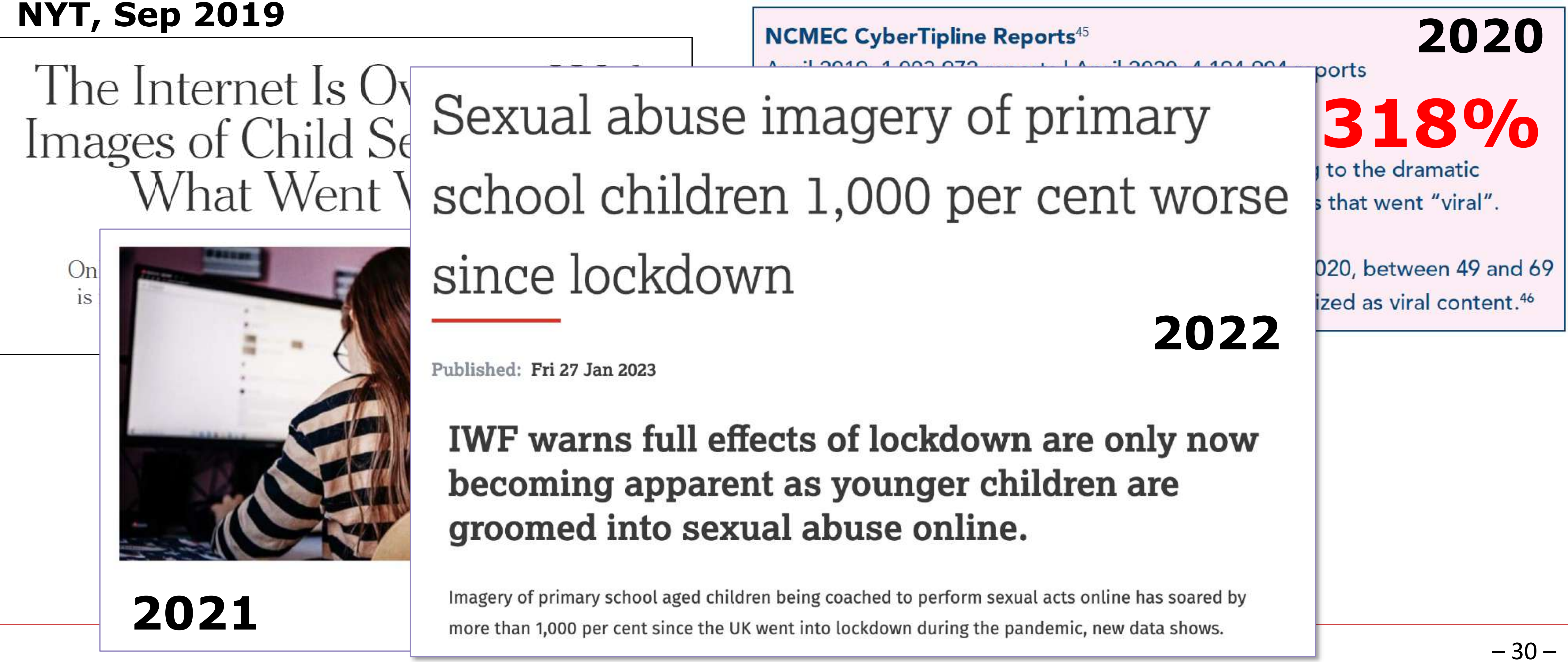
- Fraud (phishing, BEC, etc.)
- Sale of illegal goods (drug trafficking, etc.)
- Money-laundering
- IP crimes
- etc.

Cyber-enabled crimes related to interpersonal violence

- **Child sexual abuse and exploitation**
- Cyber bullying
- Sextortion
- Romance scam, Revenge porn
- etc.

Online child sexual exploitation

NYT, Sep 2019



The Internet Is O
Images of Child Se
What Went

On
is

2021

NCMEC CyberTipline Reports[45]

April 2019: 1,003,972 reports | April 2020: 4,194,904 reports

2020

318%

to the dramatic
that went "viral".

020, between 49 and 69
ized as viral content.[46]

Sexual abuse imagery of primary school children 1,000 per cent worse since lockdown

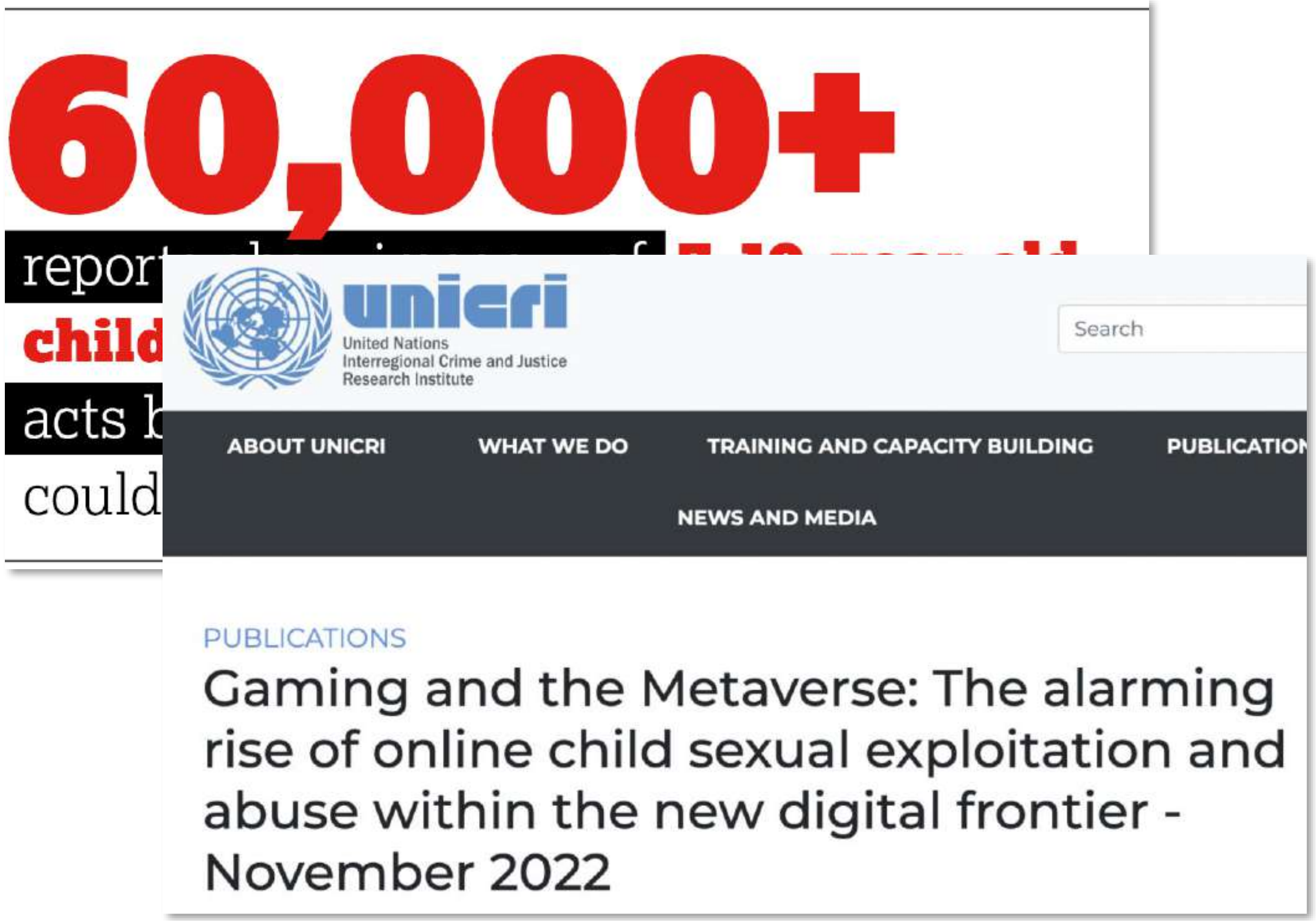
2022

Published: Fri 27 Jan 2023

IWF warns full effects of lockdown are only now becoming apparent as younger children are groomed into sexual abuse online.

Imagery of primary school aged children being coached to perform sexual acts online has soared by more than 1,000 per cent since the UK went into lockdown during the pandemic, new data shows.

Online child sexual exploitation



PUBLICATIONS

Gaming and the Metaverse: The alarming rise of online child sexual exploitation and abuse within the new digital frontier - November 2022

Increase of live streaming of child sexual abuse, which remains a particularly complex crime to investigate.

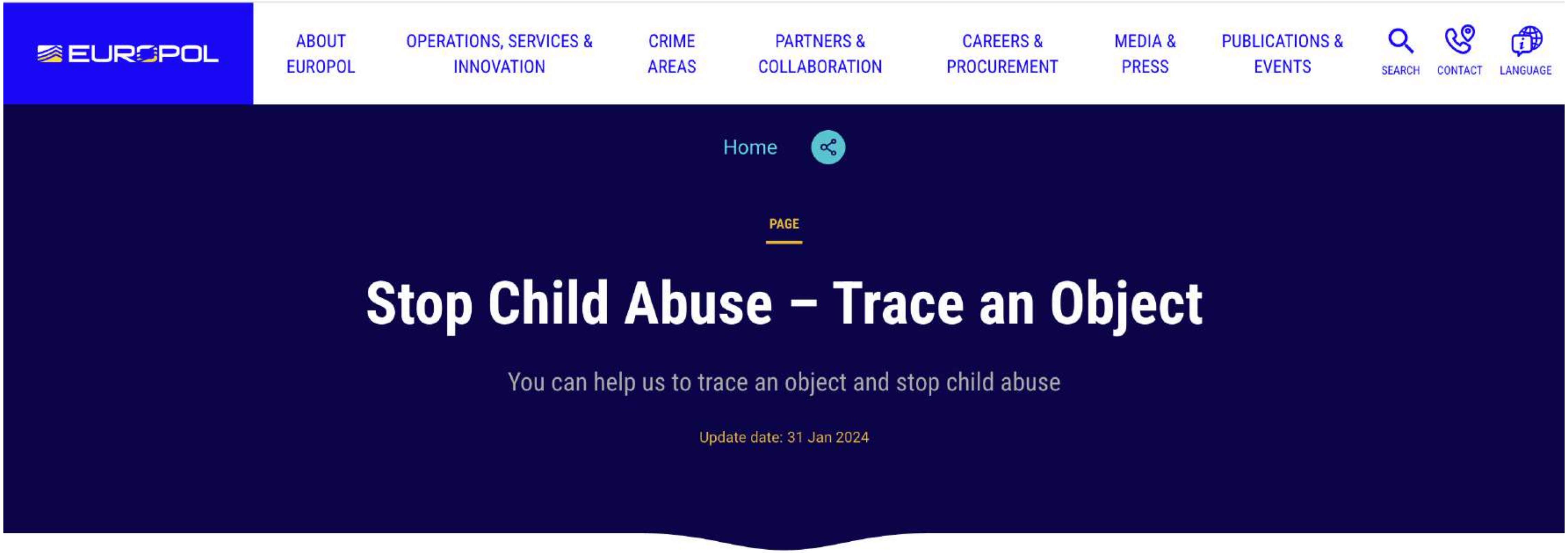
Anonymization and encryption tools

Huge increase in online solicitation, sextortion and revenge porn

NCMEC study 2020:

- 95% of CSAM hosted in EU or US
- 19% of convicted offenders had images of infants under the age of 3

An initiative by Europol



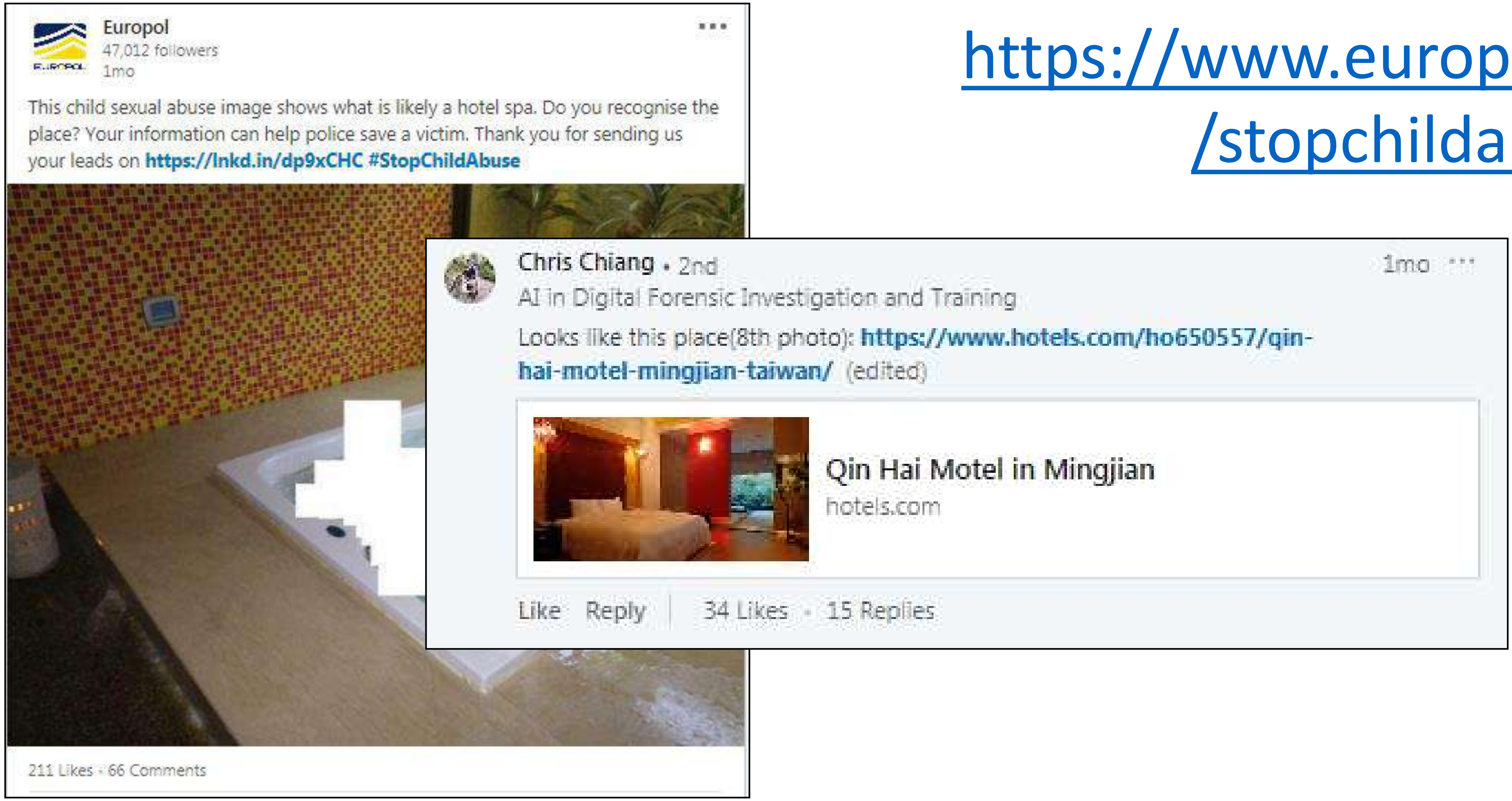
PAGE

Stop Child Abuse – Trace an Object

You can help us to trace an object and stop child abuse

Update date: 31 Jan 2024

Europol Trace An Object Campaign



Europol
47,012 followers
1mo

This child sexual abuse image shows what is likely a hotel spa. Do you recognise the place? Your information can help police save a victim. Thank you for sending us your leads on https://lnkd.in/dp9xCHC #StopChildAbuse

211 Likes · 66 Comments

Chris Chiang • 2nd
AI in Digital Forensic Investigation and Training
1mo

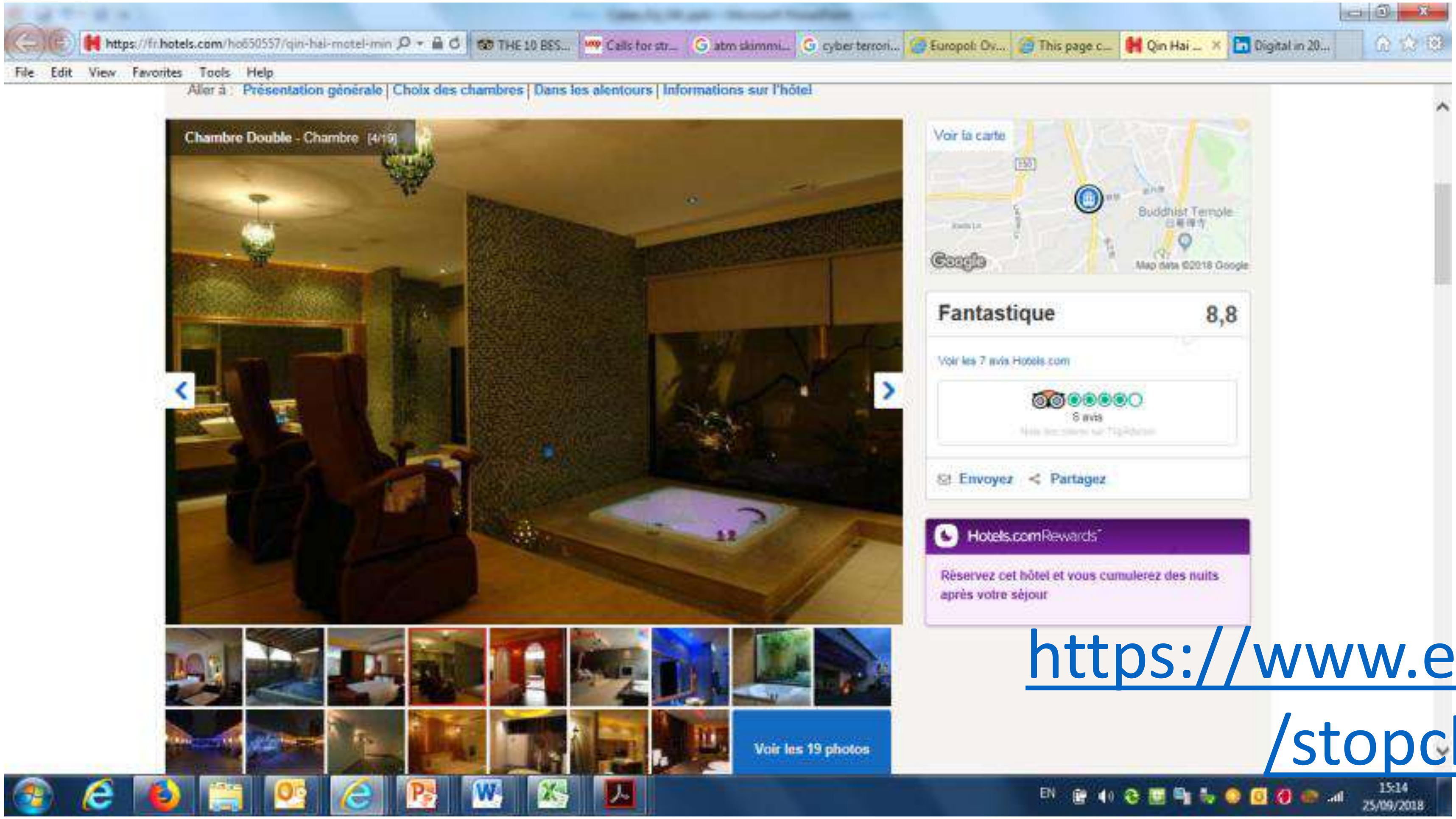
Looks like this place(8th photo): https://www.hotels.com/ho650557/qin-hai-motel-mingjian-taiwan/ (edited)

Qin Hai Motel in Mingjian
hotels.com

Like Reply | 34 Likes · 15 Replies

https://www.europol.europa.eu/stopchildabuse

Europol Trace An Object Campaign



Réservez cet hôtel et vous cumulerez des nuits après votre séjour

https://www.europol.europa.eu/stopchildabuse

Cyber-assisted crimes

- Traditional crimes, Internet is used **to assist with the organisation of a crime**
- The digital tool is not critical to these forms of crime, which would still take place if the internet was removed

Trafficking activities of collectivities

- Terrorism
- Smuggling of migrants
- Counterfeit medicines
- Illegal animal trafficking
- etc.

Criminal activities of individuals

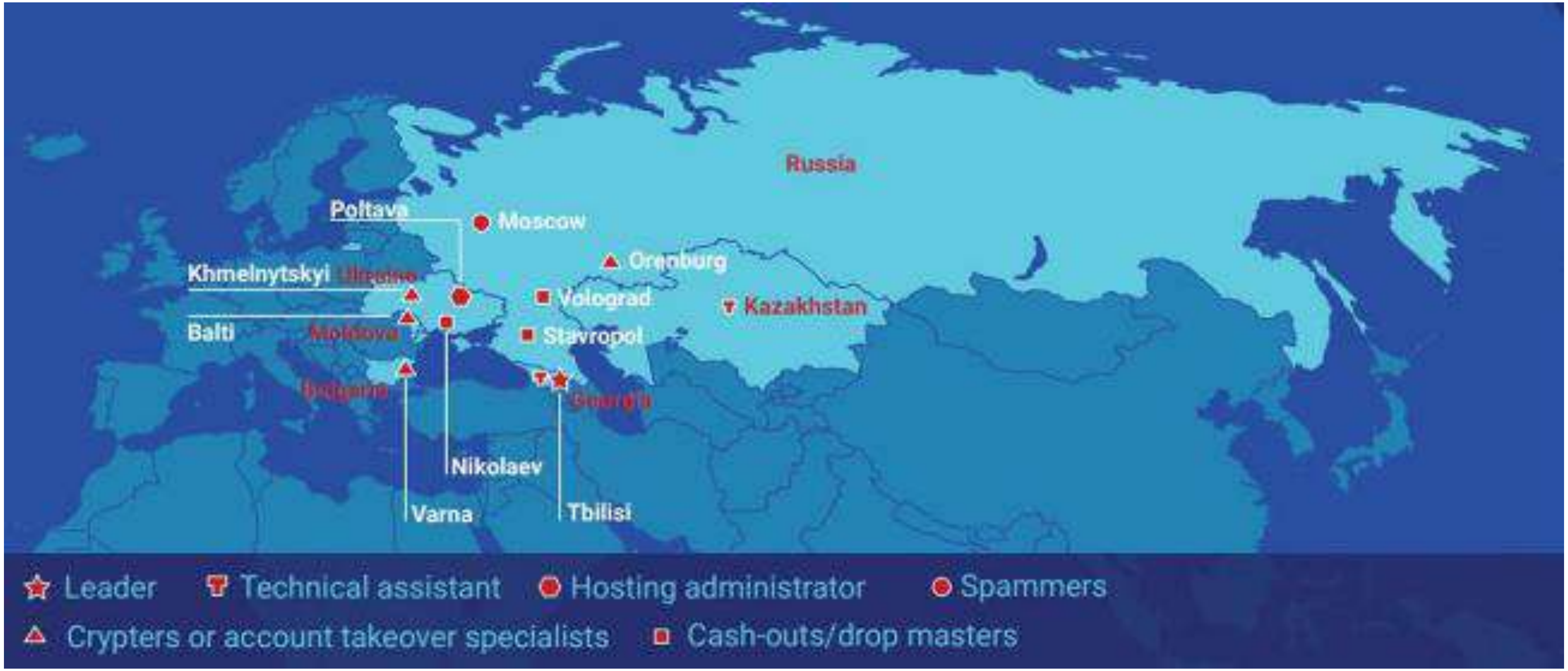
- Using internet to learn how to commit or hide a crime
- Info gathering about prospective victims
- **Crime-as-a-service**
- etc.

Cybercrime-as-a-service

- Increasing modularization, high level of specialization

<u>Goznym</u>

Crimina syndicate suspected to have committed frauds for morethan **$100 millions** against more than **41,000 victims** through the use of a **banking trojan** named **GozNym.**



The Encrochat case

Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized

Judiciary and police present first overview of results

EncroChat phones were presented guaranteeing perfect anonymity, discretion and no traceability to users. It also had functions intended to ensure automatic deletion of messages by recipients and a specific PIN code to delete all data on the device of the sender, to quickly erase compromising messages, for example at the time of arrest by the police.

In addition the device could be erased from a distance by the reseller/helpdesk. EncroChat sold crypto telephones for around EUR 1 000 each, on an international scale.

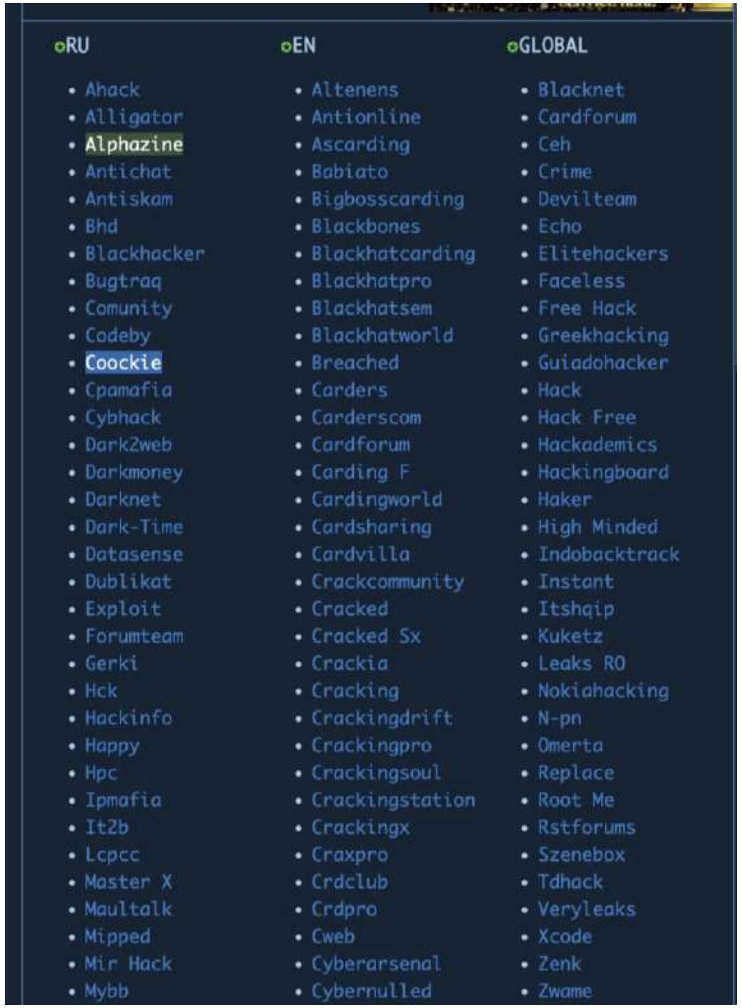
The dimantling of EncroChat helped to prevent violent attacks, attempted murders, corruption and large-scale drug transports, as well as obtain large-scale information on organised crime.

Illicit online markets

- Illicit online markets assist a number of **activities related to the commission of crimes**. Some example:
- Exchange of illicit goods and stolen data
- Offering of services and tools to launch an attack
- Job market to join criminal networks
- Information sharing on techniques and targets
- Cybercriminals fora
- etc.
- Although the large majority of illicit markets are hosted on the darkweb and only **reachable through the TOR browser**, there are fora also on the clear web..

Illicit online markets – Let’s have a look

- https://link-king.org/#forums



○RU

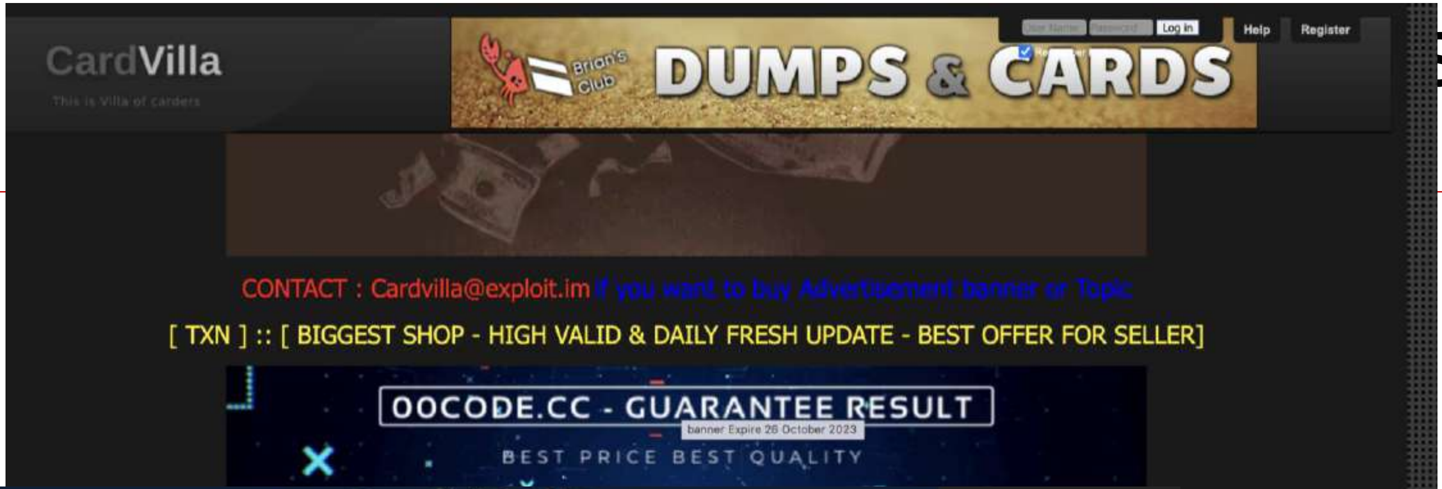
- Ahack
- Alligator
- Alphazine
- Antichat
- Antiskam
- Bhd
- Blackhacker
- Bugtraq
- Comunity
- Codeby
- Coockie
- Cpamafia
- Cybhack
- Dark2web
- Darkmoney
- Darknet
- Dark-Time
- Datasense
- Dublikat
- Exploit
- Forumteam
- Gerki
- Hck
- Hackinfo
- Happy
- Hpc
- Ipmafia
- It2b
- Lcpcc
- Master X
- Maultalk
- Mipped
- Mir Hack
- Mybb

○EN

- Altenens
- Antionline
- Ascarding
- Babiato
- Bigbosscarding
- Blackbones
- Blackhatcarding
- Blackhatpro
- Blackhatsem
- Blackhatworld
- Breached
- Carders
- Carderscom
- Cardforum
- Carding F
- Cardingworld
- Cardsharing
- Cardvilla
- Crackcommunity
- Cracked
- Cracked Sx
- Crackia
- Cracking
- Crackingdrift
- Crackingpro
- Crackingsoul
- Crackingstation
- Crackingx
- Craxpro
- Crdclub
- Crdpro
- Cweb
- Cyberarsenal
- Cybernulled

○GLOBAL

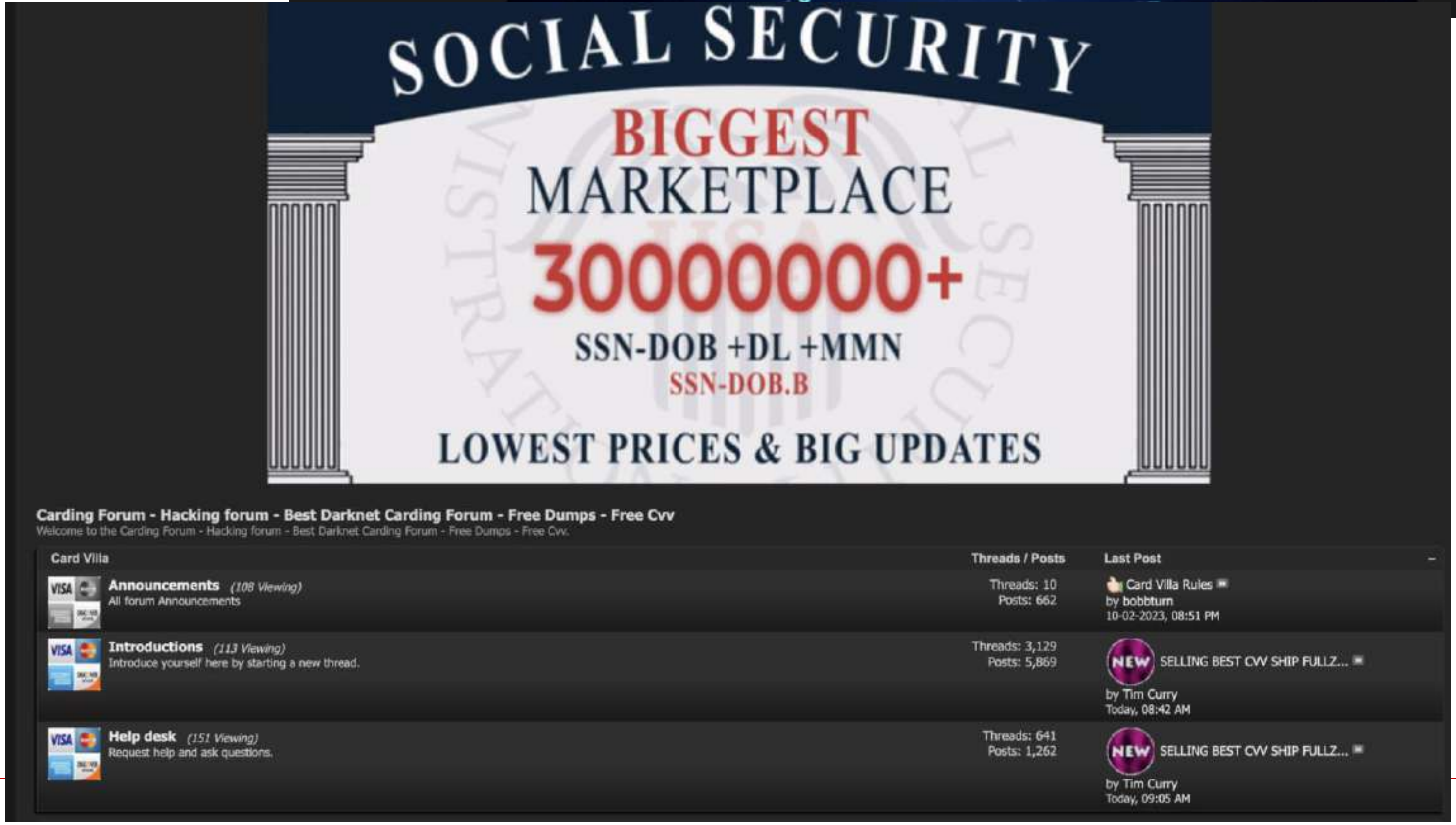
- Blacknet
- Cardforum
- Ceh
- Crime
- Devilteam
- Echo
- Elitehackers
- Faceless
- Free Hack
- Greekhacking
- Guiadohacker
- Hack
- Hack Free
- Hackademics
- Hackingboard
- Haker
- High Minded
- Indobacktrack
- Instant
- Itshqip
- Kuketz
- Leaks RO
- Nokiahacking
- N-pn
- Omerta
- Replace
- Root Me
- Rstforums
- Szenebox
- Tdhack
- Veryleaks
- Xcode
- Zenk
- Zwame



CardVilla
This is Villa of carders

CONTACT : Cardvilla@exploit.im if you want to buy Advertisement banner or Topic

[TXN] :: [BIGGEST SHOP - HIGH VALID & DAILY FRESH UPDATE - BEST OFFER FOR SELLER]



Carding Forum - Hacking forum - Best Darknet Carding Forum - Free Dumps - Free Cvv
Welcome to the Carding Forum - Hacking forum - Best Darknet Carding Forum - Free Dumps - Free Cvv.

Card Villa	Threads / Posts	Last Post
Announcements *(108 Viewing)* All forum Announcements	Threads: 10 Posts: 662	Card Villa Rules by bobbturn 10-02-2023, 08:51 PM
Introductions *(113 Viewing)* Introduce yourself here by starting a new thread.	Threads: 3,129 Posts: 5,869	NEW SELLING BEST CVV SHIP FULLZ... by Tim Curry Today, 08:42 AM
Help desk *(151 Viewing)* Request help and ask questions.	Threads: 641 Posts: 1,262	NEW SELLING BEST CVV SHIP FULLZ... by Tim Curry Today, 09:05 AM

Beyond «simple» cybercrime

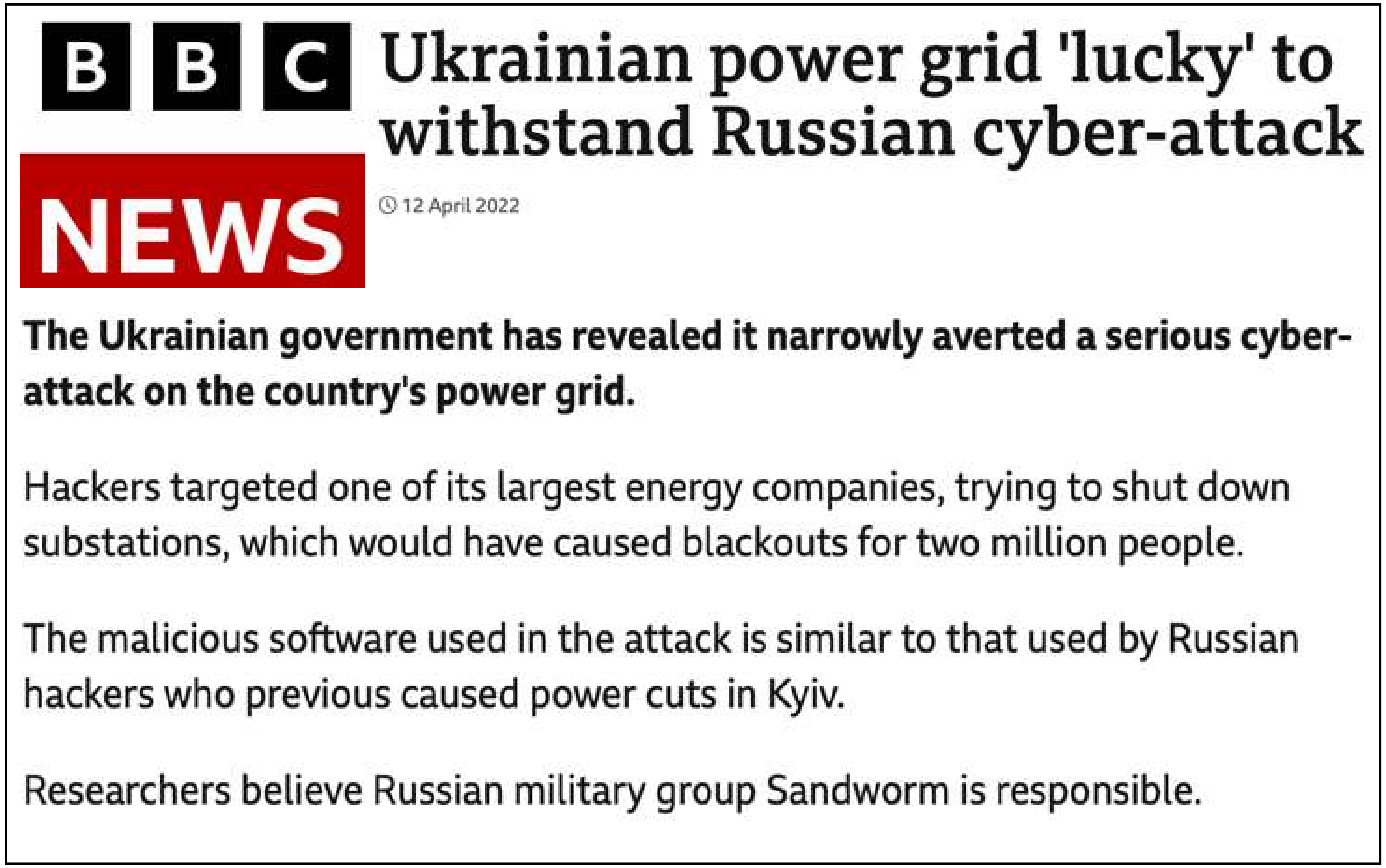
Cyber Terrorism

- Cyber-dependent terrorism (e.g. attacks against ICT infrastructure of a State/ DDoS)
- Cyber-enabled terrorism (e.g. hate crimes through the use of social media)
- Cyber-assisted terrorism (e.g. networking and anonymous communication, propaganda)

Cyber Warfare

- *“Cyberwarfare refers to a* ***massively coordinated digital assault on a government by another****,* ***or by large groups of citizens****.*
- *It is the action by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption” (Clarke and Knake, 2012).*

Cyber warfare: Attacks to critical infrastructures



Ukrainian power grid 'lucky' to withstand Russian cyber-attack

12 April 2022

The Ukrainian government has revealed it narrowly averted a serious cyber-attack on the country's power grid.

Hackers targeted one of its largest energy companies, trying to shut down substations, which would have caused blackouts for two million people.

The malicious software used in the attack is similar to that used by Russian hackers who previous caused power cuts in Kyiv.

Researchers believe Russian military group Sandworm is responsible.

Attacks connected to the Russian war of aggression against Ukraine

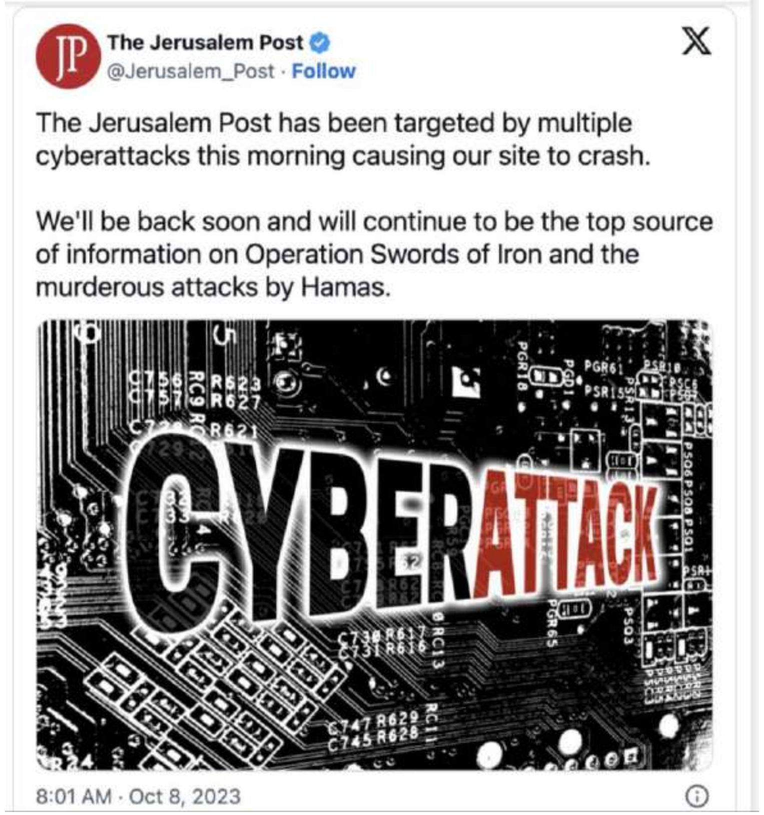
- **24 Feb 2022**, the day of the invasion.
- Cyber attack against modems and routers communicating with the satelliete network KA-SAT, providing **access to Internet to tens thousand citizens in Ukraine and Europe**
- **Wiper malware «AcidRain»**, to make the system unavailable, not to access data or systems
- Attribution → Russian Cyber Army, to make the command center of Ukraine Army unusable during the invasion
- The action had impacts in all Europe
    - A German energy company lost control over 5.800 wind turbines

Viasat™

*Ultimately, **tens of thousands of modems that were previously online and active dropped off the network, and these modems were not observed attempting to re-enter the network**. The attack impacted a majority of the previously active modems within Ukraine, and a substantial number of additional modems in other parts of Europe.*

*Subsequent investigation and forensic analysis identified a **ground-based network intrus**ion by an attacker exploiting a misconfiguration in a VPN appliance **to gain remote access to the trusted management segment of the KA-SAT network**. The attacker moved laterally through this trusted management network to a specific network segment used to manage and operate the network, and then used this network access to **execute legitimate, targeted management commands on a large number of residential modems simultaneously**. Specifically, these **destructive commands overwrote key data in flash memory on the modems, rendering the modems unable to access the network, but not permanently unusable**.*

Cyber hacktivism

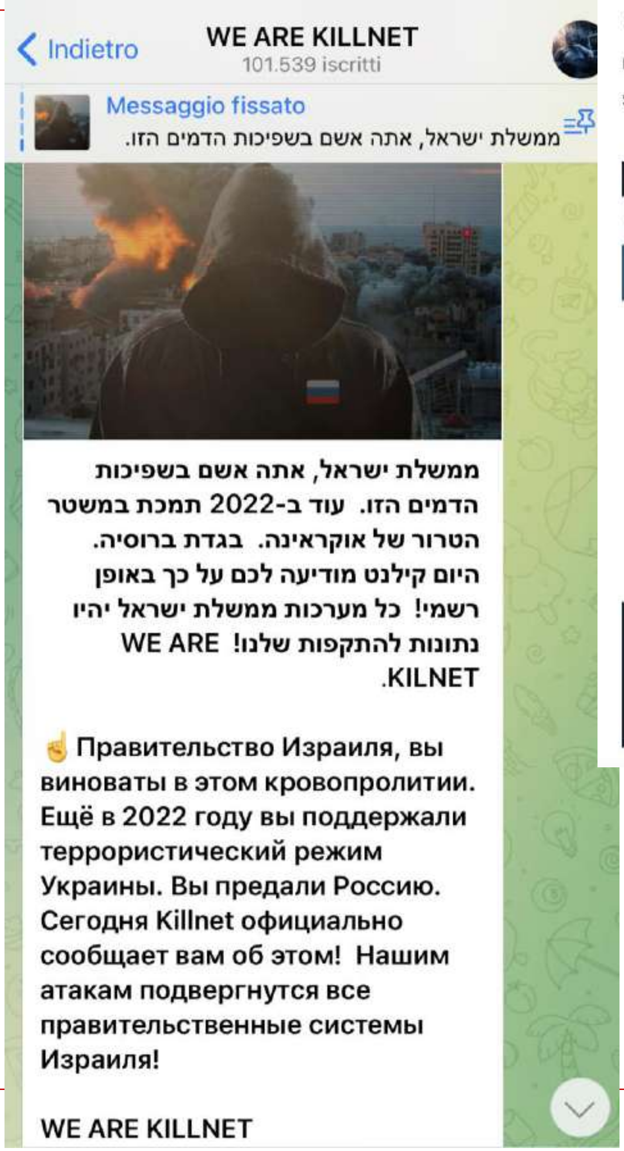


The Jerusalem Post @Jerusalem_Post · Follow

The Jerusalem Post has been targeted by multiple cyberattacks this morning causing our site to crash.

We'll be back soon and will continue to be the top source of information on Operation Swords of Iron and the murderous attacks by Hamas.

8:01 AM · Oct 8, 2023

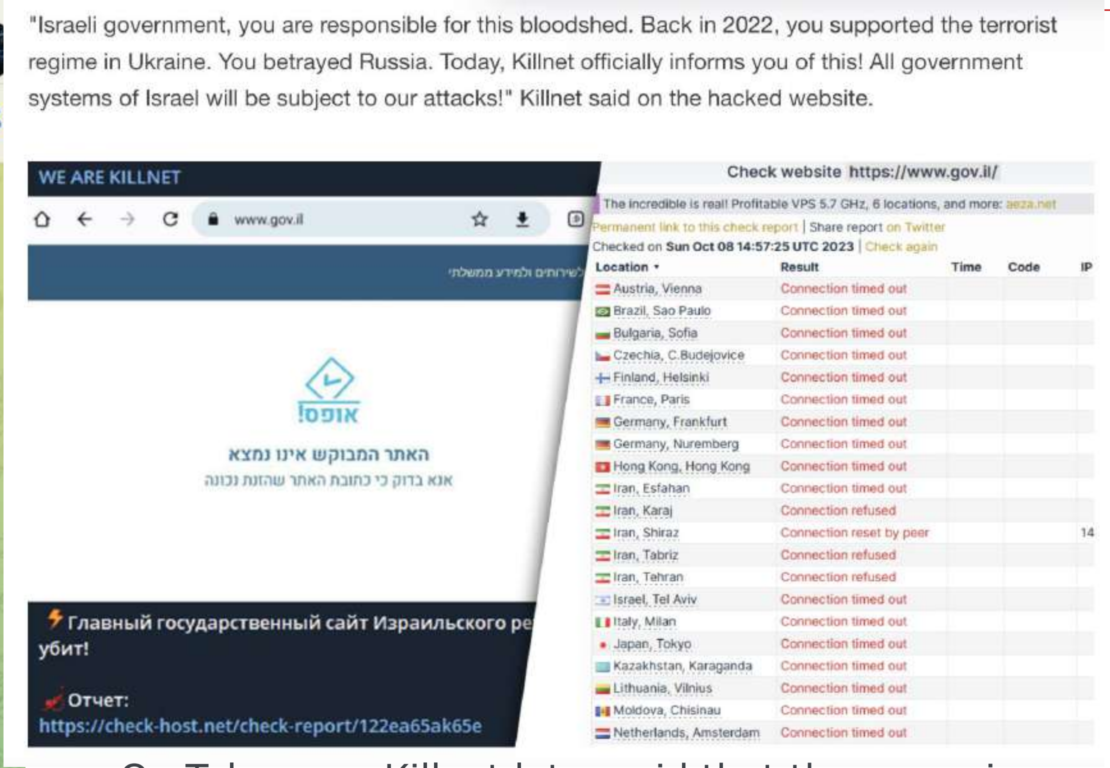


ממשלת ישראל, אתה אשם בשפיכות הדמים הזו.

ממשלת ישראל, אתה אשם בשפיכות
הדמים הזו. עוד ב-2022 תמכת במשטר
הטרור של אוקראינה. בגדת ברוסיה.
היום קילנט מודיעה לכם על כך באופן
רשמי! כל מערכות ממשלת ישראל יהיו
נתונות להתקפות שלנו! WE ARE
KILNET.

☝ Правительство Израиля, вы виноваты в этом кровопролитии. Ещё в 2022 году вы поддержали террористический режим Украины. Вы предали Россию. Сегодня Killnet официально сообщает вам об этом! Нашим атакам подвергнутся все правительственные системы Израиля!

WE ARE KILLNET



"Israeli government, you are responsible for this bloodshed. Back in 2022, you supported the terrorist regime in Ukraine. You betrayed Russia. Today, Killnet officially informs you of this! All government systems of Israel will be subject to our attacks!" Killnet said on the hacked website.

WE ARE KILLNET

האתר המבוקש אינו נמצא
אנא בדוק כי כתובת האתר שהזנת נכונה

⚡ Главный государственный сайт Израильского ре
убит!

Отчет:
https://check-host.net/check-report/122ea65ak65e

Check website https://www.gov.il/

The incredible is real! Profitable VPS 5.7 GHz, 6 locations, and more: aeza.net

Permanent link to this check report | Share report on Twitter

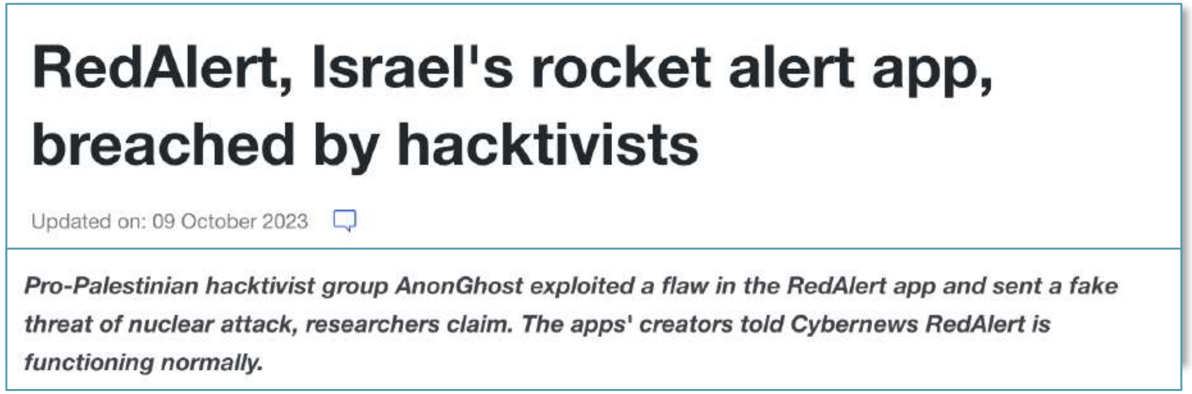
Checked on **Sun Oct 08 14:57:25 UTC 2023** | Check again

Location ▾	Result	Time	Code	IP
Austria, Vienna	Connection timed out			
Brazil, Sao Paulo	Connection timed out			
Bulgaria, Sofia	Connection timed out			
Czechia, C.Budejovice	Connection timed out			
Finland, Helsinki	Connection timed out			
France, Paris	Connection timed out			
Germany, Frankfurt	Connection timed out			
Germany, Nuremberg	Connection timed out			
Hong Kong, Hong Kong	Connection timed out			
Iran, Esfahan	Connection timed out			
Iran, Karaj	Connection refused			
Iran, Shiraz	Connection reset by peer			14
Iran, Tabriz	Connection refused			
Iran, Tehran	Connection refused			
Israel, Tel Aviv	Connection timed out			
Italy, Milan	Connection timed out			
Japan, Tokyo	Connection timed out			
Kazakhstan, Karaganda	Connection timed out			
Lithuania, Vilnius	Connection timed out			
Moldova, Chisinau	Connection timed out			
Netherlands, Amsterdam	Connection timed out			

On Telegram, Killnet later said that the group is not targeting ordinary Israeli citizens – its target is the "regime" that "sold itself to the NATO whore, the same main terrorist, with the slogan of PEACE and DEFENSE!"

The group added: "The atrocities that Hamas or Israel commit against civilians are terrible! We exclude the possibility of attacking the critical infrastructure of both sides!"

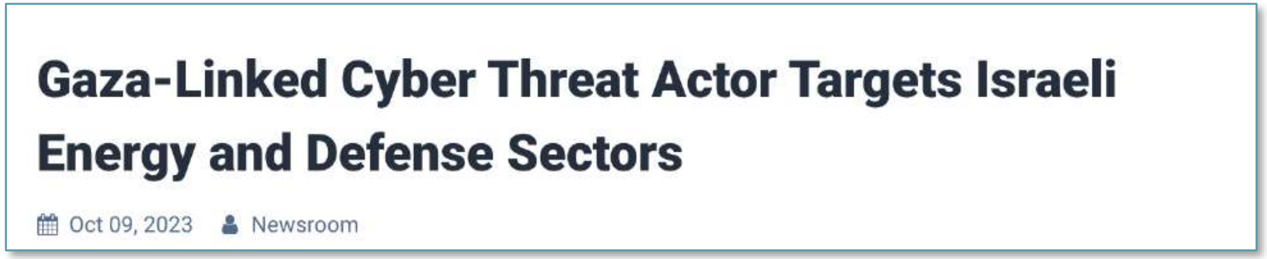
Attacks and hacktivist groups



RedAlert, Israel's rocket alert app, breached by hacktivists

Updated on: 09 October 2023

Pro-Palestinian hacktivist group AnonGhost exploited a flaw in the RedAlert app and sent a fake threat of nuclear attack, researchers claim. The apps' creators told Cybernews RedAlert is functioning normally.

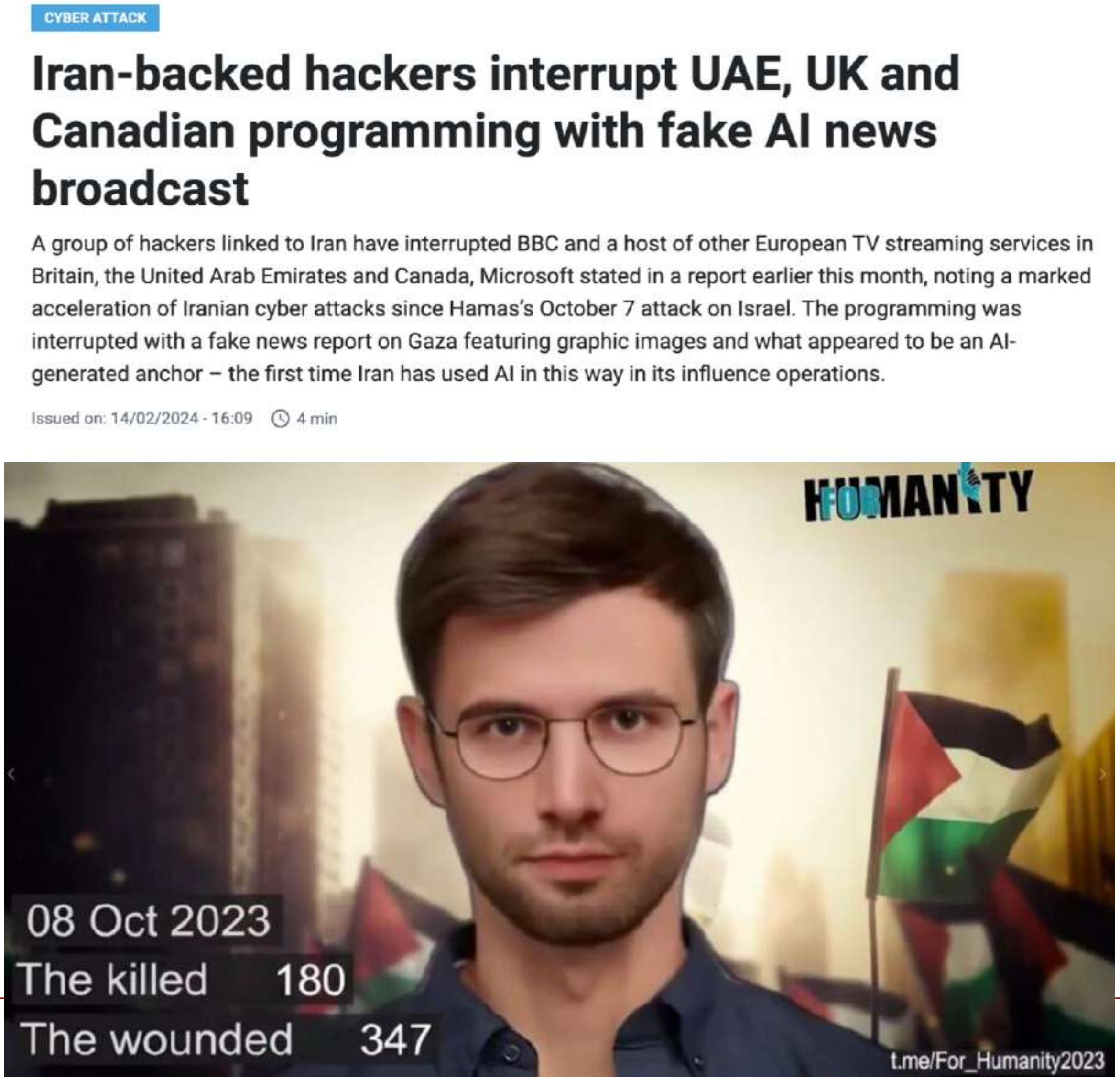


Gaza-Linked Cyber Threat Actor Targets Israeli Energy and Defense Sectors

Oct 09, 2023 Newsroom

Pro-Israel Groups	Pro-Palestine Groups			Neutral Groups
VulzSec	KillNet	Blackshieldcrew MY	Team Herox	ThreatSec
Indian Cyber Force	Anonymous Sudan	Gb Anon 17	SynixCyberCrimeMY	Cyber Army Of Russia
UCC Team	UserSec	Anonymous Morocco	Panoc team	
Garuna Ops	Anonymous Russia	Ghost Clan Malaysia	4 Exploitation	
SilentOne	Ghosts of Palestine	Mysterious Team Bangladesh	Team R70	
IT ARMY of Ukraine	Team Azrael Angel of Death	Ganosec team	Stucx Team	
	Dark Strom Team	Moroccan Black Cyber Army	The White Crew	
	Pakistani Leet Hackers	Muslim Cyber Army	Cscrew	
	Sylhet Gang-SG	GhostClan	TYG Team	
	Team_insane_Pakistan	Eagle Cyber Crew	Hizbullah Cyb3r Team	
	Hacktivism Indonesia	Kerala Cyber Xtractors	Electronic Tigers Unit	
	Garnesia Team	YourAnon T13x	StarsX Team	

Other examples



CYBER ATTACK

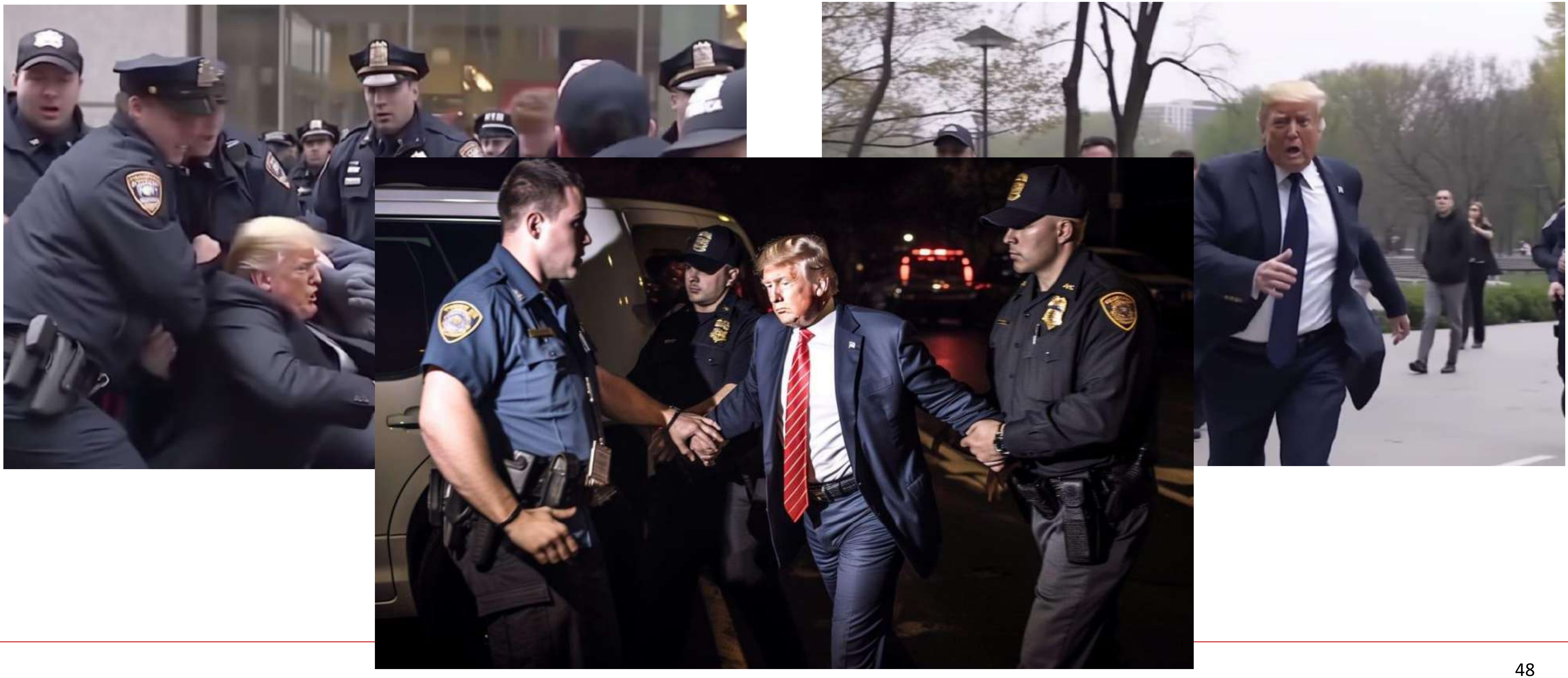
Iran-backed hackers interrupt UAE, UK and Canadian programming with fake AI news broadcast

A group of hackers linked to Iran have interrupted BBC and a host of other European TV streaming services in Britain, the United Arab Emirates and Canada, Microsoft stated in a report earlier this month, noting a marked acceleration of Iranian cyber attacks since Hamas's October 7 attack on Israel. The programming was interrupted with a fake news report on Gaza featuring graphic images and what appeared to be an AI-generated anchor – the first time Iran has used AI in this way in its influence operations.

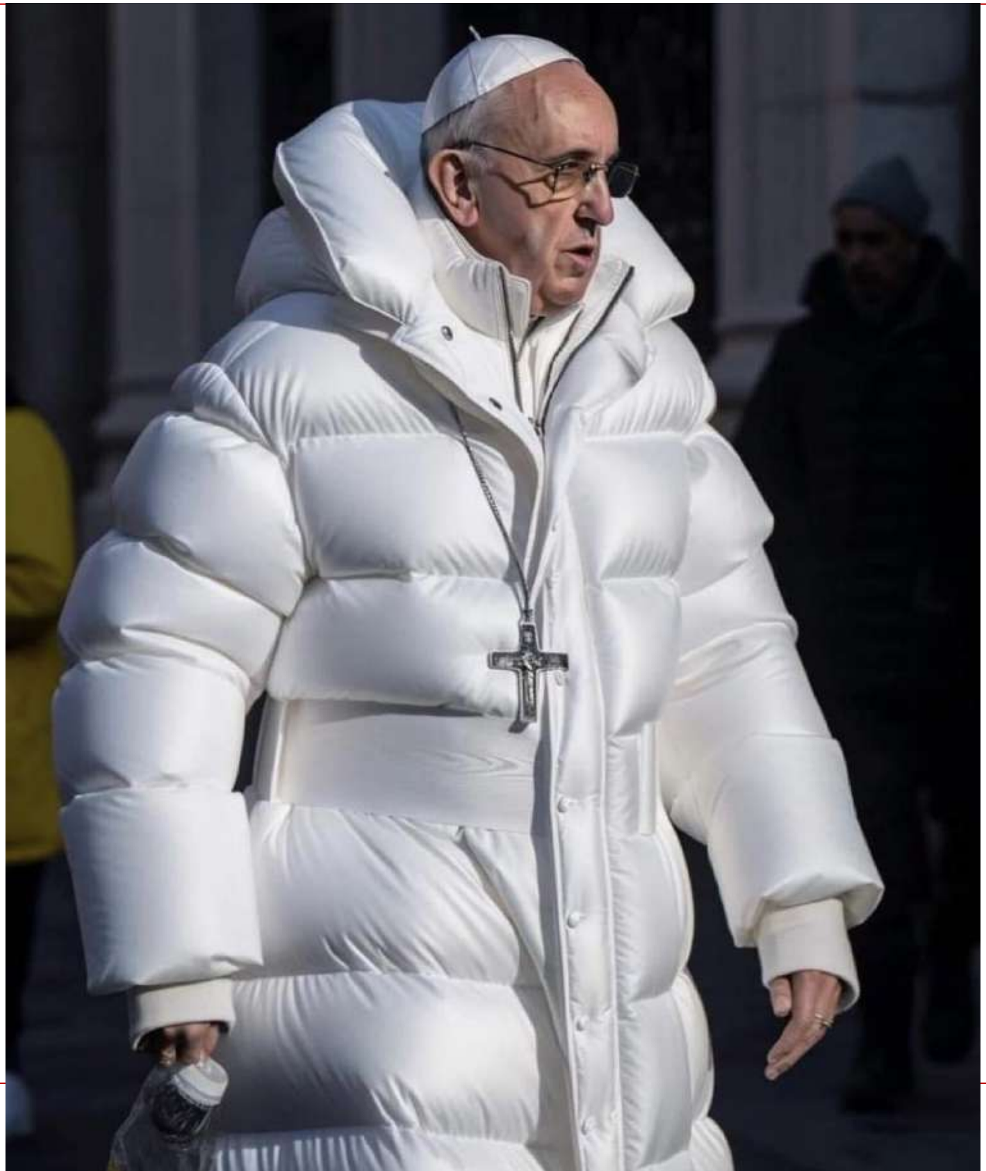
Issued on: 14/02/2024 - 16:09 4 min

New tech and cybercrime: Obama in 2018

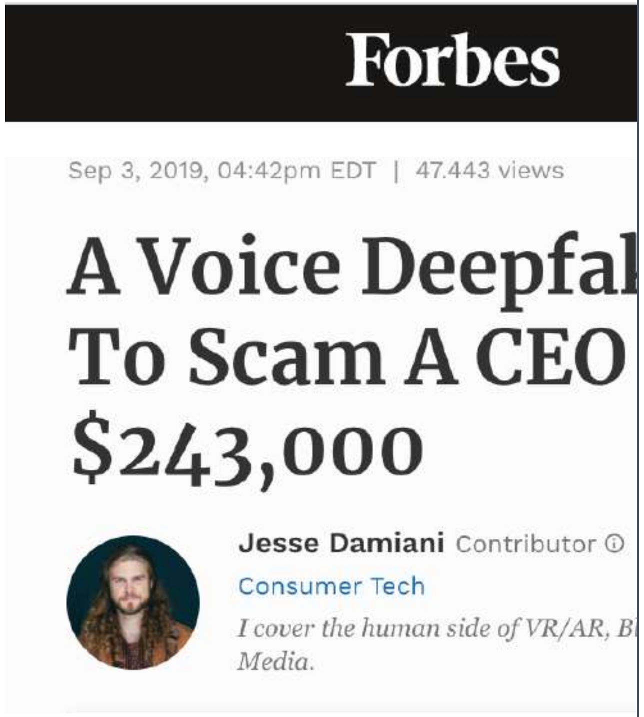
Trump in 2023



Pope Francis in 2023



Deepfake and cyber operations

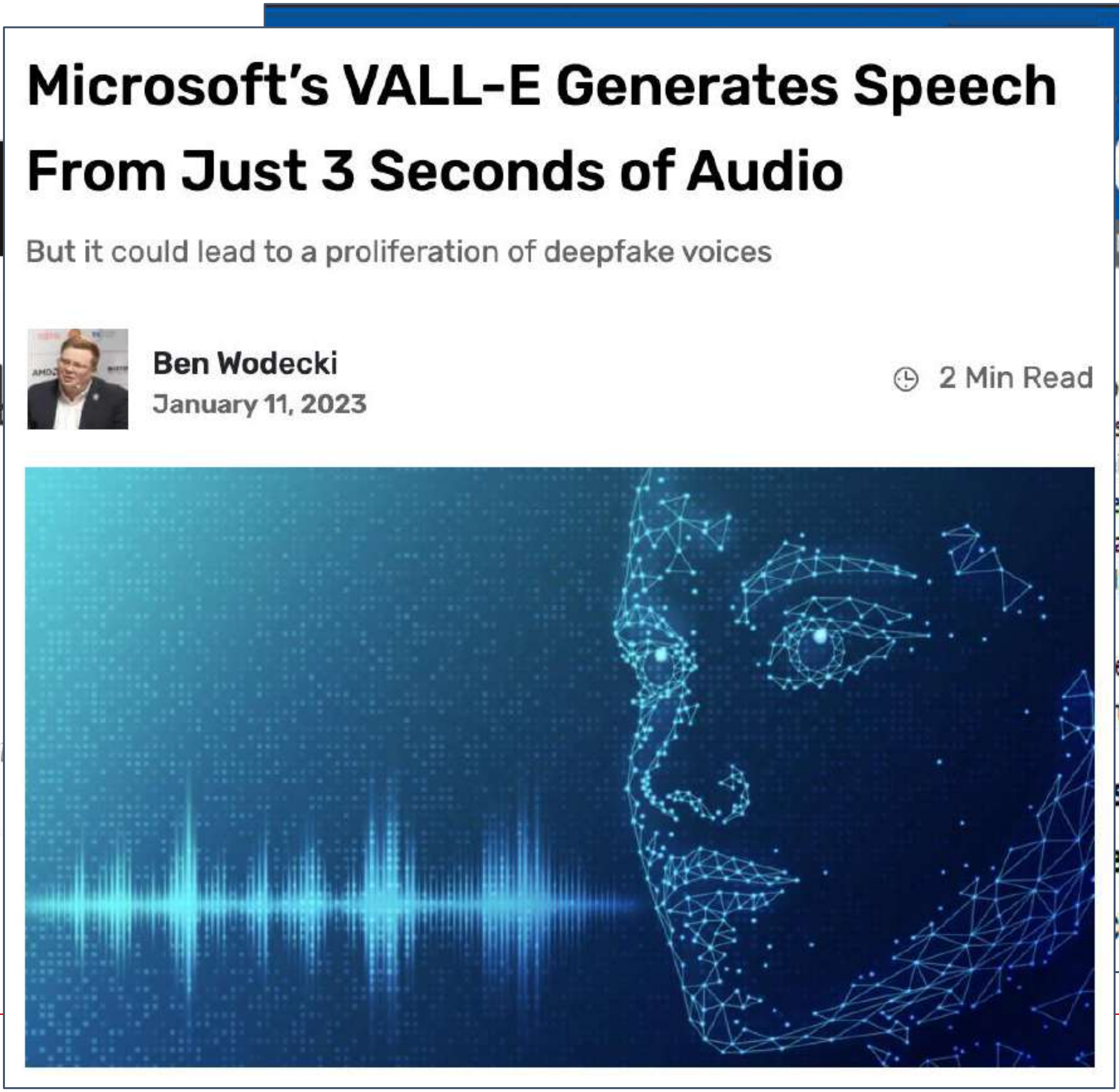


Forbes

Sep 3, 2019, 04:42pm EDT | 47.443 views

A Voice Deepfal
To Scam A CEO
$243,000

Jesse Damiani Contributor ⓘ
Consumer Tech
I cover the human side of VR/AR, Bl
Media.

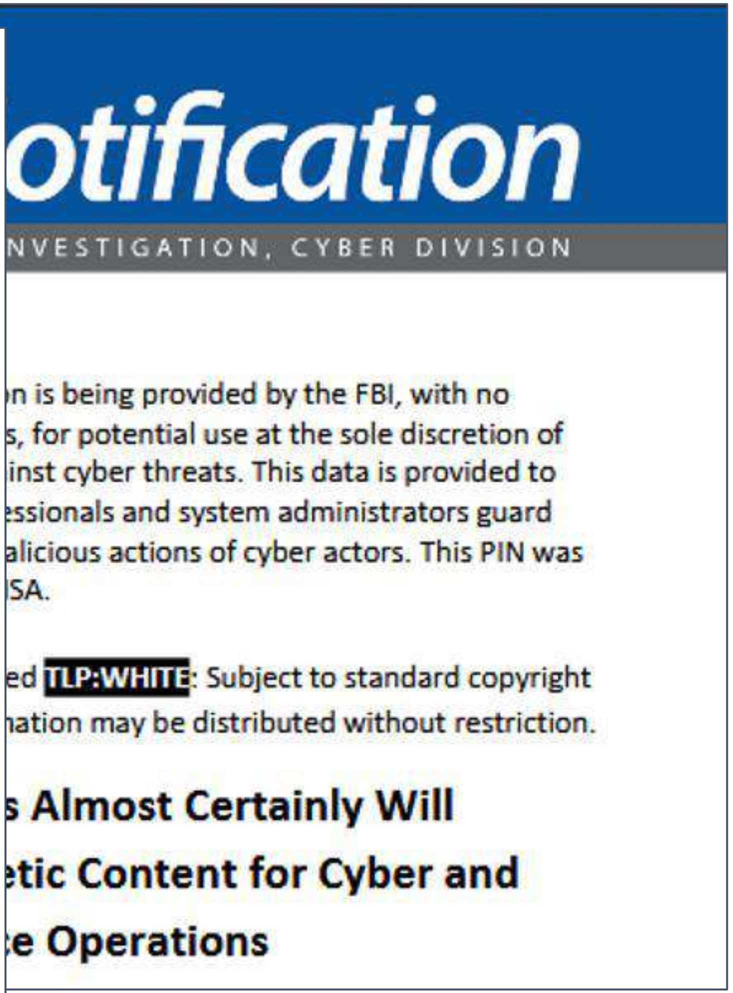


Microsoft's VALL-E Generates Speech From Just 3 Seconds of Audio

But it could lead to a proliferation of deepfake voices

Ben Wodecki
January 11, 2023

2 Min Read



otification
NVESTIGATION, CYBER DIVISION

n is being provided by the FBI, with no
s, for potential use at the sole discretion of
inst cyber threats. This data is provided to
essionals and system administrators guard
alicious actions of cyber actors. This PIN was
SA.

ed TLP:WHITE: Subject to standard copyright
nation may be distributed without restriction.

s Almost Certainly Will
etic Content for Cyber and
e Operations

Cybercrime is a threat to fundamental rights

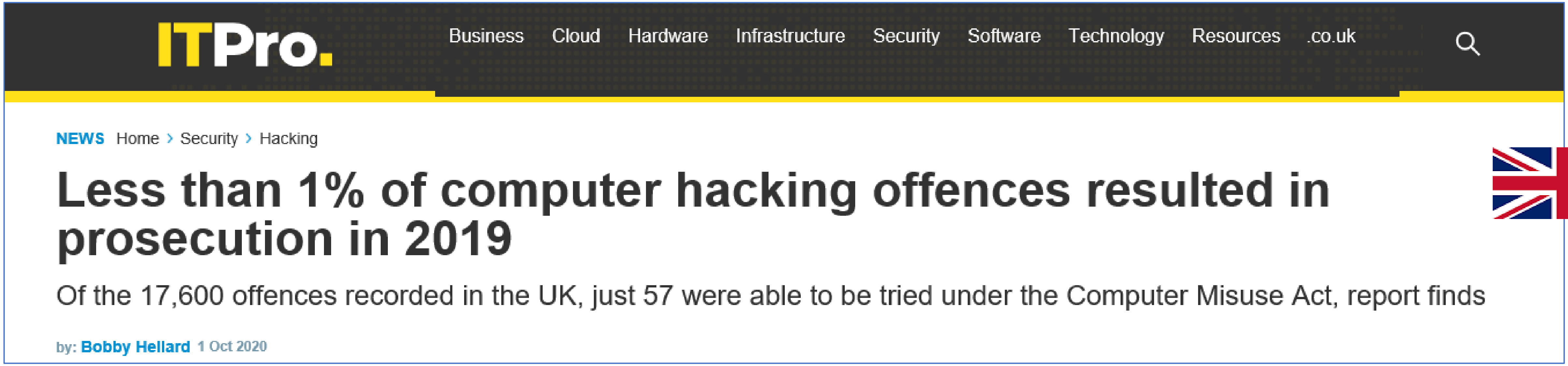
- Affects the **right to private life** of hundreds of millions of individuals whose personal data are stolen
- Can be an **attack against the dignity and the integrity of individuals**, in particular sexual exploitation and abuse of children
- Is a **threat to the freedom of expression** when attacks 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

Agenda

- The cybercrime global landscape
- **Criminal justice international cooperation – The Budapest Convention**
- The way ahead

The enforcement gap



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

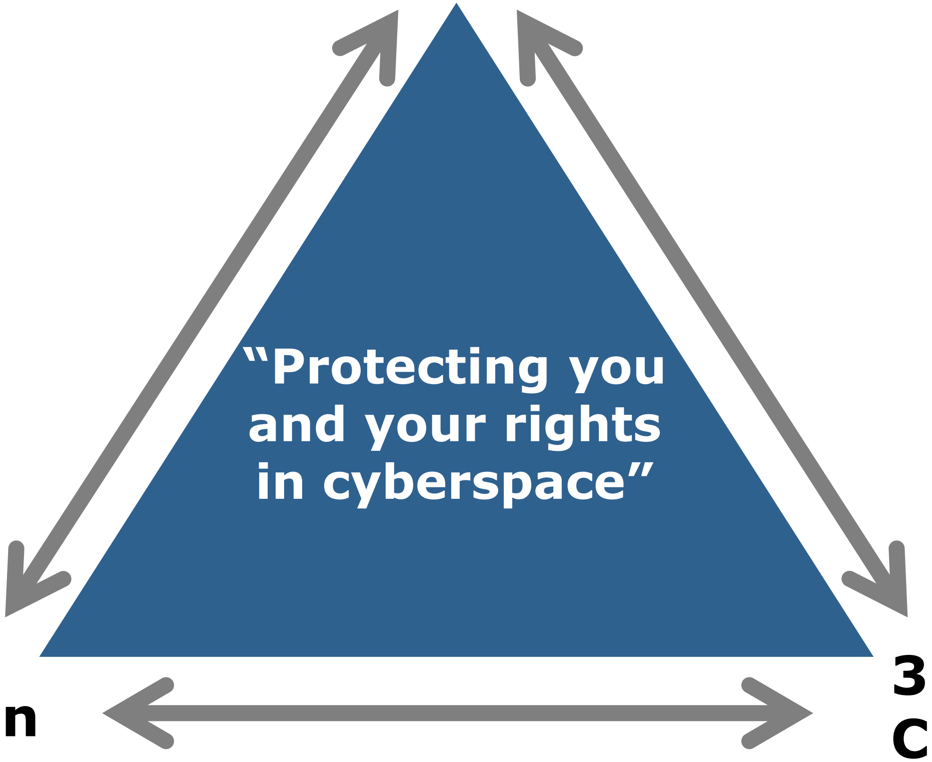
- **Scale and quantity** of criminal conducts online, data, devices, users and victims
- **Under-reporting** and the <1% problem
- **Heterogeneous legal frameworks**, international standards
- Identification, collection and use of **electronic evidence and admissibility issues**
- **Direct collaboration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

Challenges for criminal justice authorities – cont’d

- **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)

The Council of Europe approach

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



“Protecting you and your rights in cyberspace”

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**
- **Additional Protocol on Xenophobia and Racism via computer systems (2003)**
- **2nd Additional Protocol on Enhanced Co-operation and Disclosure of electronic evidence (2022)**
- **Followed by Cybercrime Convention Committee (T-CY)** – Guidance Notes, Interpretation, Monitoring
- **Open for accession by any State – 69 Accessions/ Ratifications**
- **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**

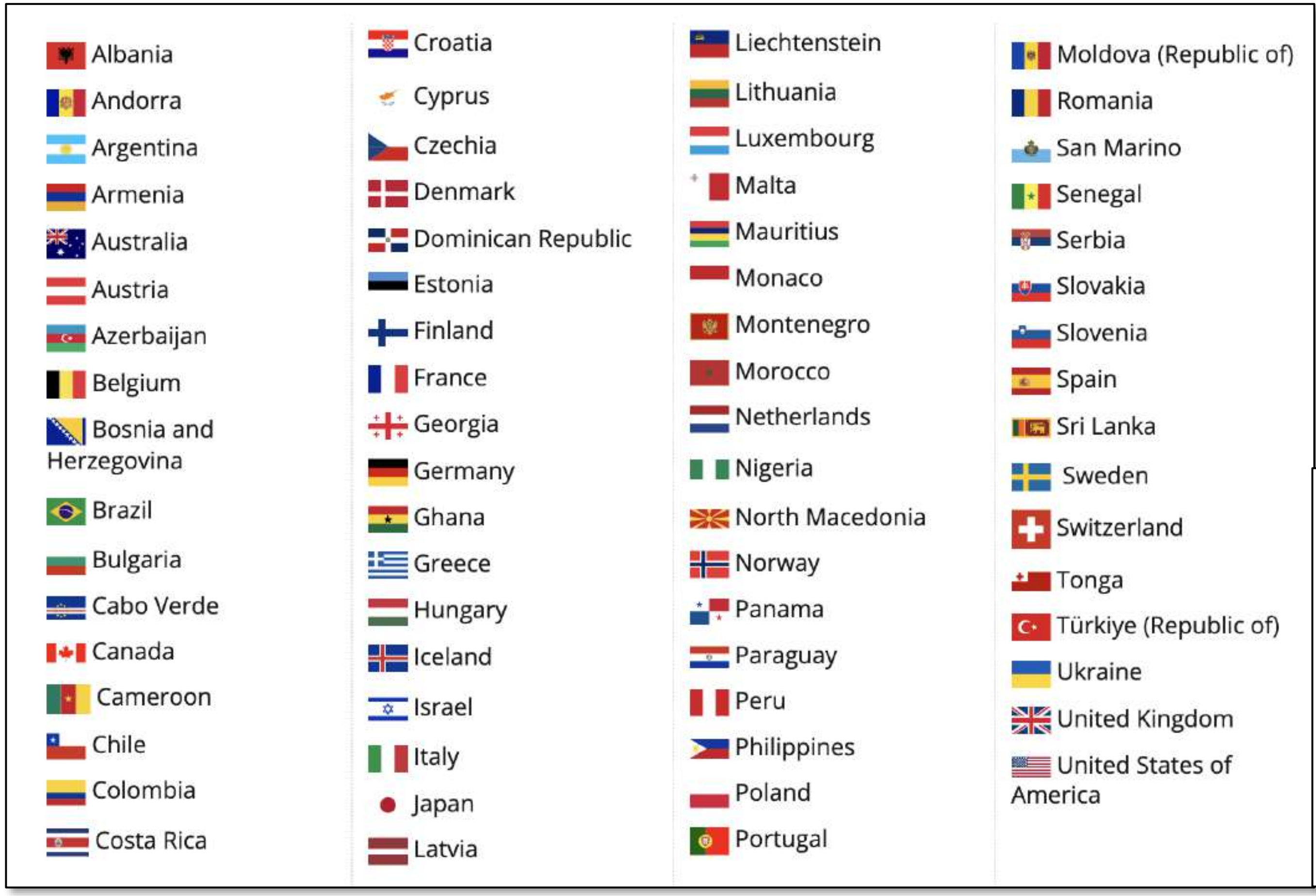
+

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!

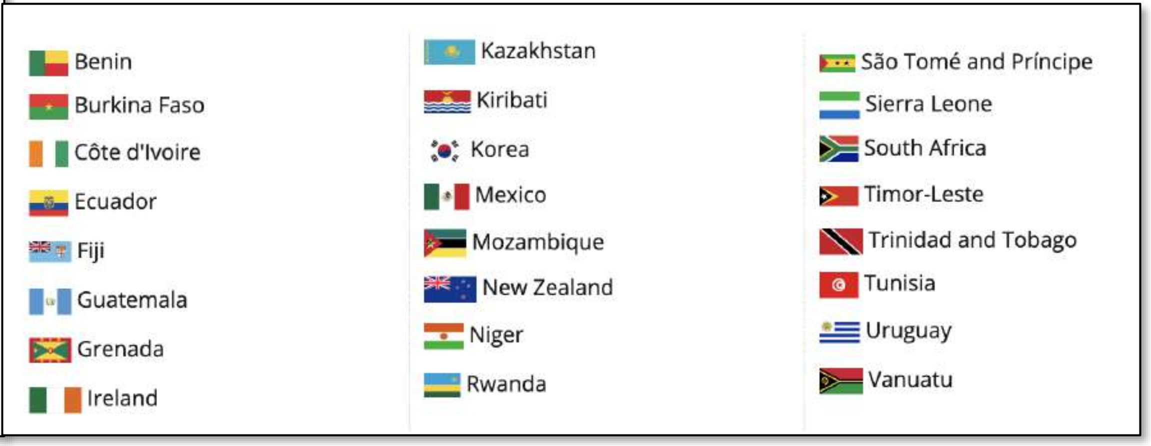
Reach of the Budapest Convention



- Albania
- Andorra
- Argentina
- Armenia
- Australia
- Austria
- Azerbaijan
- Belgium
- Bosnia and Herzegovina
- Brazil
- Bulgaria
- Cabo Verde
- Canada
- Cameroon
- Chile
- Colombia
- Costa Rica
- Croatia
- Cyprus
- Czechia
- Denmark
- Dominican Republic
- Estonia
- Finland
- France
- Georgia
- Germany
- Ghana
- Greece
- Hungary
- Iceland
- Israel
- Italy
- Japan
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Malta
- Mauritius
- Monaco
- Montenegro
- Morocco
- Netherlands
- Nigeria
- North Macedonia
- Norway
- Panama
- Paraguay
- Peru
- Philippines
- Poland
- Portugal
- Moldova (Republic of)
- Romania
- San Marino
- Senegal
- Serbia
- Slovakia
- Slovenia
- Spain
- Sri Lanka
- Sweden
- Switzerland
- Tonga
- Türkiye (Republic of)
- Ukraine
- United Kingdom
- United States of America

← 69 Full Parties

↓ 24 Observers
(signatories or Invited to accede)



- Benin
- Burkina Faso
- Côte d'Ivoire
- Ecuador
- Fiji
- Guatemala
- Grenada
- Ireland
- Kazakhstan
- Kiribati
- Korea
- Mexico
- Mozambique
- New Zealand
- Niger
- Rwanda
- São Tomé and Príncipe
- Sierra Leone
- South Africa
- Timor-Leste
- Trinidad and Tobago
- Tunisia
- Uruguay
- Vanuatu

The Budapest Convention by regions

	Party, signatory or invited to accede to Budapest Convention		
	States	**By January 2024**	
All Africa	54	14	26%
All Americas	35	16	46%
All Asia	42	6	14%
All Europe	48	46	96%
All Oceania	14	6	43%
All	**193**	**88**	**46%**

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, withuot 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

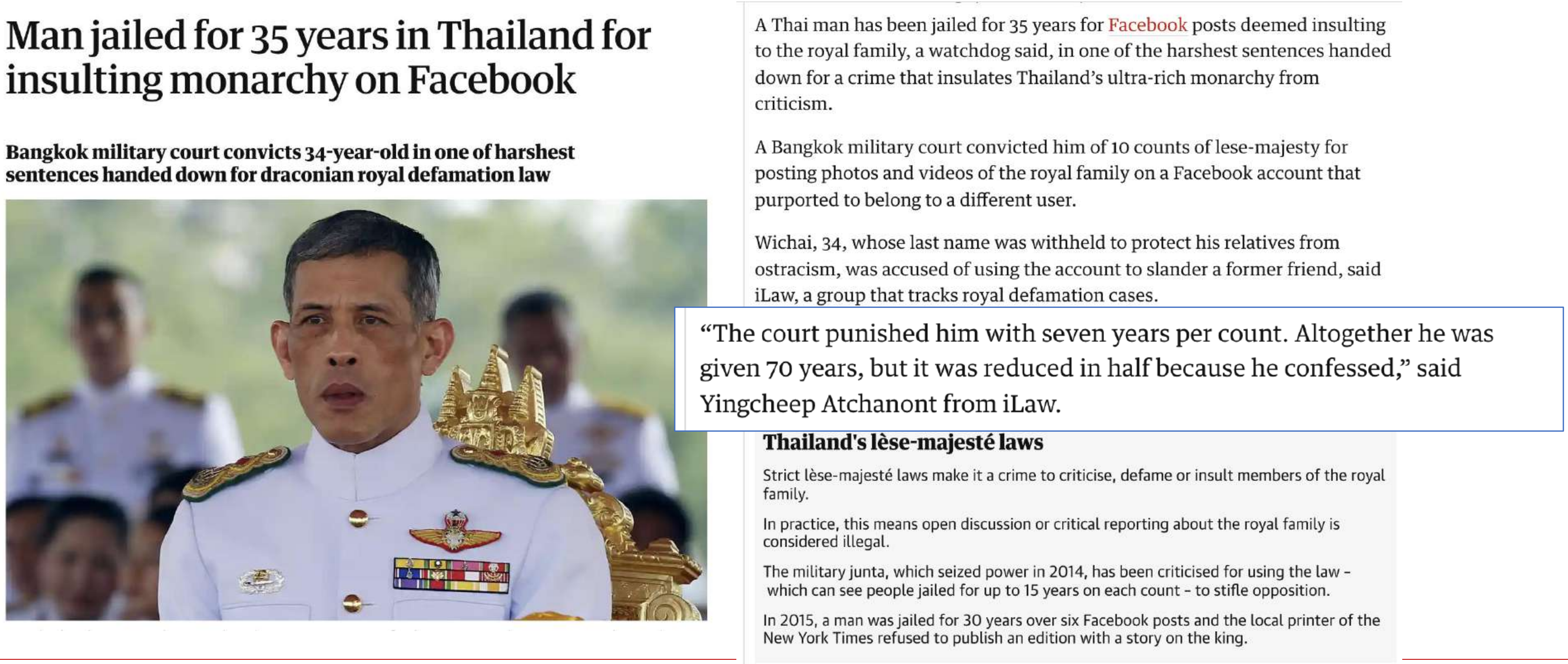
- **Child Pornography** (Art. 9)
  - Intentionally, without right
    - (a) producing child pornography for the purpose of its distribution through a computer system;
    - (b) offering or making available child pornography through a computer system;
    - (c) distributing or transmitting child pornography 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 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.

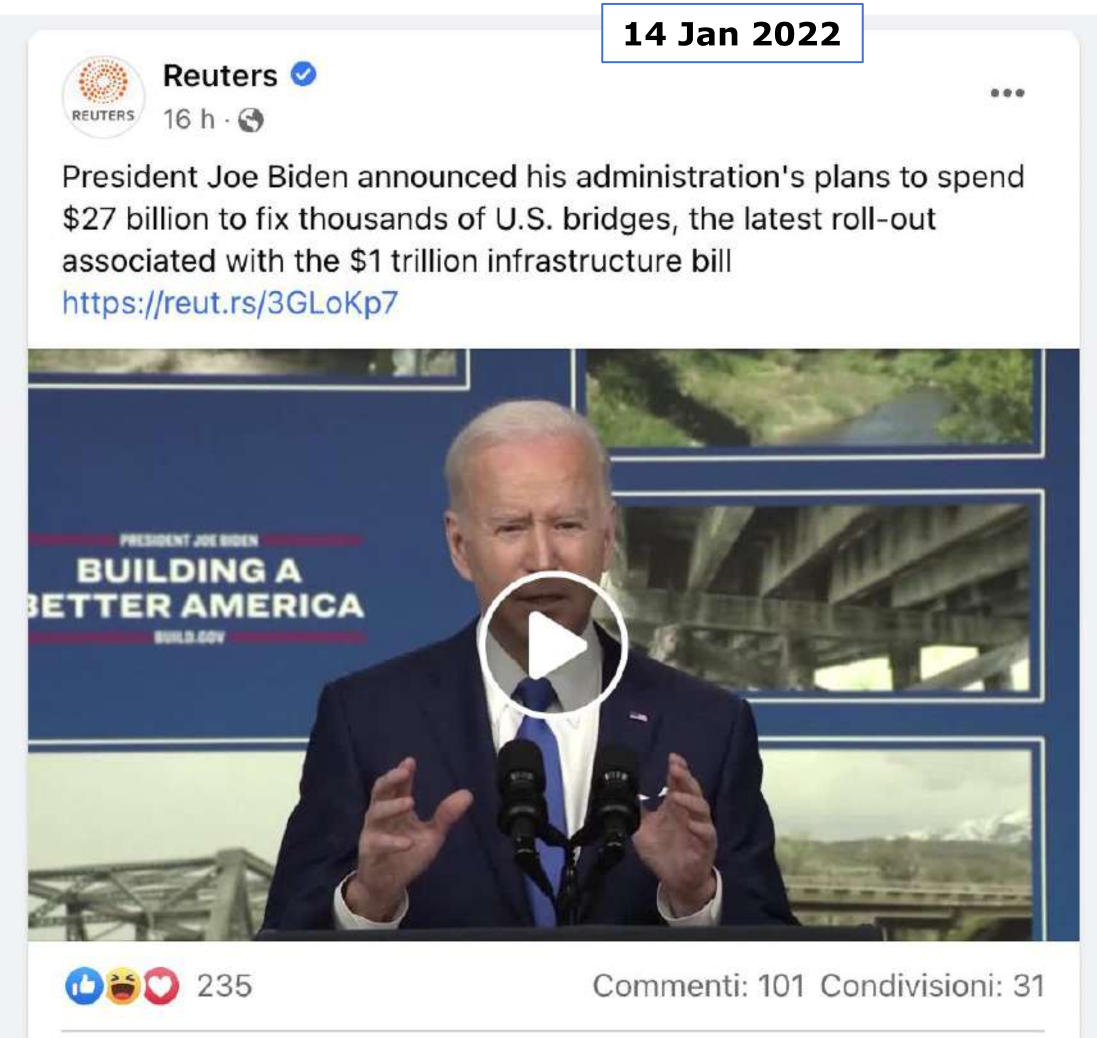
The military junta, which seized power in 2014, has been criticised for using the law – which can see people jailed for up to 15 years on each count – to stifle opposition.

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.

https://www.theguardian.com/world/2017/jun/09/man-jailed-for-35-years-in-thailand-for-insulting-monarchy-on-facebook

Online defamation in USA

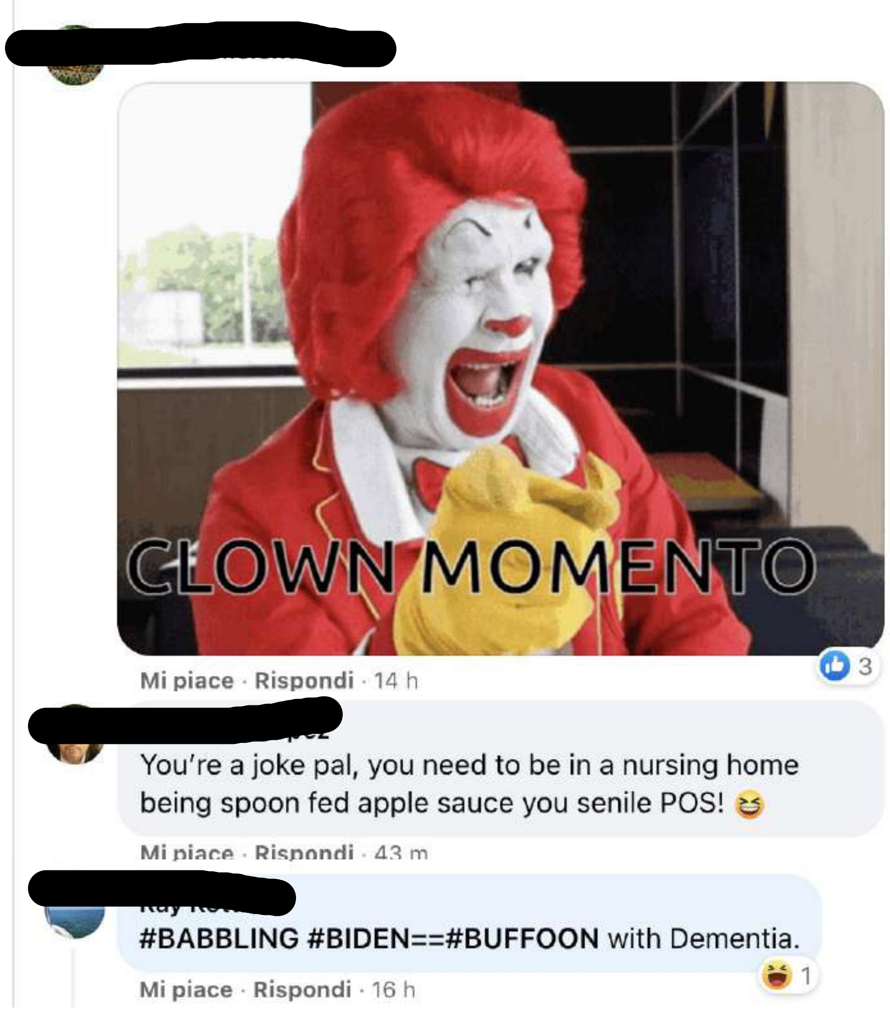
14 Jan 2022



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

https://www.facebook.com/watch?ref=search&v=338616928135242&external_log_id=3a2d5f51-8fcf-4a6d-a146-f3caaeb1fbbe&q=joe%20biden

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!

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 – 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

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 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**

International cooperation – Art. 29

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

International cooperation – Art. 31

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**

24/7 Network – Art. 35

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

Agenda

- The cybercrime global landscape
- Criminal justice international cooperation – The Budapest Convention
- **The way ahead**

MLA and Evidence in the Cloud

- 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?

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 → May 2021

Adopted: November 2021

Opened for signature: 12 May 2022

2 ratifications – Serbia and Japan

43 signatories

Will enter into force with 5 ratifications

https://www.coe.int/en/web/cybercrime/the-budapest-convention

Explainer (EN)

https://vimeo.com/646021759

Art. 4 – Language

- Requests, orders and accompanying information submitted to a Party shall be in a language acceptable to the requested Party or the Party notified under Article 7, paragraph 5, or be accompanied by a translation into such a language.
- Orders under Article 7 and requests under Article 6, and any accompanying information shall be:
  a. submitted in a language of the other Party in which the service provider or entity accepts them under comparable domestic process;
  b. submitted in another language acceptable to the service provider or entity; or
  c. accompanied by a translation into one of the languages under paragraphs 2.a or 2.b.

Art. 6 – Request for domain name registration information

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, for the purposes of specific criminal investigations or proceedings, **to issue a request to an entity providing domain name registration services in the territory of another Party for information in the entity's possession or control, for identifying or contacting the registrant of a domain name**.

2. Each Party shall adopt such legislative and other measures as may be necessary **to permit an entity in its territory to disclose such information in response to a request** under paragraph 1, subject to reasonable conditions provided by domestic law.

Art. 7 – Disclosure of subscriber information

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue **an order to be submitted directly to a service provider in the territory of another Party, in order to obtain the disclosure of specified, stored subscriber information in that service provider's possession or control**, where the subscriber information is needed for the issuing Party's specific criminal investigations or proceedings.

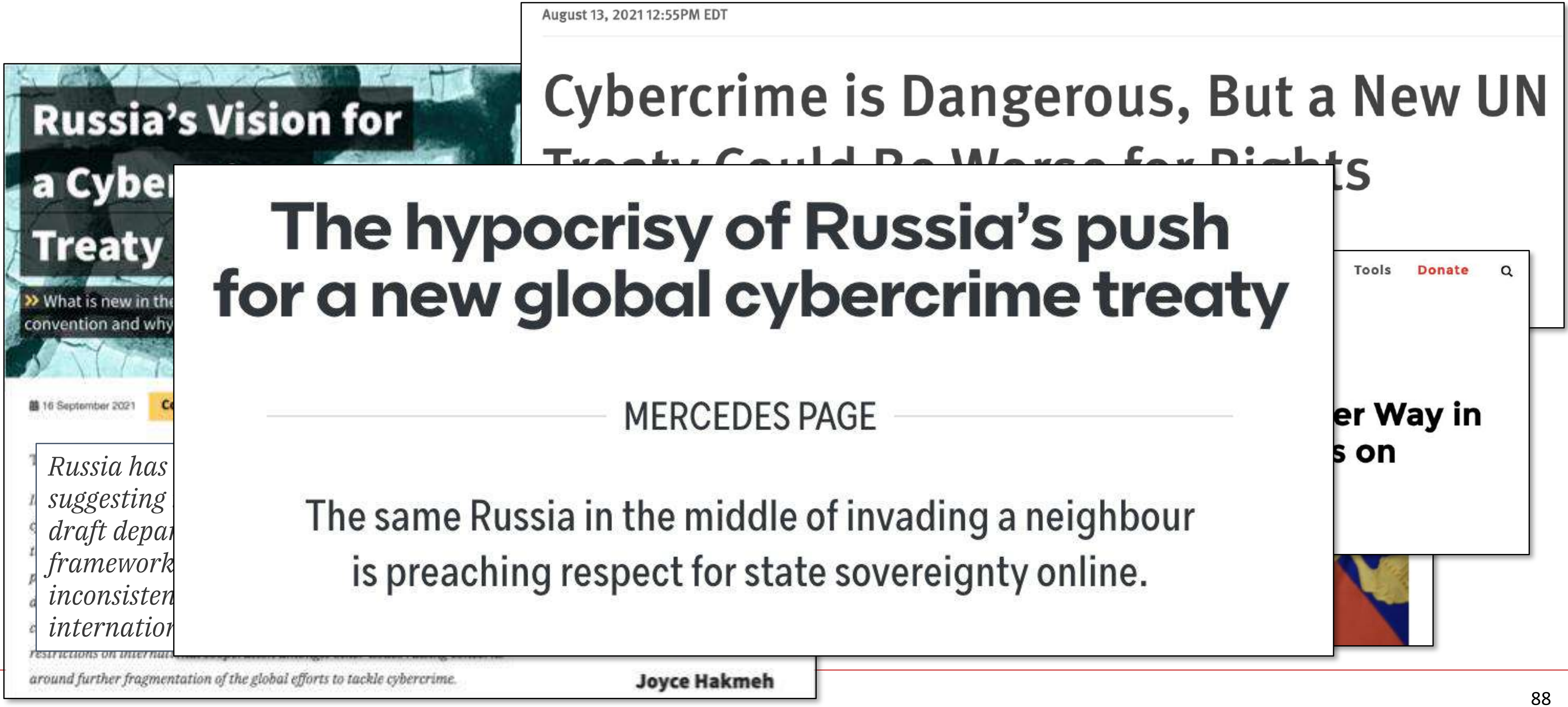
2. a. Each Party shall adopt such legislative and other measures as may be necessary for **a service provider in its territory to disclose subscriber information in response to an order under paragraph 1**.

Art. 14 – Protection of Personal Data

a. «Except as otherwise provided in paragraphs 1.b» (existing binding agreements) «and c» (other arrangements), «each Party shall process the personal data that it receives under this Protocol in accordance with paragraphs 2 to 15 of this article».

2. **Purpose and use**
3. **Quality and integrity**
4. **Sensitive Data**
5. **Retention period**
6. **Automated decisions**
7. **Data security and security incidents**
8. **Maintaining records**
9. **Onward sharing within a Party**
10. **Onward transfer to another State or an international organization**
11. **Transparency and notice**
12. **Access and rectification**
13. **Judicial and non-judicial remedies**
14. **Oversight**
15. **Consultation and suspension**

A new UN Treaty?



August 13, 2021 12:55PM EDT

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

Russia's Vision for a Cyber

Treaty

» What is new in the

convention and why

16 September 2021

Co

Russia has
suggesting
draft depar
framework
inconsisten
internation

restrictions on interna

around further fragmentation of the global efforts to tackle cybercrime.

Joyce Hakmeh

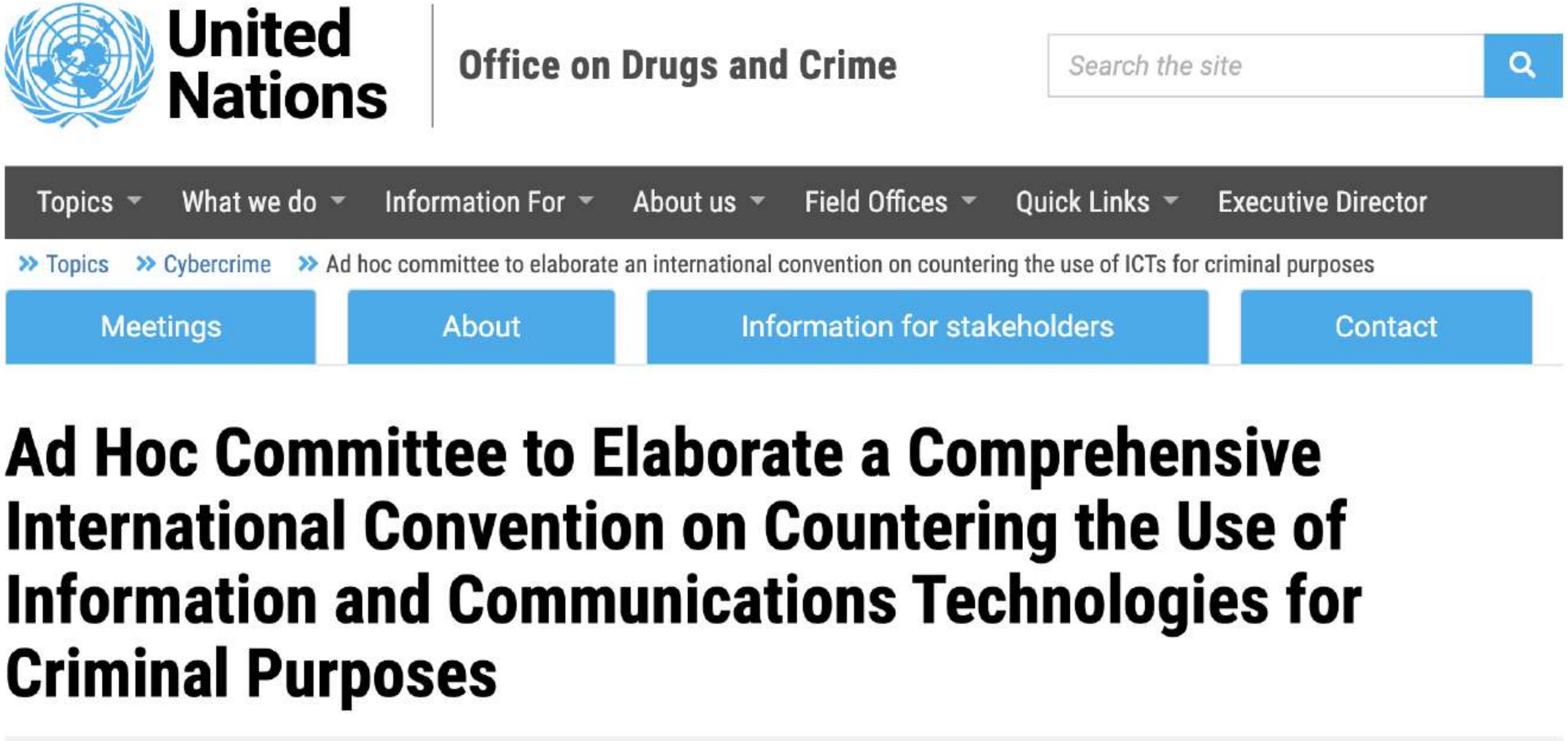
The hypocrisy of Russia's push for a new global cybercrime treaty

MERCEDES PAGE

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

er Way in
s on

The Ad-Hoc Committee


United Nations
Office on Drugs and Crime
Search the site
Topics
What we do
Information For
About us
Field Offices
Quick Links
Executive Director
» Topics » Cybercrime » Ad hoc committee to elaborate an international convention on countering the use of ICTs for criminal purposes
Meetings
About
Information for stakeholders
Contact

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

The Ad-Hoc Committee

- General Purpose of the Ad Hoc Committee is **to elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes**

- To bring together world governments and other relevant stakeholders (primarily non-governmental organizations and private companies) to form a new convention with the purpose of preventing the use of information and communications technologies for the criminal purposes

The Ad-Hoc Committee

- The work of the committee will be concluded once it presents a draft convention to the General Assembly at its seventy-eighth session in **September 2024**.
- The committee is **chaired by** Algeria, with **13 vice chairs**
- The chair can invite, as **observers**, global and regional intergovernmental organisations, representatives of United Nations bodies, and representatives of functional commissions of the Economic and Social Council (ECOSOC)
- The chair and the United Nations Office on Drugs and Crime (UNODC) has drawn up a list of relevant **NGOs, civil society organizations, academic institutions, and the private sector representatives** with expertise in cybercrime, and member states decided on who could participate.

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Sessions

- Organizational session, New York, 10-12 May 2021
- Session on organizational matters, New York, 24 February 2022
- First session, New York, 28 February - 11 March 2022
- Second session, Vienna, 30 May - 10 June 2022
- Third session, New York, 29 August - 9 September 2022
- Fourth session, Vienna, 9-20 January 2023
- Fifth session, Vienna, 11-21 April 2023
- Sixth session, New York, 21 August - 1 September 2023
- Concluding session, New York, 29 January - 9 February 2024 NOT CONCLUDED YET

Chapter I – General Provisions

- **Art. 1 – Statement of purposes**

  a) Promote and strengthen **measures to prevent and combat cybercrime** more efficiently and effectively; [agreed ad referendum]

  b) Promote, facilitate and strengthen **international cooperation** in preventing and combating cybercrime; and [agreed ad referendum]

  c) Promote, facilitate and support **technical assistance and capacity-building to prevent and combat cybercrime**, in particular for the benefit of developing countries.

Chapter I – General Provisions

- **Art. 3 – Scope of applications (TBA)**
  - This Convention shall apply, except as otherwise stated herein, to:

  a) The prevention, investigation and prosecution of the criminal offences established in accordance with this Convention, including the freezing, seizure, confiscation and return of the proceeds from such offences;

  b) The collecting, obtaining, preserving and sharing of evidence in electronic form for the purpose of criminal investigations or proceedings, as provided for in articles 23 and 35 of this Convention.

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Scope of procedural powers (domestic)

- **Art. 23 – Scope of procedural powers**

  […]

  b) Except as provided otherwise in this Convention, each State Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

     a) The criminal offences established in accordance with this Convention;

     b) Other criminal offences committed by means of an information and communications technology system; and

     c) The collection of evidence in electronic form of any criminal offence.

  […]

Scope of international cooperation

Article 35. General principles of international cooperation

1. States Parties shall cooperate with each other in accordance with the provisions of this Convention, as well as other applicable international instruments on international cooperation in criminal matters, and domestic laws, for the purpose of:

   a) The investigation, prosecution and judicial proceedings of the criminal offences established in accordance with this Convention, including the freezing, seizure, confiscation and return of the proceeds from such offences;

   b) The collecting, obtaining, preserving and sharing of evidence in electronic form of criminal offences established in accordance with this Convention;

   c) The collecting, obtaining, preserving and sharing of evidence in electronic form of any serious crime, including serious crimes established in accordance with other applicable United Nations conventions and protocols in force at the time of adoption of this Convention.

Chapter I – General provisions

- **Article 4. Protection of sovereignty [agreed ad referendum]**

  1. States Parties shall carry out their obligations under this Convention in a manner consistent with the **principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States**.

  2. Nothing in this Convention shall entitle a State Party to undertake in the territory of another State the **exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State** by its domestic law.

Chapter I – General Provisions

- **Article 5. Respect for human rights (TBA)**

- States Parties shall ensure that the implementation of their obligations under this Convention is consistent with their obligations under international human rights law.

- **Article 24. Conditions and safeguards (TBA)**

1. Each State Party shall ensure that the **establishment, implementation and application of the powers and procedures provided for** in this Chapter are subject to conditions and safeguards provided for under its domestic law, which shall provide for the protection of human rights, in accordance with its obligations under international human rights law, and which shall incorporate the principle of proportionality.

2. In accordance with and pursuant to the domestic law of each State Party, such conditions and safeguards shall, as appropriate in view of the nature of the procedure or powers concerned, **include, inter alia, judicial or other independent review, the right to an effective remedy, grounds justifying application, and limitation of the scope and duration of such power or procedure**.

3. To the extent that it is consistent with the public interest, in particular the proper administration of justice, each State Party shall consider the impact of the powers and procedures in this Chapter upon the rights, responsibilities and legitimate interests of third parties.

Chapter II – Criminalization

- **Article 6. Illegal access**

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law, when committed **intentionally**, the **access to the whole or any part of an information and communications technology system without right**. [agreed ad referendum]

2. A State Party **may require that the offence be committed by infringing security measures**, with the intent of obtaining electronic data or other dishonest or criminal intent or in relation to an information and communications technology system that is connected to another information and communications technology system.

Chapter II – Criminalization/ other articles, in line with the Budapest Convention

7. **Illegal interception**
8. **Interference with electronic data**
9. **Interference with an information and communications technology system [agr. ad r.]**
10. **Misuse of devices**
11. **Information and communications technology system-related forgery**
12. **Information and communications technology system-related theft or fraud**
13. **Offences related to online child sexual abuse or child sexual exploitation material**
18. **Liability of legal persons**
19. **Participation and attempt**

Chapter II – Criminalization/ other articles, in addition to the ones of the Budapest Convention

- **Article 14. Solicitation or grooming for the purpose of committing a sexual offence against a child**
- **Article 15. Non-consensual dissemination of intimate images**
- **Article 16. Laundering of proceeds of crime**
- **Article 17. Offences relating to other international treaties (TBA)**

Chapter III – Jurisdiction

1. Each State Party shall adopt such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when:

   a) **The offence is committed in the territory of that State Party**; or [agreed ad referendum]

   b) The offence is committed on board a vessel that is flying the flag of that State Party or an aircraft that is registered under the laws of that State Party at the time when the offence is committed. [agreed ad ref.]

2. Subject to article 4 of this Convention, **a State Party may also establish its jurisdiction over any such offence when**: [agreed ad referendum]

   a) The offence is committed **against a national of that State Party**; or [agreed ad referendum]

   b) The offence is **committed by a national of that State Party** or a stateless person with habitual residence in its territory; or [agreed ad referendum]

   c) The offence is one of those established in accordance with article 16, paragraph 1 (b) (ii), of this Convention and is committed outside its territory with a view to the commission of an offence established in accordance with article 16, paragraph 1 (a) (i) or (ii) or (b) (i), of this Convention within its territory; or [agreed ad ref.]

   d) The offence is committed **against the State Party**.

- […]

Chapter IV – Procedural measures and law enforcement, in line with BC

- **Article 25. Expedited preservation of stored electronic data**
- **Article 26. Expedited preservation and partial disclosure of traffic data**
- **Article 27. Production order**
- **Article 28. Search and seizure of stored electronic data**
- **Article 29. Real-time collection of traffic data**
- **Article 30. Interception of content data**

Chapter IV – Procedural measures and law enforcement, addition to BC

- **Article 31. Freezing, seizure and confiscation of the proceeds of crime**
- **Article 32. Establishment of criminal record**
- **Article 33. Protection of witnesses**
- **Article 34. Assistance to and protection of victims**

Chapter V – International cooperation

- **Article 36. Protection of personal data**

a) A State Party transferring personal data pursuant to this Convention shall do so in accordance with its domestic law and any obligations the transferring Party may have under applicable international law. **States Parties shall not be required to transfer personal data in accordance with this Convention if the data cannot be provided in compliance with their applicable laws concerning the protection of personal data**;

b) Where the transfer of personal data would not be compliant with paragraph 1, subparagraph (a), of this article, States Parties may seek to impose appropriate conditions, in accordance with such applicable laws, to achieve compliance in order to respond to a request for personal data;

c) States Parties are encouraged to establish bilateral or multilateral arrangements to facilitate the transfer of personal data.

- […]

Chapter V – International cooperation

- **Article 37. Extradition**
- **Article 38. Transfer of sentenced persons**
- **Article 39. Transfer of criminal proceedings**

Chapter V – International cooperation

- **Article 40. General principles and procedures relating to mutual legal assistance**

2. Mutual legal assistance shall be afforded to the fullest extent possible under relevant laws, treaties, agreements and arrangements of the requested State Party with respect to investigations, prosecutions and judicial proceedings in relation to the offences for which a legal person may be held liable in accordance with article 18 of this Convention in the requesting State Party.

3. Mutual legal assistance to be afforded in accordance with this article may be requested for any of the following purposes: (a) Taking **evidence or statements** from persons; (b) Effecting service of judicial documents; (c) **Executing searches and seizures, and freezing**; (d) Searching or similarly accessing, seizing or similarly **securing, and disclosing electronic data stored** by means of an information and communications technology system pursuant to article 44; (e) Collecting **real-time traffic data** pursuant to article 45; (f) **Intercepting content data** pursuant to article 46; (g) Examining objects and sites; (h) **Providing information, evidentiary items, evidence and expert evaluations**; (i) Providing originals or certified copies of relevant documents and records, including government, bank, financial, corporate or business records; (j) **Identifying or tracing proceeds of crime**, property, instrumentalities or other things for evidentiary purposes; (k) Facilitating the voluntary appearance of persons in the requesting State Party; (l) **Recovering proceeds of crime**; (m) **Any other type of assistance that is not contrary to the domestic law of the requested State Party.**

Chapter V – International cooperation, in line with BC

- **Article 41. 24/7 network**
- **Article 42. International cooperation for the purpose of expedited preservation of stored electronic data**
- **Article 43. International cooperation for the purpose of expedited disclosure of preserved traffic data**
- **Article 44. Mutual legal assistance in accessing stored electronic data**
- **Article 45. Mutual legal assistance in the real-time collection of traffic data**
- **Article 46. Mutual legal assistance in the interception of content data**
- **Article 48. Joint investigations**
- **Article 51. Special cooperation**

Ch. V – International cooperation, additions to BC

- **Article 47. Law enforcement cooperation**
- **Article 49. Mechanisms for the recovery of property through international cooperation in confiscation**
- **Article 50. International cooperation for the purposes of confiscation**
- **Article 52. Return and disposal of confiscated proceeds of crime or property**

Chapter VI – Preventive measures

- Preventive measures may include:

(a) Strengthening **cooperation between law enforcement agencies or prosecutors and relevant individuals and entities outside the public sector**;

(b) Promoting **public awareness** regarding the existence, causes and gravity of the threat posed by the offences established in accordance with this Convention

(c) Building and making efforts to **increase the capacity of domestic criminal justice systems, including training and developing expertise** among criminal justice practitioners

(d) Encouraging **service providers to take effective preventive measures**;

(e) Recognizing the contributions of the legitimate activities of **security researchers** when intended solely to strengthen and improve the security of service providers' products, services and customers located within the territory of the State Party;

(f) Developing, facilitating and promoting programmes and activities in order to **discourage those at risk of engaging in cybercrime** from becoming offenders and to develop their skills in a lawful manner; [agreed ad referendum]

Chapter VI – Preventive measures

g) Endeavouring to promote the **reintegration into society of persons convicted** of offences established in accordance with this Convention;

h) Developing **strategies and policies to prevent and eradicate gender-based violence that occurs** through or is amplified by the use of information and communications technologies, taking into consideration the special circumstances and needs of persons in vulnerable situations;

i) Undertaking specific and tailored efforts to **keep children safe online**, including through education and training on and **raising public awareness** of child sexual abuse or child sexual exploitation online;

j) Enhancing the **transparency**

k) Respecting, promoting and protecting the **freedom to seek, receive, [and impart public] information concerning cybercrime**; [agreed ad referendum] (l) Developing or strengthening **support programmes for victims** of the offences established in accordance with this Convention;

l) Preventing and detecting transfers of proceeds of crime and property related to the offences established in accordance with this Convention.

Chapter VII – Technical assistance and information exchange/ Capacity building (Art. 54)

(a) Methods and techniques used in the **prevention, detection, investigation and prosecution of the offences**;

(b) Building capacity in the **development and planning of strategic policies and legislation to prevent and combat cybercrime**;

(c) Building capacity in the **collection, preservation and sharing of evidence, in particular in electronic form**, including the maintenance of the chain of custody and forensic analysis;

(d) **Modern law enforcement equipment** and the use thereof;

(e) **Training of competent authorities in the preparation of requests for mutual legal assistance** and other means of cooperation

(f) **Prevention, detection and monitoring of the movements of proceeds** deriving from the commission of the offences

(g) Appropriate and efficient legal and administrative mechanisms and methods for facilitating the **seizure, confiscation and return of proceeds of offences**;

(h) Methods used in the **protection of victims and witnesses** who cooperate with judicial authorities;

(i) Training in relevant **substantive and procedural law, and law enforcement investigation powers**

Chapter VII – Technical assistance and information exchange

- Article 55. Exchange of information
- Article 56. Implementation of the Convention through economic development and technical assistance

What will happen?

Thank you

Matteo Lucchetti

Direttore Operativo

Cyber 4.0 – National Cyber Security Competence Center

Matteo.Lucchetti@cyber40.it