

**European Conference of Prosecutors
Conférence européenne des procureurs
Conferenza europea dei procuratori**



**PROCURA GENERALE
della Corte di cassazione**



**Presidency of Italy
Council of Europe
November 2021 - May 2022**

**Présidence de l'Italie
Conseil de l'Europe
Novembre 2021 - Mai 2022**

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

**The Ariadne's thread and the need to investigate in real time:
the still current vitality of the Palermo Convention and the role of the Second
Additional Protocol to the Budapest Convention in an emergency situation**



Palermo

THEME III

**FINANCIAL CRIMES IN THE
VIRTUAL ENVIRONMENT – A
PROGRAMME FOR MUTUAL
LEGAL ASSISTANCE**

Friday 6 May 2022

AGENDA/IUSSES

- ✓ the importance to have – as a public prosecutor - **some good ideas** during an investigation

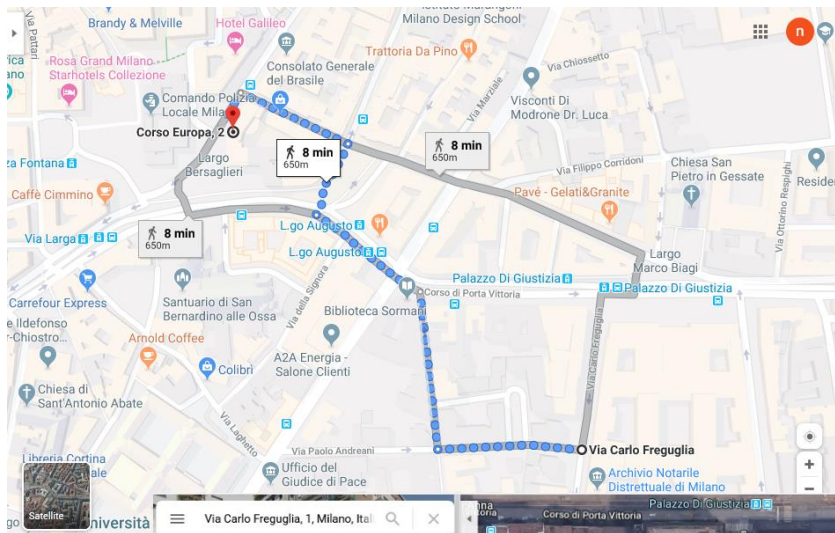
but, at the same time

- ✓ the importance to have **legal tools** as good as our investigative ideas



once upon a time (2004) in Milan, there was a little public prosecutor ...

Google Italy
650 mt



Via Carlo Freguglia, 1, Milano, Italy

20122 Milano MI
Italia

Indicazioni stradali Salva Nelle vicinanze Invia al telefono Condividi

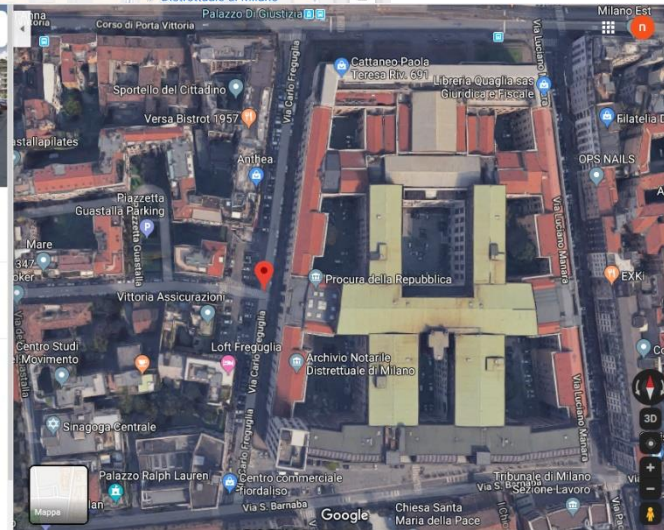
Segnala un problema relativo al seguente luogo: Via Carlo Freguglia

Aggiungi un luogo mancante

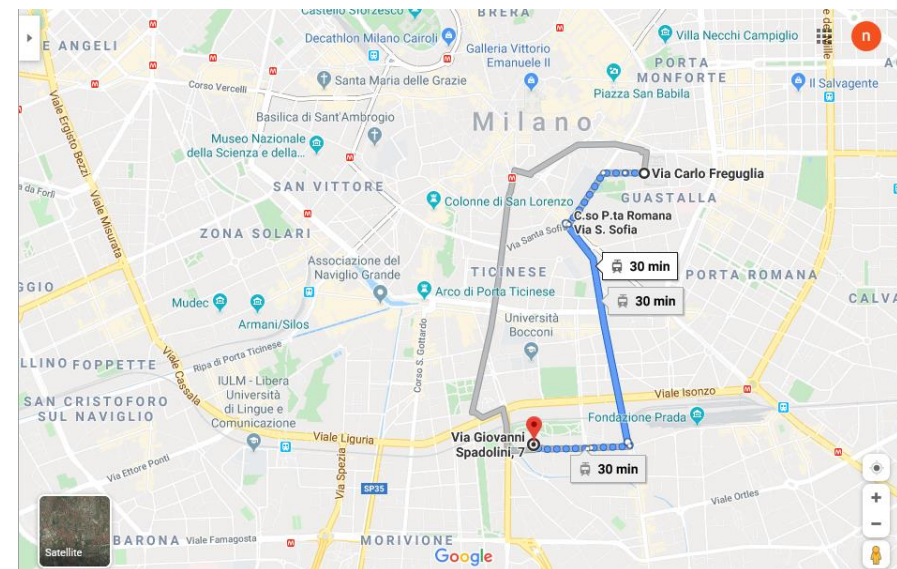
Aggiungi la tua attività

Aggiungi un'etichetta

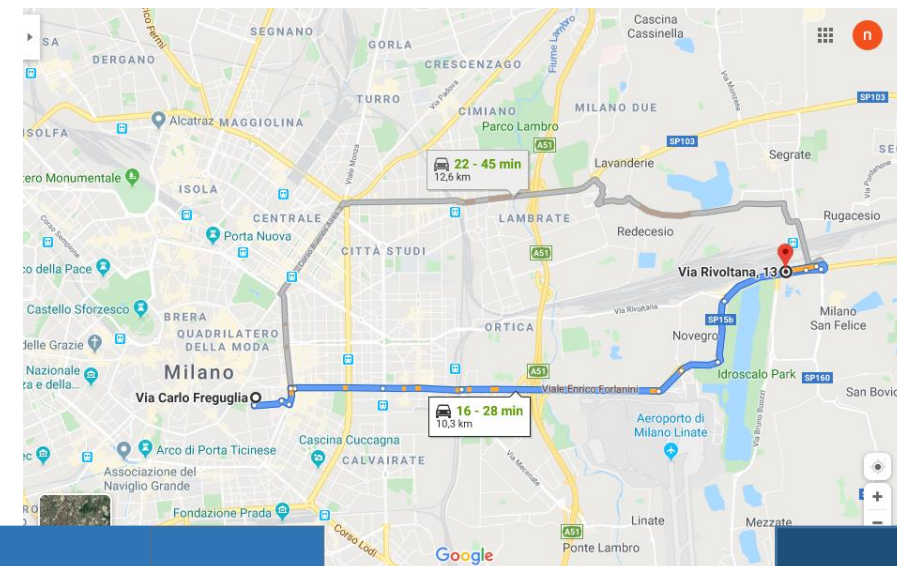
Foto



Yahoo! Italia
2,8 km



Microsoft Italia
10.3 km



2004

2008

2009

2010

2011

2012

2013

2014

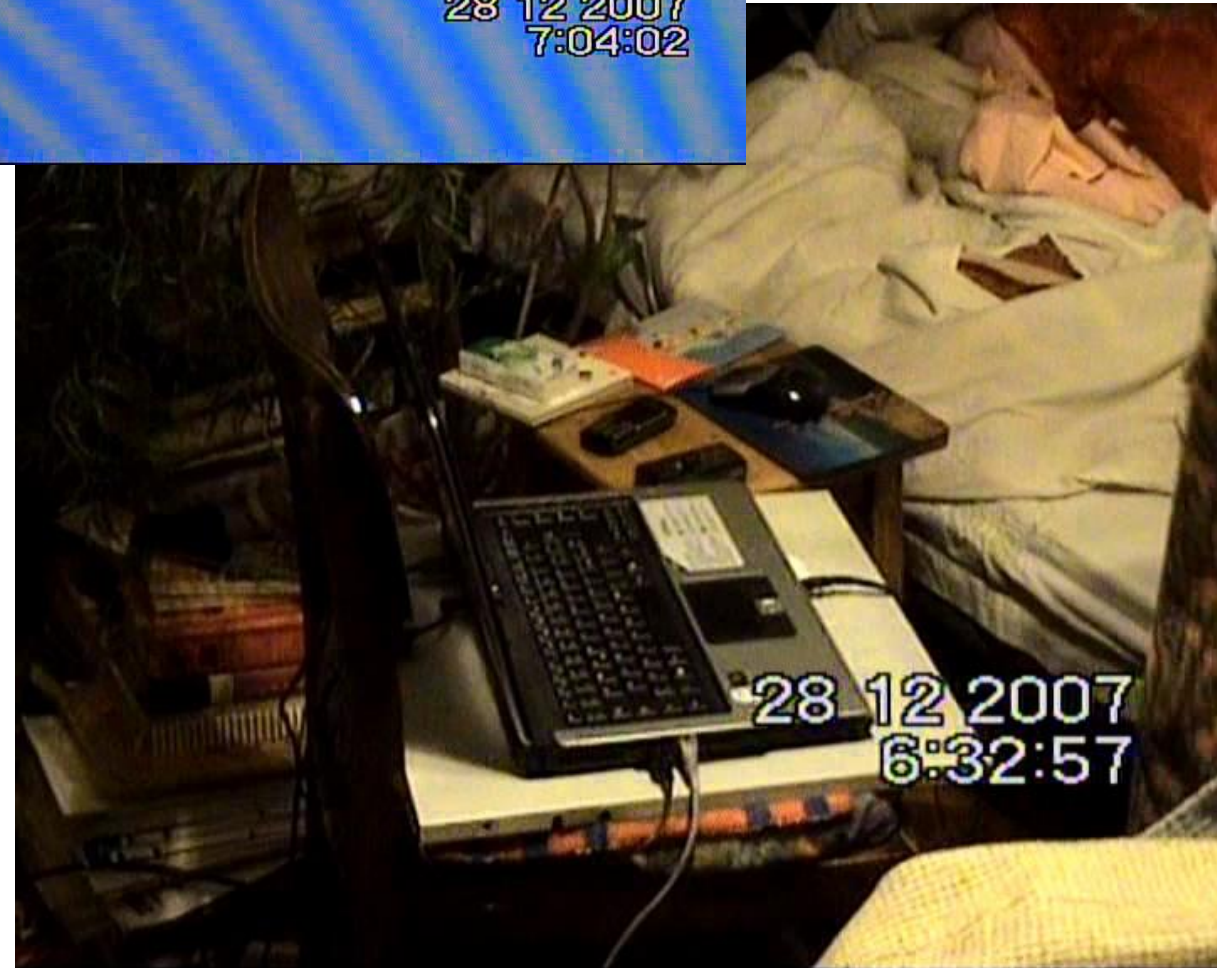
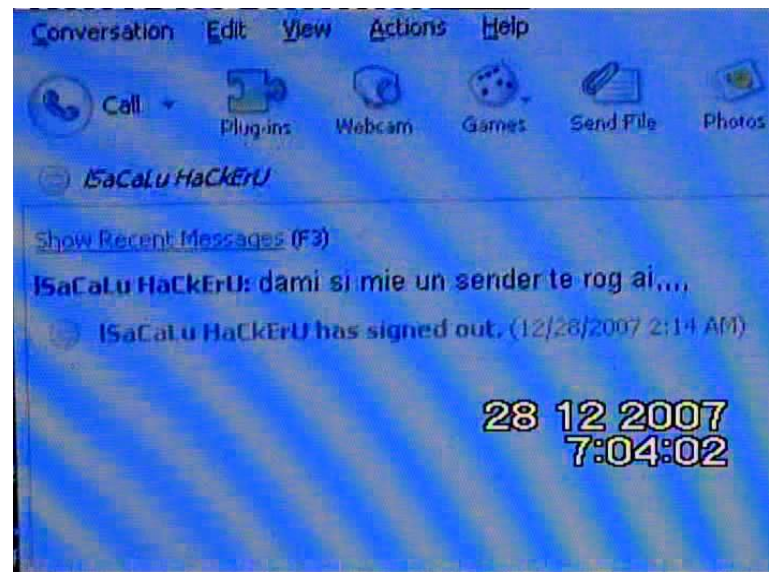
2015

2019



The Italian Job: international phishing gangs in the operation "Phish & Chip"

Digital PhishNet Conference
San Diego, CA
September 30th, 2008





*“We are sorry but the servers are in USA,
so please ask for the interception/for the
requested data with a rogatory!”*



2004

2008 2009 2010 2011 2012 2013 2014 2015

2019

UNITED STATES DISTRICT COURT
for the
Southern District of New York

13 MAG 2814

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address.))

Case No.

The PREMISES known and described as the email account)
[REDACTED]@MSN.COM, which is controlled by Microsoft Corporation)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the WESTERN District of WASHINGTON
(Identify the person or describe the property to be searched and give its location):
The PREMISES known and described as the email account [REDACTED]@MSN.COM, which is controlled by Microsoft Corporation (see attachments).

The person or property to be searched, described above, is believed to conceal (Identify the person or describe the property to be seized):
See attachments.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before December 18, 2013
(not to exceed 14 days)

in the daytime 6:00 a.m. to 10 p.m. at any time in the day or night as I find reasonable cause has been established.





“We are sorry but the servers are in USA, so please ask for the interception with a rogatory!” [2004-2014]

“We are sorry but the servers are in Europe, so please ask for the data with a rogatory!” [2014]



2004

2008

2009

2010

2011

2012

2013

2014

2015

2019



Testimonials



Francesco Cajani

COUNTER TERRORISM DEPARTMENT - PROSECUTOR'S OFFICE AT THE COURT OF LAW IN
MILAN

"When in December 2014 I expressed my willingness to be part of the Council of Europe Cloud Evidence Group, it was ten years since I really felt lost - as an Italian Public Prosecutor dealing with cybercrime - in the intricate maze of the Internet, looking for any trace (and especially the ones that only an Internet Service Provider could disclose to me, even if that ISP is located abroad but with its services offered in my territory) in order to navigate an investigation

Since then the Minotaur has become, day after day, ever bigger and more dangerous, also with the contribution of many companies that - in the same way as Phasiphae - gave him life thanks to the pride of Minos who had preferred to take personal advantage of the gift he had received. But today I trust that the Second Additional Protocol to the Budapest Convention on cybercrime can really represent the Ariadne's thread that we desperately need by now to get out of the labyrinth.

I am sure that each of the Member States of the Council of Europe, after the effort of all these last four years in working together, will be able to take up this new challenge: we owe it to a more peaceful future for our children and, even before that, to the victims of cybercrime who have remained without Justice until today."

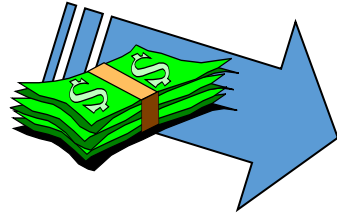
20th anniversary Budapest Convention (coe.int)



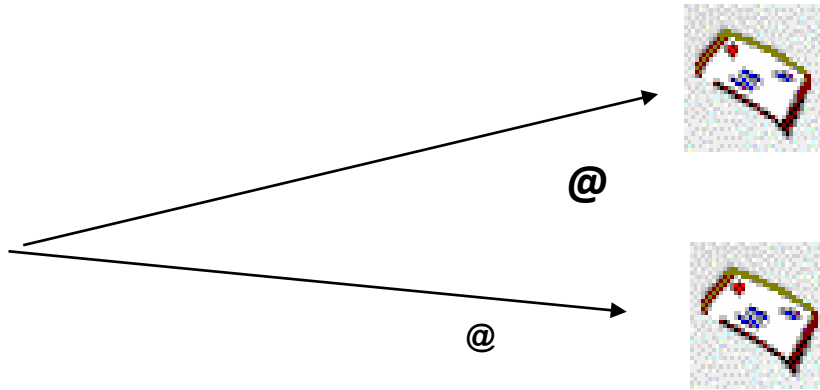
Looking for some good ideas during the investigation: the “*The international seizure warrant*” (2007) and the Phish&Chip operation (2008)



The Italian Job

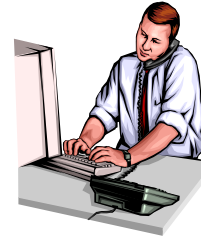


A way to transfer money abroad..



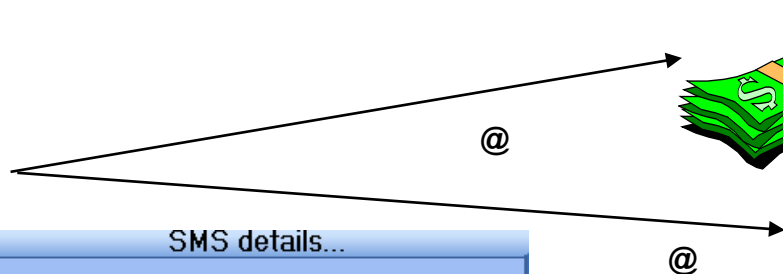
Phishing email

(1st step)



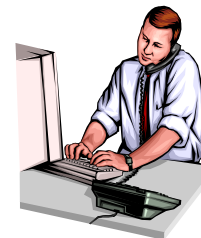
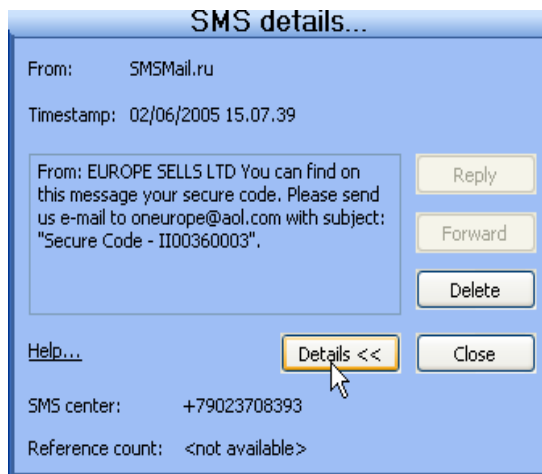
Email offering a work as financial manager

(2nd step)



Online illegal bank transfer [from victim to financial manager]

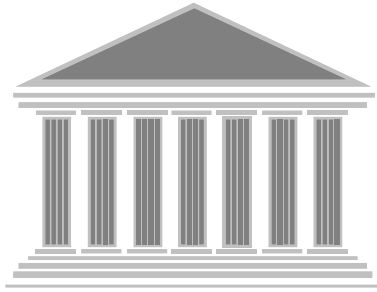
(3rd step)



Operative instructions to the financial manager [“There is money for you!”]

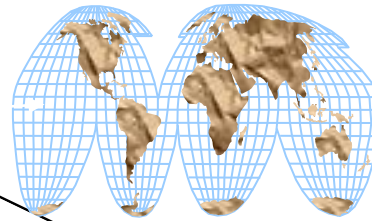
(4th step)





Wester Union money tranfer operation

(5th step)



As soon as we found out this **new criminal method**,
the Italian Judicial Authority has reached an agreement
with the Western Union Inc. in USA

(“The international seizure warrant”)

1. We asked Western Union to delay the suspect money transfers for 48 hours, which was the time needed to verify everything. We gave them some black list (concerning people, imports and destination countries)

2. They called us, in real time, to let us know the MTC code of the suspect transaction.

And every time we get the information required from Western Union

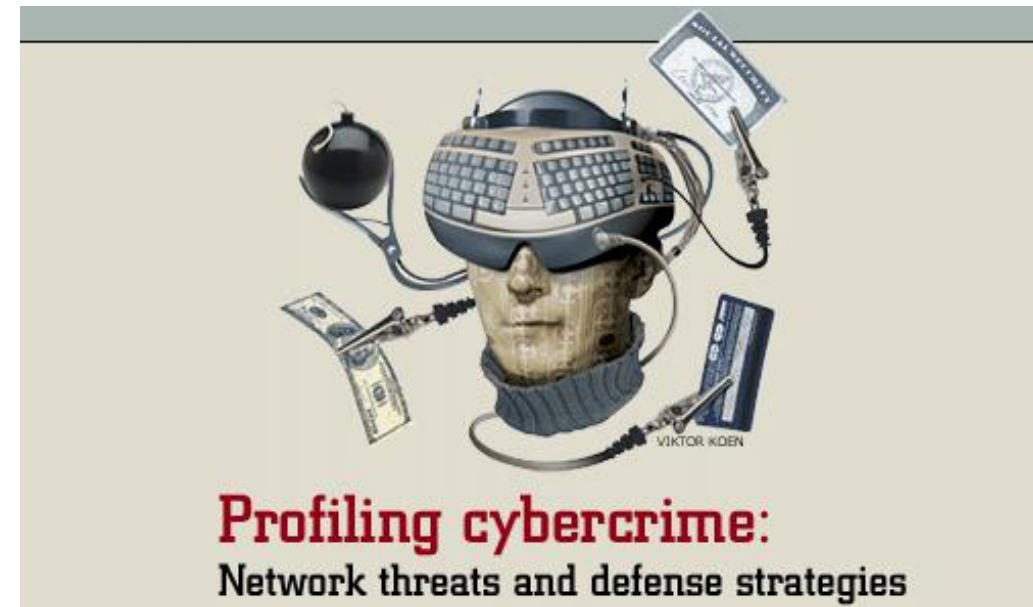
3. We ask the Italian Judge to seizure the suspect transferred money, according to our national Law.





“The international seizure warrant” can be considered a “gentleman’s agreement” rather than issued under **articles 12 and 13 of the Convention of the United Nations against Transnational Organized Crime.**

“The international seizure warrant” = to **seize over 250,000 euros** in two months





Transnational charges

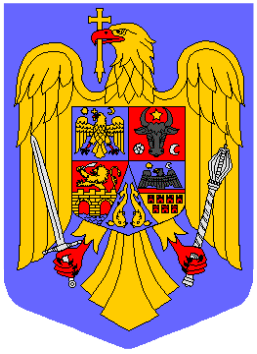
The criminal acts have taken place in Italy but have been planned for an important portion in Romania

The confiscation of assets for the equivalent value product, profit or price of the charge

[Art. 12 of the Convention of the United Nations against transnational organized crime]



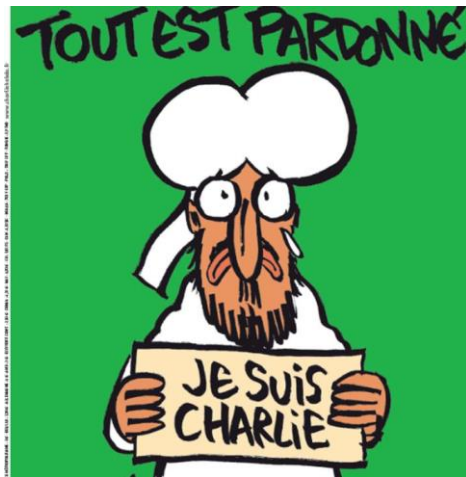
We didn't find any money on suspects' accounts because the criminal organization had spent all the illegal proceeds!





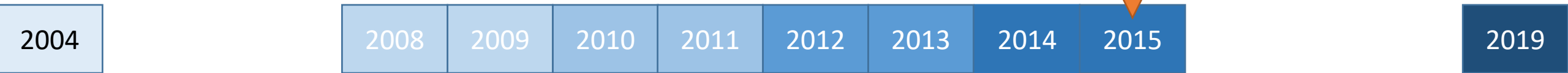
tears in the heart of Europe (2015-2016)





On January 2015 everyone in Europe discovered what we were saying from years and years: **also terrorists and not only hackers or phishers can use a computer to commit a crime and especially terrorists can use WhatsApp and other forms of electronic communication in order to organize an attack.**

That's why, the most important challenge is now related to the instant messaging system. And we still need a clear and agile regime regarding the request of data (**not only related to a computer system but also, according to our topic, related to any financial information**) in an emergency situation!





the emergency co-operation under the 2nd additional protocol (2017-2021)



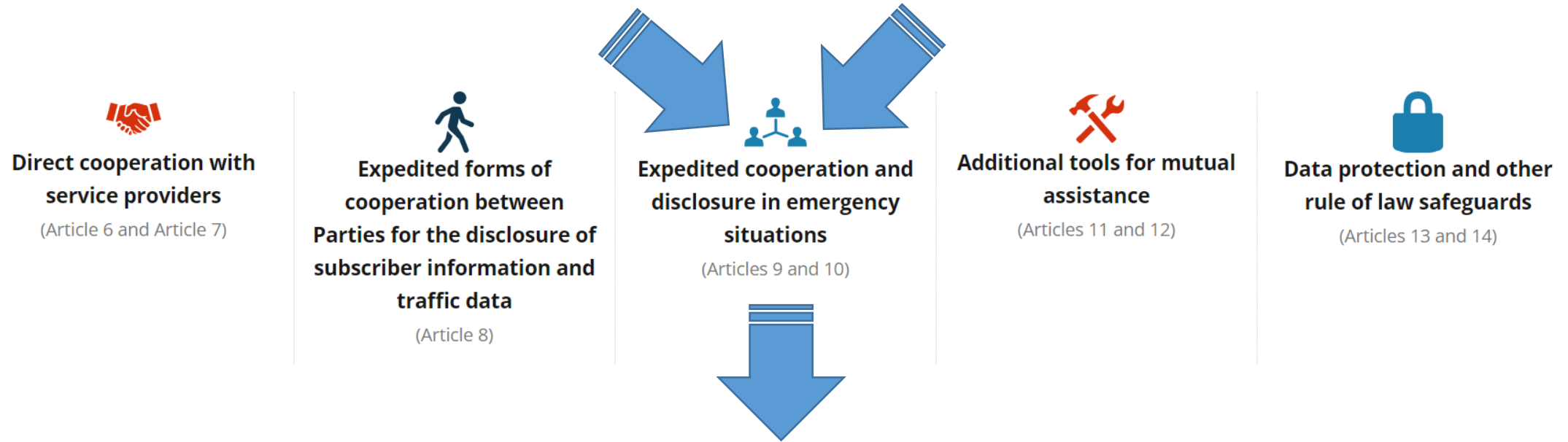


"It was much nicer before people started storing all their personal information in the cloud."

SO... we need a legal global solution!

That's why since September 2017 we've discussed – at the Council of Europe Protocol Drafting Group - a sort of provision in order to have a **clear legal regime regarding the request of data to an ISP in an emergency situation and, first of all, a general regime regarding mutual assistance in an emergency.**

The Protocol will provide for innovative tools to obtain the disclosure of electronic evidence, in particular:



- 1. a clear legal definition of “emergency” (Article 3.2.c), able to refer to many important scenarios;**
- 2. a rapidly expedited procedure for mutual assistance requests made in emergency situations (Article 10);**
- 3. a rapidly expedited procedure to obtain computer data, without an MLA request, using as a channel the 24/7 Network established by Article 35 of the Convention (Article 9).**

Article 3 – Definitions

2 For the purposes of this Protocol, the following additional definitions apply:

c. an “emergency” means a situation in which there is a significant and imminent risk to the life or safety of any natural person

FOR EXAMPLE:

- ❑ **hostage situations** in which there is a credible risk of imminent loss of life, serious injury or other comparable harm to the victim;
- ❑ **threats to the security of critical infrastructure** in which there is a significant and imminent risk to the life or safety of a natural person.



[It is possible to imagine any **illegal requests to receive a ransom in bitcoin** in order to free the hostage or in order to unlock the data of a critical infrastructure]

The innovation of the 2nd additional protocol is the elaboration of two articles that **obligate all Parties to provide, at a minimum, specific channels for rapidly expedited co-operation in emergency situations: Article 9 and Article 10.**



Rapidly expedited procedure for mutual assistance requests (not only related to stored computer data)

Article 9 – Expedited disclosure of stored computer data in an emergency

1 a Each Party shall adopt such legislative and other measures as may be necessary, in an emergency, for its point of contact for the 24/7 Network referenced in Article 35 of the Convention (“point of contact”) to **transmit a request to and receive a request from a point of contact in another Party seeking immediate assistance in obtaining from a service provider in the territory of that Party the expedited disclosure of specified, stored computer data in that service provider’s possession or control, without a request for mutual assistance.**

[...]

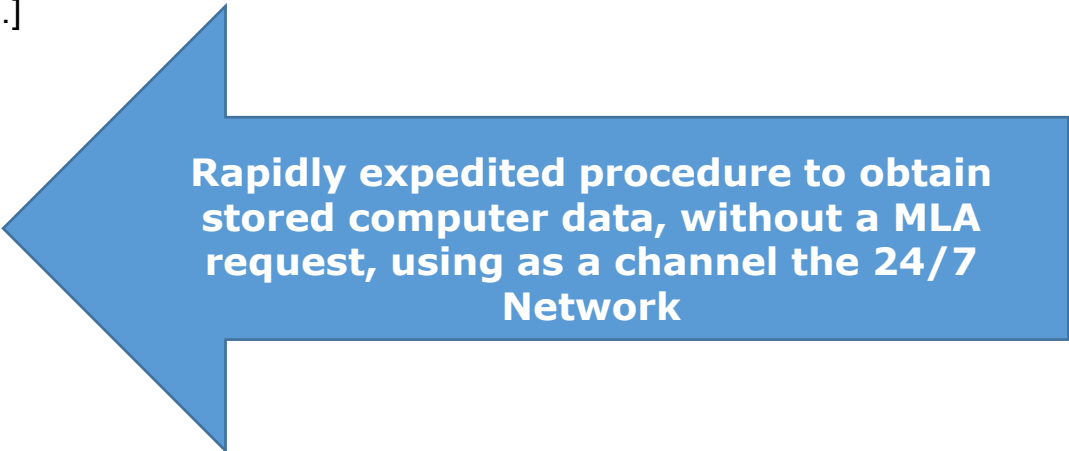
Article 10 – Emergency mutual assistance

1 Each Party may seek **mutual assistance on a rapidly expedited basis where it is of the view that an emergency exists.** A request under this article shall include, in addition to the other contents required, a description of the facts that demonstrate that there is an emergency and how the assistance sought relates to it.

2 A requested Party shall **accept such a request in electronic form.** It may require appropriate levels of security and authentication before accepting the request [...]

5 Each Party shall ensure that a person from its central authority or other authorities responsible for responding to mutual assistance requests is **available on a twenty-four hour, seven-day-a-week basis for the purpose of responding to a request under this article.**

[...]



Rapidly expedited procedure to obtain stored computer data, without a MLA request, using as a channel the 24/7 Network



"I trust that the Second Additional Protocol to the Budapest Convention on cybercrime can really represent the Ariadne's thread that we desperately need by now to get out of the labyrinth.

I am sure that each of the Member States of the Council of Europe, after the effort of all these last four years in working together, will be able to take up this new challenge: we owe it to a more peaceful future for our children and, even before that, to the victims of cybercrime who have remained without Justice until today"

Francesco Cajani

*Deputy Public Prosecutor
High Tech Crime unit and counter terrorism department
Public Prosecutors' Office – Court of Law in Milan
Italy*

francesco.cajani@giustizia.it

