ERA October 2015 Speakers' contribution

Alexandra Jour-Schröder

Alexandra JOUR-SCHRÖDER
German

Since 2011	Head of Unit European Public Prosecutor's Office (EPPO) and Criminal Law European Commission – Directorate General for Justice and Consumers
2007-2011	Head of Unit European Commission - Directorate General Enterprise and Industry
1997-2007	Member of Cabinet of EU Commissioners/Vice-Presidents in charge of Regional Policy, Justice and Home Affairs, Enterprise and Industry
1996-1997	Legal Officer European Commission - Directorate General Competition
1993-1996	German Economics Ministry – European Department
	Law studies at Universities of Münster and Geneva

Recent developments and priorities for EU criminal justice:

The perspective of the European Commission

Alexandra JOUR-SCHROEDER
DG Justice & Consumers

ERA Conference 22-23 October 2015, Trier

1

Political context

- COM Communication (2014) 144 of 11 March 2014 – consolidate, codify, complement
- European Council strategic guidelines for legislative and operational planning within the area of freedom, security and justice of 26/27 June 2014
- Priority 7 of President Juncker's political guidelines of 15 July 2014 & Priority 7 of President Juncker's letter of intent of 9 September 2015

2

Three Areas

- Transposition of EU criminal justice legislation by Member States
- On-going Negotiation of COM proposals
- Possible Initiation of new legal initiatives

3

Transposition - Post Lisbon legal instruments

Procedural measures and rights	Substantive criminal law
Directive 2010/64/EU on interpretation and translation - 27 October 2013	Directive 2011/36/EU on THB – 6 April 2013
Directive 2012/13/EU on the right to information – 2 June 2014	Directive 2011/92/EU on combating the sexual abuse / exploitation of children – 18 December 2013
Victims Directive 2012/29/EU – 16 November 2015	Directive 2013/40/EU on cybercrime – 4 September 2015
Directive 2013/48/EU on the right of access to a lawyer – 27 November 2016	Directive 2014/42/EU on freezing and confiscation of assets 4 October 2015
	Directive 2014/62/EU on counterfeiting – 23 May 2016
	Directive 2014/57/EU on market abuse – 3 July 2016

4

Transposition - Pre Lisbon legal instruments

- Environmental Crime Directives
- The former third pillar *acquis*
  - On-going fact finding exercise on transposition process

5

Negotiation

- **A The procedural rights package**
  - Presumption of Innocence Directive
  - Children's Rights Directive
  - Legal Aid Directive
- **B The protection of the EU's financial interests**
  - PIF Directive
  - EPPO Regulation
  - Eurojust Regulation

6

Presumption of Innocence Directive

COM(2013) 821

- **Aim:** strengthening certain aspects of the presumption of innocence and the right to be present at trial in criminal proceedings
- **Content**:
  - No public references to guilt before conviction
  - Burden of proof and *in dubio pro reo*
  - Right not to incriminate oneself and not to cooperate; right to remain silent
  - Right to be present at one's trial

- **Trilogue phase**
- **Issues:** scope, burden of proof and reversal, right to remain silent.

7

Children's Rights Directive

COM(2013) 822

- **Aim**: enable children to understand and follow proceedings – fair trial – prevent re-offending by children and foster their social integration
- **Content**: information of child and holder of parental responsibility – mandatory access to lawyer – individual assessment and medical examination – questioning – audio visual recording of police interviews – safeguards in case of deprivation of liberty – presence at trial

- **Trilogue phase**
- **Issues**: protection of privacy, continuation of safeguards, scope, extent of mandatory assistance by a lawyer, minor offences

8

Planned new legal criminal law initiatives

- European Agenda on Security COM(2015) 185
- European Agenda on Migration COM(2015) 240

13

European Agenda on Security

Legal criminal law initiatives

- ECRIS-TCN
- Mutual recognition of freezing and confiscation orders
- Revision of the Framework Decision on Terrorism (FD 2008/919/JHA)

14

European Agenda on Security

Some important policy initiatives

- Countering radicalisation
- Cutting the financing of criminals: strengthening cooperation between competent authorities; 4th AML Directive
- Enhancing dialogues with the IT industry: launch an EU forum with major IT companies to counter terrorist propaganda on the internet and in social media
- Enhancing the capacities of Eurojust and Europol

15

European Agenda on Migration

Legal criminal law initiatives

- Possible revision of Council Directive 2002/90/EC and Council Framework Decision 2002/946/JHA to **improve the existing EU legal framework to tackle migrant smuggling,** which defines the offence of facilitation of unauthorized entry and residence, and strengthen the penal framework

16

EPPO Regulation

COM(2013) 534

- **Aim**: strengthening the protection of the Union's financial interests – establish a more coherent, efficient and effective European system for the investigation and prosecution of offences affecting the Union's financial interests
- **Content**: central model with EDPs under direction and supervision of the EPP – exclusive competence - Single Legal Area with partly harmonised investigation measures, procedural rights, judicial control by national Courts

- **Negotiations in Council**
- **Two Interim Reports of EP** (Iacolino of 12 March 2014 and Macovei of 29 April 2015)

11

Eurojust Regulation

COM(2013) 535

- **Aim**: improving Eurojust's performance

- **Content**: reforming the structure and organisation of Eurojust, increasing its democratic legitimacy (NP/EP) and providing for a close cooperation between Eurojust and EPPO and other partners

- **Council GA in March 2015**
- **No report from EP yet**

12

Legal Aid Directive

COM(2013) 824

- **Aim**: ensuring that suspects or accused persons' right of access to a lawyer becomes effective in certain situations
- **Content**:
  - Provisional legal aid
  - Legal aid in EAW proceedings
- **Trilogue phase**
- **Issues:** extension of scope

9

PIF Directive

COM(2012) 363

- **Aim:** reduce differences in national criminal legislation to better fight crimes against the EU's financial interests
- **Content**: common definitions and sanctions of fraudulent behaviour to be criminalised in Member States; liability of public officials and contract agents, time-effectiveness, VAT fraud
- **Trilogue phase**
- **Issues:** VAT inclusion
- Taricco judgment (ECJ) of 8 September 2015

10

European Agenda on Migration

Criminal law policy initiatives

- Strengthen the role of Europol as an intelligence hub for dismantling criminal networks
- Strengthen the role of Eurojust in assisting with investigations to dismantle smuggling and trafficking networks

17

Thank you for your attention!

18

Ola LÖFGREN

Secretary to the *European Judicial Network in Criminal Matters (EJN)* since December 2014

- Head of International Unit at the Office of the Prosecutor General of Sweden (2005-2014).
- EJN National Correspondent and Tool Correspondent for Sweden (2005-2014).
- Chair of the EJN and manager for Eurojust's matters during the Swedish Presidency in 2009.
- Swedish delegate in the Council for the negotiations on the revised Eurojust Decision (2008) and the Eurojust Decision (2001-2002).
- Deputy National Member for Sweden at Eurojust (2002-2005).
- Experience as Public Prosecutor since 1995.

- Master of Law (LL.M.) at the Stockholm University.

- Expert on Swedish law on international cooperation in criminal matters to the Law Commentary KARNOV (2012-2014).
- Expert of the Swedish Commission on extradition and Commission on custody in the asylum process (2009-2011).
- Editor and author of manuals for practitioners on the application of Swedish law on a number of European and international instruments of judicial cooperation.
- Lecturer in trainings for prosecutors on international cooperation in criminal matters.

André Klip

André Klip (1965) is Professor of Criminal Law, Criminal Procedure and the Transnational Aspects of Criminal Law at Maastricht University. He conducted research at the Yale Law School, New Haven and the Max Planck Institute in Freiburg im Breisgau. He is a member of the Board of Directors of the International Association of Penal Law. He is founder and editor of the Annotated Leading Cases of International Criminal Tribunals (42 volumes since 1999). He is currently working on a third edition of European Criminal Law. An integrative Approach (Intersentia Cambridge 2016). Throughout his career, professor Klip has been frequently involved in national and international legal practice. He has been involved in cases before the Court of Justice, the ECHR, the ICTY, the Supreme Court of the Netherlands and in many first and second instance cases. He is a Judge at the 's-Hertogenbosch Court of Appeal (criminal division).

André Klip (1965) is hoogleraar strafrecht, strafprocesrecht en de grensoverschrijdende aspecten van het Strafrecht. Hij deed onderzoek aan de Yale Law School, New Haven en het Max Planck Institute in Freiburg im Breisgau. Hij is lid van de Board of Directors of the International Association of Penal Law. Hij is oprichter en redacteur van de Annotated Leading Cases of International Criminal Tribunals (42 delen sinds 1999). Hij werkt thans aan een derde druk van European Criminal Law. An integrative Approach (Intersentia Cambridge 2016). Door de jaren heen is professor Klip steeds betrokken geweest in de internationale en Nederlandse rechtspraktijk in procedures voor het Hof van Justitie, het EHRM, het Joegoslavië-tribunaal, de HR en vele strafzaken in eerste en tweede aanleg. Hij is raadsheer-plaatsvervanger in gerechtshof 's-Hertogenbosch (strafkamer).

Maastricht University *Leading in Learning!*

Maastricht University *Leading in Learning!*

Mutual Recognition and Directives on Defence Rights

Prof. André Klip

ERA 22 October 2015

Faculty of Law

Maastricht University Leading in Learning!

Mutual influence on areas of the law

- Substantive criminal law
- Criminal procedure
- Cooperation between Member States
- European Union law

Faculty of Law

Maastricht University Leading in Learning!

Merger of internal market and the area of freedom, security and justice

- European integration and criminal law
- An internal market principle: mutual recognition
- Free flow of "criminal products"?
- Can criminal law deal with the principle?

Faculty of Law

Maastricht University Leading in Learning!

European cooperation in criminal matters

- EU-rules in all areas of cooperation
- General application of the principle of Mutual recognition
- Cooperation sets its own priorities

Faculty of Law

Maastricht University Leading in Learning!

What is mutual recognition?

- No definition
- Relationship with the five freedoms
  - Services
  - Workers
  - Goods
  - Capital
  - Residence (Art. 21 TFEU)
- EU-citizen entitled to fundamental freedoms
- Charter of Fundamental Rights

Faculty of Law

Maastricht University Leading in Learning!

Examples of mutual recognition

- Driving licenses
- Regulation 44/2001 on civil judgments
- Ne bis in idem
- European arrest warrant

Faculty of Law

Maastricht University Leading in Learning!

What questions are raised?

- Who recognizes whom?
- What is being recognized?
- What is recognition?
- What is mutual recognition?

Faculty of Law

Maastricht University Leading in Learning!

Absolute recognition?

What discretion do Member States have not to recognise?

- Prevailing obligations
- Obvious shortcomings
- Applicable grounds for refusal (no grounds not in FD => 463/15 PPU
- Irreconcilable decisions

Faculty of Law

Maastricht University Leading in Learning!

Proportionality

- Art. 6 Dir. 2014/41 EIO
  - Necessary and proportionate, taking into account rights of the accused
  - Measure could have been ordered nationally
- General applicability?

Faculty of Law

Maastricht University Leading in Learning!

Division of tasks

- Issuing Member State
  - Grounds/ necessity of EAW
  - Applicability of list offence
- Executing Member State
  - Application of grounds for refusal
  - Double criminality (non list offences)
  - Purpose within the Framework Decision?
  - Assessment of the interests of the requested person

Faculty of Law

Maastricht University Leading in Learning!

Article 82, par. 1 – a closer look

- Judicial cooperation based on mutual recognition
- Approximation
- Measures to:
  - A. ensure recognition
  - B. prevent/settle conflicts of jurisdiction
  - C. support training judiciary
  - D. facilitate cooperation

Faculty of Law

Article 82, par. 2 TFEU

- Minimum rules to facilitate mutual recognition:
  - A. mutual admissibility of evidence
  - B. rights of individuals in criminal procedure
  - C. rights of victims of crime
  - D. any other aspect

Maastricht University Leading in Learning!

Procedural Rights for all criminal proceedings

- Directive 2010/64 on Interpretation and Translation
- Directive 2012/13 on the Right to Information
- Directive 2013/48 on the Right of Access to a Lawyer

Faculty of Law

Maastricht University Leading in Learning!

Directive 2010/64 on Interpretation and Translation

- Implementation 27 October 2013
- Applicable throughout the criminal proceedings
- Translation of "essential documents"
- Case Covaci, C-216/14

Faculty of Law

Maastricht University Leading in Learning!

Directive 2012/13 on the Right to Information

- Implementation 2 June 2014
- Applicable 'from the time persons are made aware that they are a suspect'
- Right to be informed about rights
- Letter of Rights on arrest
- Right of access to materials

Faculty of Law

Maastricht University Leading in Learning!

Directive 2013/48 on the Right of Access to a Lawyer

- Implementation 27 November 2016
- Applicable 'from the time persons are made aware that they are a suspect'
- Independent of arrest
- Before questioned by the police
- Right to access amounts to (3 (3)

Faculty of Law

Maastricht University Leading in Learning!

What if...

- at one police interrogation the accused had no assistance of an interpreter?
- the accused was only informed of his rights after several days of arrest and hours of interrogation?
- the lawyer could be consulted before the first interrogation, but was not allowed to be present?

Faculty of Law

Challenges for the future

- Balance between the internal market and the area of freedom, security and justice
- One single area of European Union law and 30 criminal law jurisdictions
- accused has rights vis-à-vis all MS cooperating in his case, not vis-à-vis one MS only

Ola Löfgren

Annual Conference on EU Criminal Justice 2015
Trier 22 – 23 October

The future of judicial cooperation in criminal matters – is it getting better?

Ola Löfgren
Secretary to the European Judicial Network in Criminal Matters

Judicial cooperation in criminal matters – is it getting better?

- What do we need to do to make it better?

Judicial cooperation in criminal matters – is it getting better?

- EU legal instruments
- Support at national level
- Support at EU level
- Knowledge of international cooperation

Mutual recognition

EU legal instruments

- Based on the need
- Non-fragmented
- Do we need to amend any existing instrument?
- Do we have all instruments that is needed?

EU legal instruments

One instrument is missing:

Transfer of proceedings

EU legal instruments

Implementation in time

Implementation in compliance

EU legal instruments

Is it getting better?

EAW (2002/584/JHA)

Supervision measures (2009/829/JHA)

Procedural rights

- Right to interpretation and translation
- Right to information
- Right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings etc.

Support at national level

- Handbooks
- Intranet

Support at EU level

Eurojust

European Judicial Network - EJN

Support at EU level

EJN or Eurojust?

Joint Paper – EJN/Eurojust

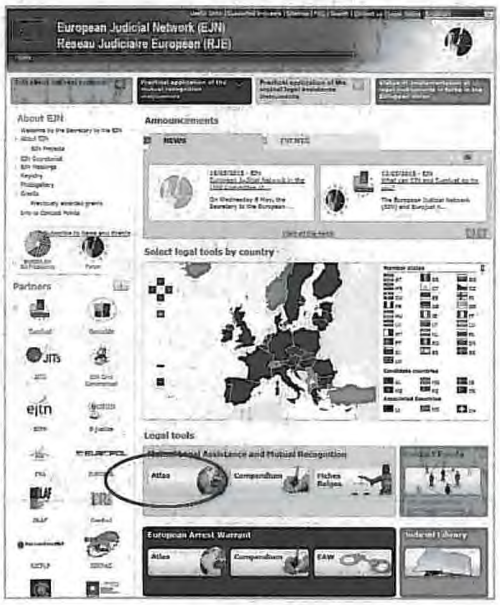
"What can we do for you?"

The EJN Website:

www.ejn-crimjust.europa.eu

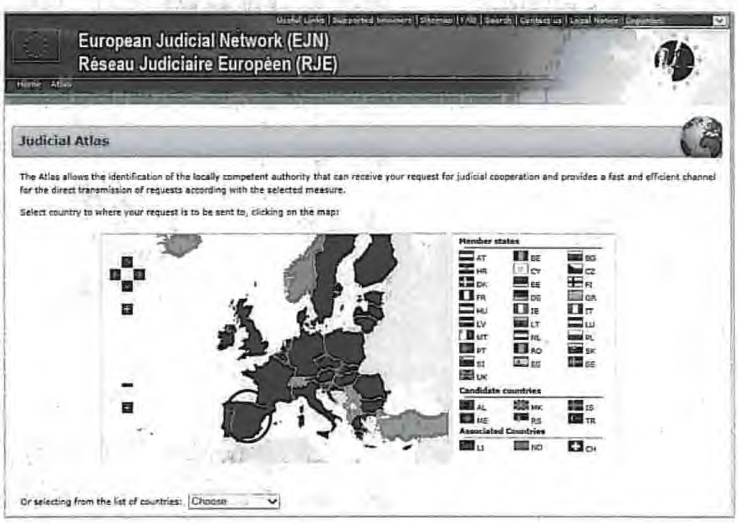
Tools for practitioners

- Judicial Atlas
- Fiches Belges
- Judicial Library
- Compendium
- Info about National Systems
- Contact Points Area



The Judicial Atlas:

Identification of Competent Authorities



The Judicial Atlas:

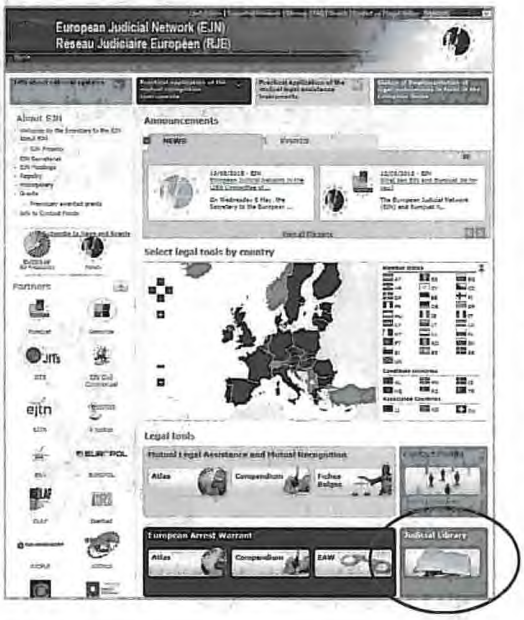
Mutual Recognition Instruments
e.g. European Protection Order (2011/99/EU)

The EJN Website:

www.ejn-crimjust.europa.eu

Tools for practitioners

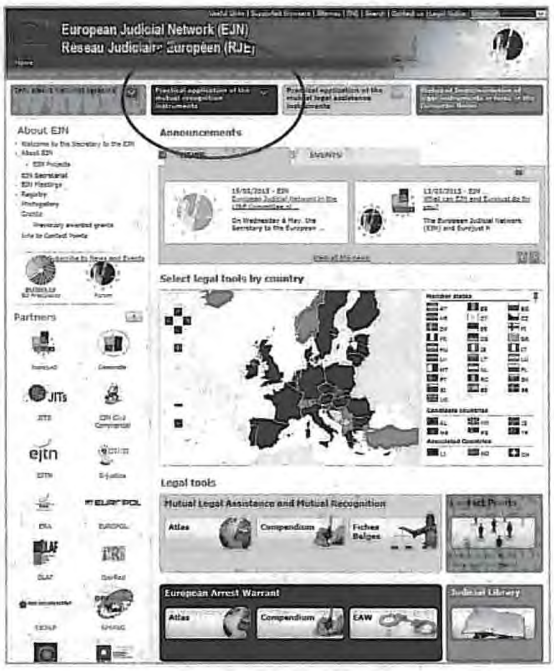
- Judicial Atlas
- Fiches Belges
- Judicial Library
- Compendium
- Info about National Systems
- Contact Points Area

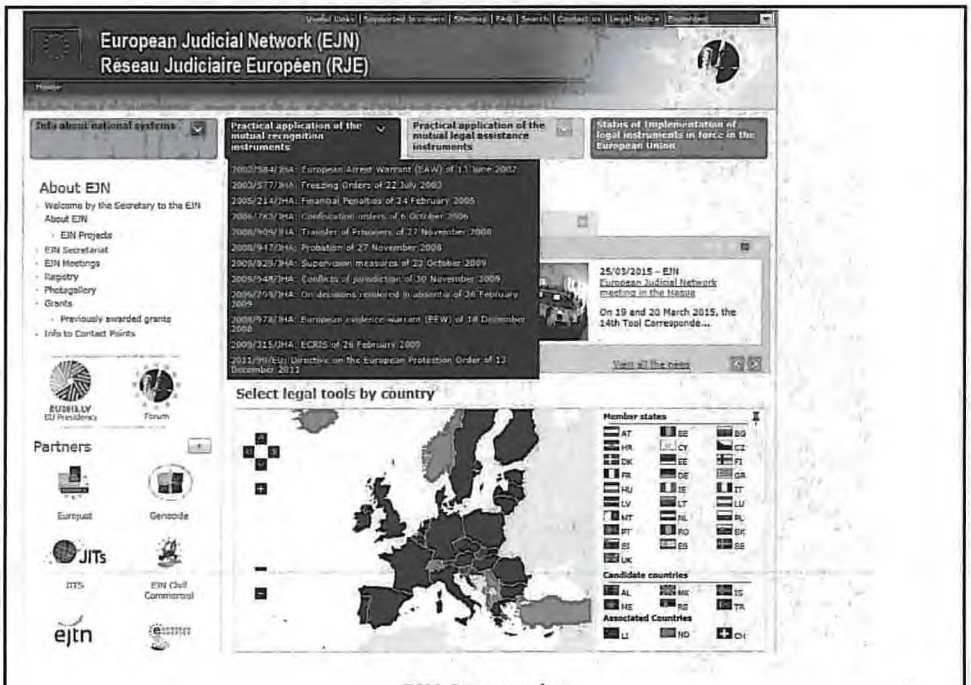


Legal instruments adopted by the European Union
Legal instruments adopted by the Council of Europe
Legal instruments adopted by the United Nations

2008/909/JHA: Transfer of Prisoners of 27 November 2008

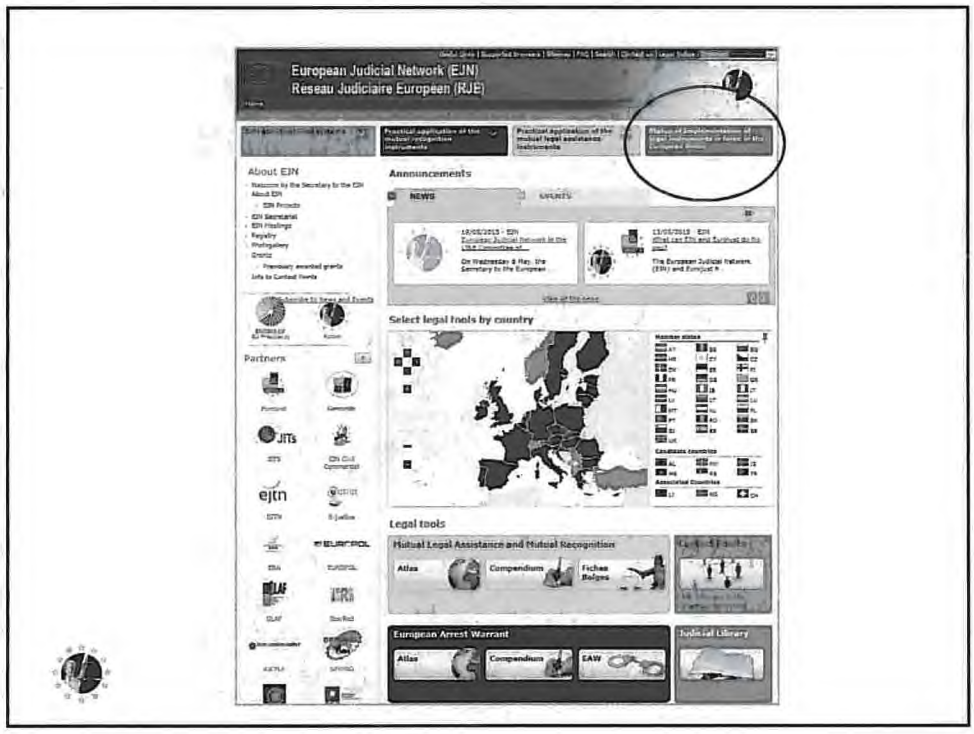
FULL TEXT OF THE LEGAL INSTRUMENT	Full text of the Transfer of Prisoners BG CS DE DK EL EN ES ET FI FR HU IE IT LT LV MT NL PL PT RO SK SL SV
AMENDING ACTS	Council Framework Decision 2009/299/JHA of 26 February 2009 amending Framework Decisions 2002/584/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA and 2008/947/JHA BG CS DE DK EL EN ES ET FI FR HU IE IT LT LV MT PL PT RO SK SL SV
CONSOLIDATED VERSIONS	Full text of the Consolidated version of the Framework Decision 2008/909/JHA on the Transfer of Prisoners BG CS DE DK EL EN ES ET FI FR HU IE IT LT LV MT SL PL PT RO SK SL SV
STATUS OF IMPLEMENTATION	Table of Implementation: 2008/909/JHA, Transfer of prisoners of liberty of 27 November 2008 ▪ EN - Details
TRANSFER OF PRISONERS	**Declarations-countries:** **Ireland** Declarations by Ireland concerning Framework Decision on Transfer of prisoners **Sweden** Declaration by Sweden in accordance with Article 26(4) of the FD on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty





EJN Secretariat

19



Member State	Implementation date	National legislation
Austria	1 Jan 2012	Complementary information provided by the Council Secretariat
Belgium	18 Jun 2012	Complementary information provided by the Council Secretariat. Law of 15 Sept. 2011 concerning the application of the principle of mutual recognition to custodial sentences or measures ordered as a substitute sanction of the kind
Bulgaria	process ongoing	Complementary information provided by the Council Secretariat
Croatia	1 Jul 2013	Act on Judicial Cooperation in Criminal Matters with Member States of the European Union of 18 June 2012 (Official Gazette No 91/11, 81/13, 143/13) / Complementary information provided by the Council Secretariat
Cyprus	23 Mar 2014	Law 87 2014 on the Procedure for the Recognition and Enforcement of Judgments of the Member States of the European Union Imposing Custodial Sentences or Measures Involving Deprivation of Liberty / Complementary information provided by Council Secretariat
Czech Republic	1 Jan 2014	Act No 104/2013 / Complementary information provided by the Council Secretariat
Denmark	1 Dec 2011	Complementary information provided by the Council Secretariat
Estonia	1 Jan 2015	Amendments to the Criminal Procedure Code, mainly in the Chapter 31 / Complementary information provided by the Council Secretariat
Finland	1 Dec 2011	1348/2011 / Complementary information provided by the Council Secretariat
France	1 Aug 2013	Complementary information provided by the Council Secretariat
Germany	✗	Complementary information provided by the Council Secretariat
Greece	✓	Law 4327/15A / Complementary information provided by the Council Secretariat
Hungary	1 Jan 2013	Complementary information provided by the Council Secretariat
Ireland	process ongoing	Transposition measures are included in the Transfer of Sentenced Persons and Transfer of Execution of Sentences Act which is currently being drafted with a view to publication in Autumn 2014 / Complementary information provided by the Council Secretariat
Italy	1 Jan 2011	Legislative Decree No 161 of September 2010, published in the Official Gazette No 250 of 4 October 2010 / Complementary information provided by the Council Secretariat
Latvia	1 Jul 2012	Complementary information provided by the Council Secretariat
Lithuania	1 Apr 2013	Complementary information provided by the Council Secretariat / [illegible]
Luxembourg	9 Dec 2011	Loi du 25 février 2011 relative à la reconnaissance de jugements en matière pénale entre pays membres de l'Union et de certaines mesures alternatives à la détention provisoire et aux peines privatives de liberté / Complementary information provided by the Council Secretariat
Malta	1 Feb 2012	Extended Framework on Mutual Recognition Decisions in Criminal Matters (Implementation of the European Union Framework) L.N. 12 of 2012, Cap. 446, Principal Legislation

The Judicial Library:

Status of Implementation e.g. Transfer of Prisoners (2008/909/JHA)

- Information on 31 Legal Instruments, including Mutual Recognition Instruments
- Newly added Directive on Protection Order

Training and raising awareness

National and EU level

Judicial cooperation in criminal matters – is it getting better?

Yes

...and no

What is needed to make international cooperation better?

- New instruments based on the need
  - Transfer of Proceedings
- Implementation phase
  - Involve practitioners
  - Exchange experiences between MS
- Assessment – is it functioning?
  - Commission (formal)
  - EJN and Eurojust (practical)

What is needed to make international cooperation better?

- Support at national level
  - Handbooks
  - Intranet
- Support at EU level: EJN and Eurojust
  - Continue to develop their respective role
  - Coordination and communication
- At national and EU level
  - Training and raising awareness

Jan Kerkhofs

Jan Kerkhofs – Jan Kerkhofs is a Federal Magistrate at the Federal Prosecutor's Office in Brussels, Belgium, assigned to the Counter-Terrorism Unit and Cybercrime Unit. He treats federal and international terrorism and cybercrime cases on a daily base.
Previously he was a Public Prosecutor in the District of Dendermonde, Belgium, specialized in cybercrime, special investigation methods and serious organized crime and was appointed as leading magistrate in matters of cybercrime for the whole region of East-Flanders.
Before he was a lawyer (barrister) at the bar of Ghent specialized in criminal law and criminal procedure. He holds a Master in Law from the KULeuven, Belgium (1996) and a Diplôme d'Études Approfondies (DEA) en Droit Pénal et Sciences Pénales, from l'Université Panthéon-Assas-Paris II, Paris, France (1997).
He is a member of the Belgian Cybercrime Cell (Belgian National Cybercrime Taskforce) and the Belgian National Platform on Telecommunication. He is assigned as expert of the Belgian delegation in the Convention Committee on Cybercrime (T-CY) of the Council of Europe.
Mr. Kerkhofs a is magistrate-cybercrime-expert for the BCCENTRE (The Belgian Cybercrime Centre of Excellence for Training, Research and Education). He is a trainer at the National Criminal Investigation School of the Belgian Federal Police and is co-responsible for the training in cybercrime of newly appointed magistrates and specialized magistrates at the Belgian Judicial Training Institute (IGO). He also gives training in cybercrime and related matters for several law enforcement agencies, bar associations and international institutions (ERA, Council of Europe, TAIEX, EJTN).
He is a member of the editorial staff of the 'Tijdschrift voor Strafrecht' (Criminal Law Journal) and publishes regularly on the subject of cybercrime.
He is - together with Investigating Judge Philippe Van Linthout - the author of the Belgian cybercrime standard work and field manual "Cybercrime".

ERA

The new terrorism threat: challenges in dealing with foreign fighters using conventional national and EU legal instruments

- The Belgian approach -

ANNUAL CONFERENCE ON EU CRIMINAL JUSTICE 2015
THE IMPACT OF NEW TECHNOLOGIES IN CRIMINAL PROCEEDINGS:
E-EVIDENCE, VIRTUAL CURRENCIES AND SOCIAL NETWORKS
22-23 October 2015
Trier, Germany

Jan Kerkhofs & Ann Fransen (team leader)
Belgian Federal Magistrate, Counter-Terrorism Unit (CTU)
jan.kerkhofs@just.fgov.be

ERA

Program

- The legal framework
  - National
  - European
  - International
- What to prove according to the law – the terrorist offences?
- Belgian approach of Foreign Fighters
  - A global approach
  - Inter-agency cooperation – brothers in arms
- Where do we find evidence, how to collect it and how to use it?

ERA

The legal framework

ERA

National law

- The 19th of December 2003 Act on terrorist offences
  - In Book II of the Belgian Penal Code, "Title I ter" is inserted, comprising articles 137 to 141ter
- The 18th of February 2013 Act amending Book II Title Iter of the Belgian Penal Code (BPC)
  - for instance the insertion of 140 *bis*, *ter*, *quater* and *quinquies* into the BPC
- The 20th of July 2015 Act on strengthening the fight against terrorism
  - Insertion of article 140 *sexies* into the BPC

ERA

The main international law

- **European Convention of 27 January 1977** on the Suppression of Terrorism
- **Protocol of 15 May 2003** amending the European Convention on the Suppression of Terrorism
- **European Convention of 16 May 2005** on the Prevention of Terrorism signed by Belgium, but still not ratified.
- **Council of Europe Convention of 16 May 2005** on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism
- International Convention (United Nations) for the Suppression of terrorist Bombings of 15 December 1997
- International Convention (United Nations) for the Suppression of the financing of terrorism of 9 December 1999

ERA

The circulars

- The circular COL 9/2005 - Circular letter of the Minister of Justice and of the Board of the General Prosecutors about the judicial approach in terrorist matters
- The circular COL 18/2006 - Addendum about the specialised Examining Judges
- The circular COL 2/2007 - Addendum about the Coordination Organ for the Analysis of the Threat (OCAD)
- The circular COL 12/13 - Addendum concerning the 18th of February 2013 Act
- **COL 10/2015 (9 July 2015) – The judicial approach of FTF**

ERA

The terrorist offences

ERA

The terrorist offences
The law of 19 December 2003: Genesis

- Transposition of the **Council of Europe Framework decision of 13 June 2002** on combating terrorism
  Purpose:
  - defining the phenomenon
  - punishing harder
  - defining a terrorist group and penalizing the persons participating in its activities

- Conform Belgian Law to the **International Convention of 9 December 1999** for the Suppression of the financing of terrorism

ERA

The terrorist offences

Principles of the 19th December 2003 Act

- The specific **terrorist offences** (art. 137 and 138 of the Belgian Penal Code)
- The **terrorist group** (articles 139 and 140 of the BPC)
- Individual **financing** of terrorism (art.141 of the BPC)
- The **exclusions** (articles 141*bis* and 141*ter* of the BPC)

ERA

The terrorist offences– Principles

The terrorist offences (articles 137 and 138 of the BPC)

- For an offence to be qualified as terrorist, **3 constitutive elements** have to be present in the case:
  - A material element
  - A moral element
  - A « contextual » element

ERA

The terrorist offences– Principles

The terrorist offences (articles 137 and 138 of the BPC)

The material element

- The offence has to be enumerated in article 137 of the Belgian Penal Code:
  - Either the offence is **already incriminated** (art. 137 §2) (10 kinds of offences)
  - Or the offence is **not yet incriminated** (art. 137 §3) (6 kinds of offences)

ERA

Already incriminated offences (art. 137 §2)

examples:

- voluntary manslaughter
- taking of hostages
- taking of a plane or boat
- massive destructions or degradations
- offences against the Act on the use of explosives

ERA

Not yet incriminated offences (art. 137 §3)

Examples:

- the massive destruction of an infrastructural device putting in danger human lives
- the release of dangerous substances
- the threat to commit a terrorist offence

ERA

The terrorist offences– Principles

The terrorist offences (articles 137 and 138 of the BPC)

The moral element

- The offence has to have been committed with the **intent of**:
  - Seriously **intimidate the population**
  - **Illegally drive** the domestic authorities or an international institution to do or omit to do something
  - Seriously **intent to destabilize or destroy** the fundamental political, constitutional, economic or social structures of a country or an international organization

ERA

The terrorist offences– Principles

The terrorist offences (articles 137 and 138 of the BPC)

The « contextual » element

- It is not enough that an individual is animated by a terrorist intent to incriminate him for a terrorist offence, there has to be present another constitutive element, **the offence** he commits or intents to commit **must by its nature or context « seriously damage a country or an international organization »**
- It is up to the judge to assess

ERA

The terrorist offences– Principles

The terrorist offences (articles 137 and 138 of the BPC)

Punishments

- For offences already incriminated in the Belgian Penal Code (art. 137 § 2 of the BPC):
  The terrorist nature qualifies as an aggravating circumstance. Punishment is more severe
  (art. 138 § of the BPC)
- For offences not yet incriminated in the Belgian Penal Code(art. 137 § 3 of the BPC):
  Specific punishments are imposed
  (art. 138 § 2 of the BPC)

ERA

The terrorist offences– Principles

The terrorist group (art.139 and 140 of the BPC)

- **Article 139** of the BPC defines the **terrorist group** as follows:

« a structured association of more than two persons, durable in time, and acting by mutual agreement with a view to committing terrorist offences in the sense of article 137 of the BPC »

ERA

The terrorist offences– Principles

The terrorist group (art.139 and 140 of the BPC)

Article 140 of the BPC incriminates:

- **Participation** in the group (§1)
  - by supplying information or material resources to a terrorist group
  - or by financing its activities in any way
  - **With knowledge of the fact that such participation will contribute** to the criminal activities of the terrorist group

It is not participation at a terrorist offence, nor at an offence committed by the terrorist group

It is not being member of a terrorist group

It is not sharing the ideas of a terrorist group

It means **"to commit an act allowing or susceptible of allowing the terrorist group to operate"**

- Reclusion of 5 to 10 years and a fine
  (after transfer to a court of summary jurisdiction : Max. = 5 years)

ERA

The terrorist offences – Principles

The terrorist group (art.139 and 140 of the BPC)

Article 140 of the BPC also incriminates:

- **Leadership** of the group (§2)

  not only the supreme leader of the terrorist group
  But every leading role

- Reclusion of 15 to 20 years and a fine
  (after transfer to a court of summary jurisdiction :
  Max. = 15 years)

ERA

The terrorist offences

Genesis of the 18 February 2013 Act

- Transposition of the Council Framework Decision of 28 November 2008
- 3 new incriminations inserted in the BPC
  - **public provocation** to commit a terrorist offence, directly or indirectly, if a danger is caused that one or more such offences may be committed (140bis BPC)
  - **Recruitment** to commit a terrorist offence or to participate in the activities of a terrorist group (140ter BPC)
  - **Training** – active and passive – to commit a terrorist offence (140quater, 140quinquies BPC)

ERA

The terrorist offences

The 20 July 2015 Act

- The new article 140 sexies:

  Will be punished with reclusion from 5 to 10 years en a fine of 100 to 500 EUR:

  1° ***Every person who leaves the national territory*** with the intent to commit, in Belgium or abroad, a terrorist offence as ment in the articles 137, 140 to 140quinquies and 141, ...;

  2° ***Every person who enters the national territory*** with the intent to commit, in Belgium or abroad, a terrorist offence as ment in the articles 137, 140 to 140quinquies en 141, ...;

ERA

The terrorist offences– Principles

The exclusions (art. 141bis and 141ter of the BPC)

The 19 December 2003 Act stipulates **2 exclusions:**

- Article 141*bis*:
  - The activities of the **armed forces in an armed conflict** under the rules of International Humanitarian Law
  - The **activities of armed forces of a State** when exercising their official function under other international law rules
- Article 141ter: No clause can be interpreted as a reduction of fundamental rights or liberties

ERA

IHL vs. Terrorism?

Article 3 of the Convention (III) relative to the Treatment of Prisoners of War - Geneva, 12 August 1949

vs.

Article 141bis BPC

ERA

Article 141bis BPC

*"This title is not applicable on actions commited by **armed forces** during the period of **armed conflicts** as defined in and subject of the international humanitarian law, nor on actions of the **armed forces of a State** in the exercice of their official duties, inasmuch as they are governed by other rules of international law."*

ERA

Convention (III) relative to the Treatment of Prisoners of War - Geneva, 12 August 1949

Article 3. In the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties, each Party to the conflict shall be bound to apply, as a minimum, the following provisions:

(1) Persons taking no active part in the hostilities, including members of armed forces who have laid down their arms and those placed ' hors de combat ' by sickness, wounds, detention, or any other cause, shall in all circumstances be treated humanely, without any adverse distinction founded on race, colour, religion or faith, sex, birth or wealth, or any other similar criteria.

To this end, the following acts are and shall remain prohibited at any time and in any place whatsoever with respect to the above-mentioned persons:

(a) violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture;

(b) taking of hostages;

(c) outrages upon personal dignity, in particular humiliating and degrading treatment;

(d) the passing of sentences and the carrying out of executions without previous judgment pronounced by a regularly constituted court, affording all the judicial guarantees which are recognized as indispensable by civilized peoples.

(2) The wounded and sick shall be collected and cared for.

An impartial humanitarian body, such as the International Committee of the Red Cross, may offer its services to the Parties to the conflict.

The Parties to the conflict should further endeavour to bring into force, by means of special agreements, all or part of the other provisions of the present Convention.

The application of the preceding provisions shall not affect the legal status of the Parties to the conflict.

ERA

Council Framework Decision of 13 June 2002 on combating terrorism

Preambul consideration (11)

Actions by armed forces during periods of armed conflict, which are governed by international humanitarian law within the meaning of these terms under that law, and, inasmuch as they are governed by other rules of international law, actions by the armed forces of a State in the exercise of their official duties are not governed by this Framework Decision,

ERA

How to deal with that?

- Are **IS/JAN/AL-QAEDA** a bunch of terrorists or are they subject of IHL?
- ICTY, *Prosecution v. Tadić*, "Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction", 2 oktober 1995, IT-94-1-AR72, para. 70:

  "On the basis of the foregoing, we find that an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State. International humanitarian law applies from the initiation of such armed conflicts and extends beyond the cessation of hostilities until a general conclusion of peace is reached; or, in the case of internal conflicts, a peaceful settlement is achieved. Until that moment, international humanitarian law continues to apply in the whole territory of the warring States or, in the case of internal conflicts, the whole territory under the control of a party, whether or not actual combat takes place there."

ERA

Rome Statute of the International Criminal Court

Article 8(2)(f):

[For the purpose of this Statute, 'war crimes' means:]

Paragraph 2 (e) applies to armed conflicts not of an international character and thus does not apply to situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence or other acts of a similar nature. ***It applies to armed conflicts that take place in the territory of a State when there is protracted armed conflict between governmental authorities and organized armed groups or between such groups.***

ERA

The proof of the pudding is in the eating

- Court The Hague 01/12/2014:
  Difference between '**armed civilions**' and official organized, recognizable and identifiable armed forces of a state
- Court Brussels 29/07/2015:
  '**Clandestine armed forces**' ("misty") not to be confused with 'armed forces in the sence of IHL
- Sharia4Belgium:
  No organization in the sence of IHL, **no responsable nor identifiable chain of command that can be held responsable for the group**

ERA

Investigative approach set-up & scope

ERA

Exercise of the Public Prosecution

- The non-exclusive competency of the Federal Prosecutor
  But in practice: terrorism is treated on a **federal** level (Act – the circular Col 9/2005)
- The **Counter-Terrorism Unit** of the Belgian Federal Prosecutor's Office (only 8 federal magistrates)
  - Cooperation with the Public Prosecutor's Offices of Brussels, Antwerp, Gent, Liège and Charleroi
  - Weekly and monthly reunions
  - Delegations
- **Specialized investigating judges** (13) competent for the whole Belgian territory

ERA

The judicial approach

The privileged partners

- Federal police (Brussels, Antwerp, Gent, Liège and Charleroi, DGJ/DJP/terro)
- State Security Service
- GISS (General Intelligence and Security Service - Army)
- CUTA (Coordination Unit for Threat Assessment)
- FIU (Financial Intelligence processing Unit)
- The Crisis Centre
- The Board of Intelligence and Security

ERA

Obligation of the Judicial Services and the Intelligence Services to cooperate

- Principle:

  « the intelligence and security services, the law enforcement services and the administrative and judicial authorities see to it, that between them there is a mutual cooperation as efficient as possible » (article 20, §1)
- Consequence: **at any moment contacts are possible, even informal ones**

ERA

Cooperation between the services

- Obligation of cooperation between the Police and the Intelligence Services (IS)
- Formalized extension: **technical assistance**

  « if demanded by the judicial and administrative authorities, the intelligence services may (...) lend support and more specifically their technical assistance to the judicial and administrative authorities » (art. 20, §2)

ERA

Technical assistance in practice

- **The Belgian Federal Public Prosecutor's Office designates automatically the intelligence services as technical assistant**
- The intelligence services (almost) always accept
- The investigating judges can also call in technical assistance

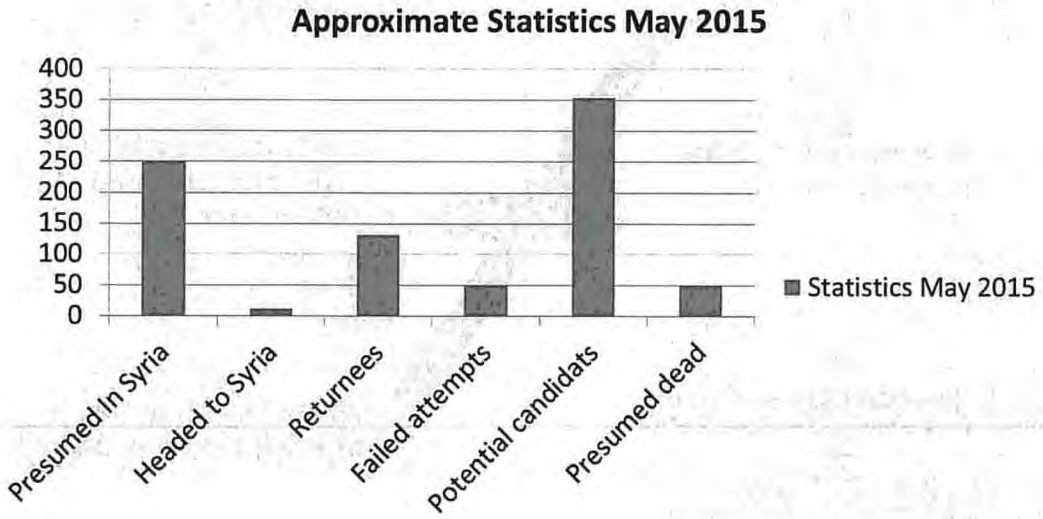
ERA

The judicial approach of foreign fighters - coordination

- Many Belgian foreign fighters
- **List** established by the **CUTA (Coordination Unit for Threat Assessment)** within the framework of the national plan on radicalism – **7 categories**:
  1. Those persons thought to be in Syria
  2. Those thought to be under way to Syria
  3. In Belgium, those thought to have sojourned in Syria
  4. In Belgium, those thought to have tried to reach Syria
  5. In Belgium, candidates for departure / those with risk profiles
  6. Individuals with a statute to be further specified (contradictory or elliptic information)
  7. Recruiters / Financiers

ERA

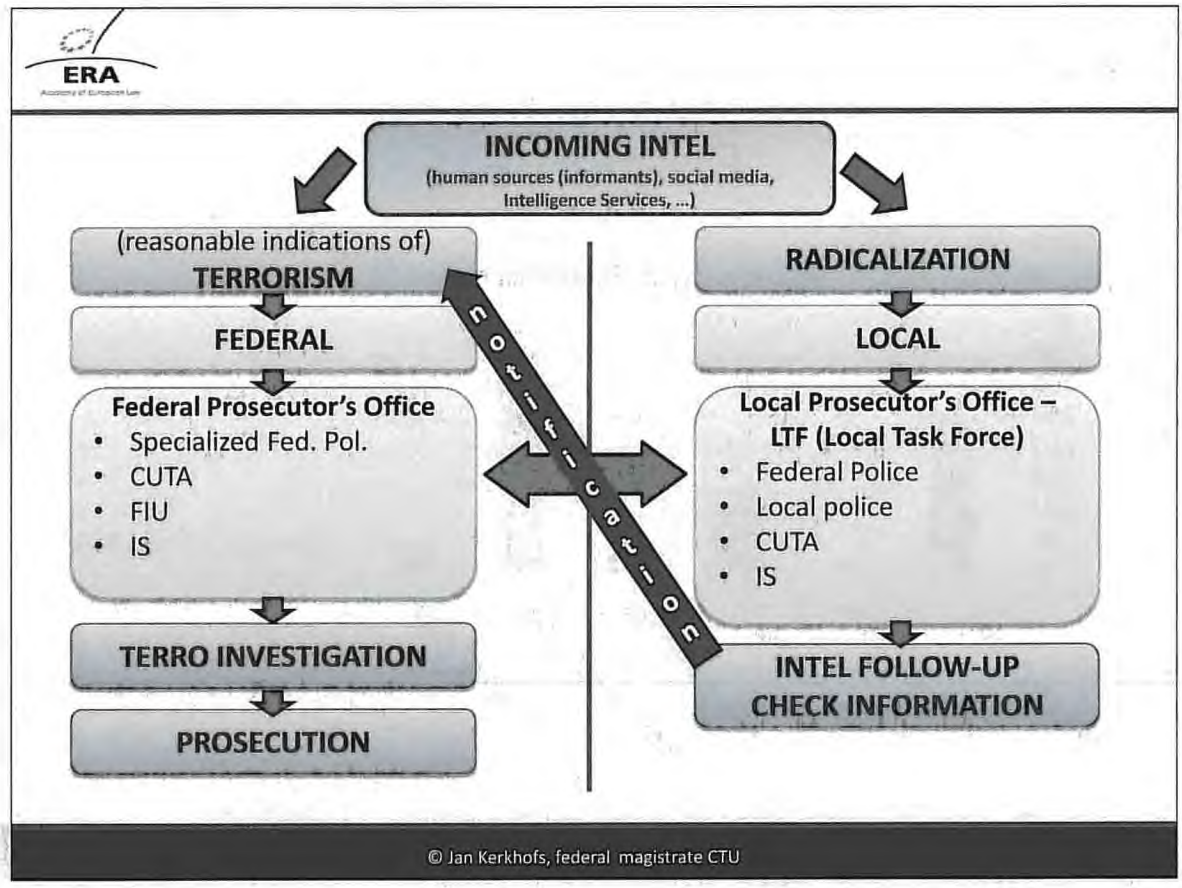
Belgian FTF



ERA

The judicial approach - coordination

- Established on the basis of **information and intelligence** of all services and on the basis of open sources
- **Sent to all services concerned**: Federal Prosecutor's Office, Federal Police, State Security Service, GISS (General Intelligence and Security Service), FPS Foreign Affairs
- Identities handed over to **Local Taskforces (LTF's)**
- Each service takes the measures it is entitled to take



ERA

The judicial approach
Police record for each departure

- Linked to an existing terrorist group
- Known in a terrorist context
- Denouncement of disappearance
- Departures for the 'regular' opposition

Priority to departures for joining salafist/jihadist groups

If not yet departed: arrest them – thorough control

ERA

The judicial approach - returnees

- Criterion: **really have stayed in Syria**
- **The Federal Prosecutor's Office informs the CUTA** (Coordination Unit for Threat Assessment) about the persons against who a federal judicial inquiry has been started, as well as about the judiciary measures taken against them
- CUTA (Coordination Unit for Threat Assessment) distributes this consolidated **list**, providing the intelligence and the measures to be taken by each service
- **Monthly meetings** at the Federal Prosecutor's Office

ERA

The judicial approach - minors

Confer with the **local youth prosecutor's offices** – no competence of the federal prosecution office:

- Disappearance to be considered disquieting
- Clear out their last contacts (social media!!)
- Urgent international portrait description for localization and repatriation
- Explicitly inform the airport police about the description
- Inform the Federal Prosecutor's Office

If not departed yet:
police record of problematic educational situation

ERA

BELGIAN APPROACH - SUMMARY

- Attempt to leave for Syria to join the Jihad ➔ intervention/arrest, criminal prosecution
- To leave for Syria to join the Jihad ➔ European and international arrest warrants, criminal prosecution
- Returnees ➔ immediate arrest, criminal prosecution
- Women? ➔ it depends

Ex. Criminal Court Antwerp 18/05/2015:
- Joined the Jihad in Syria: 5 years
- Attempt to leave for Syria: 30 months (from which 1 year effective)
- Financing the travel to Syria: 30 months (from which 1 year effective)
- Drive to the airport: 20 months with suspension

ERA

Where is the evidence & How to collect it

ERA

Real world	Online world
Wire tapping	Communication interception
Communication traffic data	Communication traffic data
Informants	Social media analysis
Interrogations	Open sourcing (!)
Bank records, flight records...	Specials Investigation Methods (obs + infilt)
Specials Investigation Methods (obs + infilt)	Seized computers & data carriers (encryption)
House searches	Online intrusion, hacking
SCI	

ERA

Real world

BORDERS

Online world

Terrorists

LE/Justice

NO BORDERS

BORDERS

ERA
Academy of European Law

Human Intel

- Crucial
- Starter info
- Be careful
- Be sceptic
- Better safe than sorry

"In exchange for my testimony, they gave me a whole new identity – 00761."

ERA
Academy of European Law

Communication & connection data

- Traffic data investigation on:
  - Phone numbers
  - IMEI numbers
  - IMSI numbers
- Transnational – localization in Syria/Iraq:

bics
a belgacom company

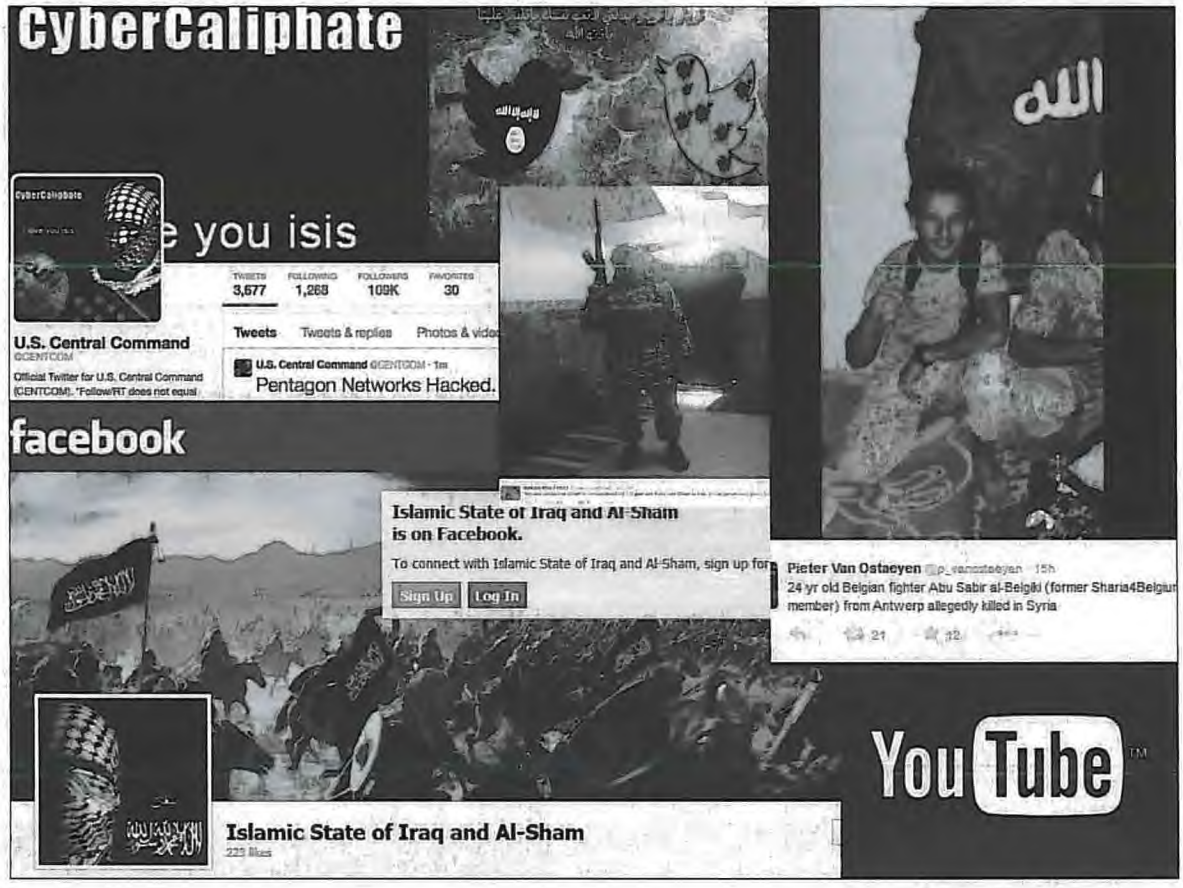
BICS NV/SA
Rue Lebeau 4
1000 Brussels
Belgium
Phone number: +32 2 547 52 10
Fax number: +32 2 547 52 12
bics-com@bics.com

ERA
Academy of European Law

Communication & connection data

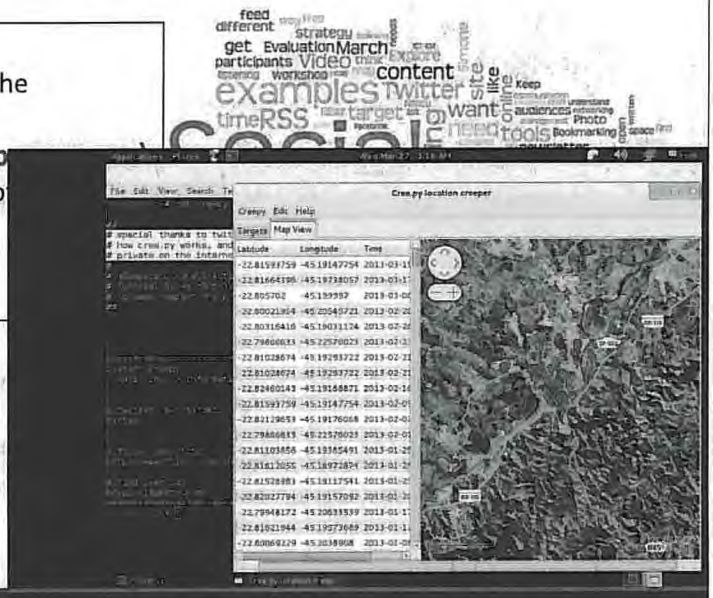
bics
a belgacom company

- Routering/roaming big parts of **Europe, Asia, Africa**
- **Localization** data
- **Connection** data
- Not always succesful, but often worth trying
- MLA-request to Belgium: Federal Prosecutor's Office, Wolstraat 66 bus 1, 1000 BRUSSEL



Social media search & localization

CONVENTION ON CYBERCRIME
Article 32 – A Party may, without the authorisation of another Party:
a) access **publicly available (op**
stored computer data, regardless o
data is located geographically;
...



- www.echosec.net
- http://www.geocreepy.com/

Localization through Skype?

- MLA to Luxemburg: SKYPE COMMUNICATIONS SARL
  - Daughter of Microsoft?
  - IP date of creation account
  - No logs available
  - Skype Out: financial data + IP's
  - **Cannot be wire tapped** (?)

Not Like

- https://www.hanzresolver.com/skype2

ERA

BSI & Traffic Data (Convention on Cybercrime)

- Expedited preservation (and partial disclosure) of traffic data (art. 16-17)
- Production order (art. 18) to "*a service provider **offering its services in the territory** of the Party to submit subscriber information relating to such services in that service provider's possession or control*"
- Search and seizure of stored computer data (art. 19)
- General principles relating to international co-operation and extradition (art. 23-28)
- Expedited preservation of stored computer data (art.28)
- Expedited disclosure of preserved traffic data (art. 29)
- Trans-border access (art. 32)
- 24/7 Network (art. 35)

ERA

US providers

- They **can work directly together** with you for **BSI** (basic subscriber information) or **traffic data** (*18 US Code Chapter 121 – Stored wire and electronic communications and transactional records access, Section 2702: Voluntary disclosure of customer communications or records + Section 2510: definitions*)
- **No data retention** in the USA (30-60-90 days)
- Historical **content** only through **MLA**
- The USA does <u>never</u> deliver a **wire tap**

ERA

Identification & traffic data

= OK ! ☺

Google

= Good but can do better
(ip addresses in Europe)

facebook

= Good but can do better
(ip addresses in Europe)
(take care of the precision of you request: ID-number, replace www with graph)

ERA

Identification & traffic data

= BAD only through MLA,
takes 23-52 months if no imminent threat

twitter

= COULD BE A LOT BETTER
OK if imminent threat, but very strict policy
(they warn the user)

skype

= POOR only IP of the date of creation
and financial data if Skype-out

ERA

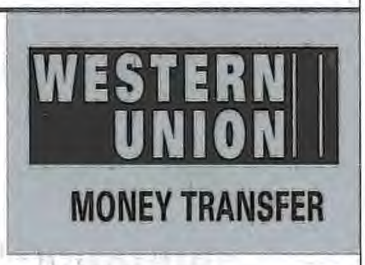
Whatsapp

- Terrorist communication tool n° 1
- No direct cooperation
- No server content if account is active
- IP from date creation, some traffic data, pictures…
- No mirror possible, no counter measures possible

confusion with the linked phone number!!!

ERA

Bank records



- The policy for the fight against terrorism:
  - in every 'classic' terrorism case: ***financial investigation***
  - FTF often **take loans and empty accounts** before going to the Jihad!!!
- The **cooperation with the FIU** (Financial Intelligence processing Unit)
  - Existing terrorism file: information joined
  - Not existing terrorism file: analysis
    - enough indications for terrorism: new investigation on terrorism
    - not enough indications for terrorism: money laundering investigation
    - Starting from suspicious financial transactions and prove financing of terrorism: *no succes*

ERA

Interrogations & searches

- Interrogations:
  - Friends
  - Witnesses
  - Family
  - The Imam
- House search(es):
  - Computers, routers (internet history, plane tickets, ...)
  - (school) books, documents, clothing, pictures, ...
  - iCloud connection if possible
  - SIM-cards, old phones, ...

ERA

Special Investigation Methods

- Observation
- Infiltration (difficult)
- Sneak and peek
- Direct tap/listening

ERA
Academy of European Law

Technical assistance I.S.

ERA
Academy of European Law

CSI: forensics

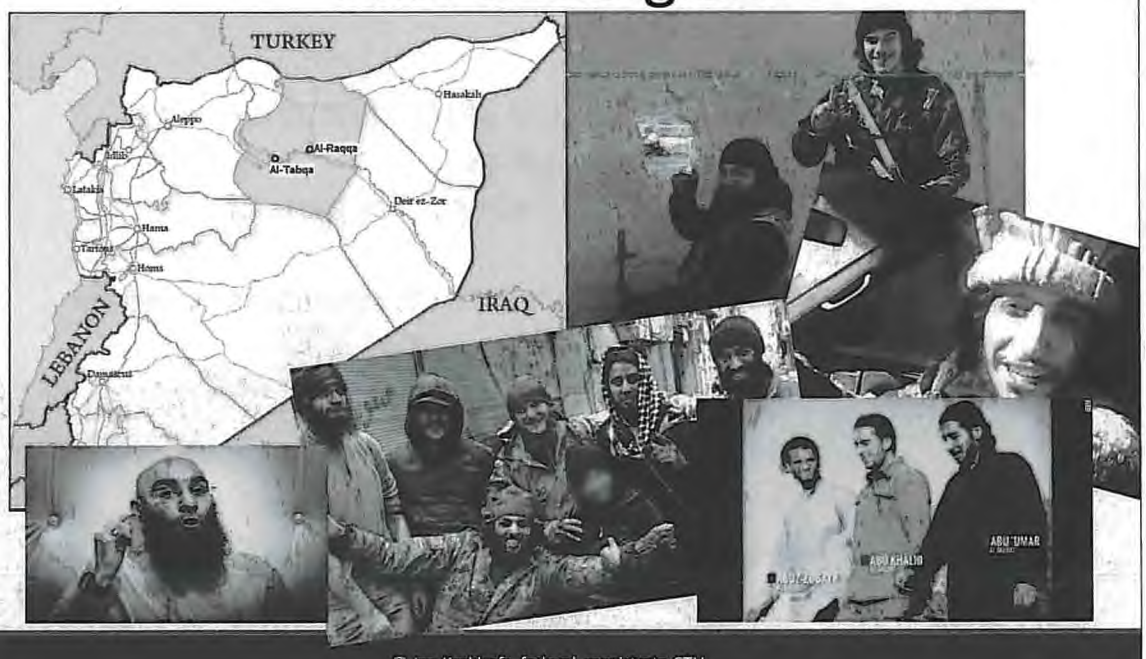
- **Best practice:**
  - Immediately after arrest: strip of the clothes and seize luggage and personal belongings
  - Scientific investigation and forensics for parts of gunpowder and metal
  - **Criminal Court Brussels 26/06/2015**: conviction based on that!!!

ERA
Academy of European Law

What evidence convinces the judge?

ERA
Academy of European Law

Sharia4Belgium



ERA

The Sharia4Belgium Case

- First trial **'Foreign Terrorist Fighters'**: 46 defendants
- First Instance Court Judgement 11 February 2015
- Many **questions** of law were opposed:
  - **The exclusion of International Humanitarian Law (article 141bis Criminal Code)!!!!!**
  - What is a terrorist group (article 139 CC)
  - The link between Sharia4Belgium and the terrorist groups Majlis Shura al-Mujahideen and Jabhat al-Nusra
  - What is a leader/participant of a terrorist group
- Appeal is pending

ERA

The evidence considered by the court

- statements of the defendants;
- statements of fighters who returned from Syria;
- statements of family members of fighters in Syria;
- contents of intercepted conversations;
- various audio-visual files, including videos showing some defendants appearing and/or speaking during activities organized by Sharia4Belgium; videos calling for armed struggle in Syria, for travel to Syria and for offering one's blood in Syria; videos addressing youngsters and undermining the educational system and their parents;
- contents of various letters;
- various photographs, including photographs posted on Facebook accounts;
- outcomes of the surveillance carried out by the authorities;
- analysis of telephone traffic;
- analysis of information found on a laptop;
- outcomes of house searches;
- police information, including from Bulgaria, etc.

ERA

The judgement S4B 11/02/2015

- Sharia4Belgium = a **terrorist group** (art. 139 CC)
  - S4B is a structured organization of more than 2 persons
  - It is not required that a terrorist attack/offence has already been commited
  - It is sufficient **that the group has the intention** to commit – one day – in Belgium or abroad a terrorist offence
  - The evidence shows that apparently S4B wanted, from the ideology of the **violent Jihadi Salafism**, to destroy the existing political regimes and replace them with an Islamic Califat or a non-democratic Islam State based on Sharia

ERA

The judgement S4B 11/02/2015

- The punishment:

ERA

Other examples

- Antwerp 30/03/2015:
  - even '**cooking and driving**' for a terrorist group
- Antwerp 18/05/2015:
  - the proof of the **intent** resulted from the **farewell letter**
- Brussel 25/06/2013:
  - The intent was proven by the declarations of the defendant: *"I wanted to commit an agression to revenge the Muslim community"*
- Brussels 26/06/2015:
  - Gunpowder traces on the clothes (!)
  - **All elements of evidence together** have to be taken into account
  - The defence may **not "salami-slice"** the evidence

ERA

Lions and men make no compacts, nor are wolves and lambs in sympathy: they are opposed, to the end.

The Iliad
Homer
800 B.C.E

ERA
Academy of European Law

Thank you for your attention

Jan Kerkhofs
Federal magistrate
Jan.kerkhofs@just.fgov.be

Hans-Holger Herrnfeld

Hans-Holger *Herrnfeld*

Dr. Hans-Holger Herrnfeld has been Head of the Division on International Criminal Law, European and Multilateral Cooperation in Criminal Matters at the German Federal Ministry of Justice from 2003 until 2010. From 2010 to 2013 he has been serving as National Member for Germany at Eurojust in The Hague.

In June 2013 he returned to the Criminal Law Department of the Federal Ministry of Justice where he is now responsible for the negotiations on the project to establish a European Public Prosecutors Office as well as general European criminal law policy matters.

Mr. Herrnfeld also is a member of the Bureau of the Council of Europe's Committee on Crime Problems (CDPC) since 2007 and has been serving as CDPC Chair in 2010/2011.

The proposed European Public Prosecutor's Office (EPPO): where do we currently stand?

Hans-Holger Herrnfeld

ERA, Trier 22/23. October 2015

A) What did we do? – Current status of negotiations

B) Where are we now?

1) Structure of the EPPO at central level
   - European Chief Prosecutor and College, Chambers
   - European Prosecutors, European Delegated Prosecutors
2) Role and competences of the European Delegated Prosecutors – supervision by the Central Office
   - Double hatted prosecutors in the Member States
   - Independence and monitoring/supervision/direction
3) Investigative measures
   - Minimum standards or own code of procedure?
   - Catalogue of measures – conditions of national law
4) Cross-border cooperation within the EPPO
   - Single legal area – more than MLA/mutual recognition?
   - *lex fori* and/or *lex loci*?
   - Role of investigating EDP and "cooperating" EDP
5) Evidence
   - Admission of evidence
   - Freely assessing the evidence
6) Procedural safeguards
   - Applicable national law – EU Directives based standards
   - Possible lacunae
7) Rules on Prosecution
   - Prosecution before national courts
   - Dismissal
   - Referral and transfer of proceedings

C) Where are we going?

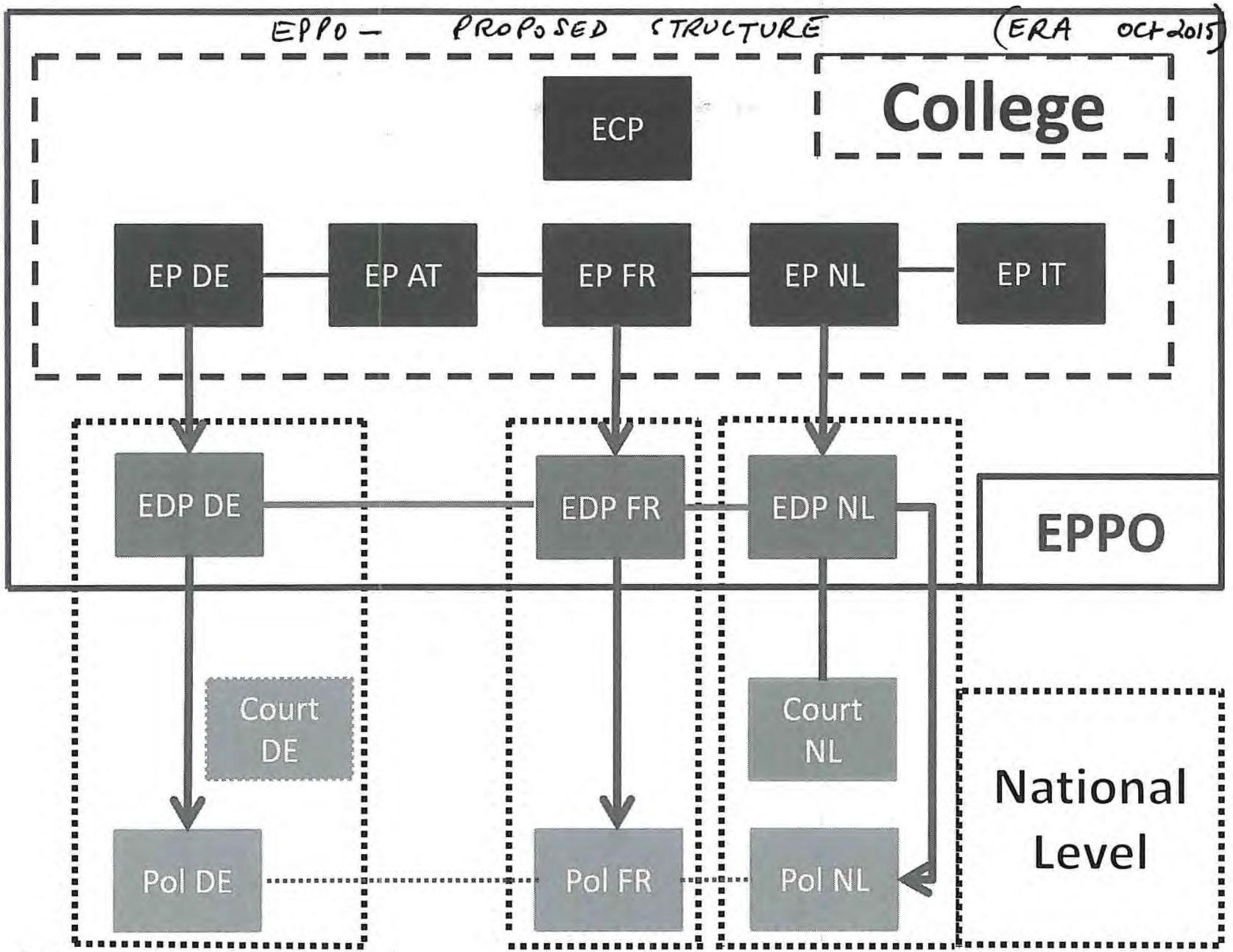
1) EPPO competences in terms of substantive law
   - PIF crimes
   - "Ancillary competences"
2) Exercise of competences – concurrent competence and right of Evocation
   - From exclusive to shard/concurrent competence
   - Right of evocation
3) Initiation/conduct of investigations
   - Choice of EDP/EP
   - Applicable national law – impact on suspects
4) Judicial control
   - Judicial control by national courts and/or ECJ?
   - Judicial review of decisions on investigative measures

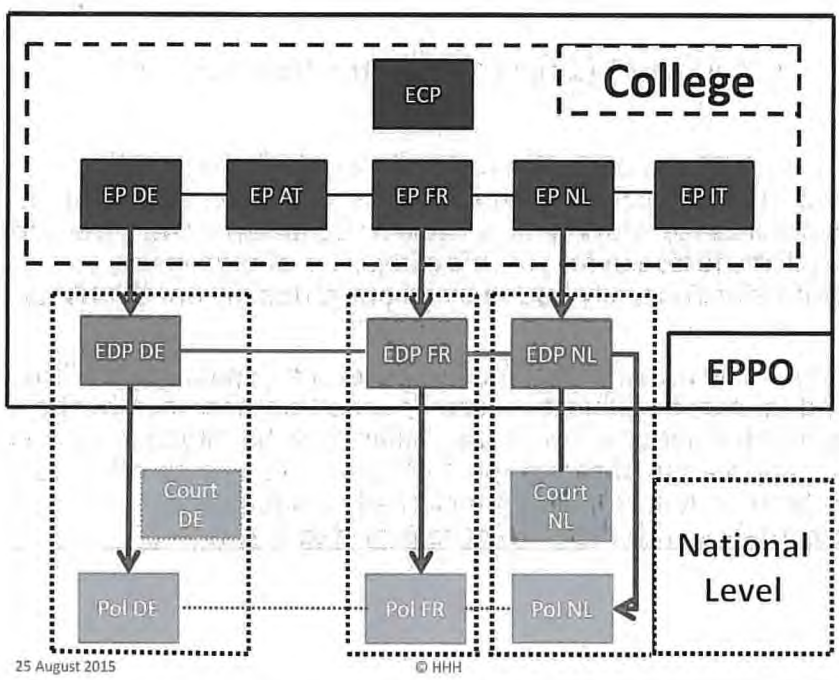
C) What else is left?

1) Information Management – Data Protection
2) Financial and staff provisions
3) Relations with third partners
   - Eurojust
   - OLAF
   - Other EU agencies
   - Non-participating Member States
   - Third states
4) General provisions

D) Where we do – but do we stand? – A new mile stone ahead?

EPPO – PROPOSED STRUCTURE (ERA OCT 2015)





25 August 2015 © HHH 1

Article 25 (1) Investigation measures

(1) At least in cases where the offence subject to the investigation is punishable by a maximum penalty of at least four years of imprisonment, Member States shall ensure that the European Delegated Prosecutors are entitled to order or request the following investigation measures:

a) search any premises, ... private homes... and take any conservatory measures...

b) obtain the production of any relevant object or document either in original or in some other specified form;

bb) obtain the production of stored computer, ... including banking account data and traffic data (except retained data)

c) freeze instrumentalities or proceeds of crime

d) intercept electronic communications.

Article 25 (1a), (1b) Investigation measures

(1a) Without prejudice to Article 24, the investigation measures set out in paragraph 1 may be subject to conditions in accordance with the applicable national law if the latter are explicitly foreseen for specific categories of persons or professionals legally bound by an obligation of confidentiality.

(1b) The investigation measures set out in paragraph 1(bb) and (d) may be subject to further conditions foreseen by the applicable national law. In particular, Member States may limit the application of paragraph 1(d) to specific serious offences as listed in Annex X. This Annex shall be updated in accordance with the procedure provided in Article Z.

Article 26 Cross-border investigations

1. ..... Where a measure needs to be undertaken in a Member State other than the Member State of the European Delegated Prosecutor handling the case, the latter shall decide on the adoption of the necessary measure and assign it to a European Delegated Prosecutor located in the Member State where that measure needs to be carried out.

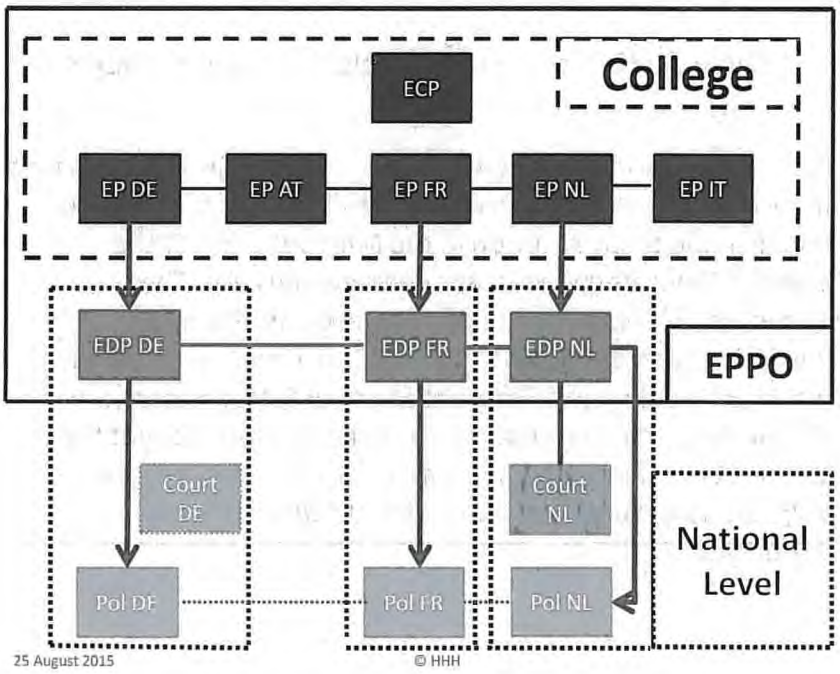
2. The European Delegated Prosecutor handling the case may assign any measures, which are available to him or her in accordance with Article 25. The adoption and justification of such measures shall be governed by the law of the Member States of the European Delegated Prosecutor handling the case.

4. If a judicial authorisation for the measure is required under the law of the Member State of the assisting European Delegated Prosecutor such authorisation shall be obtained by the latter in accordance with the law of that Member State.

6. Where the assisting European Delegated Prosecutor considers that:

   d) the assigned measure does not exist or would not be available in a similar domestic case under the law of his or her Member State,

   he or she shall consult with the European Delegated Prosecutor handling the case in order to resolve the matter bilaterally.



25 August 2015 © HHH 5

Article 31 (1), (2) Evidence

(1) Evidence presented by the prosecutors of the European Public Prosecutor's Office or the defendant to a Court shall not be denied admission on the mere ground that the evidence was gathered in another Member State or in accordance with the law of another Member State.

Where the law of the Member State of the trial Court requires that the latter examines the admissibility of evidence, it shall ensure it is satisfied that its admission would not be incompatible with Member States obligations to respect the fairness of the procedure, the rights of defence, or other rights as enshrined in the Charter, in accordance with Article 6 TEU.

(2) The power of the trial Court to freely assess the evidence presented by the defendant or the prosecutors of the European Public Prosecutor's Office shall not be affected by this Regulation.

Article 30 (2) Prosecution before national courts

(2) When more than one Member State has jurisdiction over the case, the Permanent Chamber shall in principle decide to bring the case to prosecution in the Member State of the European Delegated Prosecutor handling the case. The Permanent Chamber may, taking into account the report provided in accordance with Article 29(1), decide to bring the case to prosecution in a different Member State, if there are sufficiently justified grounds to do so, taking into account the criteria set out in Article [22(3)] and [22(4)], and instruct a European Delegated Prosecutor of that Member State accordingly.

Article 22 (3) Initiation of investigations

(3) A case shall in principle be handled by a European Delegated Prosecutor from the Member State where the focus of the criminal activity is or, if several connected offences within the competences of the Office have been committed , the Member State where the bulk of the offences has been committed. A Permanent Chamber may only instruct a European Delegated Prosecutor of a different Member State to initiate an investigation where that Member State has jurisdiction for the case and where a deviation from the above mentioned principles is duly justified, taking into account the following criteria, in order of priority:

a) the place where the suspect or accused person has his/her habitual residence;
b) the nationality of the suspect or accused person;
c) the place where the main financial damage has occurred.

Klaus Meyer-Cabri van Amelrode

Eurojust

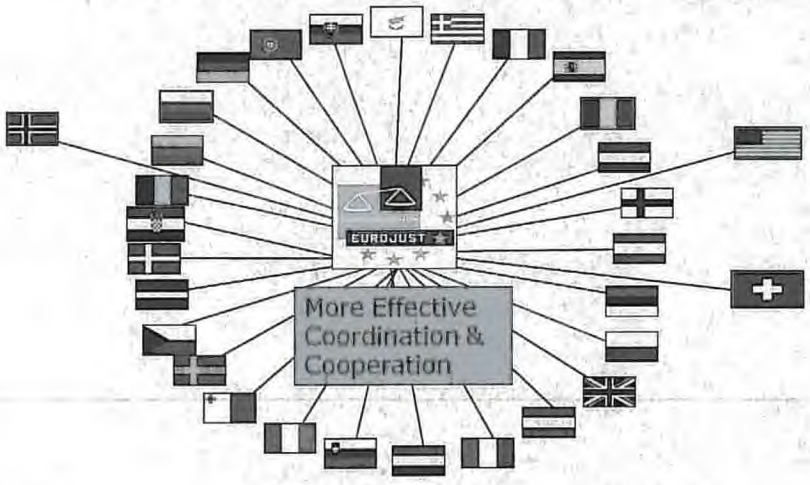
The European Union's
Judicial Cooperation Unit

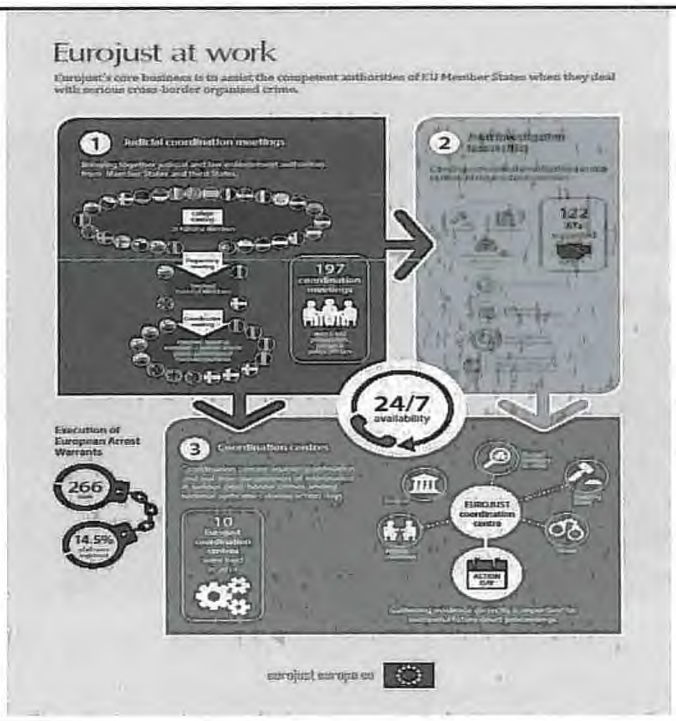
EUROJUST'S SUPPORT IN FIGHTING CYBERCRIME, TERRORISM AND ILLEGAL IMMIGRANT SMUGGLING

Klaus Meyer-Cabri
National Member for Germany
and Chair of the Brussels Team
EUROJUST

EUROJUST

28 EU PROSECUTORS/JUDGES





EU Renewed Internal Security Strategy

EU level emphasis on the importance of judicial cooperation (Eurojust) to:

- Enable operational cooperation to disrupt criminal and terrorist networks through coordinated investigations and prosecutions, also with third States
- Ensure that information exchange results in gathering of admissible evidence
- Overcome issues of multiple jurisdictions, inherent to the international nature of the main threats identified, to ensure effective prosecutions
- Allow investigations and prosecutions to pursue the financial aspects of crime, to ensure freezing and confiscation of criminal proceeds

Three priority areas:

1. Tackling terrorism and radicalisation
2. Disrupting serious and organised crime
3. Fighting cybercrime

FTFs: The evolving threat

- Increasing number of Foreign Terrorist Fighters (FTFs), including FTFs with a criminal/terrorist record
- Increasing number of plotted, attempted or executed attacks by FTFs or supporters of IS
- Increasing number of prosecutions and convictions

However, the number of prosecutions and convictions remains considerably small compared to the estimated number of FTFs

FTFs: The challenges

1. Common, comprehensive and cooperative approach
2. Evolving legal framework
3. Solid criminal justice response
4. Gathering and admissibility of e-evidence
5. Multidisciplinary approach
6. International judicial cooperation

Eurojust - Terrorism

- **Operational support** to authorities from EU Member States, e.g. 2004 Madrid bombings, 2011 lone actor attack in Norway, 2015 Bardo museum attack in Tunisia
- Annual strategic meetings of **Eurojust National Correspondents for Terrorism** and tactical meetings with focus on judicial response to the FTF phenomenon
- **Eurojust contact points in 36 non-Member States** and enhanced cooperation with the countries of the Western Balkans, Turkey, MENA countries
- Analysis of **judgements** in terrorism cases: best practice and experience; input to EU institutions on counter-terrorism policy / legal frameworks

Eurojust Counter-Terrorism Products

- **Terrorism Convictions Monitor**
  EUROJUST LIMITED
- Maritime Piracy Judicial Monitor
  EUROJUST LIMITED
- Memorandum on Terrorist Financing
  EUROJUST LIMITED
- CBRN-E Handbook
  PUBLIC DOCUMENT
- Contributions to Europol's TE-SAT Report
  TE-SAT Reports are publicly available
- **Eurojust judicial analysis of the Sharia4 Belgium judgment**
  EUROJUST LIMITED
- **Eurojust Reports on Foreign Fighters 2013 and 2014**
  EUROJUST RESTRICTED

Cybercrime case - BlackShades

FBI identified BlackShades malware through another unrelated investigation

BlackShades is an organisation developing and selling malware which enables buyers to intrude, monitor and remotely control a victim's computer

Cybercrime case - BlackShades

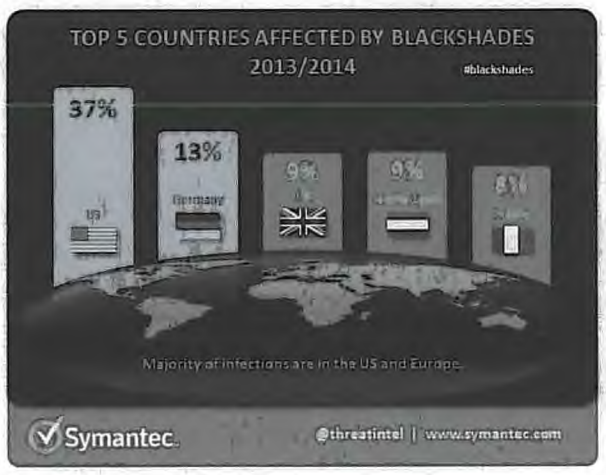
Background

- Malware distribution as a business
- Cost: $40 USD / license
- Paid positions within organization
- Software updates for life of product
- Online community
- Forum
- Marketing and Advertising
- Hacking forums

BlackShades Functions:

- Remote Desktop Control
- Keylogging
- Webcam Control
- Password Stealer
- Distributed Denial of Service (DDOS)
- Ransomware
- And more...
- Websites: www.bshades.eu/www.blackshades.ru

Cybercrime case - BlackShades



BlackShades -Role of EUROJUST

FBI > NL PPO > **Eurojust > Coordination Meetings**

- 1st: Nov 2013 > NL, BE, DE, FR, RO, USA, Europol
- 2nd: Jan 2014 > NL, AT, BE, DE, EE, FI, FR , RO, UK, USA, Europol
- 3rd: Apr 2014 > NL, AT, BE, DE, EE, FI, FR , RO, UK, USA, CA, CL, Europol

Coordination Centre 13 and 14 May 2014

- Real-time information and overview actions and results
- All countries, FBI and Europol present
- Judicial support by Eurojust in own language
- Preparation press release Eurojust-Europol

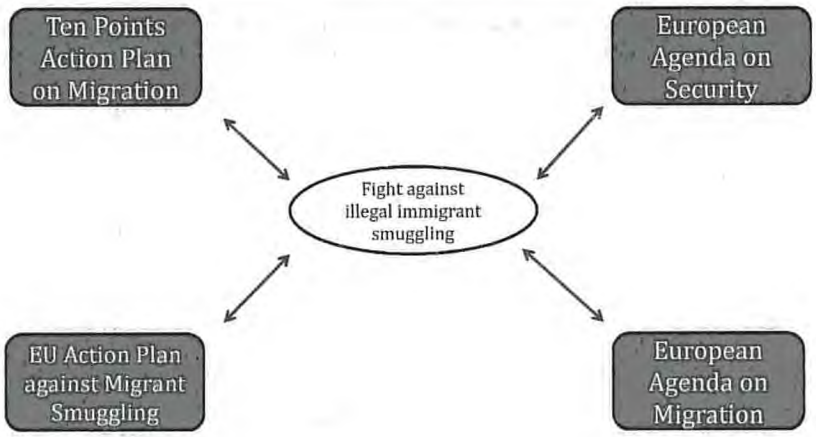
Cybercrime case - BlackShades - Results

Country	*Total nr. of arrests made*	*Total nr. of planned searches*	*Total nr. of house searches executed*
NL	0	38	34
BE	4/0	72	74
FI	8	26	27
FR	59	71	67
DE		145	111
DK	2	10	10
UK	17	20	6
CA	2	n.a.	14
USA	5	n.a.	10
GRAND TOTAL	97	382	353

Eurojust - Cybercrime

- Expertise and experience in cybercrime cases, in particular swift handling of MLA requests, admissibility of e-evidence, data retention
- Eurojust Task Force on Cybercrime
- Eurojust Seconded National Expert on Cybercrime
- Cooperation with EC3
- Annual strategic/tactical meetings on cybercrime
  →Setting up of a judicial cybercrime network of prosecutors

EU Framework on Migrant Smuggling



Eurojust - Illegal Immigration

Encourage Member States to:

- Make use of Eurojust's **judicial coordination tools** in place, i.e. coordination meetings, coordination centres and JITs
- Make full use of the **Eurojust National Coordination Systems** (ENCS) and to appoint, within the existing ENCS, dedicated Contact Points on illegal immigrant smuggling
- Foster **cooperation with third States** on the basis of Eurojust cooperation agreements and contact points

Eurojust: Taken and envisaged actions

- Appointment of a Eurojust **Contact Point on illegal immigrant smuggling**
- Eurojust's **Thematic Group** on Migrant Smuggling
- Eurojust's participation in the "**Hotspot" approach**
- CSDP operation **EUNAVFOR MED**
- **Consultative Forum** December 2015
- **Inter EU Agencies cooperation**
- Cooperation with **third countries**

Statistical overview of Illegal Immigrants Smuggling cases

Year	Illegal Immigration
Registered cases	
2014	32
2015 (as of 21.9.2015)	40
Coordination meetings / Coordination centres	
2014	10 CMs, 1 CC
2015 (as of 21.9.2015)	12 CMs
Joint investigation teams	
2014	4 new JITs, 5 still active from previous years
2015 (as of 21.9.2015)	1 new JIT, 6 still active from previous years

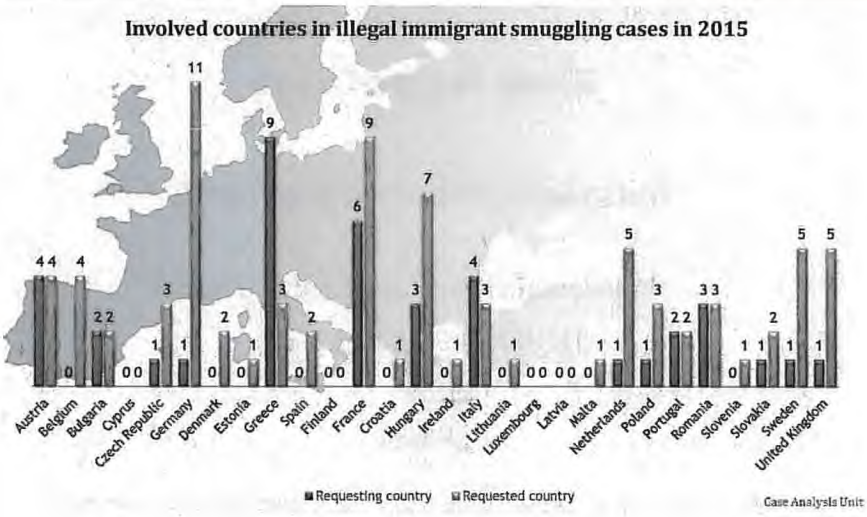
Note of caution: Statistics on Illegal Immigration cases at Eurojust have to be read with caution, due to different or overlapping classification in the Member States, or changes in the classification in the course of the investigation (for example in the beginning of an investigation it is sometimes unclear whether a case qualifies as THB or illegal immigration).

Case Analysis Unit

Illegal Immigrant Smuggling

Requesting/Requested Countries 2014

Requesting/Requested Countries 2015



Eurojust organisational developments

EPPO	EUROJUST	
- Crimes affecting the EU's financial interests - not all 28 MS	- Terrorism - Cybercrime - Illegal immigration - Drug trafficking - Trafficking in human beings - Organised crime groups	- Fraud - Corruption - Money laundering - Environmental crime - Maritime piracy - Eurojust Contact Point for Child Protection

Contact Information

Klaus Meyer-Cabri

National Member for Germany

kmeyercabri@eurojust.europa.eu

Tel 00 31 70 412 51 30

www.eurojust.europa.eu

Annual report available at http://www.eurojust.europa.eu/doclibrary/corporate/Pages/annual-reports.aspx

Stephen Mason

Stephen Mason is a barrister and an Associate Research Fellow at the Institute of Advanced Legal Studies in London.

He has written books for lawyers and judges:

> *Electronic Signatures in Law* (3rd edn, Cambridge University Press, 2012)

Author and general editor:

> *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012), covering: Australia, Canada, England & Wales, European Union, Hong Kong, India, Ireland, New Zealand, Scotland, Singapore, South Africa and the United States of America

General editor:

> *International Electronic Evidence* (British Institute of International and Comparative Law, 2008), covering: Argentina, Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, Norway, Poland, Romania, Russia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Thailand and Turkey.

Stephen is the founder and editor of the international open source journal *Digital Evidence and Electronic Signature Law Review*, now in its 12th year, available at http://journals.sas.ac.uk/deeslr.

Some of Stephen's most recent work includes:

Council of Europe

Stephen is undertaking a comparative study of electronic evidence for the Council of Europe with Uwe Rasmussen, an avocat at the Paris Bar. The exercise is to analyse existing national legal provisions that have been adopted or adapted on the effect of electronic evidence on the rules of evidence and modes of proof, with a focus on proceedings relating to civil law, administrative law and commercial law. The first draft was presented to the 90th plenary meeting of the European Committee on Legal Co-operation in Strasbourg, 28 October 2015.

Home Office, United Kingdom

Stephen is a member of an *Expert Panel on Digital Signatures in the Acquisition of Communications Data within the Criminal Justice System* for the Home Office. The work of this Panel will radically alter the method by which some evidence goes before courts in criminal proceedings in England & Wales, Scotland and Northern Ireland.

Commonwealth Secretariat

Stephen was the legal expert that conducted a needs assessment of the cyber capabilities of Antigua and Barbuda and Barbados between 28 September 2015 to 7 October 2015 with specific reference to the legal framework, criminal justice response, child online protection, adequacy of cybercrime legislation, electronic evidence (if any) and to identify capacity gaps in the justice system (law enforcement, prosecution and judiciary).

THE LEGAL CHALLENGES RELATED TO ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS

Stephen Mason, Barrister

L' Accademia di Diritto Europeo – Academy of European Law – Europäische Rechtsakademie – l' Académie de droit européee

Annual conference on EU Criminal Justice

Trier, 22-23 October 2015

In the beginning

Finding the perpetrators

Once you have found the accused, you must prove it was them

Finding the evidence

Where is the evidence?

Fixed computers; networked computers; laptops; smartphones; mobile telephones; hand-held devices; satellite navigation systems; logs of office doors opening/closing; internet (+ cloud); mice; hard drives; USB sticks, etc. etc. etc.

Obtaining evidence appropriately by using the appropriate guidelines where possible

Guidelines for handling evidence

Australia (1)

European Union (1)

International (4)

Interpol (1)

Scientific Working Group for Digital Evidence (2)

United Kingdom (1)

United States of America (8)

A detailed list is here: Stephen Mason, gen ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012), 3.04

The 'cloud'

Some problems:

- No physical location
- The data is not in a fixed location
- The cloud provider might not know where the data is located (just the specific data center)
- How to collect the data fast enough
- Administrators might help, but might not be competent
- Question about how to copy the data
- Question which tools to use (e.g. F-Response Cloud Connector)

The evidence

Some of the problems:

- Getting the evidence in a format that can be used
- Having the relevant expertise to analyse the evidence appropriately
- Identifying witnesses and obtaining witness statements

Subject areas of expertise

'digital evidence specialist':

- a person that is capable of investigating and examining digital evidence

Such specialists are required to:

- make judgements about the appropriateness of the tools and techniques they use to carry out their work
- provide an analysis of their findings, setting out the basis upon which their judgement is formulated
- to identify any data that appear to be inconsistent with their assessment

Retrieval of digital data

Analysis of digital data

Interpretation of digital data

Jurisdiction

Jurisdiction

Using the 24/7 network

Having the expertise to deal with the evidence

Charging

Who to charge

What offences to charge with

Disclosure of evidence

There tends to be so much evidence that there is a great deal of unused materials

From the perspective of the prosecution, the defence tend to want to see the unused materials – this can be a burden

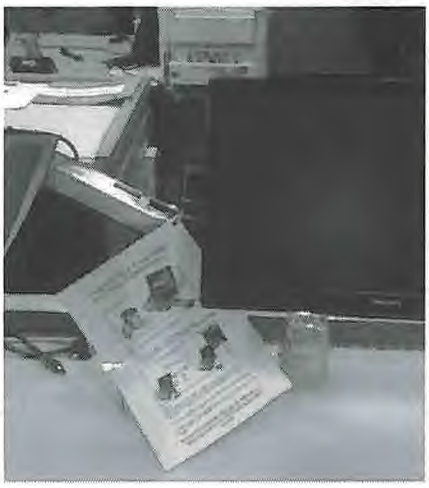
Trial

Presenting the evidence in court

Getting the judge and members of the jury to understand the nature of the charges and the evidence

How the court is beginning to look

Developments in the Crown Court



Practical responses in England

The introduction of a produce called 'Case Lines' that the prosecution will use for the purpose of:

- Disclosing evidence and statements
- During trial

The Justice Video Network will be linked to this system

Advocates benches will all have monitors, as will the judge and members of the jury

Large screen technology is being installed in some courts

'Clickshare' will be used in Magistrates' Courts to connect devices by wi fi to screens in the court

More recent problem areas

Crypto currencies

The dark web

Encryption

Rules

Streamlined Forensic Reporting has been designed to enable investigators, scientists, prosecutors and the defence to comply with the Criminal Procedure Rules in the interests of justice

There are two publications:

National Streamlined Forensic Reporting – Section 1 (Supporting Information)

National Streamlined Forensic Reporting – Section 2 (SFR Guidelines for Providers of Forensic Science and a Practical Step Guide)

http://www.cps.gov.uk/legal/s_to_u/scientific_evidence/sfr_guidance_and_toolkit/

Links with more information

CJS Efficiency Programme:

http://www.justice.gov.uk/about/justice/transforming-justice/criminal-justice-system-efficiency-programme2/criminal-justice-system-efficiency-programme

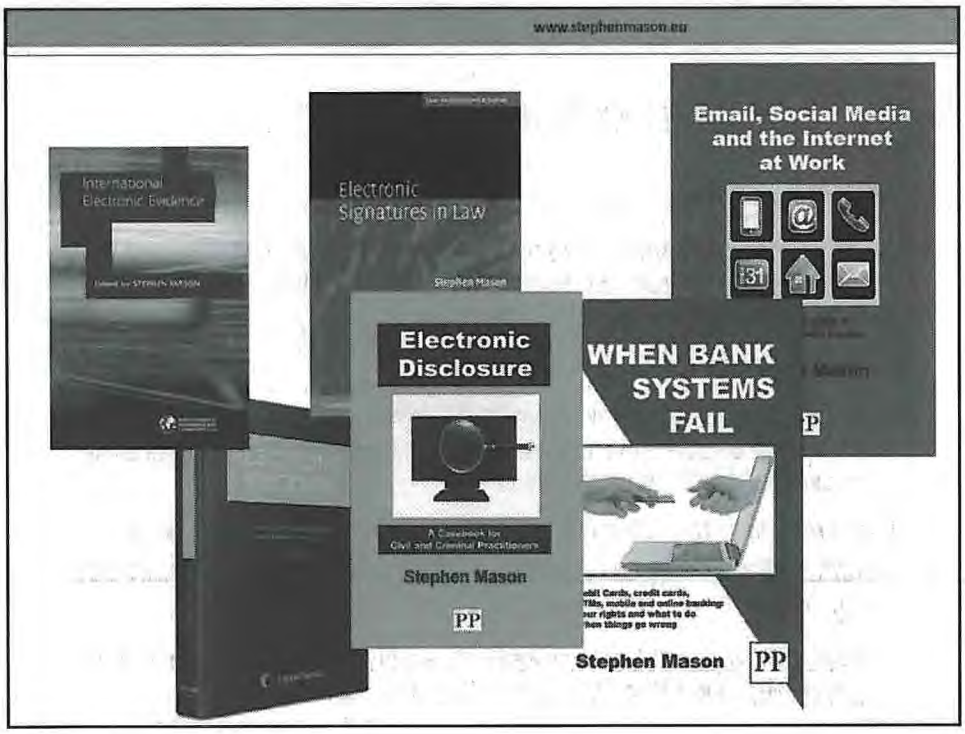
For defence practitioners:

http://www.justice.gov.uk/about/justice/transforming-justice/criminal-justice-system-efficiency-programme2/criminal-justice-system-efficiency-programme/defence-practitioners

Transforming the Criminal Justice System Strategy and Action Plan – Implementation Update (Ministry of Justice, July 2014, Cm 8868)

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/330690/cjs-strategy-action-plan.pdf

Thank you


www.stephenmason.eu
International Electronic Evidence
Electronic Signatures in Law
Stephen Mason
Email, Social Media and the Internet at Work
Electronic Disclosure
A Casebook for Civil and Criminal Practitioners
Stephen Mason
PP
WHEN BANK SYSTEMS FAIL
Stephen Mason
PP

THE *AMERO* CASE, THE CHAIN OF CUSTODY AND OTHER RELEVANT ISSUES

Stephen Mason, Barrister

L' Accademia di Diritto Europeo – Academy of European Law – Europäische Rechtsakademie – l' Académie de droit européee

Annual conference on EU Criminal Justice

Trier, 22-23 October 2015

State of Connecticut v Julie Amero (2007)

A detailed analysis of this case is provided in *International Electronic Evidence* (British Institute of International and Comparative Law, 2008), Introduction, pp xxxvi – lxxv

[http://www.biicl.org/international-electronic-evidence]

Proof of intent

There was no dispute that the text 'Female sex enhancers' that appeared in the Temporary Internet Files as the colour red

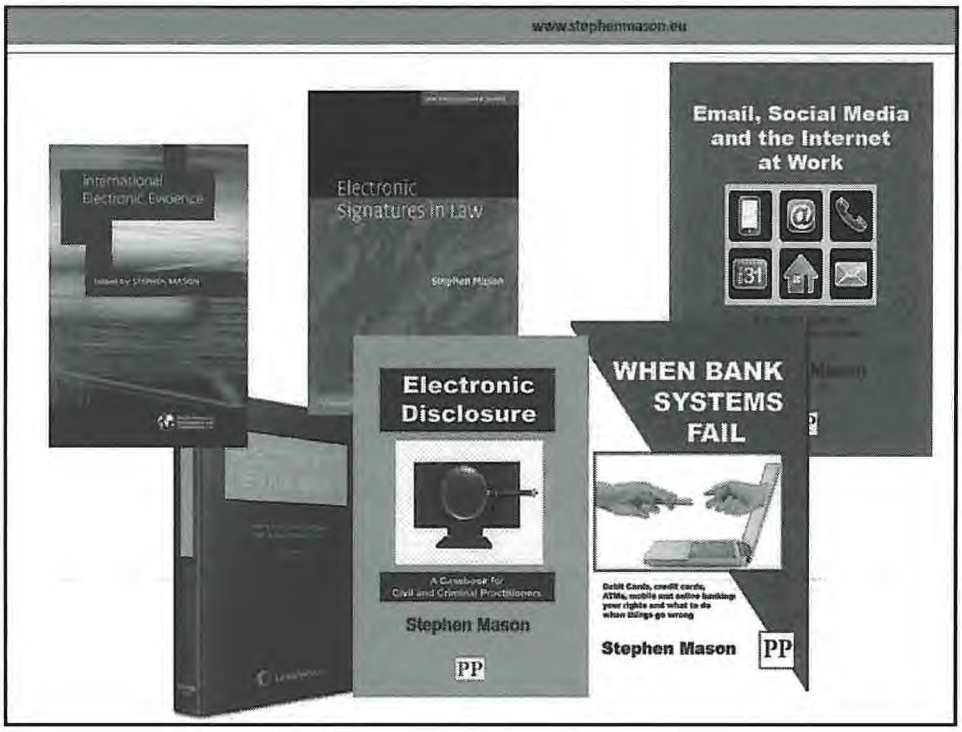
The investigator did not look at the HTML source on the relevant page, which read:

```
<img src="images/folder_25a.gif" width="18" height="12"
align="absbottom"><a target="_blank" href="viagra-cream-for-
woman.htm"><font color="#FF0000">Female sex enhancers!</font></a>
```

The text <font color="#FF0000"> indicates the colour of the link, as given by the web designer, i.e. the person that wrote the software code

That the text was the colour red did not prove that it was clicked by the user of the computer

Thank you


www.stephenmason.eu
International Electronic Evidence
Electronic Signatures in Law
Stephen Mason
Email, Social Media and the Internet at Work
Electronic Disclosure
A Casebook for Civil and Criminal Practitioners
Stephen Mason
PP
WHEN BANK SYSTEMS FAIL
Stephen Mason
PP

Annual conference on EU Criminal Justice

Trier, 22-23 October 2015

State of Connecticut v Julie Amero (2007)

A series of 5 exercises by Stephen Mason

1. Outline of facts of the case, p 2
2. Exercise for everyone

    Qualifications of the experts, pp 3 – 4
3. Exercise for group 1

    Analysis of the investigation – the hard drive, pp 5 – 6
4. Exercise for group 2

    Analysis of the presentation of the evidence in court – colour of links in Temporary Internet Files, pp 7 – 8
5. Exercise for group 3

    Analysis of the investigation – the physical evidence, pp 9 – 10
6. Exercise for group 4

    Unfairness of a prejudicial nature, p 11

A detailed analysis of this case is provided in Stephen Mason, general editor, *International Electronic Evidence* (British Institute of International and Comparative Law, 2008), pp xxxvi – lxxv

Outline of the facts

Mr Matthew Napp taught children in the age range 12 – 13 years at Kelly Middle School, Connecticut in the United States of America. On 19 October 2004, Mr Napp went into his classroom and logged in to the teacher's computer under his own username and password before permitting the temporary teacher to use it. Ms Amero took his class because he was on a course for the day. Mr Napp left the classroom at around 8.15 am. Ms Amero went to the ladies cloakroom, and when she returned, her evidence was that Mr Napp was no longer in the room, and she found two children on the teacher's computer. There was a web site showing hair styles displayed on the monitor. Ms Amero told the children to leave the computer.

Ms Amero returned to the teacher's desk and the computer after giving the class their assignment. When she returned to the teacher's desk, she found images popping up on the computer screen, which she described as images 'that were not for children to see'. During the course of the day, various images in the form of pop-ups appeared on the screen of the computer, and Ms Amero gave evidence that the images did not stop: 'The pop-ups never went away. It was one after another. They were continuous. Every time I clicked the box in the corner, the red box, the red X, more were generated.' It appears that six male children saw pornographic images on the teacher's screen during the course of the morning.

The indictment

The charges read out to Ms Amero that she entered a plea to were phrased as follows:

> Connecticut General Statute Section 53-21(a) (1) and charges that on or about October 19th, 2004, in the City of Norwich, the defendant did willfully and unlawfully cause a child under the age of sixteen years to be placed in such a situation that the morals of said child were likely to be impaired.

Exercise for everyone

Qualifications of the experts

Instructions

Please read the extracts from the transcript of the trial (printed on the following page), and consider the following points for discussion:

1. One report has suggested that the police officer 'completed two two-week FBI training seminars on computer security and other continuing education programs. He is also a certified user of the computer monitoring software ComputerCOP Pro.' (Apparently the ComputerCOP Pro course is a one hour discussion over the telephone). Consider whether this police officer had the appropriate qualifications.

2. Consider whether the defence expert had the appropriate qualifications.

Exercise for everyone – excerpts from the transcript of the trial

The police officer

To establish the qualifications of Mark Lounsbury, the prosecution lawyer asked the following questions of the police officer:

Q How long have you been a police officer?

A Almost eighteen years now.

Q How long have you been involved in the investigation of computer crimes?

A Approximately seven years.

Q And do you have any training and experience specifically in investigating computer crimes?

A Yes, I do.

The defense expert

Mr Wilson H. Horner gave a long employment history and later set out the actions he took after being approached by the defense:

Q Mr. Horner, can you tell us what actions you took concerning this case.

A Basically I – what I had to do is determine as much as I can about this forensic analysis of this particular computer. The first thing we did, my group and my company, we went out and found as much information as we possibly could, either through seminars or through the Internet and libraries on how to conduct this examination. And the reason I did that, even though I had a lot of experience doing that type of thing, I just wanted to make sure that I did not leave anything out. And I wanted to make it as thorough as I possibly could. So what I am showing here are all the references that I used to assist us with this investigation. And I don't know if it is necessary to read them all, but I can. And I also listed up there the authors and either the websites or where they were located.

Exercise for group 1

Analysis of the investigation: The hard drive

Instructions

Please read the extracts from the transcript of the trial (printed on the following pages), and consider the following points for discussion:

1. Did the police officer conduct his examination of the hard drive on the original hard drive or a copy of the hard drive?

2. How important was the tool that was used to take a copy of the hard drive?

3. Should you take more than one copy of the hard drive with different tools?

4. The prosecutor was surprised that there was malicious software on the computer. Should he have been surprised?

Exercise for group 1: excerpts from the transcript of the trial

Copying the hard drive: Evidence of Detective Mark Lounsbury

Q At some point, you had this computer powered up, correct?

A Yes.

Q And you were in the process of conducting a forensic examination of the hard drive, is that correct?

A Yes, sir.

Examination of the hard drive: Evidence of Detective Mark Lounsbury

Q Could you tell the jury what you did in order to begin this investigation.

A I utilized a program known as Computer Cop Pro. It's an examination software. What it does is it examines the hard drive for stuff that I tell it to look for. In this case, I told it to look for things that are associated with the Internet and web pages. So pictures that are commonly used are known as GIFs and JPGs and variations of JPGs. Also, I instructed it to search for certain types of words, and again, in the Internet there is not your words as we know them there, it's HTML, which is a language. HTML, rich text format, TXT's, and I told it to search specifically for them, and then there were specific words that are utilized that give you the most information with that group of words looking for pornographic-type stuff.

Mark Lounsbury was explicitly asked if he had tested the hard drive for viruses and spyware in cross-examination:

Q Did you examine the hard drive for spyware, adware, viruses or parasites?

A No, I didn't.

Malicious software: Evidence of Mr Robert Hartz, the information services manager for the Norwich Public Schools System

Q To your knowledge, was the PC in question, Mr. Napp's PC, to your knowledge at the time infected with any viruses?

A Not to my knowledge.

He confirmed this when cross-examined:

Q Was there any adware, spyware or virus found on the computer?

A I did not find any of that, although I did not look for adware or spyware.

Content filtering: Evidence of Mr Robert Hartz

Q You mentioned in your testimony today that you have content filtering on your computer, your firewall wasn't updated, is that correct?

A That is correct. It had not been updated, I would say, for a few weeks.

Exercise for group 2

Analysis of the presentation of the evidence in court: Colour of links in Temporary Internet Files

Instructions

Please read the extracts from the transcript of the trial (printed on the following page), and consider the following points for discussion:

1. Is it factually correct that a link changes colour when it is clicked?

2. Can a web designer actually decide on the colour a link will be? The police officer asserted that if a web page was in the Temporary Internet File, it proved the user actually clicked on to the web site.

3. Is it factually correct that a web page must be clicked for it to appear in the Temporary Internet Files?

4. Will all the evidence of the web sites visited be included in the Temporary Internet Files?

Exercise for group 2: excerpts from the transcript of the trial

The police officer, Mark Lounsbury, was recalled to give further evidence on the third day of the trial. He gave evidence in particular in relation to the change of colour of a link:

Q Are there any specific characteristics that may occur to a web page when you click on specific link?

A Yes. When you click on a link, again, links are Javascripted, you click on a link, it changes color and then you will get sent to that new address, that new page or site.

.....

Q I will take your attention specifically to this, Female Sex Enhancers; anything different about that link as opposed to the other links?

A The color, it's red.

Q And to your knowledge, based on your forensic examination of this machine, what may that indicate to you?

A That indicates that that link was actively clicked on and you were then sent to that page.

Q Okay. So a person would actually have to click on the Female Sex Enhancers link to go to another page, correct?

A. Yes.

When examined by the defense attorney, the police officer continued:

Q Detective Lounsbury, you indicated that, I guess, the coloration in the photograph shown to you by Mr. Smith indicates that links were clicked on, is that correct?

A Yes, sir.

Q When you say indicated, you are not saying a hundred percent?

A I've never seen anything other than that.

Q But you're not saying a hundred percent?

A In my mind it is.

Q Are you saying you're positive?

A Based on my knowledge of how it works, yes.

Q What about the science of it also?

A Which is based on my knowledge of the science.

Exercise for group 3

Analysis of the investigation: The physical evidence

Instructions

Please read the extracts from the transcript of the trial (printed on the following pages), and consider the following points for discussion:

1. What items should have been seized?

2. What actions should the police have carried out with the computer?

3. How should the computer have been stored and handled?

4. What information should the police have recorded when seizing the computer?

5. What evidence should the prosecution give to the court before introducing the evidence of the hard drive?

Exercise for group 3: excerpts from the transcript of the trial

Actions of Mr Napp, the teacher

He went into the classroom on 20 October 2004 after being informed what happened the previous day. From the transcript of the trial:

Q What did you do?

A I turned on the computer and there is a way I can just check basic files that have been placed on the computer within however long you make the time frame, and I just searched for yesterday.

.....

Q Did you see various Internet access sites?

A I saw a bunch of different sites of some pictures that had questionable names.

Q On the Internet site as you say, as an example, what drew your attention to those various sites?

A Some of the names. I clicked on one and I don't remember the name, but it ended up being a discussion board about lesbians.

Mr Napp sent an e-mail to the principle, asking how to proceed. During the afternoon of 20 October, the principle visited the classroom, and Mr Napp showed him the 'log' (probably the temporary cache file).

Actions of Mr Robert Hartz

He attend the school on 20 October and took the following action (from the transcript):

'I then went to the teacher's computer in that room, his computer, and the first thing I did was I took the IP address, because I was going to need that later, so I recorded the IP address. And then I went into the cookies file. The cookies didn't show me a whole lot. But then I went into the temporary Internet files, and that is a number of files that were dated the previous day, October 19th, with time stamps starting I believe around 8:30, 8:35, and going through the end of the day. And so I looked at these and I saw certain sites that were accessed from this PC.'

Computer taken into custody by the police

The computer was taken into custody by Michael Belair, a sergeant with the Norwich Police Department on or about 27 October 2004. He logged the computer as evidence and placed it in the evidence room.

Mark Loundsbury, a crime prevention officer and the computer crimes officer in the Norwich Police Department, retrieved the computer from the evidence officer on an unknown date some two years later. He gave evidence that the computer was last used on 26 October 2004.

Exercise for group 4

Unfairness of a prejudicial nature

Instructions: Please consider the following points for discussion:

1. Sequence of events

The prosecution did not provide evidence of the sequence of events, the times that the seven children that gave evidence were actually in the classroom, at what time they saw the images, the size of the images they saw, and precisely what images they saw.

Was it necessary to prove the proper sequence of events?

2. The prosecution illustrated some images to the members of the jury through a computer and projected on to a screen in the court, but did not indicate whether any of the images shown to the members of the jury had been seen by any of the child witnesses, and also did not indicate which image was related to each of the four charges. It is not certain whether any of the images seen by the members of the jury corresponded to the images seen by the children.

Was it necessary to prove which child saw which images?

3. Size of the images shown to the members of the jury

The images that were shown to the members of the jury were viewed many sizes greater than the image that originally appeared on the computer screen. This means that where a pop-up was only a matter of two inches square, for instance, the image would be magnified many times on the screen shown to the members of the jury.

Should the members of the jury have been shown the actual size of the image as it would have appeared on the screen?

Should the court have had a number of computers made available so the images could have been shown on the screen as it would have actually appeared?

4. Advanced notification of the defense expert witness

The defence hired an expert witness. The prosecution requested the report to be given to them before trial. It was not. The judge did not admit the expert report into evidence, and did not permit the defense expert to give evidence of what was contained in the report.

Was this a correct response by the judge?

Hein Dries-Ziekenheiner

VIGILO consult

Social media, big data, investigations

ERA

Trier – October 2015

1

Introduction

- Mr. Hein Dries-Ziekenheiner
- (LL.M)…
- Background
  - Leiden University eLaw dpt.
  - NL ISPA (ISP industry association)
  - Netherlands telecoms agency (OPTA, now ACM): spam and internet safety
  - VIGILO (enforcement online, security)

VIGILO consult

2

Program

- Introduction
- Subject: Social media (=big data =cloud computing)
- Identity
  - Explanation
  - Issues with identifying users
  - Cooperation
- Investigations
  - Opportunities
  - Risks
- Discussion and conclusions..

VIGILO consult

3

Indentity "Say my name"

Stills from series "Breaking Bad" © AMC

VIGILO consult

4

Attribution:"Say My Name"

- "Heisenberg"
- Walter White ("Walt")
- Bryan Cranston
- Breaking Bad
- And (well..maybe):
  - On 9 feb 2015 at 1500 GMT: 92.78.121.12
  - +1 819 122312341
- Social Media?

VIGILO consult

5

Social Media

- Cybercrime:
  - Often clear "WHAT"
  - Not so clear "WHO"
- Regular crime: online identities often at stake
  - Facebook
  - Linkedin
  - (..)

VIGILO consult

6

VIGILO consult

Social media

Attribution?

7

Links between people

VIGILO consult

8

Who is who?

HELP, I'M TRAPPED IN FACEBOOK'S ABSURD PSEUDONYM PURGATORY

VIGILO consult

9

Issues

- Attribution
- Investigating social media (risks, opportunities)
- Big data
- Legal risks
  - Searching evidence?
  - Decriminating evidence?

VIGILO consult

10

VIGILO consult

Issue: Finding People

Attribution

11

Know your customer?

VIGILO consult

12

Where to ask

- Facebook, Twitter, LinkedIN(?) (...)

VIGILO consult

13

Problem:

- Apache log (default):
  - "**80.160.72.242** - - [19/Jan/2015:18:17:43 +0100] "GET /templates/moviestore/modules/jload.js HTTP/1.1" 404 235 "http://www.vigilo.nl/" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)"

VIGILO consult

14

IP addresses

- Unique address
- But only unique on the network
- May have several people behind it
  - NAT
- May only be allocated for a (very) short period of time
  - Dynamic
- Time and date!

VIGILO consult

15

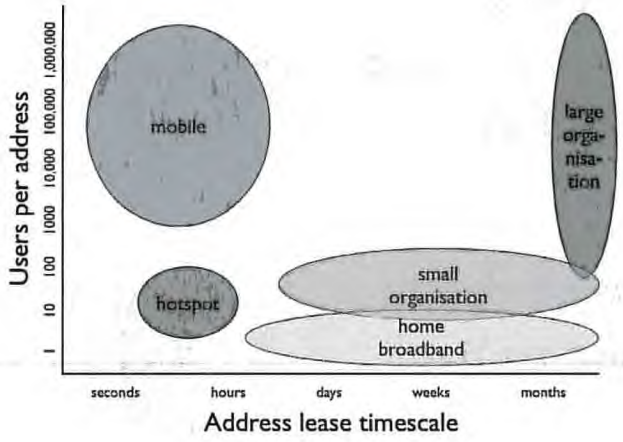
ISPs

- Allocate IP address
- Have the IP-> user mapping
- But
  - Data retention
  - Increased scrutiny on privacy
- And: does not necessarily know end user
  - LAN
  - NAT

VIGILO consult

16

Lease times vs users per address



VIGILO consult

17

Other issue

- TOR
- VPN
- PROXY

- DEMO

VIGILO consult

18

Remarks

- Time and date
- Username and ALL identifiers
- Use "LEA desk"?
  - Yes
  - But..
- Make good contacts
- Budapest/MLAT...

VIGILO consult

19

VIGILO consult

Investigating social media

Risks?

20

Investigations

- Traces:
  - High impact (traces on target machines)
  - Low (database query at a third party)
- Interaction:
  - Undercover op (entrapment!)
  - One off (stolen goods on eBay)
  - Automated system ("public information")

VIGILO consult

21

Low risk: transactions

- Just a "one off"?
  - Buying selling
  - Interacting with server?
  - Infrastructure.
  - Higher risk if they "want a chat"/"smart up"

VIGILO consult

22

High risk: interaction

- Undercover?
  - Legend
  - Needs to have every detail covered
  - Infrastructure!
  - No 9-17 job

VIGILO consult

23

Issue: they have big data too

SLEEPING TIME

Find the sleeping schedule of anyone on Twitter

TECH BLOG TALL TWEETS HUNDRED ZEROS PODCAST GALLERY

What is Sleeping Time?

Specify the Twitter username of your friend, or even your favorite celebrity, and we will figure out the sleeping pattern of that person. See sample report.

Sign-in with Twitter

How does it work?

Sleeping Time will fetch the last 1000 tweets of a Twitter user and then determines the approximate sleeping schedule based on the time when he or she is least active on Twitter.

There's no rocket science involved but lot of people say that the results are pretty accurate. We only index "public" Twitter profiles and will never post anything to Twitter on your behalf.

VIGILO consult

24

Main issue

- Identifiers – such as:
  - IP addresses
  - Profiles
  - History
  - Network
  - Friends
  - **Location**
  - Working hours
  - Phone numbers
  - Usernames
  - Cookies
  - Mac addresses
  - Bluetooth MAC addresses

VIGILO consult

25

Case

1.1.6 To avoid compromise the following must be adhered to:

- The covert mobile phones are equipped with BLUETOOTH and therefore they MUST not be switched on or used within a 50-mile radius of Cheltenham and within this radius the battery must be removed from the phone.
- The covert mobile phone MUST NOT be recharged at the officer's home address or at temporary residence e.g. a hotel room, if it is within the 50 miles radius. If a phone needs to be charged then it is acceptable to do so either at the airport or at your destination.

Page 5 of 6

SECRET

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [redacted] (non-sec) or email [redacted]@gcnx

SECRET

Ref: DOT/1636/5040/102
28 June 2010

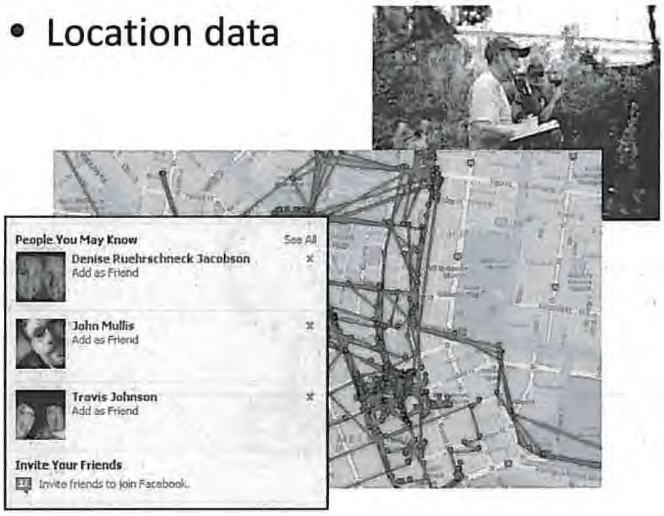
- All contact with GCHQ should be via the OUT OF AREA numbers listed above.
- Calls are not allowed between a covert mobile phone and a family or friends home or mobile phone registered to an address within 50 miles of Cheltenham
- If you are carrying a covert mobile phone, you MUST NOT carry any personal communications device e.g. mobile phone, ipad, notebooks, PDAs, laptops etc.
- Calls between covert mobiles are permissible provided both are more than 50 miles from Cheltenham.

VIGILO consult

26

Observation?

- Location data



VIGILO consult

27

Legal intercept

- Facebook messenger
- Whatsapp
- Skype
- Threema
- Telegram
- (...)

VIGILO consult

28

Dawn raid?

- More data
- More devices
- More network based storage
- (Moore's law anyone?)

VIGILO consult

29

VIGILO consult

Big Data

Big data aspects of social media

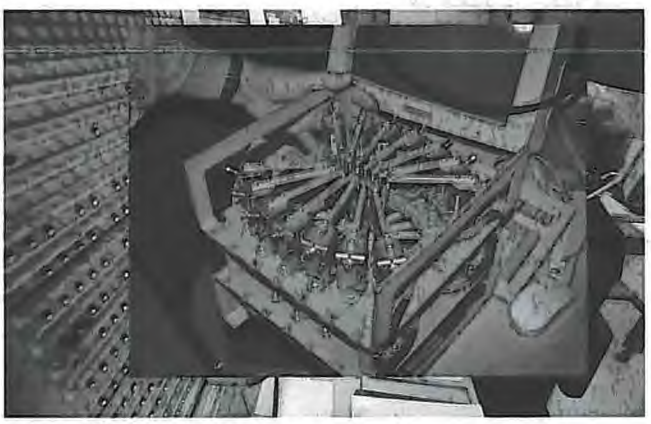
30

Where is all that data?

VIGILO consult

31

Big data?



VIGILO consult

32

Enter Really big data

Microsoft

Microsoft case: DoJ says it can demand every email from any US-based provider

Microsoft counsel addresses question of US search warrant for Hotmail emails stored in Ireland: 'We would go crazy if China did this to us'

33

Clouds?

- Different providers
- Easy to move services

But

- What can be done?
  - Usually accessible somewhere!
  - 32 CCC: accessible in jurisdiction or consent
  - 29/31 Expedited preservation and access
  - Encryption…

VIGILO consult

35

VIGILO consult

Legal issues

36

Undercover: Entrapment

- Increasing interaction
  - Reviews
  - Communications and comments
  - Social media presence
- Even in "one off" transactions this may require quite a "legend"/"persona"

VIGILO consult

37

Undercover:

- Covert search?
  - Often illegal
- Undercover?
  - Safeguards
- Open Source?
- Shades of grey

VIGILO consult

38

Admissabilty

- Privacy
  - Klaus Hoffmann
  - https://eucrim.mpicc.de/archiv/eucrim_12-03.pdf
  - Open account?
  - Friends only?
  - Police looking over the shoulder of a party?

VIGILO consult

39

Admissabilty

- Searching in data
  - Harder.. MapReduce.. Anyone?
  - Decriminating evidence
  - Trusting Social Media operators?
- Forensic safeguards:
  - Can procedure be reproduced?
  - Original copy of "all data"?
  - Selection criteria?

VIGILO consult

40

Chain of custody

- Internet based evidence!
- Digital evidence:
  - Easy to copy
  - Alter
  - Delete
- Hashing (one way signature)
  - Imperfect safeguard
- Paper forms? ☺

VIGILO consult

41

Encryption

- Self incrimination
- Differing legal POVs
- Diferig legislation
  - Decryption order
  - Decryption order to suspect
  - Consequences?

VIGILO consult

42

Conclusions

- All issues
- Q&A

Hein Dries-Ziekenheiner LL.M
hein@vigilo.nl
+31 71 7113243

VIGILO consult

43

Dave O'Reilly

Challenges and Opportunities Presented by New Technologies in the Payment Ecosystem

Dave O'Reilly, Chief Technologist, FTR Solutions

FTR solutions

FTR Solutions Introduction

- The mission of FTR Solutions is to increase the security of financial services.
- Established by Dave O'Reilly in 2012.
- Anti-fraud/security technology evaluation and selection.
- Online banking (authentication/authorisation solutions), mobile banking solutions, ATMs (skimming, card trapping, malware solutions).
- Also expertise in IT/information security and data protection.

FTR solutions

Agenda

- Brief history of payment card security
- Payment card crime and crime model
- Evolution of payment card security
- PINs and alternatives to PINs
- Micropayments
- Virtual currencies

FTR solutions

info@ftrsolutions.com | www.ftrsolutions.com

BRIEF HISTORY OF PAYMENT CARD SECURITY

Card security features and why they are there.

FTR solutions

info@ftrsolutions.com | www.ftrsolutions.com

Fraud Evolution

Card Cloning
- Creating a fake card using the information contained on the front of the card.
- Protections involve making it difficult to reproduce these features.

Card Cloning
- When convincing clones of cards can be made using only information on the front of the card, additional protection is required.
- Store additional information on the rear of the card (e.g. signature and magnetic stripe)

Card Skimming
- Capturing the data from the magnetic stripe and using this to make a cloned card.
- Protections involve migration to EMV (chip and pin).

Card not Present
- Fraud conducted online
- Protections involve CVC2/CVV2 codes and other technologies such as 3D Secure.

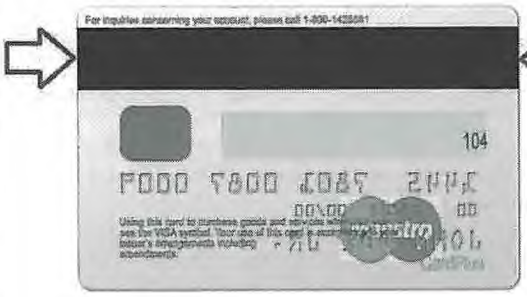
FTR solutions

Card Security Features

- Embossed Numbers
- Hologram
- Microprinting
- Expiry Date
- Issue Date/Issue Number

FTR solutions

Card Security Features



- Signature
- CVV1/CVC1
- CVV2/CVC2

FTR solutions

Card Security Features

- Chip security features
- Cryptographic security
- Prevents card cloning

FTR solutions

PAYMENT CARD CRIMES

FTR solutions

Crimes Targeting Payment Card Data

Skimming	Card trapping	Cash trapping
Malware (ATM)	Malware (POS)	Malware (data harvesting from customer PCs)

FTR solutions

Crimes Using Payment Card Data

- Card not present fraud (Various types)
- Cash withdrawals
- Card cloning
- Other illegal use of compromised cards or card data

FTR solutions

Current Card Fraud Model

Capture Card Data
- Can be performed in lots of different ways.
- Card skimming (e.g. at ATMs)
- Harvested from customer or merchant computers (e.g. by malware)

→

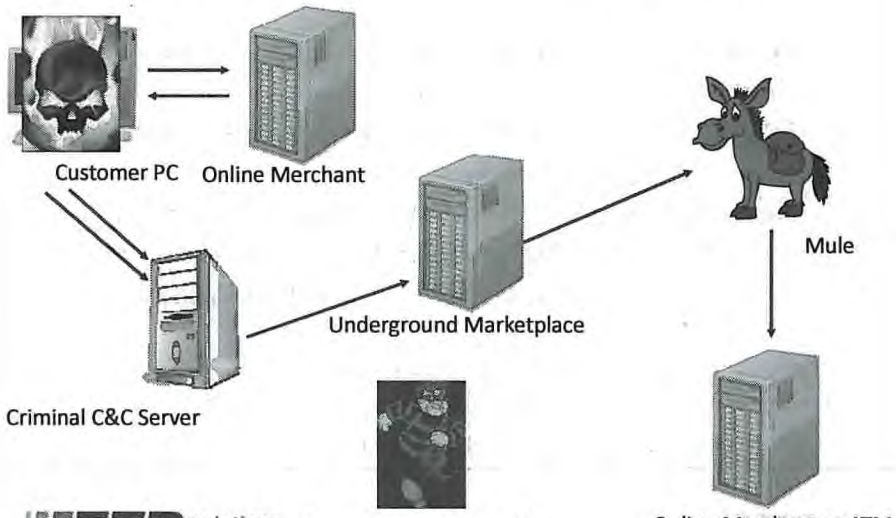
Card Data Traded Online
- Extensive criminal infrastructure exists for the sale of compromised card data.
- Almost always in a different jurisdiction to where the card data was captured.

→

Card Data Used
- Card data purchased on an underground forum.
- Almost always used in a different (third) jurisdiction to where the card data was captured and purchased.

FTR solutions

How does it work? – Malware Example



FTR solutions

Where is the criminal?

- Malware development
- Customer PC infection service
- Operating C&C infrastructure (including hosting)
- Card trading websites/forums
- Money mules and mule handlers
- Operating cash-out infrastructure

FTR solutions

Challenges of Current Crime Types

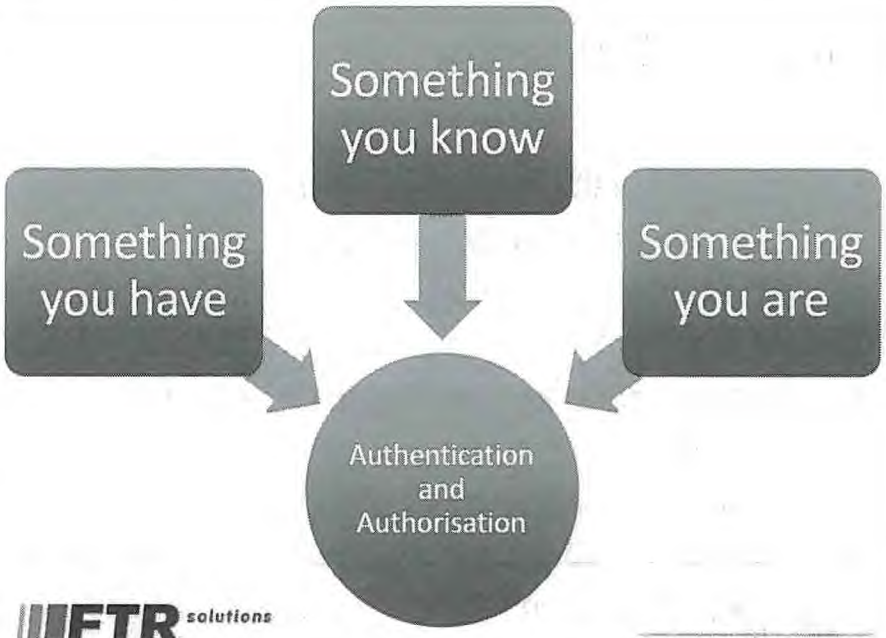
- Fraudsters arrested have relatively low influence on the criminal organisation.
- Criminal operations are organised from abroad.
- Many jurisdictions involved
- Jurisdiction where card data harvested almost never jurisdiction where stolen card data is used.
- Criminal infrastructure very difficult to locate and take down.
- Criminal actors most influential on the scale of crime often not directly involved in individual crimes (e.g. malware authors)

FTR solutions

EVOLUTION OF PAYMENT CARD SECURITY

Where are we going from here?

FTR solutions



FTR solutions

Key Security Features of Chip and PIN

- "Write only" cryptographic key storage.
- Negotiation of transaction security parameters between card and terminal (allows both issuers and acquirers to manage risk).
- Digital signing of transaction data.

FTR solutions

Security Concepts

- Communication between chip and terminal
  - Doesn't necessarily need a physical connection.
  - -> Contactless
- Cryptographic key stored in a "secure element"
  - Doesn't necessarily need to be a chip on a payment card.
    - -> Mobile payments

FTR solutions

Challenges Presented

- New technologies will inevitably lead to new challenges.
- Contactless:
  - Transaction relaying
  - Repudiation
- Mobile payments:
  - Mobile malware
  - Regulation of non-FI actors

FTR solutions

PINS

...and the problem with PINs.

FTR solutions

info@ftrsolutions.com | www.ftrsolutions.com

FTR solutions

info@ftrsolutions.com | www.ftrsolutions.com

PINs

- Typically 4-6 digit number.
- Rarely or never changes.
- Useful in the context of multiple transactions.
- Customers are very bad at protecting their PIN.
- Huge infrastructure and investment in the end-to-end protection of customer PINs.

FTR solutions

Alternatives to PINs

- Alternatives typically involve replacement of PIN with a single use "token" that authenticates or authorises an individual transaction. For example:
  - Two factor authentication
  - One time passwords
  - Transaction staging

FTR solutions

Biometrics

- "Something you are" instead of "Something you know".
- Technology exists and is widely deployed in some parts of the world.
- Significant data protection and privacy challenges to the use of biometric identifiers.
- Customers do not like biometrics.

FTR solutions

MICROPAYMENTS

FTR solutions

What are Micropayments

- Tiny payments (e.g. for purchases of EUR0.99) that have not traditionally been carried out using electronic payment infrastructure.
- Developing a viable business around these types of payments represents a unique challenges for the payment industry.
- Specifically, transaction fees represent a significant percentage of the total transaction

FTR solutions

Micropayments

- Most micropayment brokers involve creation and management of some form of account (e.g. PayPal).
- Transactions are aggregated over a period of time so that a single, larger, transaction can be applied to a payment card.
- Additional layers of fraud management are often applied in these cases.

FTR solutions

Challenges

- Regulation of micropayment service providers.
- Cross-jurisdictional issues
- Cooperation of large multinational corporations in local investigations.
- Potentially significant investigative burden for what may appear to be very low value crime.

FTR solutions

VIRTUAL CURRENCIES

FTR solutions

Virtual Currencies

- Extensively discussed already.
- Simultaneously a huge opportunity and a huge challenge.
- Currently, regulatory hurdles are preventing widespread adoption.
- However, various avenues for the use of virtual currencies are being actively investigated by a large range of financial institutions.

FTR solutions

Thank You! Any Questions?

Dave O'Reilly
Chief Technologist
FTR Solutions

+353 (87) 231 3257
dave.oreilly@ftrsolutions.co
m

FTR solutions

Federico Paesano

Federico Paesano

Federico Paesano graduated from the Military Academy of the Guardia di Finanza in L'Aquila (Italy) and holds a Master of Business Administration degree from the Università degli studi del Molise (Italy). For fourteen years, he worked for the Italian Financial Police, ending his career as Chief Investigator, leading and conducting judicial and financial investigations, focusing in particular on economic crimes such as corruption and money laundering.

Since July 2009, he was seconded by the Italian Government to the European Union Police Mission in Afghanistan (EUPOL) as Mentor to the Minister of Interior on Anticorruption: as part of a group of experts, he provided technical advice on transparency and accountability measures to the Minister of Interior as well as advice on the development of national and sector policies, collaborating closely with the AGO, the High Office of Oversight, the Supreme Court of Afghanistan and other external partners.

Federico joined the International Centre for Asset Recovery as Senior Financial Investigations Specialist in 2010, delivering technical training programmes on financial investigations and asset recovery in South America, Africa, Asia and Europe.

Cryptocurrencies and block chain technologies

INTERNATIONAL CENTRE FOR
ASSET RECOVERY

federico.paesano@baselgovernance.org

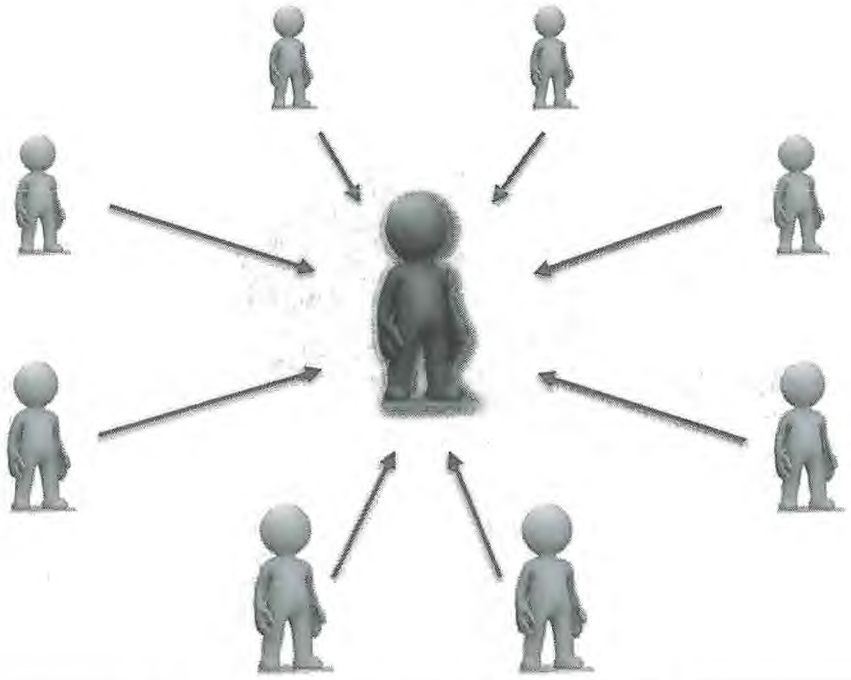
2010s Internet of things & blockchain technologies

1. Technology
2. Regulations
3. Asset Recovery

Centralised
vs.
Decentralised

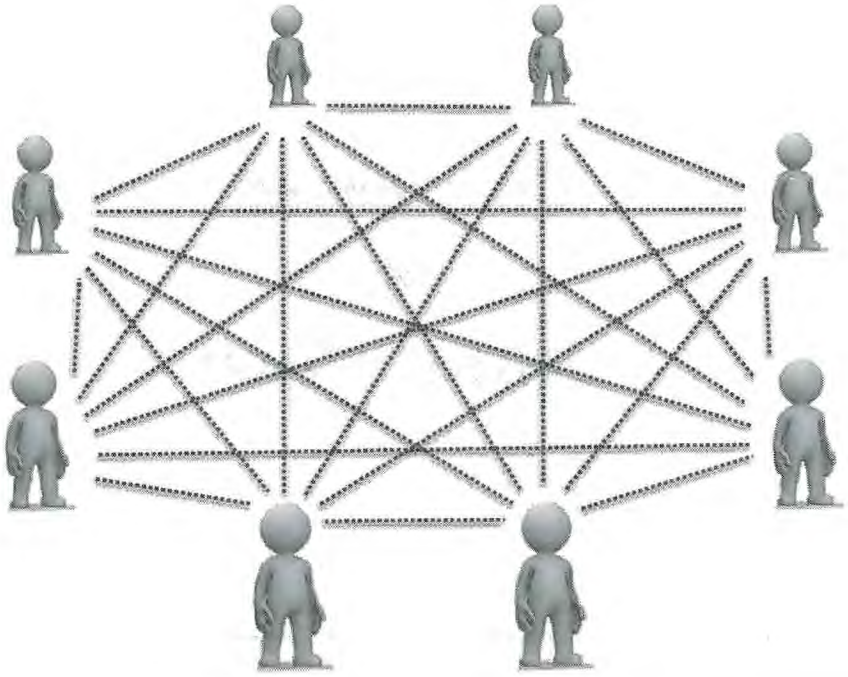
1 Technology

Centralised system



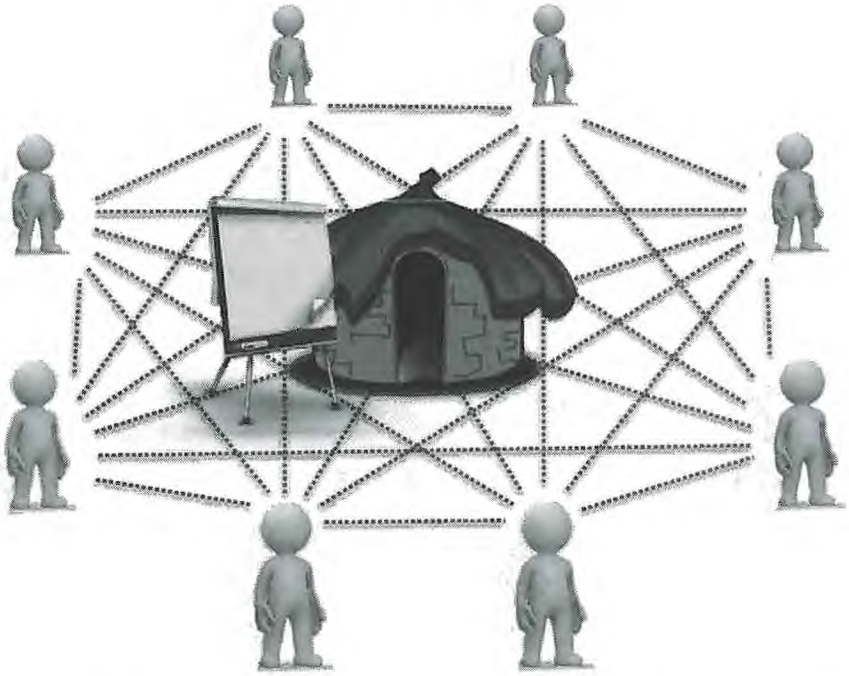
1 Technology

Decentralised system



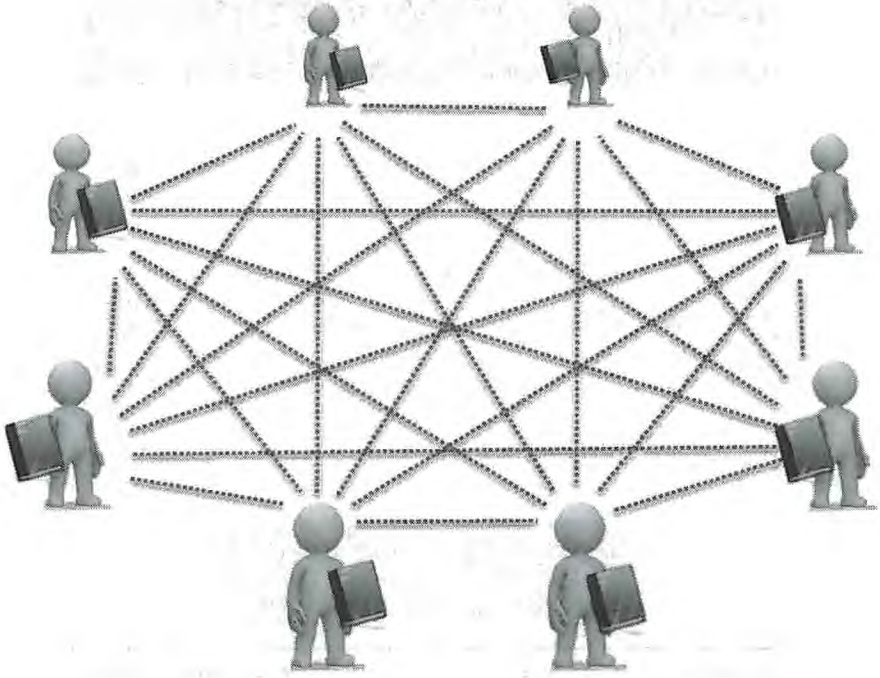
1 Technology

Decentralised Money



1 Technology

Decentralised Money



1 Technology

2 Regulations

3 Asset Recovery

Federico Paesano | 2015

blockchain

Alice: 10 - Bob 10 - Charlie 5 - David 15

Alice sends 5 to Bob

David sends 5 to Charlie

Alice sends 5 to Charlie

Bob sends 10 to David

David sends 10 to Bob

Bob sends 5 to Edward

David sends 5 to Edward

Edward sends 5 to Alice...

Edward sends 10 to David

Edward sends 5 to David

1 Technology

Decentralised Money

1FFyCP3m7fX7fQAdw4r3Cm5ggBBvYM44Mx

1NKD8CzGBJRMPCHCzhuy3CFzgy3RK5JCX5

Transaction:

1FFyCP3m7fX7fQAdw4r3Cm5ggBBvYM44Mx
sends **1,50** to
1NKD8CzGBJRMPCHCzhuy3CFzgy3RK5JCX5

1 Technology

Decentralised Money

Transaction View information about a bitcoin transaction

46d012ba9a557926581 4ff3609226283bfaa206efaaf9f956fe31314de42f34d

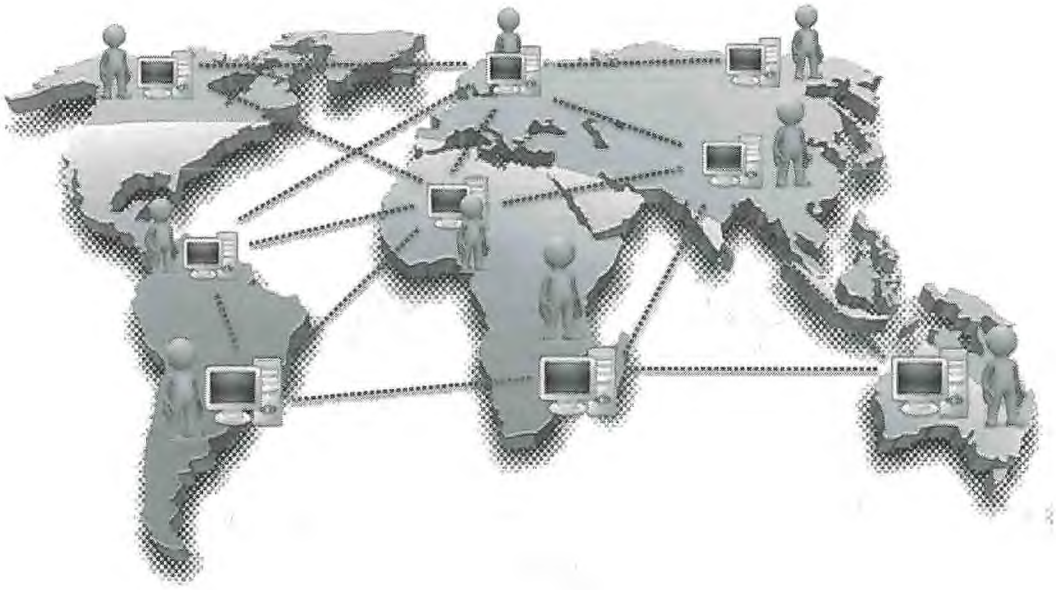
17nPMuxSMqCc3nq9jjFpxBt258u3nfqywW → 14Rm4c94MLiDUFCJSrZ4MRV2KEGHGNNLkA 2 BTC

1 Confirmations 2 BTC

Summary		Inputs and Outputs	
Size	223 (bytes)	Total Input	2 BTC
Received Time	2014-11-06 20:30:13	Total Output	2 BTC
Included In Blocks	328858 (2014-11-06 20:35:52 +6 minutes)	Fees	0 BTC
Confirmations	1 Confirmations	Estimated BTC Transacted	2 BTC
Relayed by IP	98.212.196.147 (whois)	Scripts	Show scripts & coinbase
Visualize	View Tree Chart		

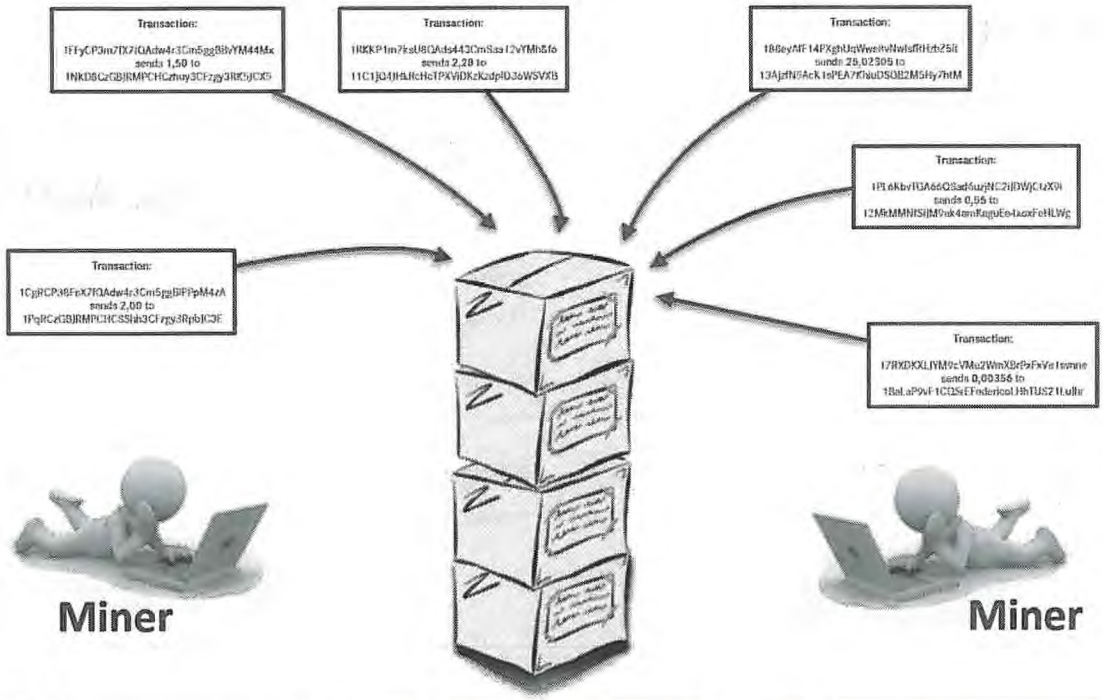
1 Technology 2 Implications 3 Asset Recovery

Decentralised Money



1 Technology 2 Implications 3 Asset Recovery

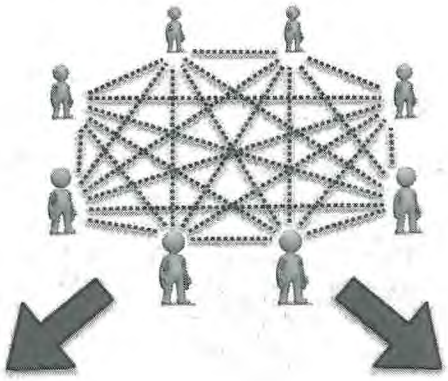
Decentralised Money



1 Technology

Federico Paesano | 2015

Decentralised system



No Bitcoin™

No Bitcoin Ltd.

No Bitcoin CEO

No Mr. Bitcoin

Who must report?

Mint

Sender/receiver

Bank

Clearing house

1 Technology

Federico Paesano | 2015

Identified players

Users

Miners

Banks

Exchanges

Money transmitters

1 Technology

2 Regulations

3 Asset Recovery

NEW YORK STATE

DEPARTMENT OF FINANCIAL SERVICES

PROPOSED

NEW YORK CODES, RULES AND REGULATIONS

TITLE 23. DEPARTMENT OF FINANCIAL SERVICES

CHAPTER I. REGULATIONS OF THE SUPERINTENDENT OF FINANCIAL SERVICES

PART 200. VIRTUAL CURRENCIES

Section 200.1 Introduction
Section 200.2 Definitions
Section 200.3 License
Section 200.4 Application
Section 200.5 Application fees
Section 200.6 Action by superintendent
Section 200.7 Compliance
Section 200.8 Capital requirements
Section 200.9 Custody and protection of customer assets
Section 200.10 Material change to business
Section 200.11 Change of control; mergers and acquisitions
Section 200.12 Books and records
Section 200.13 Examinations

- Identifies roles
- Identifies **obliged** Entities
- Identifies **exempted** Entities
- List obligations
- List violations

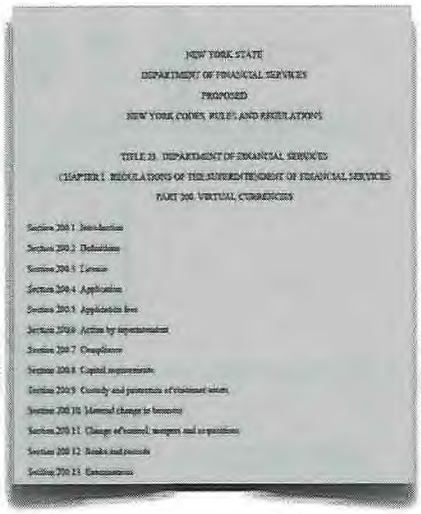
1 Technology

2 Regulations

3 Asset Recovery

Identified players

- Users
- Miners
- Exchanges
- Money transmitters
- Banks


NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
PROPOSED
NEW YORK CODES, RULES AND REGULATIONS

TITLE 23. DEPARTMENT OF FINANCIAL SERVICES
CHAPTER I. REGULATIONS OF THE SUPERINTENDENT OF FINANCIAL SERVICES
PART 200. VIRTUAL CURRENCIES

Section 200.1 Introduction
Section 200.2 Definitions
Section 200.3 License
Section 200.4 Application
Section 200.5 Application fees
Section 200.6 Action by superintendent
Section 200.7 Compliance
Section 200.8 Capital requirements
Section 200.9 Custody and protection of customer assets
Section 200.10 Material change to business
Section 200.11 Change of control; mergers and acquisitions
Section 200.12 Books and records
Section 200.13 Examinations

1 Technology | 2 Regulations | 3 Asset Tokenizing

Requirements

- Amount involved (in fiat and digital currency)
- Date of the transaction and exact time
- Additional payment instructions or comments
- Full identification of parties
- Report transaction(s) > 10.000 USD/day/customer

1 Technology | 2 Regulations | 3 Asset Tokenizing

BITSTAMP

Home Account Buy / Sell Order book Deposit Withdrawal

- About Us
- News
- Fee Schedule
- Terms Of Use
- Privacy Policy
- AML Policy
- Cookie Statement
- Risk Warning

BITSTAMP'S NEW VERIFICATION REQUIREMENTS

BITCOIN IS REAL MONEY

Bitcoin is growing rapidly. Governments are taking notice and even starting to acknowledge Bitcoin as real money.

BITSTAMP IS PROACTIVE ABOUT COMPLIANCE

To ensure reliable, uninterrupted service Bitstamp has been working hard towards greater compliance with the relevant regulations which apply in the financial world. As such, Bitstamp takes a proactive approach with its compliance efforts to prevent money laundering.

BITSTAMP RESPECTS CUSTOMER PRIVACY

Bitstamp continues its policy of diligently protecting its customers privacy.

NEW VERIFICATION REQUIREMENTS

Bitstamp's verification procedures are in accordance with high standards already adopted in today's financial world and assure Bitstamp's service providers as well as regulators. To be in line with financial standards, as of September 30th, 2013, bitcoin and bank transfers will only be available to verified customers.

1 Technology 2 Regulations 3 Asset Exchanges

Federico Paesano | 2015

Analytical tools

1 Technology 2 Regulations 3 Asset Exchanges

www.blockchain.info

Federico Paesano | 2015

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary		Transactions	
Address	1FKcouJP2KaiZTPAreVwSHUfj7z6pBEPV2	No. Transactions	5
Hash 160	0d1720cc0f6ebce3a76b55cb6e0d2b2c83d9d124	Total Received	750 BTC
Tools	Taint Analysis - Related Tags - Unspent Outputs	Final Balance	250 BTC

Request Payment | Donation Button

Transactions (Oldest First) — Filter

1de94b02066e041ec5b089de7e02190a94f2fd94309c41f37900e79ffb9b27ef			2014-11-06 20:32:56
1FKcouJP2KaiZTPAreVwSHUfj7z6pBEPV2	→	1JPdRJS9KgMGYxyu2q4oY48QKvGxArpDmE 1DG3bYoNYDhVUWYsmzPKZstyKSRfN5gyF	175 BTC 75 BTC 1 Confirmations -250 BTC
11d5dec86e6637357f85e060ebece6697e72e69d39fe070d7e37c0051e77ce0			2014-11-06 15:20:37
1FKcouJP2KaiZTPAreVwSHUfj7z6pBEPV2	→	1bazSPF4CxTEnqR4uaVKDycKaLArWY7CAK 1J6ta7ajevk2JKNyGUCVwDuj67hfiEbYJF	102.941 BTC 147.059 BTC 32 Confirmations -250 BTC
6be828b87a44d578f4a0da6b4312a6cd97341f91111732fa0d66c6b2f20ca7cee			2014-10-29 21:41:16
17RbbBnbCwz2cN4bcA1uFe592YzrkxVLZS 1C1qLXg3VpnQxwU58KP7WZKUVjQRR9zZd	→	1FKcouJP2KaiZTPAreVwSHUfj7z6pBEPV2	250 BTC -250 BTC

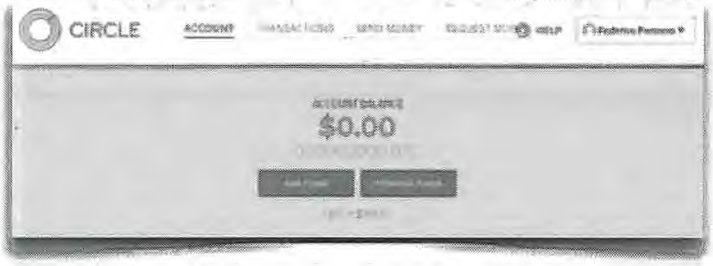
1 Technology | 2 Regulations | 3 Market Regulation

Analytical tools

Extracting Intelligence from the Bitcoin Network
bitiodine.net - Michele Spagnuolo

1 Technology | 2 Regulations | 3 Market Regulation

The "physical" world



1 Technology

2 Regulations

3 Asset Recovery

Risk of over-regulation

1 Technology

2 Regulations

3 Asset Recovery

Re-thinking Asset Recovery

NEWS • SILK ROAD NEWS

FBI proves seizing bitcoins isn't the same as owning them

Daniel Cawrey (@danielcawrey) | Published on October 30, 2013 at 15:00 BST

* http://www.coindesk.com/fbi-proves-seizing-bitcoins-isnt-owning/

Re-thinking Asset Recovery

= 1KsngpmcxXw6b6RkXVBmDpUepzKtb968EE

Public Key

= 5Kb8kLf9zgWQnogidDA76MzPL6TsZZY36hWXMssSzNydYXYB9KF

Private Key

* http://www.coindesk.com/fbi-proves-seizing-bitcoins-isnt-owning/

Re-thinking Asset Recovery

29.600 BTC + 144.000 BTC "seized"

Controlled Bitcoin addresses

* Ross Ulbricht is currently in New York's Detention Center, awaiting a trial set to begin 3rd November.

FOR SALE
50,000 bitcoins

THIS SEALED BID AUCTION IS FOR A PORTION OF THE BITCOINS CONTAINED IN WALLET FILES THAT RESIDED ON CERTAIN COMPUTER HARDWARE BELONGING TO ROSS WILLIAM ULBRICHT, THAT WERE SEIZED ON OR ABOUT OCTOBER 24, 2013 ("COMPUTER HARDWARE BITCOINS").

6 November 2014

3 Asset Recovery

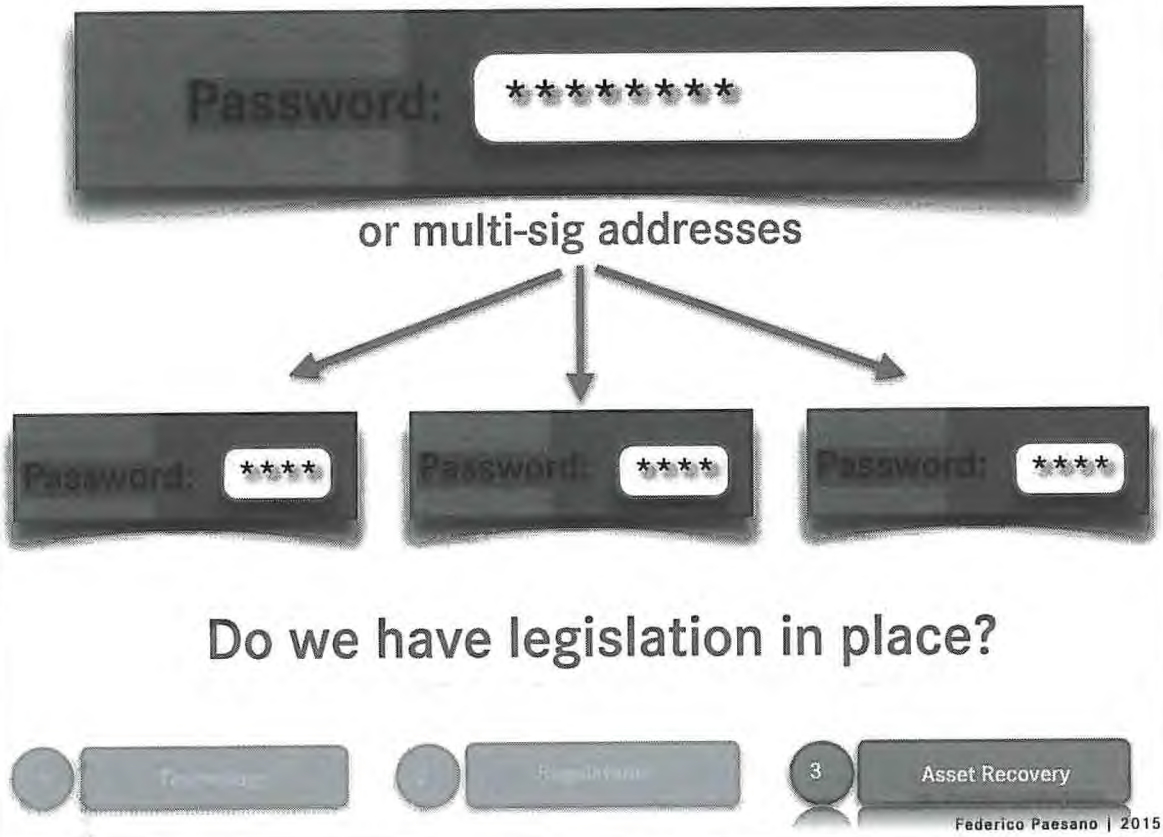
http://www.fbi.gov/newyork/press-releases/2014/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court

Operation "Onymous"

- Countries involved: Bulgaria, the Czech Rep., Finland, France, Germany, Hungary, Ireland, Latvia, Lithuania, Luxembourg, the Netherlands, Romania, Spain, Sweden, Switzerland, UK and USA
- 17 arrests
- 27 websites (narcotics, fake credit cards, IDs and money)
- Hardware and digital media seized
- Cash and bitcoins seized

3 Asset Recovery

http://www.eurojust.europa.eu/press/PressReleases/Pages/2014/2014-11-07.aspx



federico.paesano@baselgovernance.org