

1<sup>st</sup> Anti-Finter online webinar  
July 6<sup>th</sup>, 2022

# Anti-FinTer

Versatile artificial intelligence investigative technologies for revealing online cross-border financing activities of terrorism

**Dr. Asterios Leonidis**

Institute of Computer Science (ICS)  
Foundation for Research and Technology – Hellas (FORTH)

**Ass. Prof. Georgios Th. Papadopoulos**

Harokopio University of Athens (HUA)  
Anti-FinTer Technical Manager



This project has received funding from the European Union's Horizon 2020 – Coordination and support action under the Grant Agreement No. 101021669

# Contents

- Anti-FinTer '**follow-the-actor**' financial investigation strategy for online terrorism financing
- Use of **AI-empowered visual analytics** for boosting conventional financial investigations



# Basic project info

- **Anti-FinTer:** Versatile artificial intelligence investigative technologies for revealing online cross-border financing activities of terrorism
- Program: ISFP-2020-AG-TERFIN
- Topic: Countering terrorist financing associated with activities in the Dark Web, crypto-assets, new payment systems and darknet marketplaces
- Duration: 2 Years (January 2022 – December 2023)
- Consortium: 10 Partners



This project has received funding from the European Union's ISFP-2020-AG-TERFIN program under the Grant Agreement No. 101036262

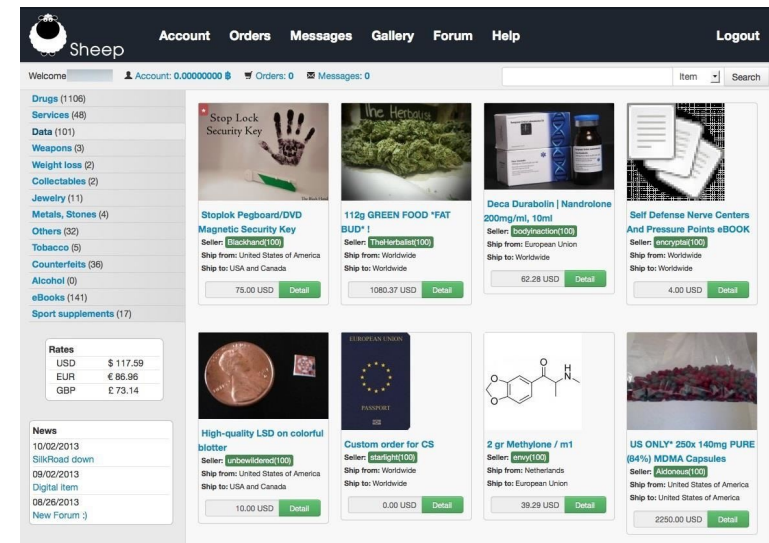
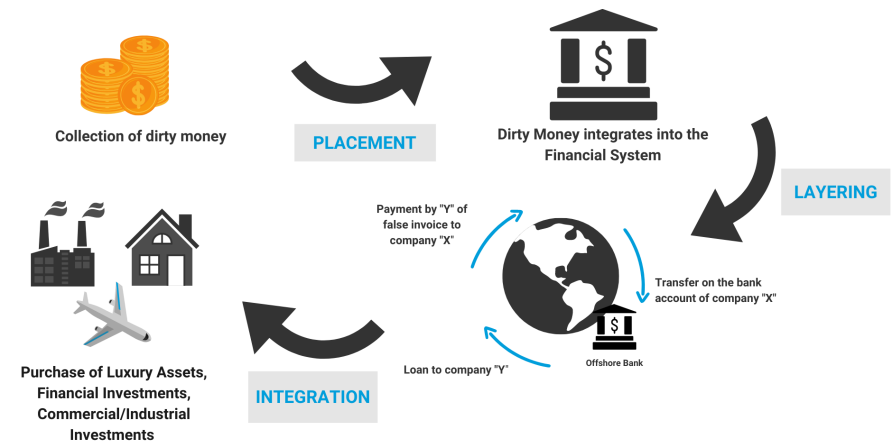
# Problem statement

“Some EU countries are among the best in the world at implementing technical recommendations to combat money laundering ... only 1.1 percent of estimated illicit proceeds are seized by authorities.”

Source: *POLITICO: The world's dirty money by the numbers, May 19, 2020*

“Despite enforcement actions over the last six years that led to the shutdown of about half a dozen sites ... there are still close to 30 illegal online markets, according to DarknetLive...”  
(Source: *The New York Times: Dark Web Drug Sellers Dodge Police Crackdowns, June 11, 2019*)

## Money Laundering Cycle



# Problem statement

**“The hacking group created online platforms to sell user login credentials known as ‘combos’ ... project managers distributed subscriptions against cryptocurrency payments.”** (Source: *Europol press release: Hacker group selling databases with millions of user credentials busted in Poland and Switzerland, May 5, 2020*)



**“... the terrorism threats have continued to evolve ... funds flow cross-border to providing resources for nationally designated organizations, and many jurisdictions continue to suffer from persistent attacks from small cells and radicalized lone actors...”** (Source: *Financial Action Task Force (FATF): Terrorist Financing Risk Assessment Guidance, July 2019*)



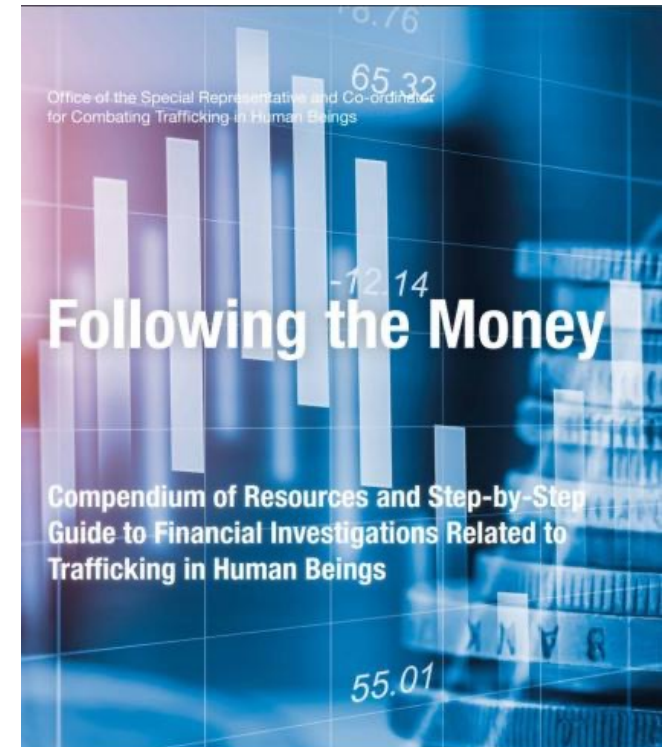
# Financial investigation strategy

- Goals of financial investigation
  - Analysis of the **origin** of the money/capital
  - Examination of how it has been **transferred**
  - Inspection of how it has been **used**



# Financial investigation strategy

- Currently established methodologies
  - **“Follow the money”** approach
    - ✓ Formalized and documented by “Organization for Security and Co-operation in Europe” (**OSCE**)
    - ✓ Fundamental principle: Tracking the **flow of money** will very likely lead to the detection and identification of the suspects behind the illicit activities



# Financial investigation strategy

- Currently established methodologies
  - Concept of “**parallel financial investigations**”
    - ✓ Introduced by “Financial Action Task Force” (**FATF**) ‘Recommendation 30’
    - ✓ Basic conceptualization: Conducting a financial investigation alongside, or in the context of, a (traditional) **criminal investigation** into money laundering, terrorist financing and/or predicate offence(s)



# Financial investigation strategy

- Proposed “follow the actor” approach

## ➤ Key observations

- ✓ Reported by Europol in “Internet Organised Crime Threat Assessment” (IOCTA) ‘21
- ✓ Tendency of Organized Crime Groups (OCGs) to **fragment their business and activities**, in an attempt to confront LEAs operations
- ✓ Regarding Dark Web, OCGs maintain **multiple online profiles** (on multiple platforms), in order to operate as multiple distinct individuals rather than a single entity

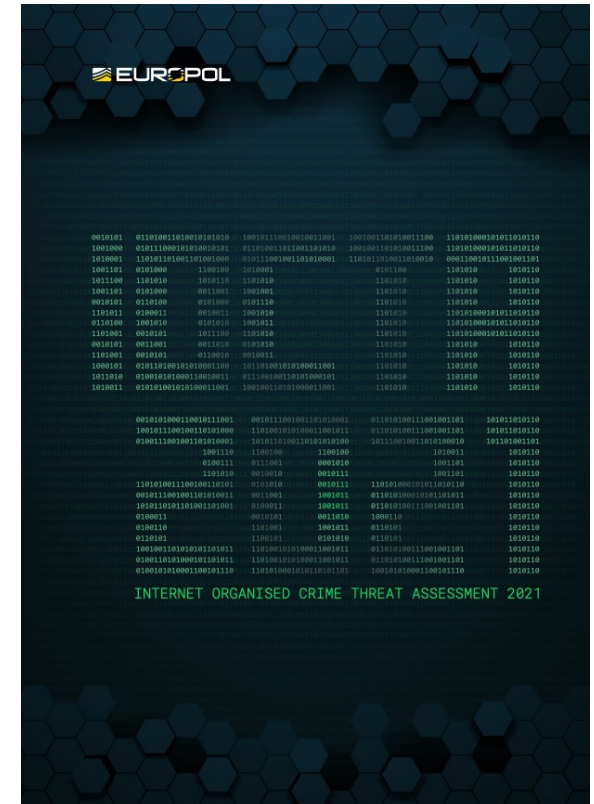


# Financial investigation strategy

- Proposed “follow the actor” approach

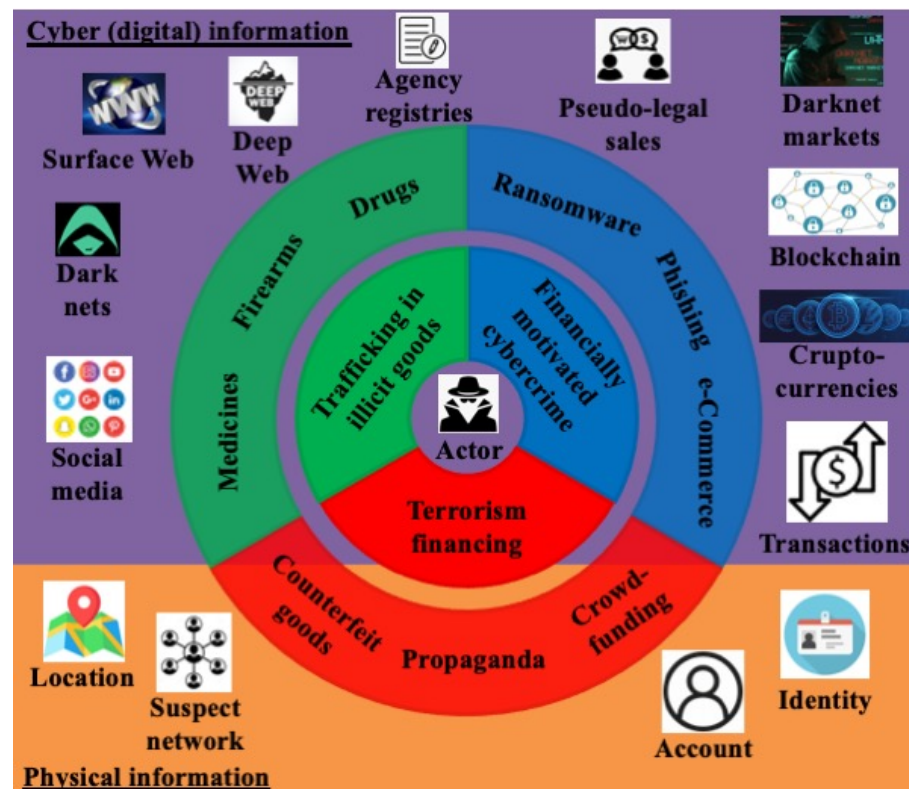
➤ Fundamental principle

- ✓ Focus on jointly analyzing **multiple financial investigations/cases** (of the same or different criminal activity areas), in order to reveal the identities of the exact same (group of) actors that are behind all these incidents



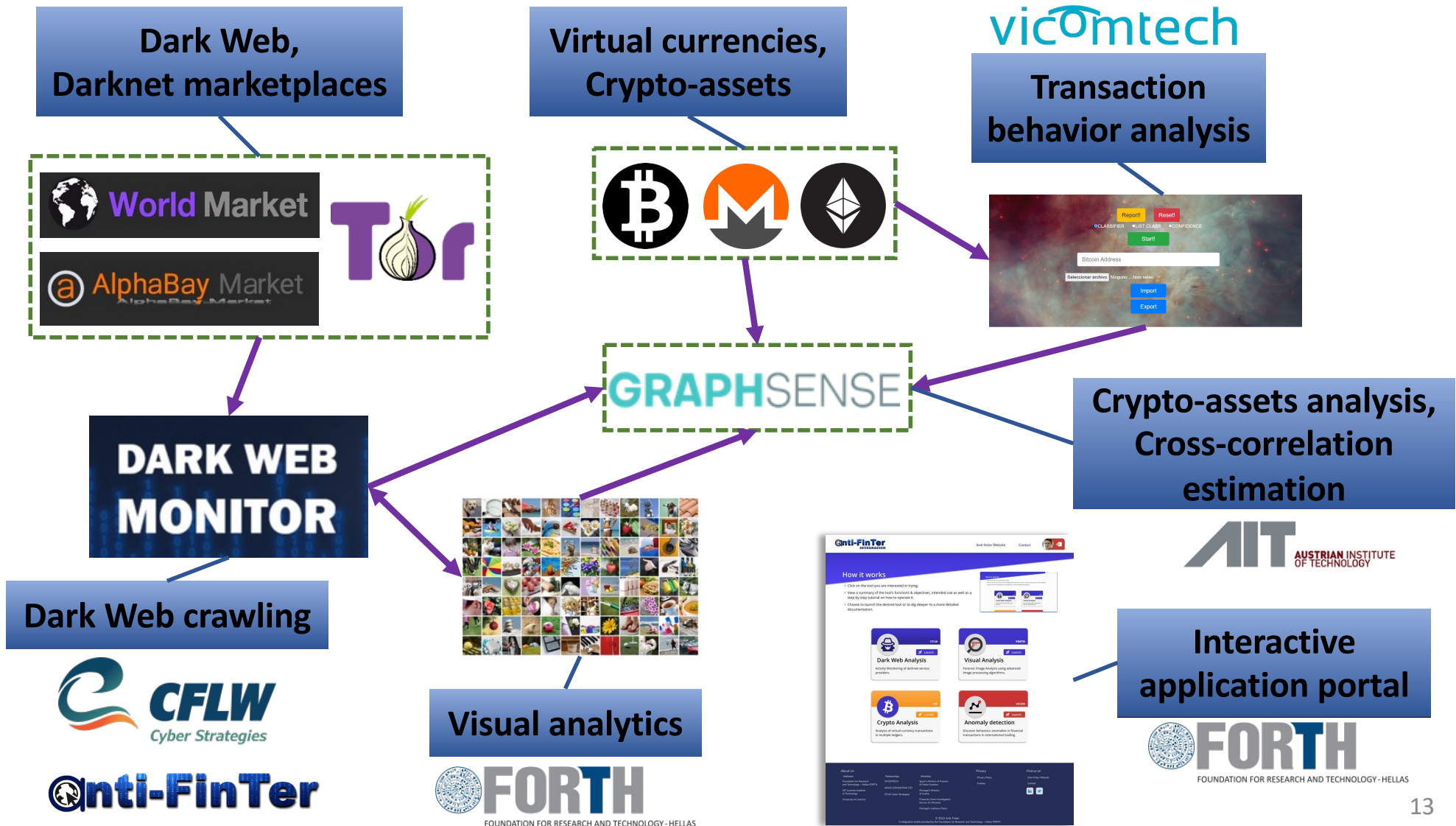
# Financial investigation strategy

- **Fundamental conceptualization** of the “follow the actor” strategy
  - Analyze **multiple** co-occurring and inter-related **crimes**
  - Investigate and cross-correlate **multiple/different application fields**



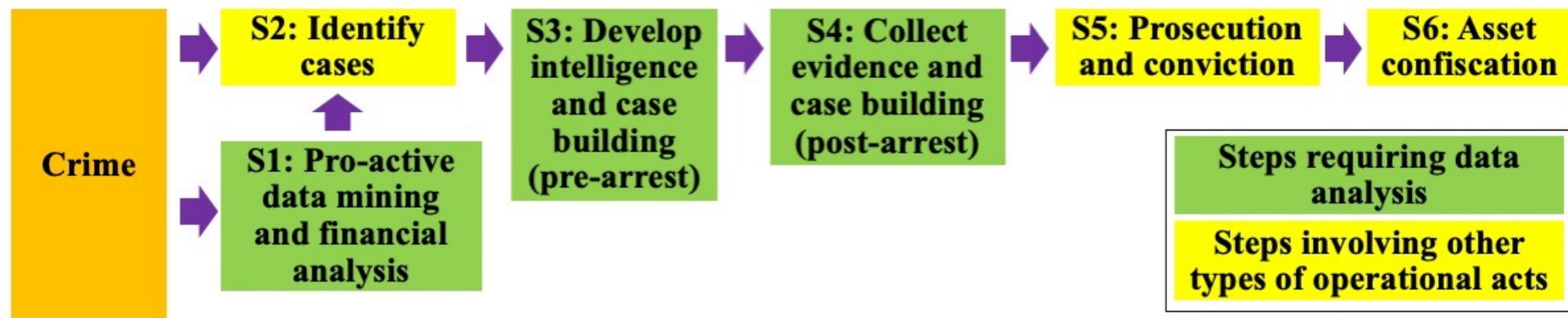
# Financial investigation strategy

- Overview of developed **AI-empowered technologies**

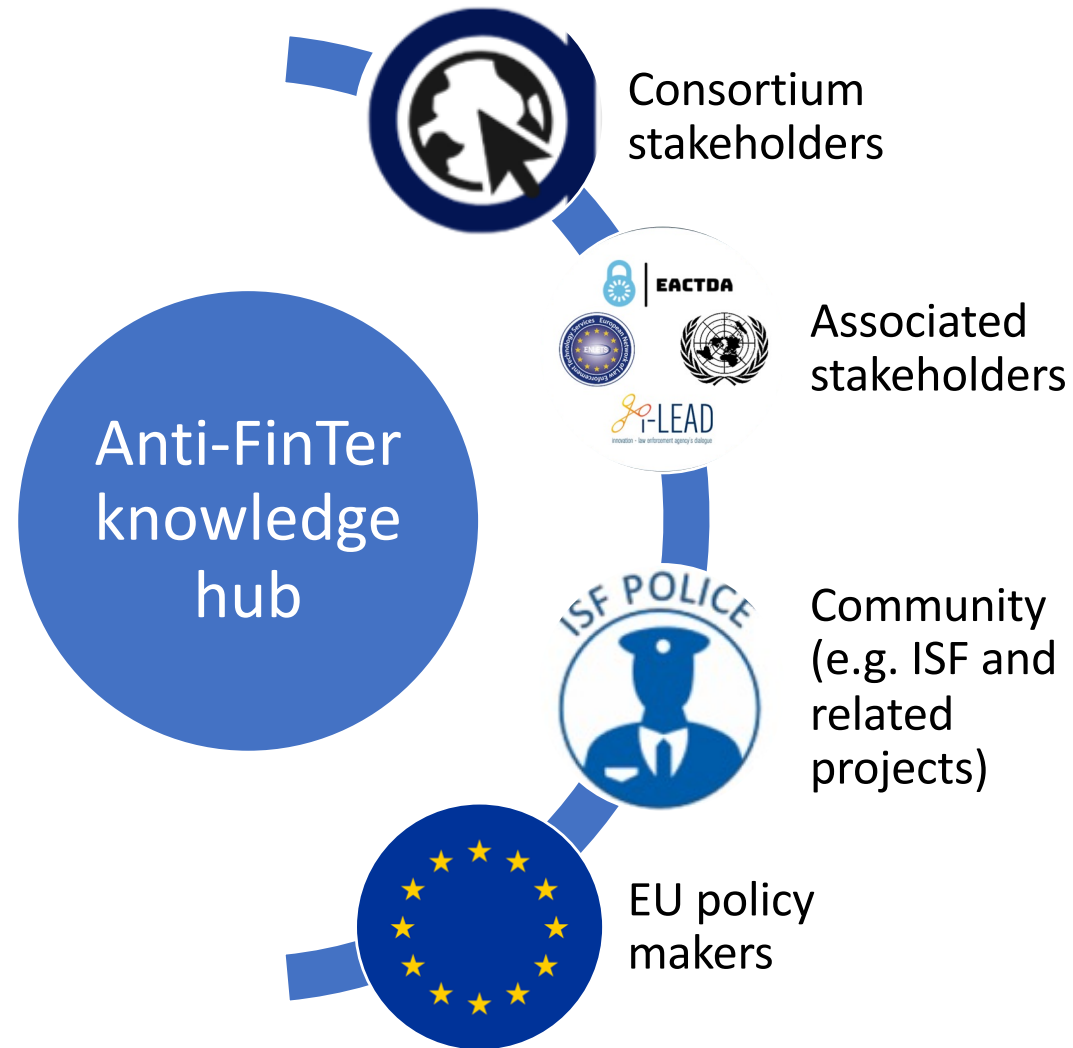


# Financial investigation strategy

- **Fundamental conceptualization** of the “follow the actor” strategy
  - Envisaged **operational methodology**



# Knowledge hub creation



# Consortium

Partner	Short Name	Country
AIT Austrian Institute of Technology GmbH	AIT	AT
IDRYMA TECHNOLOGIAS KAI EREVNAS	FORTH	EL
Fundacion Centro de Tecnologias de Interaccion Visual y Comunicaciones Vicomtech	VICOM	ES
University of Limerick	ULIM	IE
IANUS Consulting Ltd	IANUS	CY
CFLW Cyber Strategies BV	CFLW	NL
FINANSINIU NUSIKALTIMU TYRIMO TARNYBA PRIE VIDAUS REIKALU MINISTERIJOS	FCIS	LT
AGENCIA ESTATAL DE ADMINISTRACION TRIBUTARIA	AEAT	ES
Ministério da Justiça	MJPJ	PT
GLAVNA DIREKTSIA BORBA S ORGANIZIRANATA PRESTUPNOST	GDCOC	BG

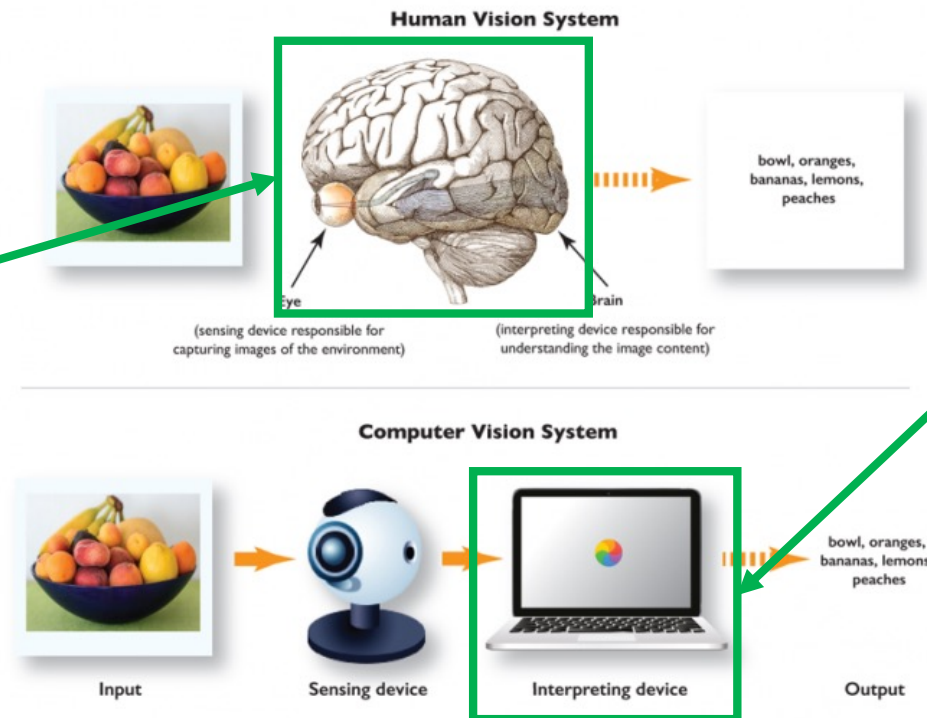


## AI-empowered visual analytics

# Visual analytics basics

- Goal: Creation of digital systems that can **process, analyze** and **make sense** of visual data (images or videos) in the same way that humans do
- Research aim: To **teach** computers to process and understand an image in a human compliant fashion

Makes use of knowledge structures learned from experience




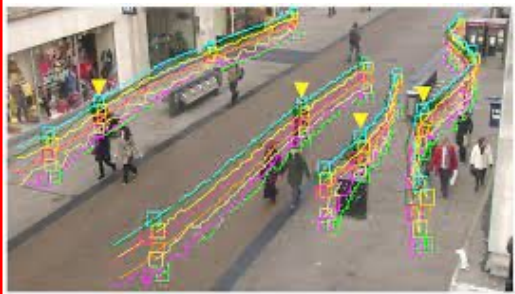
Based on AI modules learned from data

# Types of visual analytics

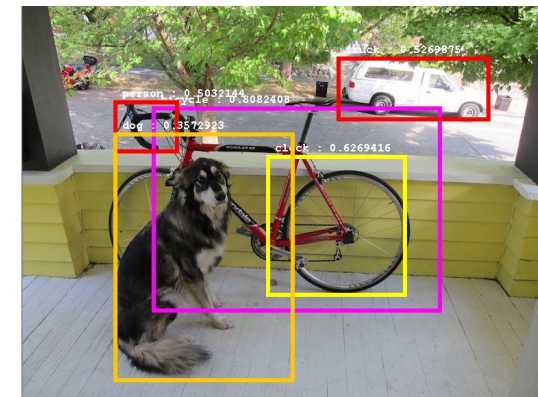
airplane  
automobile  
bird  
cat  
deer  
dog



Concept detection



Object tracking



Object detection



Semantic segmentation



Instance segmentation



A cute little dog sitting in a heart drawn on a sandy beach.



A dog walking next to a little dog on top of a beach.

Image captioning

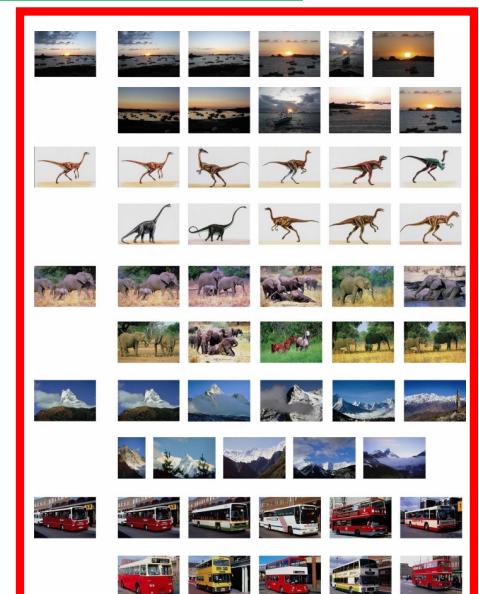


Image indexing



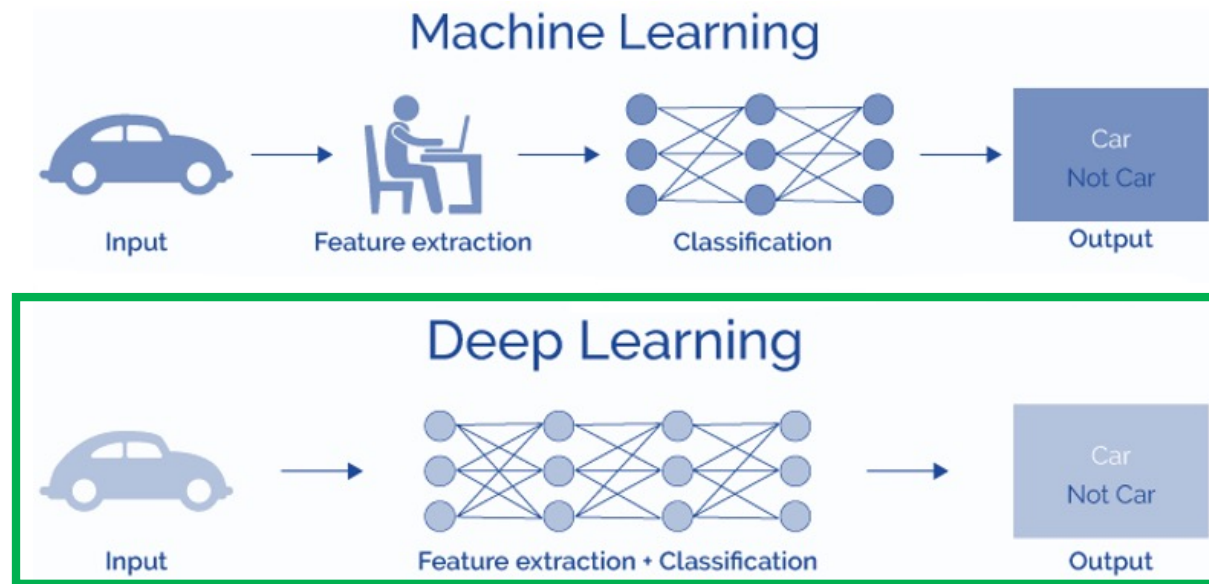
Social Distancing Violations: 15

Event detection

Investigated in Anti-FinTer

# AI technologies for visual analytics

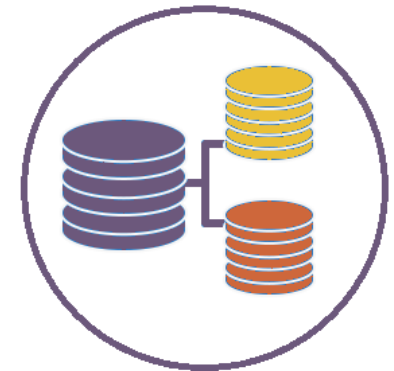
- Dominated by the so-called '**deep learning**' paradigm, i.e. the use of large-scale neural networks
  - Significantly outperforms all other types of machine learning techniques in all visual analysis tasks
  - An '**end-to-end**' engineering approach is followed
  - Demand of very **large training datasets**



Implementation of an 'end-to-end' approach

# Datasets formation

- Creation of an image dataset of **~9K annotated images**
- A list of **14 semantic concepts** defined related to terrorism financing activities on the Web
  - Different **types of criminal activities** have been considered: firearms trafficking, drugs trafficking, terrorist activities, etc.
  - Particular emphasis given to the analysis of content originating from **Dark Web** marketplaces and firearms trafficking
  - The concepts are by definition **visually meaningful**, i.e. they can be detected using visual content (images)



# Datasets formation

- List of currently supported **semantic concepts**
  - **Glock**: Popular Austrian handgun. Has a distinct design. Comes in many very similar models.
  - **Kalashnikov**: Popular rifle used by terrorists. Has a distinct design. Comes in many very similar models.
  - **RPG**: RPG-7 (rocket propelled grenade) or similar looking rocket launchers. Popular rocket launcher used by terrorists.
  - **Military knife**: Straight blade knives usually carried by soldiers.
  - **Weed**: Cannabis in large quantities.
  - **Cigarettes**: Cigarettes in large quantities. Not in boxes. Usually linked with terrorism funding.
  - **Pills**: Pills in large quantities.

# Datasets formation

- List of currently supported **semantic concepts**
  - **Powders**: Drugs in powder form in large quantities.
  - **Military Personnel**: Soldiers pictured in different climates.
  - **Counterfeit money**: American dollars in large quantities. Possibly linked with illegal trade.
  - **Grenade**: MK 2 NATO style grenades.
  - **Rover**: Common military vehicle that is primarily used to transport soldiers.
  - **Tank**: Heavy armored military vehicle. Regularly appearing in propaganda sites.
  - **Revolver**: Handguns that use a revolving cylinder containing multiple chambers for firing. Popular even today. Often sold in legal and illegal gun auction sites.

# Datasets formation

- Exemplary images of the defined semantic concepts



Glock



Kalashnikov

# Datasets formation

- Exemplary images of the defined semantic concepts



RPG



Military knife

# Datasets formation

- Exemplary images of the defined semantic concepts



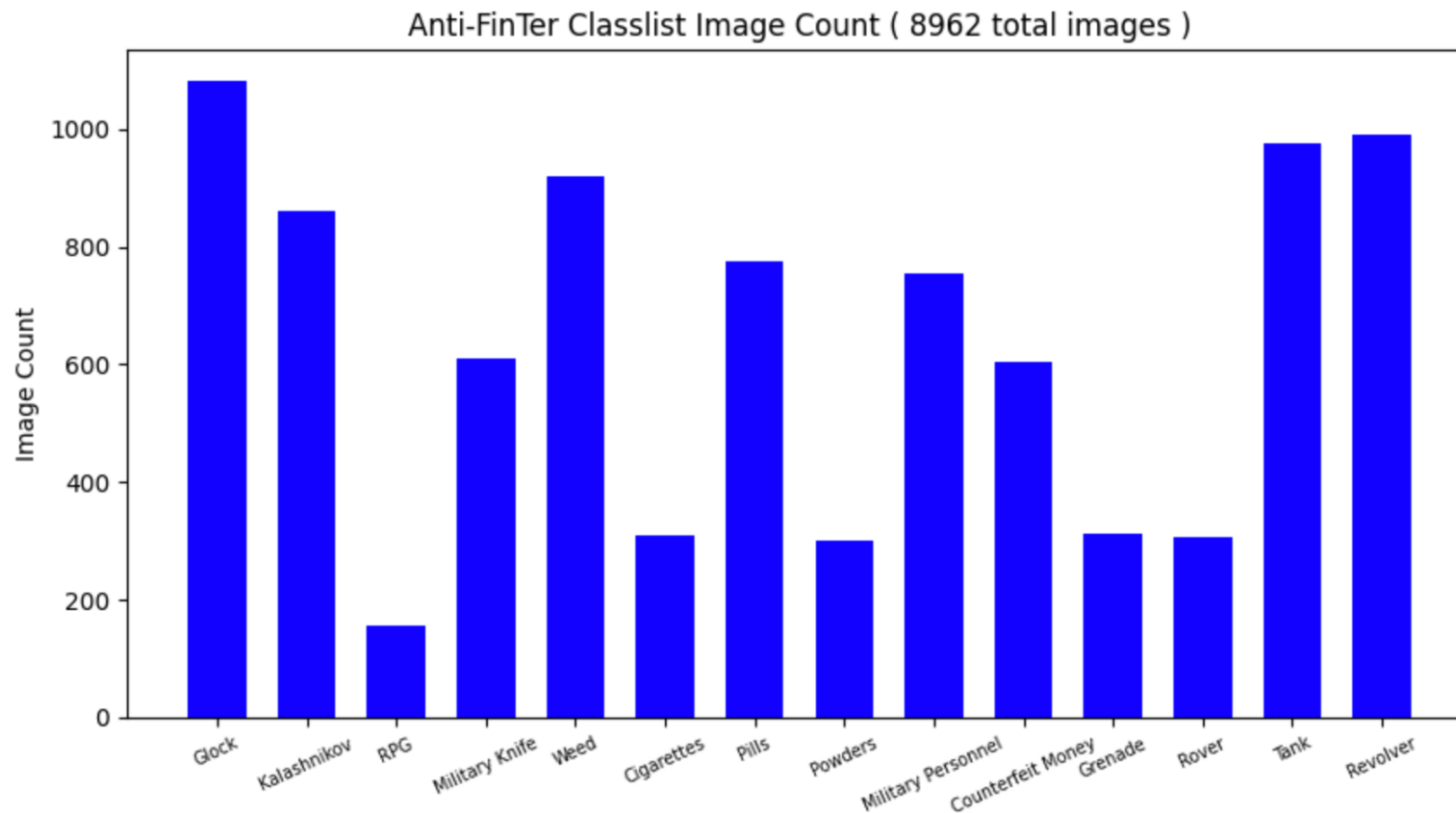
Weed



Cigarettes

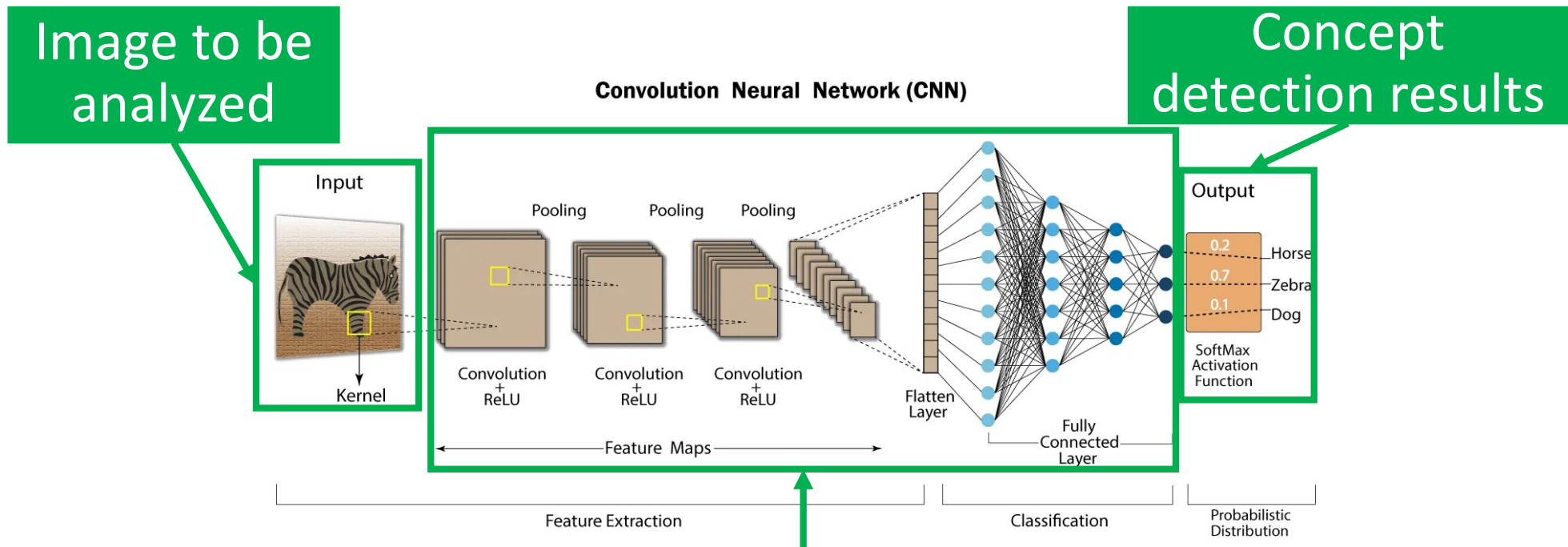
# Datasets formation

- Annotated dataset statistics



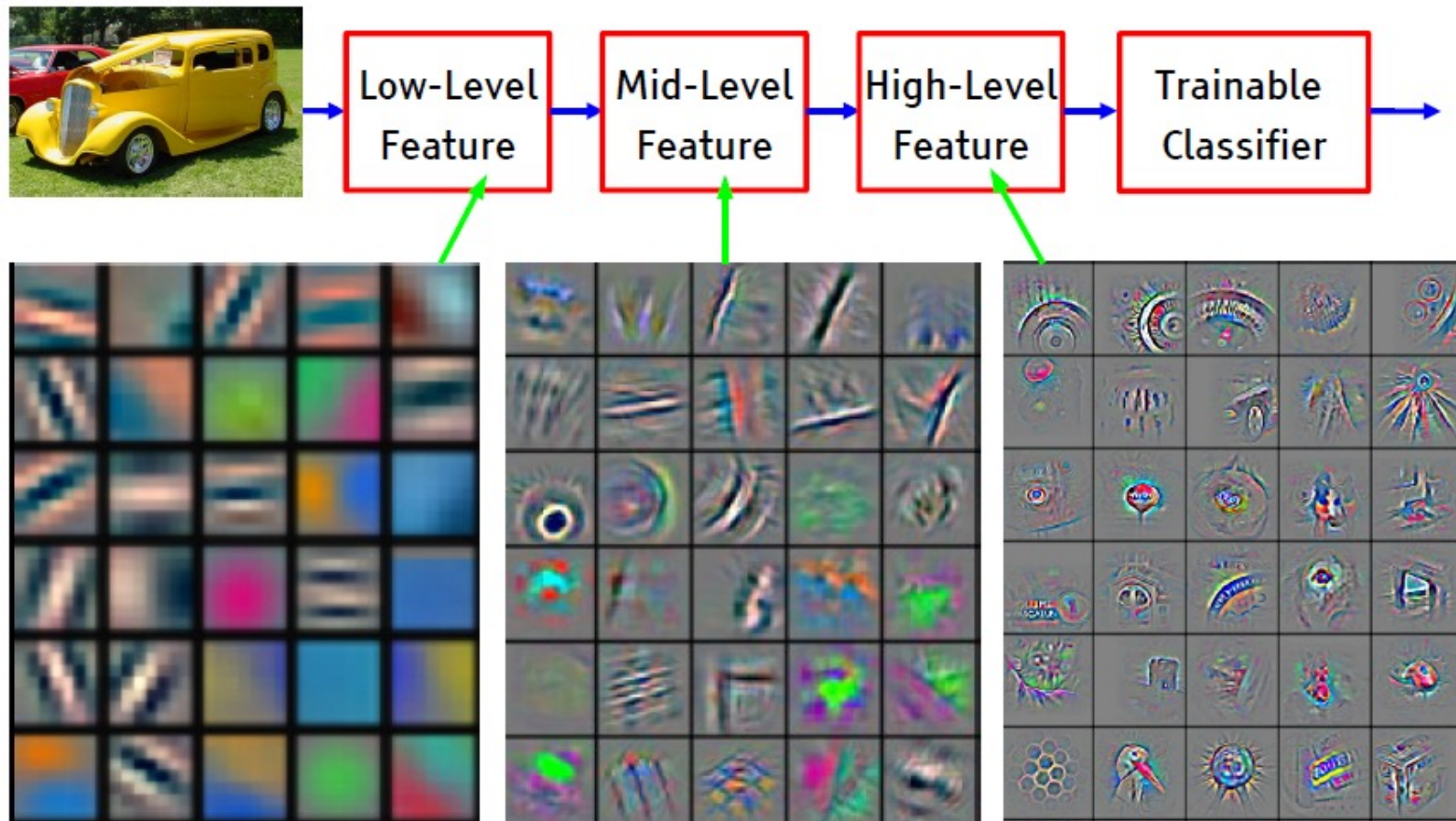
# Concept detection

- Aim: To automatically identify the presence of **high-level semantic concepts** of interest in the examined images
  - Deployment of suitable **deep learning** architectures
  - Evaluation of various types of **neural networks**: Inception ResNet v2, Inception v4, NasNet, AlexNet, VGG16, DenseNet



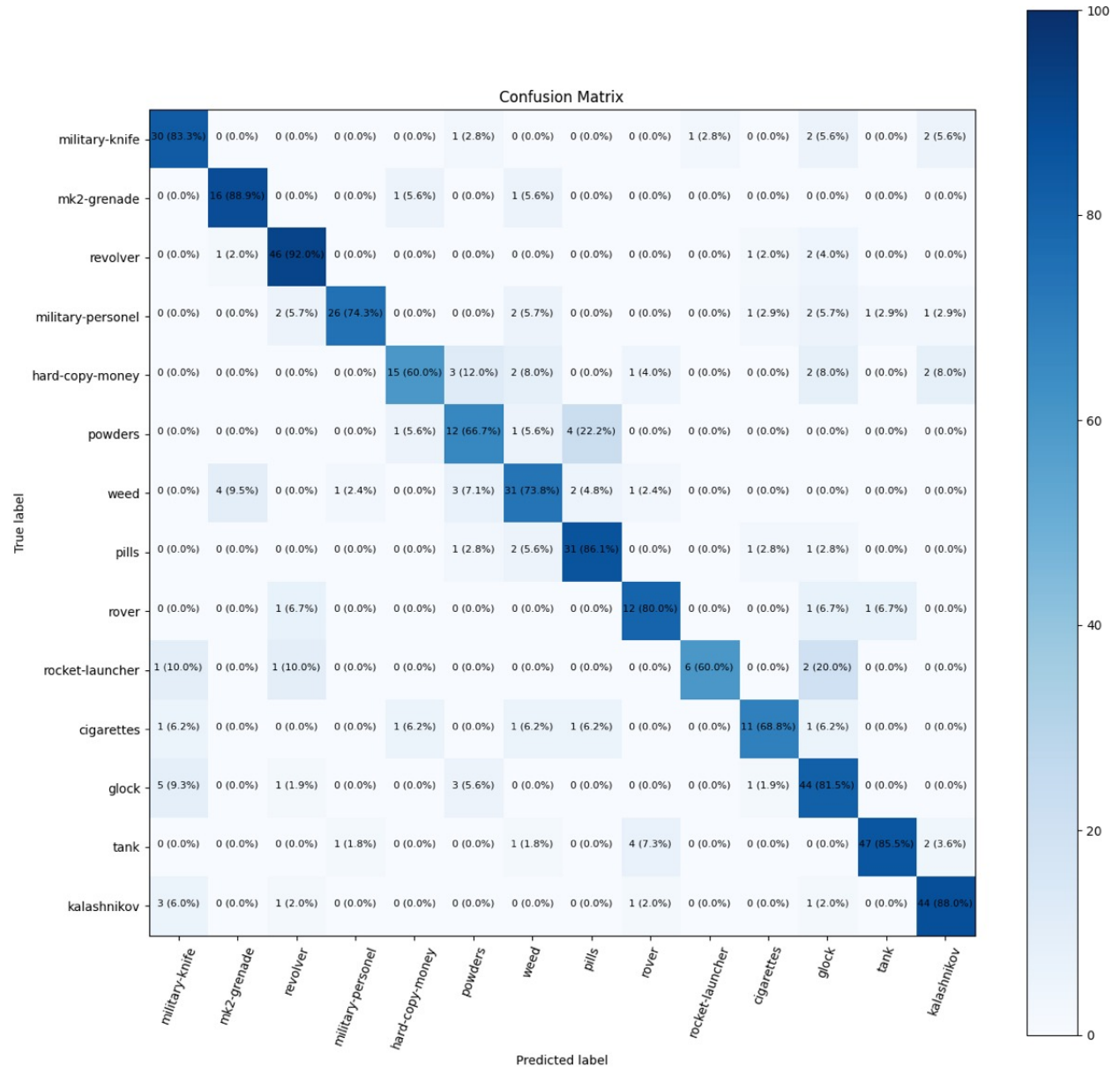
# Concept detection

- Neural networks gradually learn concepts of **increasing complexity**



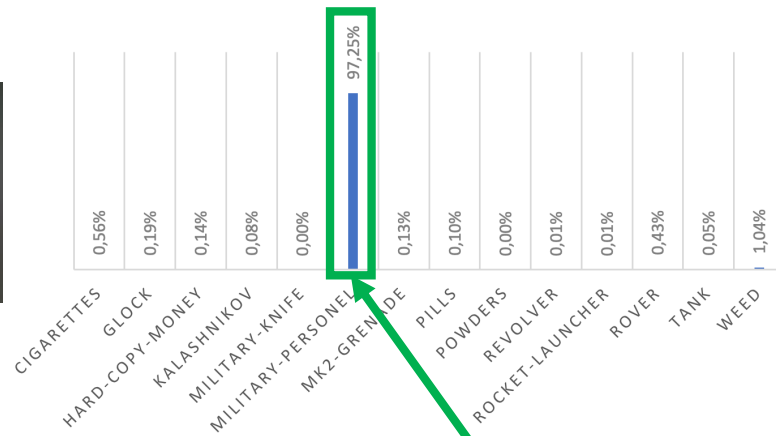
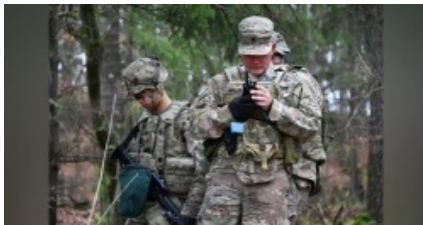
# Concept detection

- Achieved results
  - Indicative quantitative concept detection results

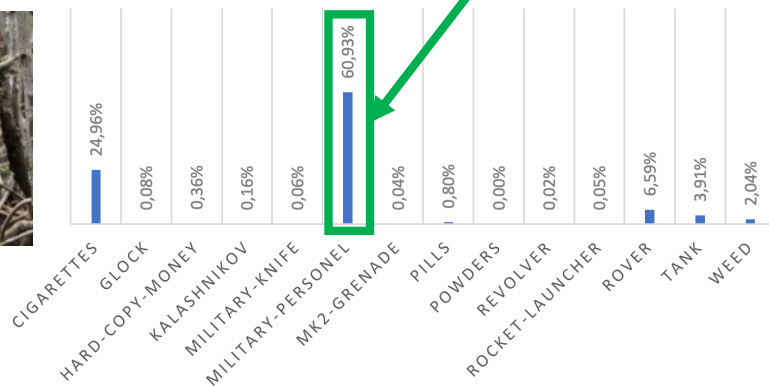
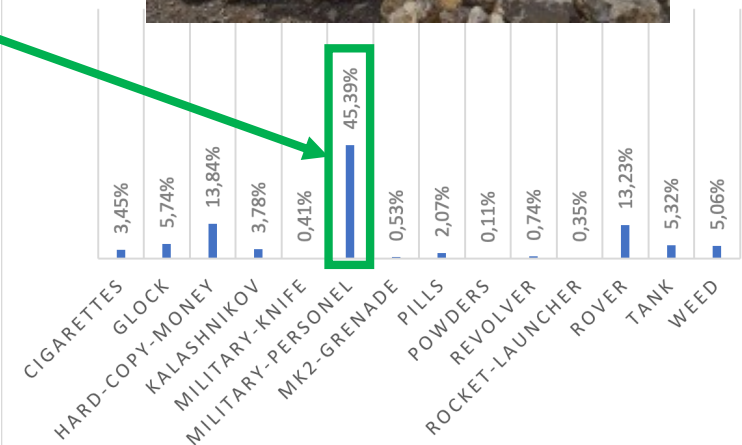


# Concept detection

- Achieved results:** Indicative qualitative concept detection results

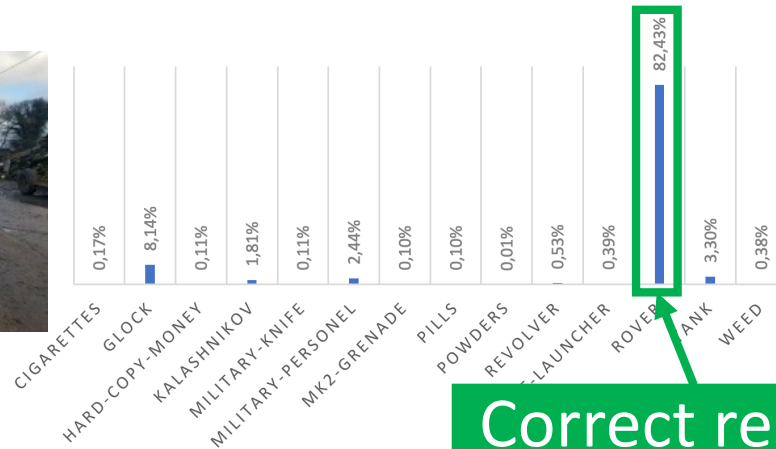


Correct results

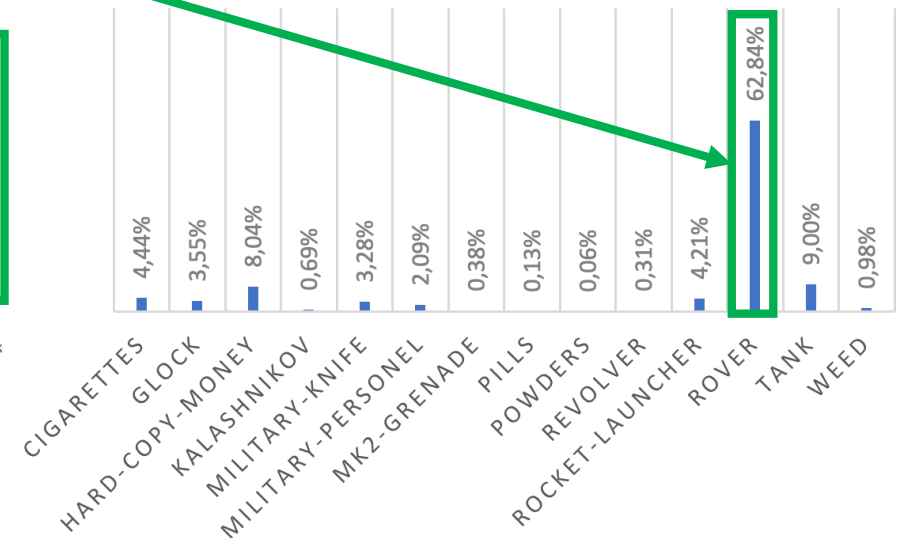
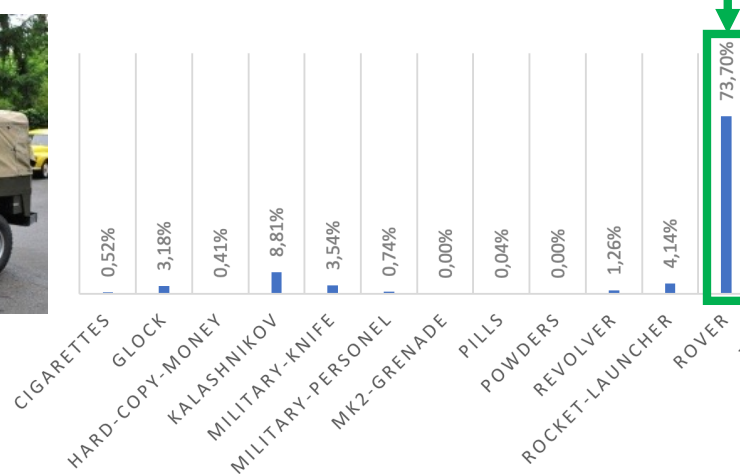


# Concept detection

- Achieved results:** Indicative qualitative concept detection results

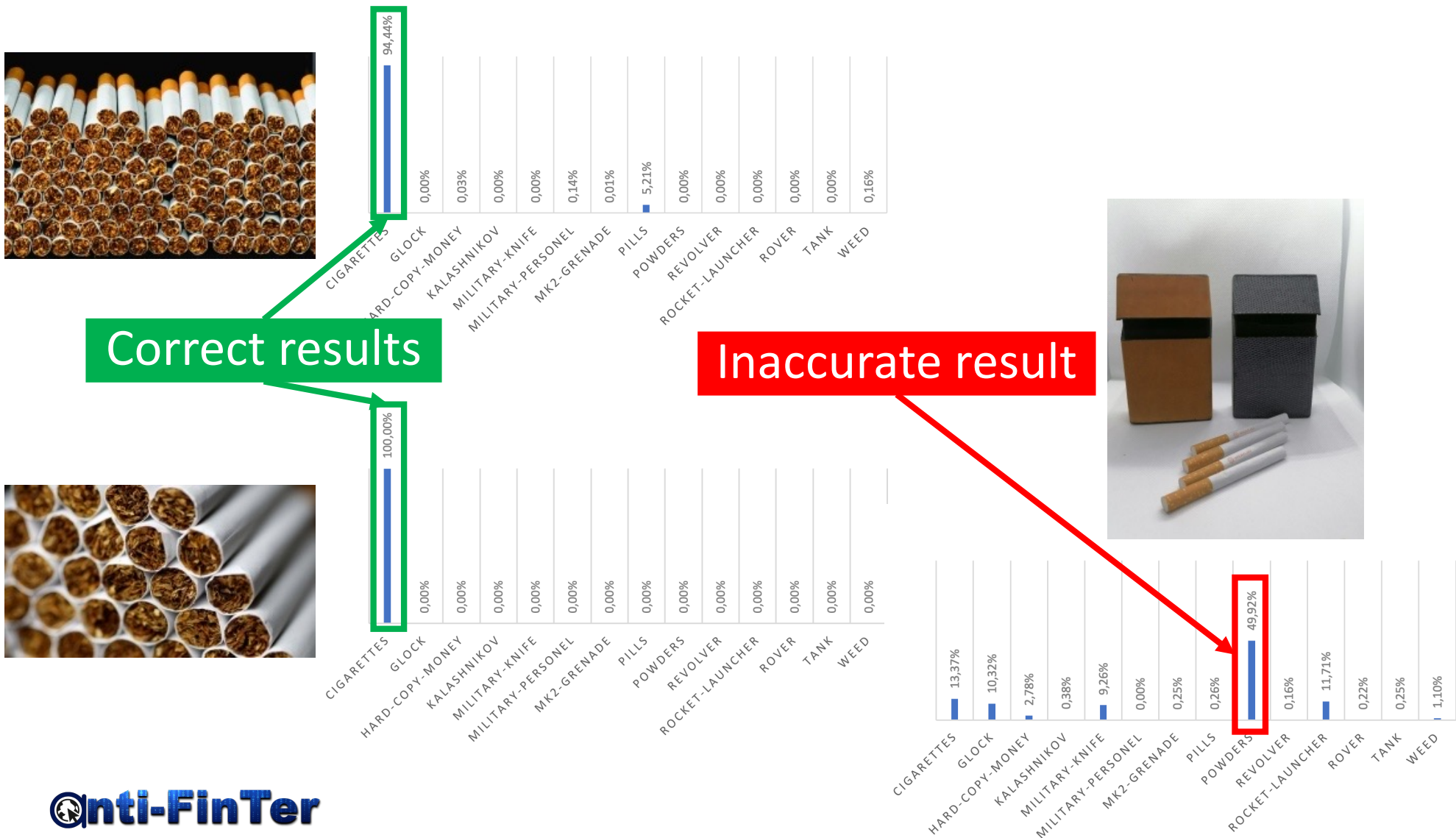


Correct results



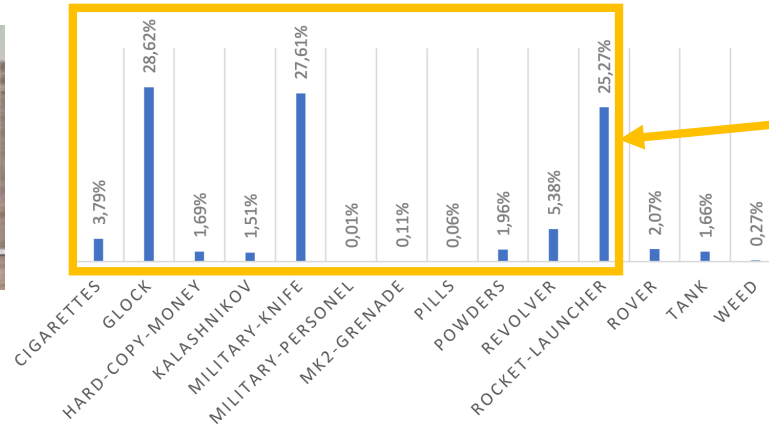
# Concept detection

- **Achieved results:** Indicative qualitative concept detection results



# Concept detection

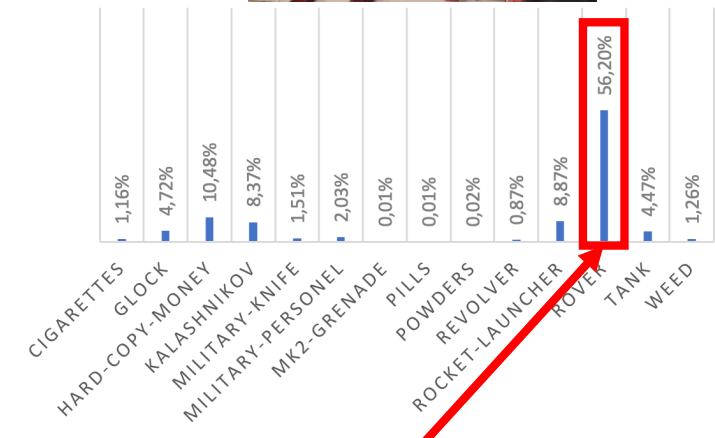
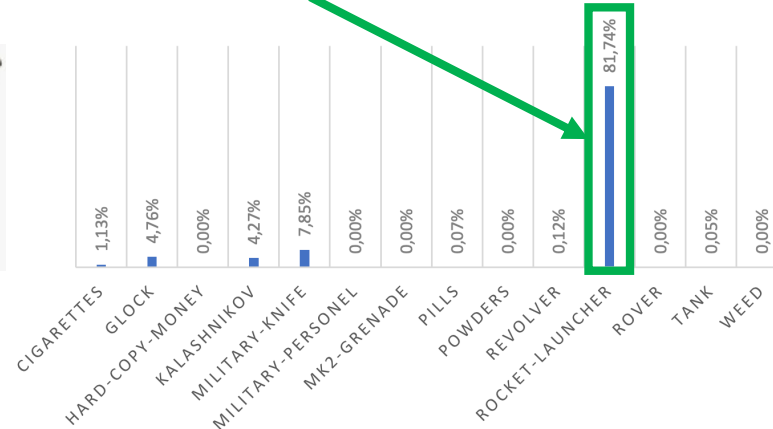
- Achieved results:** Indicative qualitative concept detection results



Ambiguous result



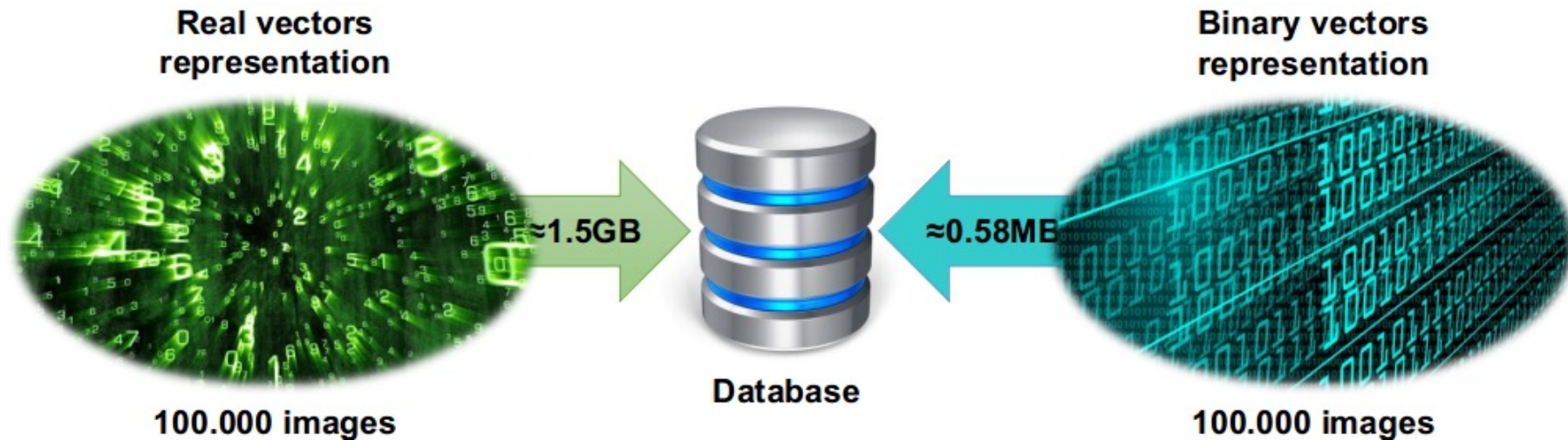
Correct result



Inaccurate result

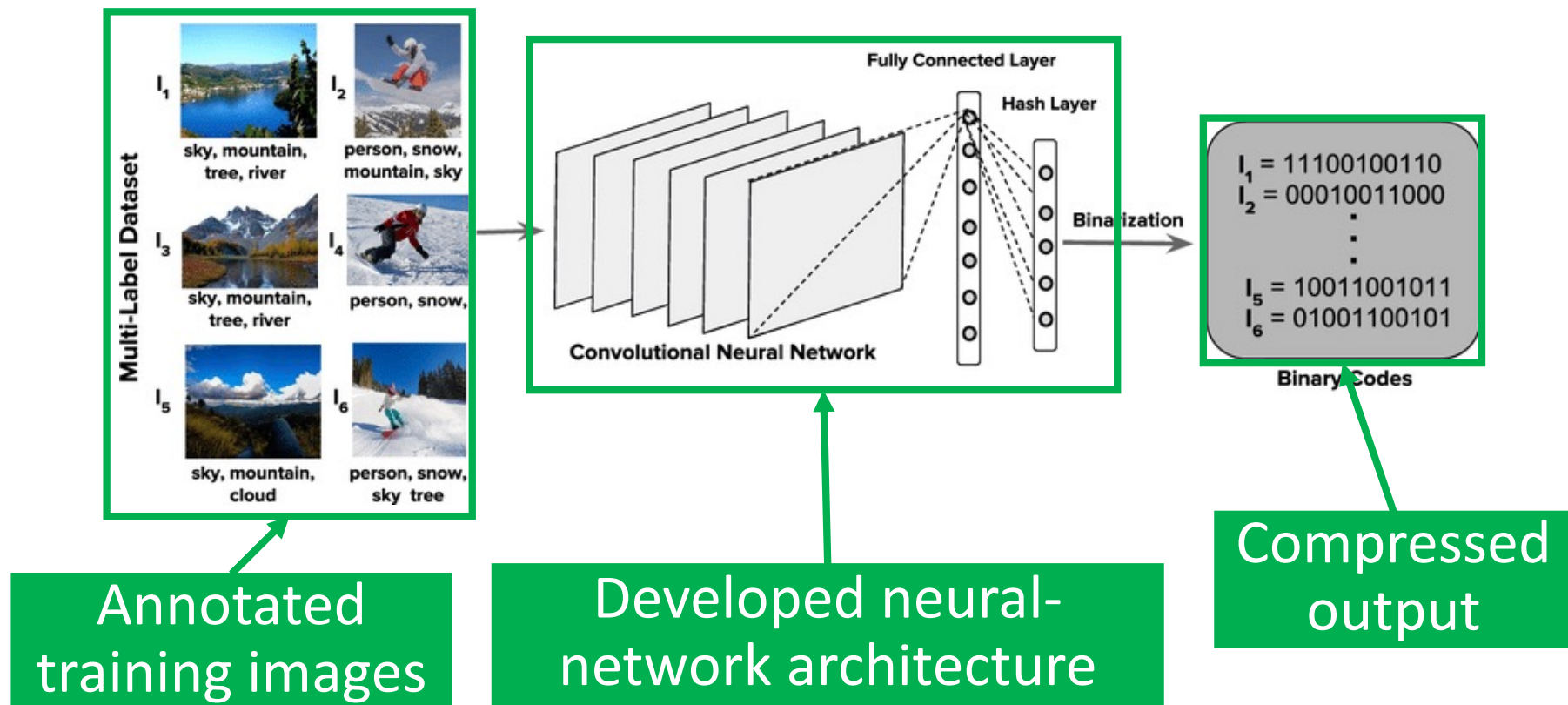
# Visual indexing

- Aim: To automatically retrieve **visually and semantically similar** content (images) from very large databases
  - **Time-efficient** retrieval
  - **Low usage** of memory
  - **Increased** accuracy in retrieved results



# Visual indexing

- Design of neural network-based techniques to efficiently and accurately **compress** the visual information



# Visual indexing

- **Achieved results:** Indicative qualitative visual data indexing results

Query image  
*[glock]*



**RESULTS**



# Visual indexing

- **Achieved results:** Indicative qualitative visual data indexing results

Query image  
[cigarettes]



## RESULTS



# Visual indexing

- **Achieved results:** Indicative qualitative visual data indexing results

Query image  
[revolver]



**RESULTS**



# Visual indexing

- Achieved results:** Indicative qualitative visual data indexing results

Query image  
[revolver]



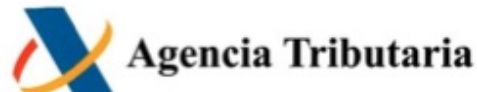
**RESULTS**

 89%	 87%	 87%	 85%	 85%
 85%	 85%	 85%	 85%	 85%

# Anti-FinTer

Dr. Asterios Leonidis  
Anti-FinTer Partner  
Post-doctoral researcher  
Institute of Computer Science (ICS),  
Foundation for Research and Technology –  
Hellas (FORTH)  
email: [leonidis@ics.forth.gr](mailto:leonidis@ics.forth.gr)

Dr. Georgios Th. Papadopoulos  
Anti-FinTer Technical Manager  
Assistant Professor  
Department of Informatics and Telematics  
Harokopio University of Athens, Greece  
email: [g.th.papadopoulos@hua.gr](mailto:g.th.papadopoulos@hua.gr)



Republic of Bulgaria  
Ministry of Interior

