The use of social networks for terrorist purposes

Challenges, gaps and related innovation solutions in the field of steganalysis

17.02.2023 **10:00 AM - 12:00 PM CET**

NOTIONES + UNCOVER | SYNYO

Host: SYNYO GmbH

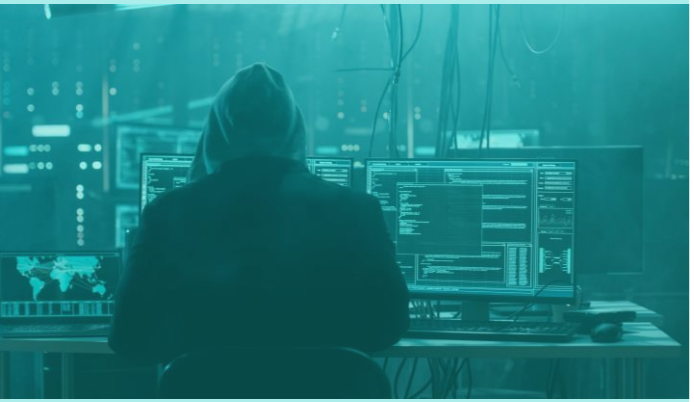
Estonian Police and Border Guard Board

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021853.

Agenda

Time	Topic	Presenter
10:00 - 10:05	**Introduction to the webinar and expected results**	**Alexander Nikolov** SYNYO GmbH, Austria
10:05 - 10:20	**NOTIONES project**	**Alexander Nikolov** SYNYO GmbH, Austria
10:20 - 10:35	**UNCOVER project**	**Vaila Leask** Royal Military Academy, Belgium
10:35 - 10:55	**TATE project**	**Andrew Staniforth** SAHER Europe, Estonia
10:55 - 11:15	**ExpertAI**	**Ciro Caterino** Expert.ai, Italy
11:15 - 11:35	**iPS**	**Michele de Masi** iPS Visionary Intelligence, Italy
11:35 - 11:50	**Questions and discussion**	**Alexander Nikolov** SYNYO GmbH, Austria
11:50 - 12:00	**Final remarks**	**Alexander Nikolov** SYNYO GmbH, Austria

HOUSEKEEPING RULES



The session will be entirely recorded and published on the NOTIONES project website.

All participants except speakers and moderators will be **muted by default**.

Feel free to post your questionsions in the **chat**.

If you would like to speak, raise your hand and wait for the moderator to give you the floor.

NOTIONES

iNteracting netwOrk of inTelligence and securIty practitiOners with iNdustry and acadEmia actorS

Alexander Nikolov
DCE manager of NOTIONES
alexander.nikolov@synyo.com

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021853.

PROJECT OVERVIEW

Acronym:	NOTIONES
Title:	iNteracting netwOrk of inTelligence and securIty practitiOners with iNdustry and acadEmia actorS
Duration:	01.09.2021 – 31.08.2026
Topic:	SU-GM01-2020
Call:	Pan-European networks of practitioners & other actors in the field of security
Funding:	H2020
Type:	Coordination and Support Action (CSA)
GA Number:	101021853
Coordinator:	Fundacion Tecnalia Research & Innovation
Consortium:	30 Partners
Website:	www.notiones.eu
Cordis:	CORDIS Project Profile

OVERVIEW

CONSORTIUM

Fundadcion Tecnalia Research and Innovation (TECNALIA)

Spain

Zanasi & Partners (Z&P)

Italy

Laura-Ammattikorkeakoulu (LAU)

Finland

Institut Po Otbrana (BDI)

Bulgaria

Defence Research Institute (DRI)

France

Intelligence Culture and Strategic Analysis (ICSA)

Italy

Bar-Ilan University (BIU)

Israel

Agenzia Per La Promozione Della Ricerca Europea (APRE)

Italy

Teknologian Tutkimuskeskus Vtt OY (VTT)

Finland

Expert System SPA (EXPSYS)

Italy

SAHER (SAHER)

Estonia

MarketScape

Denmark

TECOMS SRL (TECOMS)

Italy

SYNYO GmbH

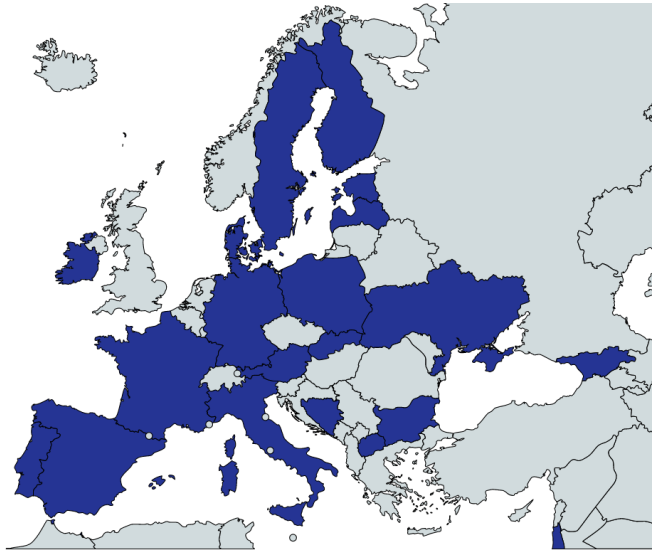
Austria

Masovian Police (KWPR)

Poland

DURZHAVNA AGENTSIYA NATSIONALNA SIGURNOST (DANS)

Bulgaria



LESO LEONARDO (LL)

Italy

Financial Intelligence Unit Latvia (FIU)

Latvia

Beyond the Horizon International Strategic Studies Group (BtH)

Belgium

International Security and Emergency Management Institute (ISEM)

Slovakia

Kharkiv National University of Internal Affairs (KhNUIA)

Ukraine

Politsei- ja Piirivalveamet

Estonia

Ministry Of Internal Affairs (MIA)

Georgia

Police Service of Northern Ireland (PSNI)

Ireland

POLISMYNDIGHETEN SWEDISH POLICE AUTHORITY (SPA)

Sweden

Ministério da Justiça (PJ)

Portugal

Military Academy Skopje (MAGMA)

North Macedonia

HOCHSCHULE FUR DEN ÖFFENTLICHEN DIENST IN BAYERN (HföD)

Germany

Ertzaintza (ERTZ)

Spain

KEY OBJECTIVES

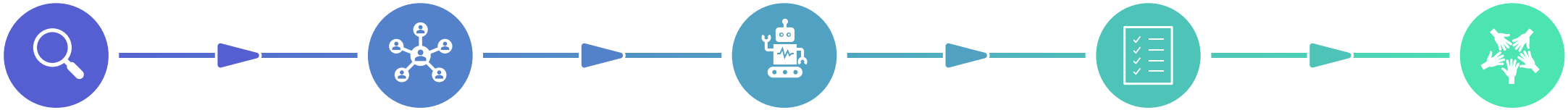
Elicitation of the needs of intelligence and security practitioners.

Promote interaction of technology providers and academy with intelligence and security practitioners.

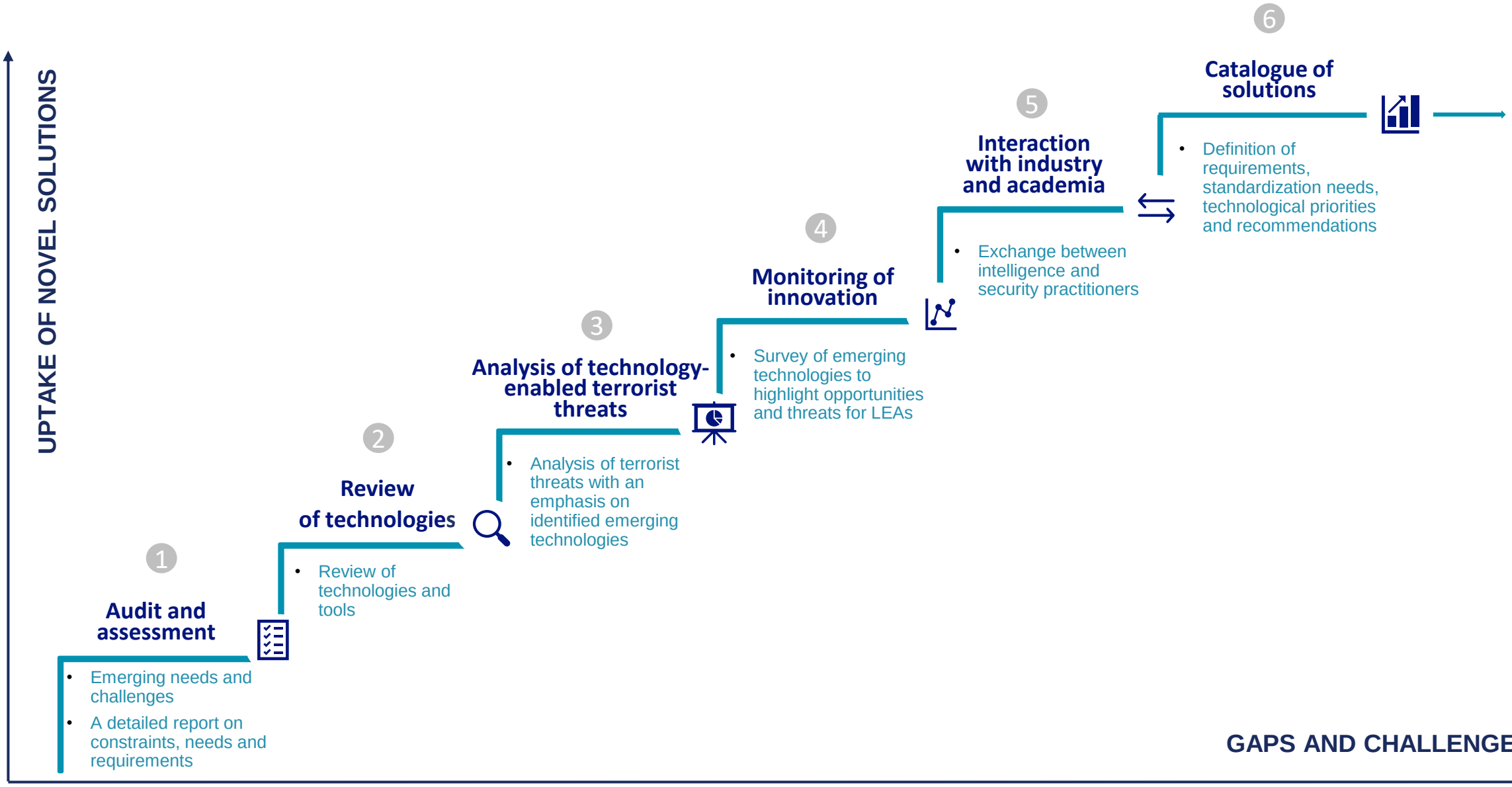
Identification of novel technologies relevant for practitioners through research monitoring.

Periodically publish a **report, which summarise findings** in order to orientate future research project programming.

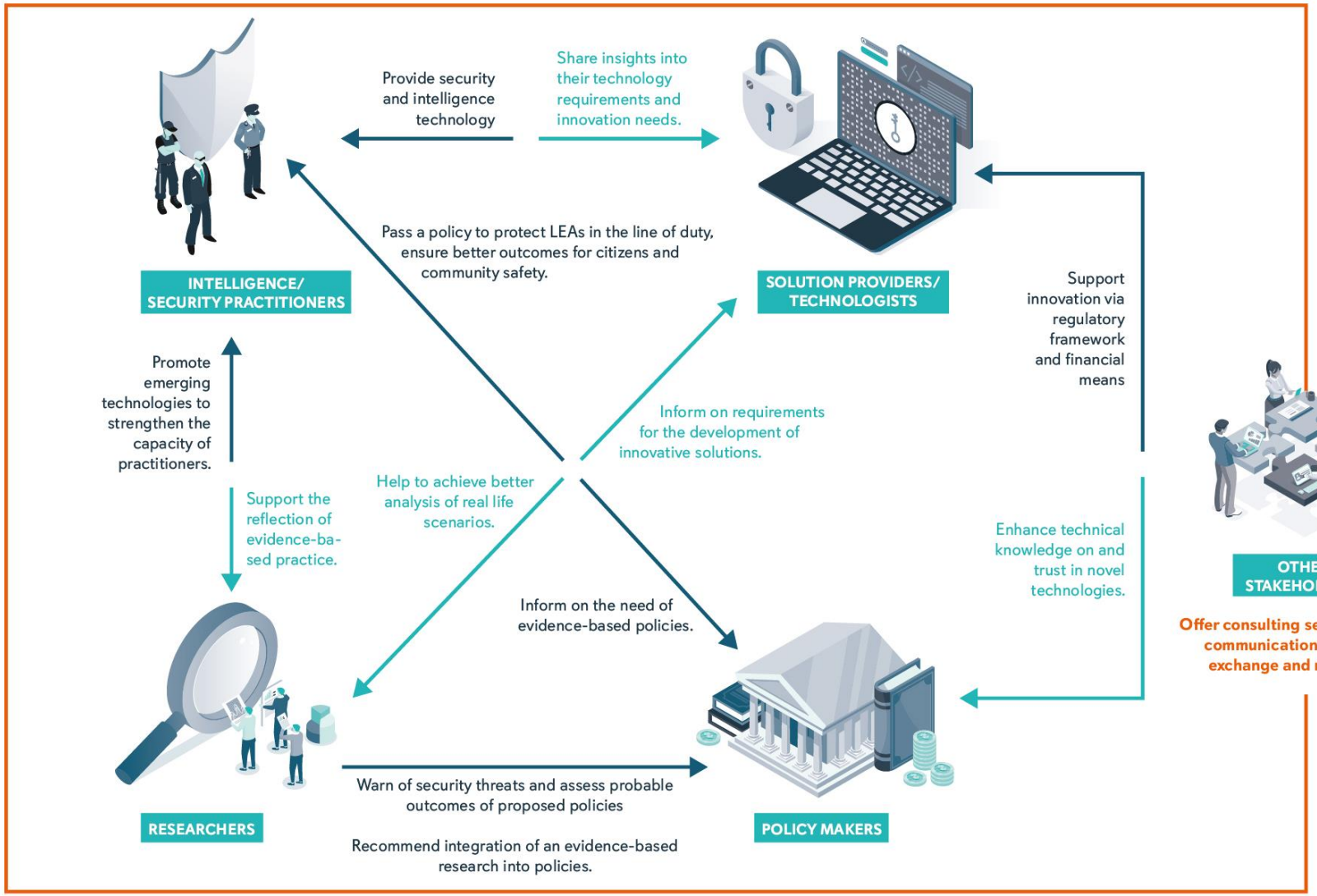
Ensure the **commitment and involvement of new organisations** in the pan-European NOTIONES network.



PROJECT APPROACH



NOTIONES NETWORK



NOTIONES PERSONAS

Susanne Huber
43/Female
Germany

Susanne works as an innovation manager at a company, which is specialised in the development of AI-based solutions for social media surveillance. Working in this fast-paced sector, she needs to constantly keep innovating in order to stay ahead of the competition.

She must understand what technology solutions are needed in the security sector and how they can be developed accordingly.

SUSANNE'S WORK HAS THE FOLLOWING LIMITATION

The language used at online platforms changes fast, which has to be handled by the system somehow.

The quality of the text is very important for language modelling. For example, multilingualism and speech-to-text transformations are currently a challenge.

The "human in the loop" in the development and training of AI systems.

SUSANNE IS LOOKING FOR A SOLUTION WHICH

- creates the possibility to store sensitive or confidential data via Edge AI
- enables security and encryption improvements for existing technologies and solutions
- can collect intel and monitor platforms to combat terrorism

SUSANNE IS USING A SOLUTION

- to secure data sharing and dissemination
- for data storage optimization
- for technological data sanitation

Carla Luterotti
29/Female
Italy

Carla works on security-related projects at her university in Bologna. As a project manager, she tries to identify possible capability gaps of LEAs and connect them with technologists who develop solutions for them.

Her primary goal is to enhance organisational understanding of current schemes and directions of research and innovation as well as to establish opportunities for bi-lateral cooperation on sercurity-related topics.

CARLA HAS THE FOLLOWING LIMITATIONS

As a researcher, she has only limited access to the practitioners' requirements and can therefore barely realize new solutions tailored to intelligence and security activities.

She is completely dependent on cooperation with technology developers and practitioners.

CARLA IS LOOKING FOR A SOLUTION WHICH

- can identify threats to national security;
- can identify persons behind the anonymous profiles who participate in or direct darknet activities
- can help her prevent and deter organized crime relating to child pornography

CARLA IS USING A SOLUTION

- to collect information about common strategies for illegal activities taking place on the darknet
- to gain an overview of relevant practitioners involved in the field
- to research the state of the art of Artificial Intelligence algorithms and tools at the service of the Intelligence and Security practitioners

Johan Smith
36/Male
UK

Johan Smith is a 36-year-old security practitioner at the armed forces in the UK. His unit is responsible for reconnaissance and surveillance. Therefore, he is constantly faced with the challenge of finding and using the latest technologies that give him a strategic advantage in the field.

His main goal is to explore the most important advancements in the technology sector when it comes to aerial imagery possibilities. Especially in connection with AI support, the most modern developments are taking place here, which are of great importance for his field.

JOHAN'S WORK HAS THE FOLLOWING LIMITATIONS

While modern imagery offers great possibilities to detect and identify all kinds of targets, specific knowledge is still required to select the appropriate data source, be able to collect and process the data, or even be aware of the technology's capabilities and limitations. However, there exists a lack of awareness and capabilities in these regards.

JOHAN IS LOOKING FOR A SOLUTION WHICH

- allows it to combine new technology for aerial imagery with the military's existing strategic software and
- can find and adapt advanced artificial intelligence-based computation suitable for use in the field

JOHAN IS USING SOLUTIONS WHICH

- collect intelligence and monitor platforms to detect and prevent organized crime,
- secure data sharing and dissemination (internally and externally) and
- applys Image and Signal based intelligence (IMINT and SIGINT).

Kristoffer Martin
55/Male
Sweden

Kristoffer is a government official in Stockholm, who is responsible for the analysis, elaboration and preparation of security concepts at the country level.

As a policy maker, it is his job to identify vulnerabilities in national security and support the armed forces with modern solutions.

KRISTOFFER HAS THE FOLLOWING LIMITATIONS

Even though a lot of threats are spread through online media, Kristoffer is not able to search the world wide web for potential threats on his own.

More training is required to educate employees on online safety.

Multiple pieces of software are used at once, which often generates certain limitations during the exchange of information.

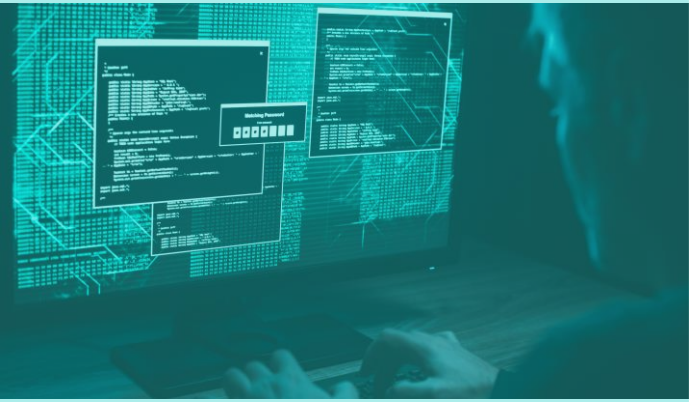
KRISTOFFER IS LOOKING FOR A SOLUTION TO

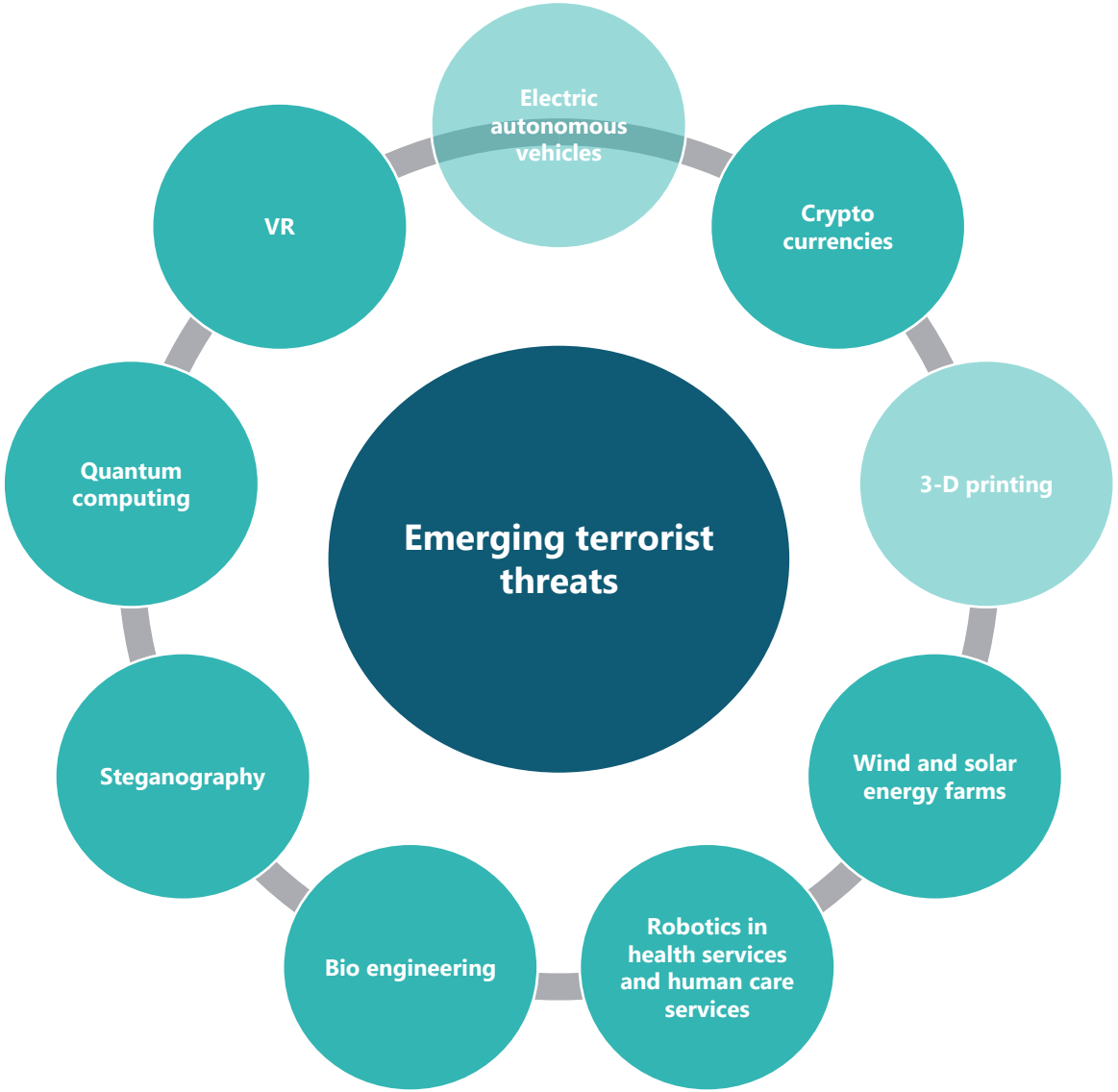
- counter potential terrorist threats via social media,
- increase communication with the intelligence services for better identification of potential threats and
- communicate the needs of his government to the security practitioners.

KRISTOFFER IS USING A SOLUTIONS FOR

- data enrichment from external databases and
- decision management.

NOTIONES APPROACH TO STUDY TERRORIST PROCESS





RELATED GAPS AND CHALLENGES

Lack of skills
(unlikely to realize that a hidden file exists)

No consistently available tools
(unmet needs)

STEGANALYSIS

(Gaps and Challenges)

No unified approach
(a maze of regulations and laws)

Questions & Answers

NOTIONES

UNCOVER

Notoines Webinar

Vaila Leask
Royal Military Academy, Brussels
vaila.leask@mil.be
17/02/2023

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021853.

NOTIONES

The problem

Solving the problem → the solution: UNCOVER

How do we do it? Details & conclusion

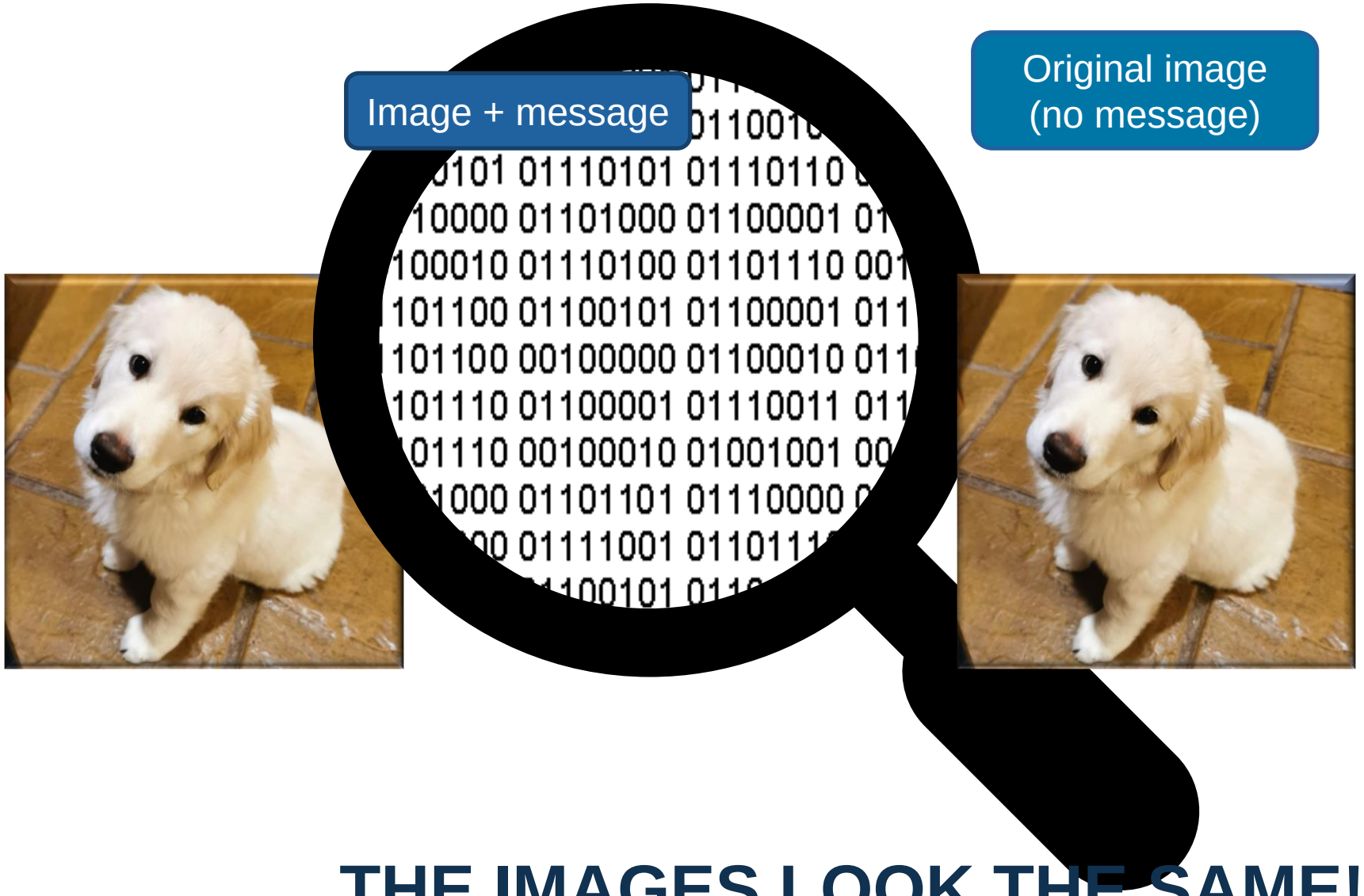
The problem

The problem


01101000 0110010
0100 01110101 01110100
10010 01101001 01100001 01
100000 01110100 01101111 001
101100 01100101 01100001 011
101110 00100000 01100010 011
101110 01100001 01110010 011
01110 00100000 01001001 00
1000 01101111 01110000
00 01111001 0110111

The problem

The problem



THE IMAGES LOOK THE SAME!

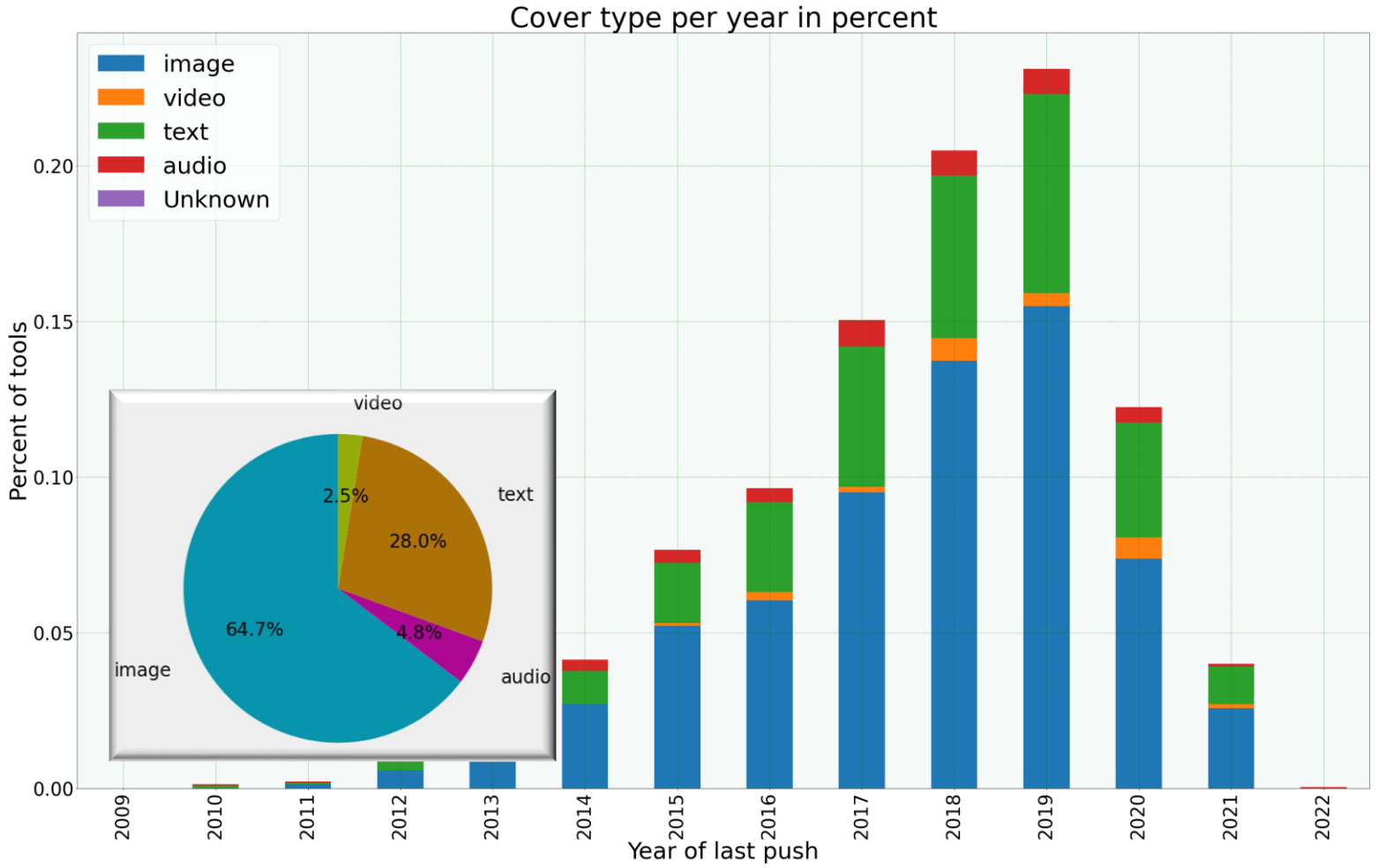
The problem: illicit uses

- Hiding communi
  criminals/terrorists
- Cyber espionage, information leakage
- Hiding criminal activities (e.g. child pornography)
- Malware (hiding code, C&C-server addresses,…)

The problem: law enforcement perspective

Solving the problem: starting point

- 8000+ repositories
- ~400 applications with little to no information about them

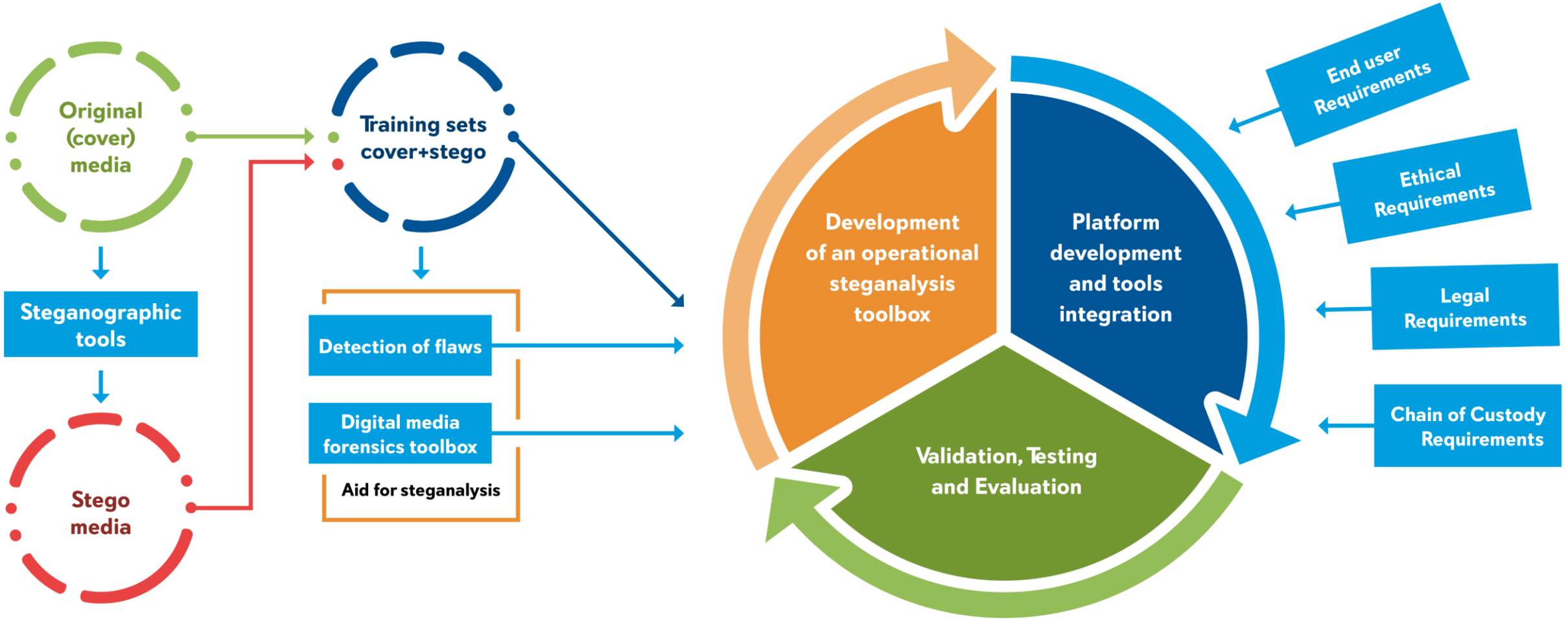


The Solution

UNCOVER

The development of an efficient steganalysis framework for uncovering hidden information in digital media.

The Solution: How do we do it?



The Solution: Shortlist

How do we do it?: KPIs

Description of KPI	Planned value	Reached value at M18
No. steganographic tools collected & analysed	>150	>2000
No. steganographic tools examined (source code analysis, reverse engineering, signature extraction)	>30	4
No. tools developed to enhance steganalysis detectors	>15	4 release candidates, 10 more tools in development
Creation of training and validation sets of cover media: • Number of raw image files • Number of audio files • Number of video files • Number of text files	≥50 000 ≥10 000 ≥10 000 ≥10 000	Image files: > 100 k Audio files: > 500 k Text files: > 2000 k
No. test cases/scenario provided for the evaluation	>10	12
Workshops, webinars and project presentations: • for stakeholders. Aim: *present, test and refine training materials.* • for LEAs and forensic specialists. Aim: *understand basic steganalysis concepts.* • for LEAs, citizens, scientific & research community, citizens, policy makers & public institutions. Aim: *raising awareness.*	≥5 ≥10	1 (workplan defined for 2023) 31
Steganalysis contest: "Operational UNCOVER Challenge" Target group: Scientific & research community, but experienced practitioners (within the LEA and forensic community) • Number of competitors participating in the contest	≥ 50	

How do we do it?: KPIs

Description of KPI	Planned value	Reached value at M18
No. steganographic tools collected & analysed	>150	>2000
No. steganographic tools examined (source code analysis, reverse engineering, signature extraction)	>30	4
No. tools developed to enhance steganalysis detectors	>15	4 release candidates, 10 more tools in development
Creation of training and validation sets of cover media: • Number of raw image files • Number of audio files • Number of video files • Number of text files	≥50 000 ≥10 000 ≥10 000 ≥10 000	Image files: > 100 k Audio files: > 500 k Text files: > 2000 k
No. test cases/scenario provided for the evaluation	>10	12
Workshops, webinars and project presentations: • for stakeholders. Aim: *present, test and refine training materials.* • for LEAs and forensic specialists. Aim: *understand basic steganalysis concepts.* • for LEAs, citizens, scientific & research community, citizens, policy makers & public institutions. Aim: *raising awareness.*	≥5 ≥10	1 (workplan defined for 2023) 31
Steganalysis contest: "Operational UNCOVER Challenge" Target group: Scientific & research community, but experienced practitioners (within the LEA and forensic community) • Number of competitors participating in the contest	≥ 50	

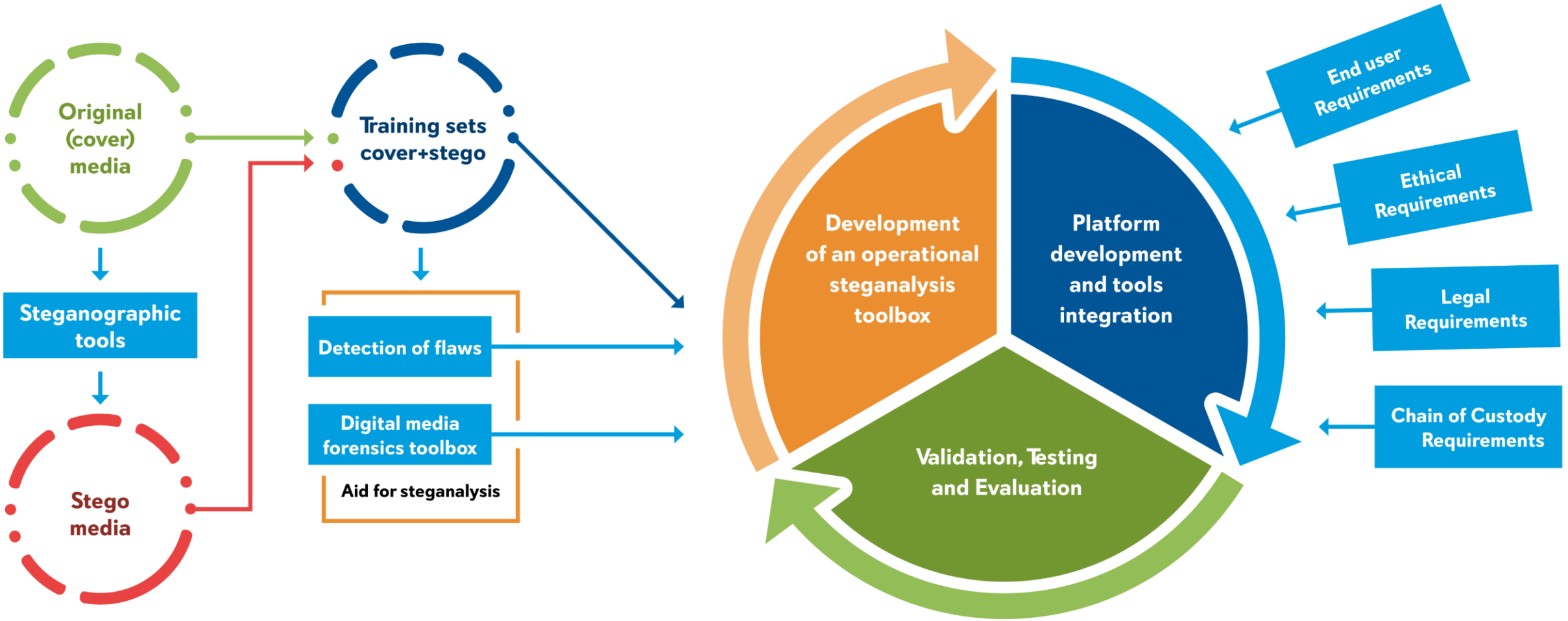
How do we do it?: KPIs

Description of KPI	Planned value	Reached value at M18
No. steganographic tools collected & analysed	>150	>2000
No. steganographic tools examined (source code analysis, reverse engineering, signature extraction)	>30	4
No. tools developed to enhance steganalysis detectors	>15	4 release candidates, 10 more tools in development
Creation of training and validation sets of cover media: • Number of raw image files • Number of audio files • Number of video files • Number of text files	 ≥50 000 ≥10 000 ≥10 000 ≥10 000	 Image files: > 100 k Audio files: > 500 k Text files: > 2000 k
No. test cases/scenario provided for the evaluation	>10	12
Workshops, webinars and project presentations: • for stakeholders. Aim: *present, test and refine training materials.* • for LEAs and forensic specialists. Aim: *understand basic steganalysis concepts.* • for LEAs, citizens, scientific & research community, citizens, policy makers & public institutions. Aim: *raising awareness.*	 ≥5 ≥10	 1 (workplan defined for 2023) 31
Steganalysis contest: "Operational UNCOVER Challenge" Target group: Scientific & research community, but experienced practitioners (within the LEA and forensic community) • Number of competitors participating in the contest	 ≥ 50	

How do we do it?: KPIs

Description of KPI	Planned value	Reached value at M18
No. steganographic tools collected & analysed	>150	>2000
No. steganographic tools examined (source code analysis, reverse engineering, signature extraction)	>30	4
No. tools developed to enhance steganalysis detectors	>15	4 release candidates, 10 more tools in development
Creation of training and validation sets of cover media: • Number of raw image files • Number of audio files • Number of video files • Number of text files	≥50 000 ≥10 000 ≥10 000 ≥10 000	Image files: > 100 k Audio files: > 500 k Text files: > 2000 k
No. test cases/scenario provided for the evaluation	>10	12
Workshops, webinars and project presentations: • for stakeholders. Aim: *present, test and refine training materials.* • for LEAs and forensic specialists. Aim: *understand basic steganalysis concepts.* • for LEAs, citizens, scientific & research community, citizens, policy makers & public institutions. Aim: *raising awareness.*	≥5 ≥10	1 (workplan defined for 2023) 31
Steganalysis contest: "Operational UNCOVER Challenge" Target group: Scientific & research community, but experienced practitioners (within the LEA and forensic community) • Number of competitors participating in the contest	≥ 50	

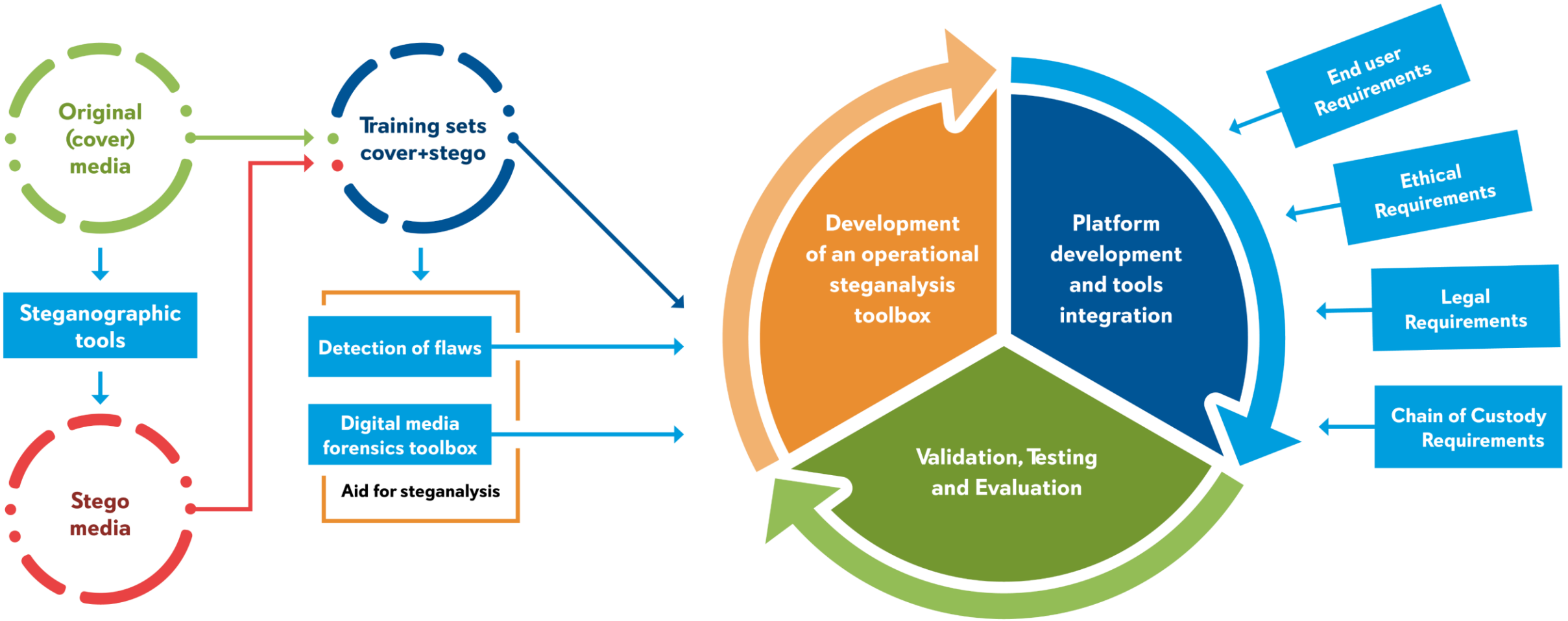
How do we do it?: KPIs



How do we do it?: KPIs

Description of KPI	Planned value	Reached value at M18
No. steganographic tools collected & analysed	>150	>2000
No. steganographic tools examined (source code analysis, reverse engineering, signature extraction)	>30	4
No. tools developed to enhance steganalysis detectors	>15	4 release candidates, 10 more tools in development
Creation of training and validation sets of cover media: • Number of raw image files • Number of audio files • Number of video files • Number of text files	≥50 000 ≥10 000 ≥10 000 ≥10 000	Image files: > 100 k Audio files: > 500 k Text files: > 2000 k
No. test cases/scenario provided for the evaluation	>10	12
Workshops, webinars and project presentations: • for stakeholders. Aim: *present, test and refine training materials.* • for LEAs and forensic specialists. Aim: *understand basic steganalysis concepts.* • for LEAs, citizens, scientific & research community, citizens, policy makers & public institutions. Aim: *raising awareness.*	≥5 ≥10	1 (workplan defined for 2023) 31
Steganalysis contest: "Operational UNCOVER Challenge" Target group: Scientific & research community, but experienced practitioners (within the LEA and forensic community) • Number of competitors participating in the contest	≥ 50	

How do we do it?: KPIs



How do we do it?: KPIs

Description of KPI	Planned value	Reached value at M18
No. steganographic tools collected & analysed	>150	>2000
No. steganographic tools examined (source code analysis, reverse engineering, signature extraction)	>30	4
No. tools developed to enhance steganalysis detectors	>15	4 release candidates, 10 more tools in development
Creation of training and validation sets of cover media: • Number of raw image files • Number of audio files • Number of video files • Number of text files	≥50 000 ≥10 000 ≥10 000 ≥10 000	Image files: > 100 k Audio files: > 500 k Text files: > 2000 k
No. test cases/scenario provided for the evaluation	>10	12
Workshops, webinars and project presentations: • for stakeholders. Aim: *present, test and refine training materials.* • for LEAs and forensic specialists. Aim: *understand basic steganalysis concepts.* • for LEAs, citizens, scientific & research community, citizens, policy makers & public institutions. Aim: *raising awareness.*	≥5 ≥10	1 (workplan defined for 2023) 31
Steganalysis contest: "Operational UNCOVER Challenge" Target group: Scientific & research community, but experienced practitioners (within the LEA and forensic community) • Number of competitors participating in the contest	≥ 50	

How do we do it?: KPIs

Description of KPI	Planned value	Reached value at M18
No. steganographic tools collected & analysed	>150	>2000
No. steganographic tools examined (source code analysis, reverse engineering, signature extraction)	>30	4
No. tools developed to enhance steganalysis detectors	>15	4 release candidates, 10 more tools in development
Creation of training and validation sets of cover media: • Number of raw image files • Number of audio files • Number of video files • Number of text files	 ≥50 000 ≥10 000 ≥10 000 ≥10 000	 Image files: > 100 k Audio files: > 500 k Text files: > 2000 k
No. test cases/scenario provided for the evaluation	>10	12
Workshops, webinars and project presentations: • for stakeholders. Aim: *present, test and refine training materials.* • for LEAs and forensic specialists. Aim: *understand basic steganalysis concepts.* • for LEAs, citizens, scientific & research community, citizens, policy makers & public institutions. Aim: *raising awareness.*	 ≥5 ≥10	 1 (workplan defined for 2023) 31
Steganalysis contest: "Operational UNCOVER Challenge" Target group: Scientific & research community, but experienced practitioners (within the LEA and forensic community) • Number of competitors participating in the contest	 ≥ 50	

How do we do it?: KPIs

Description of KPI	Planned value	Reached value at M18
No. steganographic tools collected & analysed	>150	>2000
No. steganographic tools examined (source code analysis, reverse engineering, signature extraction)	>30	4
No. tools developed to enhance steganalysis detectors	>15	4 release candidates, 10 more tools in development
Creation of training and validation sets of cover media: • Number of raw image files • Number of audio files • Number of video files • Number of text files	≥50 000 ≥10 000 ≥10 000 ≥10 000	Image files: > 100 k Audio files: > 500 k Text files: > 2000 k
No. test cases/scenario provided for the evaluation	>10	12
Workshops, webinars and project presentations: • for stakeholders. Aim: *present, test and refine training materials.* • for LEAs and forensic specialists. Aim: *understand basic steganalysis concepts.* • for LEAs, citizens, scientific & research community, citizens, policy makers & public institutions. Aim: *raising awareness.*	≥5 ≥10	1 (workplan defined for 2023) 31
Steganalysis contest: "Operational UNCOVE Target group: Scientific & research commu community) • Number of competitors participating in the	≥ 50	

UNCOVER: The development of an efficient steganalysis framework for uncovering hidden information in digital media.

Vaila Leask, Rémi Cogranne, Dirk Borghys, Helena Bruyninckx

DOI: 10.1145/3538969.3544468

The problem - STEGANOGRAPHY

The solution - UNCOVER

How do we do it?

Combined efforts from LEAs, research partners and forensic institutes all following end-user, ethical, legal and CoC requirements through a feedback loop until the final product is complete.

Thank you for listening!

Questions & Answers

Tackling Terrorist Content Online – Tech Against Terrorism Europe (TATE)

Andrew Staniforth | Director of Innovation | SAHER (Europe) | TATE Project Coordinator

NOTIONES & UNCOVER | The Use of Social Networks for Terrorist Purposes

17th February 2023

TATE is funded by the European Union Internal Security Fund (ISFP-2021-AG-TCO-101080101)

Tech Against Terrorism Europe (TATE)

- Internal Security Fund (ISFP-2021-AG-TCO-101080101)
- 24 month duration (January 2023 – December 2024)
- 7 partners from 5 EU MS & 2 from the UK
- 1 of 3 projects to be funded under the 2021 TCO call
- Partner projects include FRISCO and ALLIES

Delivered by

Coordinated by

Consortium partners

Funded by

TATE is funded by the European Union Internal Security Fund (ISFP-2021-AG-TCO-101080101)

Tech Against Terrorism Europe (TATE)

TATE aims to support smaller hosting services providers (HSPs) in preventing terrorist actors from disseminating terrorist content as defined in the EU's terrorist content online (TCO) regulation and in Directive (EU)2017/54 by:

1) increasing the capacity for consortium partners to deliver HSP support programme;
2) identifying priority at-risk platforms to target support mechanisms;
3) increasing HSP understanding of TCO regulation and best practice implementation and;
4) Support HSPs in the practical implementation of the TCO regulation

Delivered by

Coordinated by

Consortium partners

Funded by

TATE is funded by the European Union Internal Security Fund (ISFP-2021-AG-TCO-101080101)

tech against terrorism europe

www.tate-project.eu

Delivered by

tech against terrorism

Coordinated by

SAHER EUROPE

Consortium partners

DCU

jos

GHENT UNIVERSITY

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Swansea University Prifysgol Abertawe

Funded by

TATE is funded by the European Union Internal Security Fund (ISFP-2021-AG-TCO-101080101)

Questions & Answers

Expert.ai

NLP solutions for terrorism usage of social media

Ciro Caterino
Senior SW Engineer / Expert.ai
ccaterino@expert.ai

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021853.

Description of the organisation

Expert.ai

Expert.ai turns language into data so teams can make better decisions. Our solutions and low code LangOps platform helps teams automate their language-intensive processes and find the ‘signal through the noise’ to deliver actionable insights and recommendations. Combining symbolic and machine learning, our Hybrid AI approach delivers the highest degree of accuracy, explainability, and flexibility in a responsible and sustainable way.

We have 300+ proven deployments of natural language solutions across insurance, financial services and media leveraging our expert.ai Platform technology. Our platform and solutions are built with out of the box knowledge models to make you ‘smarter from the start’ and get to production faster. Our Hybrid AI and natural language understanding (NLU) approach accelerates the development of highly accurate, custom, and easily explainable natural language solutions.

Cooperation idea

Searching for organizations and application cases

Expert.ai is continously looking for cooperations in the fields of crime/cyber-crime, terrorism/cyber-terrorism, security and counter-crimes/terrorism, with all the interested actors (LEAs, intelligence, Ministries, etc…). Also, many other domains are welcome (health, big-data, banking/financing, social media, etc…).

In particular, it's important to underline the contribution that agencies and government organizations could provide in terms of business/study cases, datasets, events and so on.
In this context, Expert.ai is able to provide rule based and AI based solutions.

Expertise request

Financed Projects Group's Vision

Expert.ai is open for cooperating with all companies/organizations/public administrations that are searching for cooperations. We are able to provide support and team playing with a large kind of partners, technicals, academycs, administratives, solutions providers, study case requesters.

Our vision is projected towards a shared growth, in which each actor contributes to bring its expertise to build innovative solutions together, in various fields of application (crime/terrorism, health, big-data, etc…).

For us, the good outcome of each partnership is to create a demo/poc/methodology/prototype for addressing one ore more issues of the real world.

Expertise offer 1/3

Expert.ai Business Core

Expert.ai has its main core in the textual contents analysis. We are able to transform unstructured data in structured, by applying NLP/NLU techniques.
Our analysis engines are mainly rule based, even if during last years we are experimenting AI techniques for extracting the same entities and topics, and they can be used for the analysis of all kind of texts, included social media (OSINT).
Our systems are exploited by intelligence, security, law agencies, mainly in Italy, Europe, USA.

Main analysis can be performed on textual documents:

Extraction -> the operation of finding entites whitin the text; example of extracted entities can be 'people', 'places', 'organizations', but also domain specific entities (Text Mining).

Categorization -> recognizing main topics of a whole document; topics are used for classifying a document regarding its content, and come from well-known or customized taxonomies (or even ontologies) related to the domain of each project.

Writeprint -> extraction of stylometryc features, that can be used for ML purposes

Expertise offer 2/3

Social media and terrorism purposes

Based in our experience gained through the partecipation to European projects and cooperation with law/intelligence agencies, Expert.ai has found the following main areas of usage of the Social Media by the terrorists:

TERRORISM NARRATIVES and PROPAGANDA

TERRORISM FUNDING -> ILLEGAL TRAFFICKINGS

TERRORISM FUNDING -> FAKE CHARITIES

Expertise offer 3/3

Expert.ai solutions

During the work whitin European projects such as CICERO, DANTE, ANITA, Expert.ai provided the following analysis/solutions:

TERRORISM NARRATIVES and PROPAGANDA

The analysis phase has regarded almost 80000 documents crawled from web and social media, for three different types of extremisms: Islamist, Far-Right and Far-Left.

Example of results (categories):
“group identity”
“spirituality / religious topics”
“anger”
“racism, hatred, repulsion”
“recruitment and radicalization”
“antifascism”
“politics / governments”
“action”

TERRORISM FUNDING -> ILLEGAL TRAFFICKINGS

Social media are very often used for disseminating and publishing black markets on dark web and illegal traffickings of drugs and weapons. A good example is Reddit, considered a bridge between dark and surface webs. Gains of such criminal activities are very often used for terrorism fundings.

Through the activities of crawling, extraction/writeprint and analysis of data (semantic reasoning) coming from these socials, during ANITA project we found an example of this relation:

REDDIT nickname: “elcolombiano”
Active in BLACK MARKETS: DreamMarket, Dutch, SilkRoad, Sheep

TERRORISM FUNDING -> FAKE CHARITIES

Some websites and social media discussions disseminate fake charity companies/websites. Expert.AI trained a model, based on stylometryc features, for trying to recognize such cases. We performed both ML and Deep Learning.

ML: With a dataset of 6000 documents for training and 2000 for testing -> 85% accuracy (Logistic)

NN: 10200 training docs + 1800 for testing (4 hidden layers and 100 epochs) -> 91% accuracy

Contacts

WEBSITE
https://www.expert.ai/
https://www.expert.ai/contact-us/?

Vincenzo Masucci| European Financed Projects Director - Branch Manager at Expert.ai Naples
Via Nuova Poggioreale, Centro Polif. Inail , tower 7°, floor 10°, 80143 Napoli, Italy
Tel: +39 081 6586702 | Mobile +39 3389361039 | Email: vmasucc@expert.ai
http://it.linkedin.com/pub/vincenzo-masucci

Ciro Caterino | Senior SW Engineer
Via Nuova Poggioreale 60L Napoli, 80100, Italy
Email: ccaterino@expert.ai
LinkedIn: https://www.linkedin.com/in/ciro-caterino-44844b43

Questions & Answers

IPS S.P.A.

OSINT and Steganography - MEDUSA® Approach

Michele De Masi
Business Development / IPS S.P.A.
m.demasi@ips-intelligence.com

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021853.

Description of the organisation

IPS – The Company

***IPS** is global supplier of **Cyber Intelligence technology** and **solutions for government**.*
*The company is based in Italy and is specialized in designing products in the domain of **Lawful Interception**, **Open Source Intelligence**, **Internet Monitoring**, **Electronic Surveillance** and **Maritime Intelligence**.*

- *Private and independent company*
- *30+ years experience in tech arena*
- *100+ LEAs served worldwide*
- *150+ employees*
- *Focus on IT, Networking and Cyber*
- *In-house development of core solutions*
- *Know-how transfer*

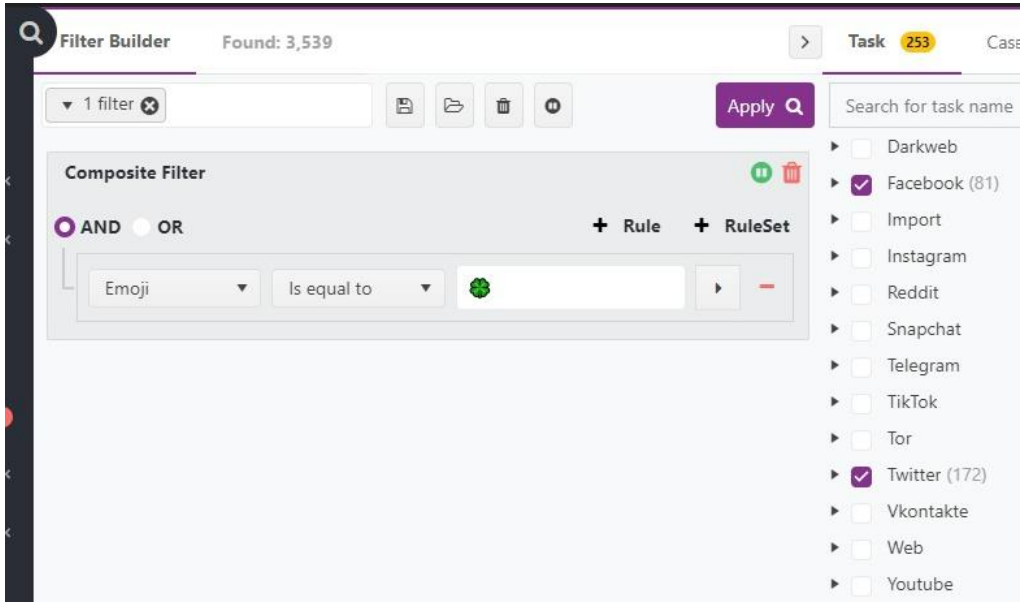
IPS in Numbers:

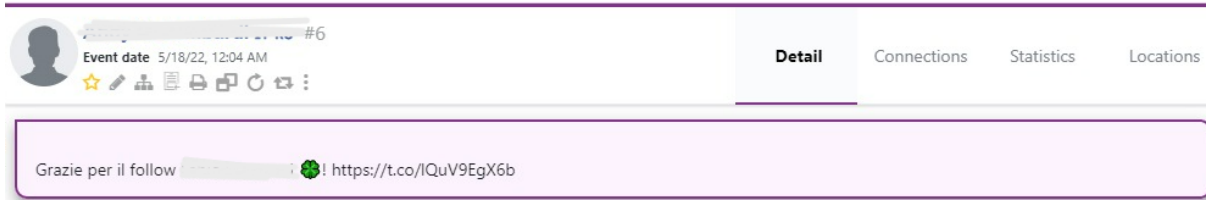
- *6 branches in Italy;*
- *Projects in around 30 countries in the world;*
- *Thousands of Law Enforcement and Security Agencies users worldwide.*

Cooperation idea

MEDUSA® Approach

PILLAR	**Steganography** is a method of **concealing** a hidden message within **regular files**. Due to their innocence, these files serve as **hidden** communication carriers;
PROBLEM	Today Steganography is used by **Criminals** and **Terrorists** all over the world, particularly through the Social Media (**Digital Steganography**) as a covert conduit to communicate hidden messages, in particular through **Image** and **Text Steganography;**
OSINT	For **National Security** reasons, Governments must equip themselves with suitable solutions, among which using **OSINT** tools to quickly map and analyze Social Media;
MEDUSA	**MEDUSA®** is the most performing platform to gather and analyze digital data from Social Media, Web, Dark Web, Forums and Closed Database;
OUTPUT	**MEDUSA® -** once the input data (Image, Text, Emoji...) is fixed - is able to provide the results that include the searched elements as immediate output.





Expertise request

There are **two main issues**:

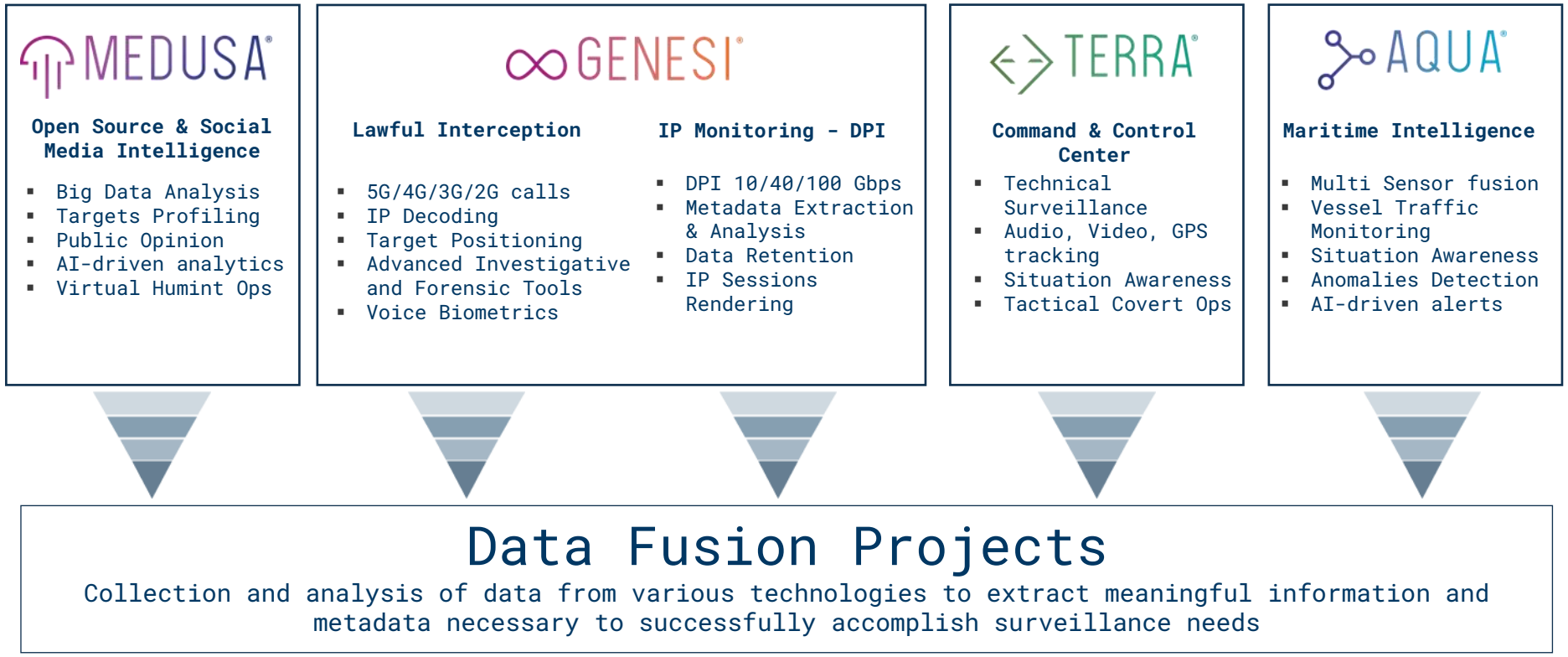
- in Digital Steganography there are **language barriers** (e.g. slang or emoji) and the problem generated by the sharing of **non-text data** (e.g. images) that are difficult to read;
- **the large amount of data** that must be analyzed to search for hidden messages makes the task very complex;

MEDUSA® manages to address these issues:

- is equipped with the **Analysis Function,** which operates on text as well as **multimedia contents** (images, emoji, etc.) by applying sophisticated AI and ML algorithms;
- is capable of **Link Analysis, OCR, collecting Big Data** and analyzing **related multimedia contents**, allowing to set the basis of a StegAnalysis structure.

Expertise offer

Solutions Portfolio



Contacts

Via Monticello, 7 - 04011 Aprilia (LT) - ITALIA

Tel. +39-06.92710.500 (r.a.)

Web: www.ips-intelligence.com

E-mail: info@ips-intelligence.com

Dott. Michele DE MASI

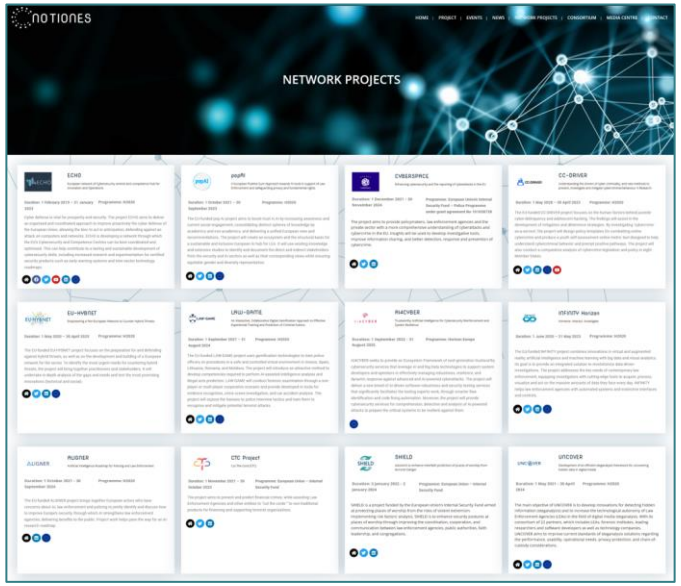
Tel. +39 334 2 28 26 29

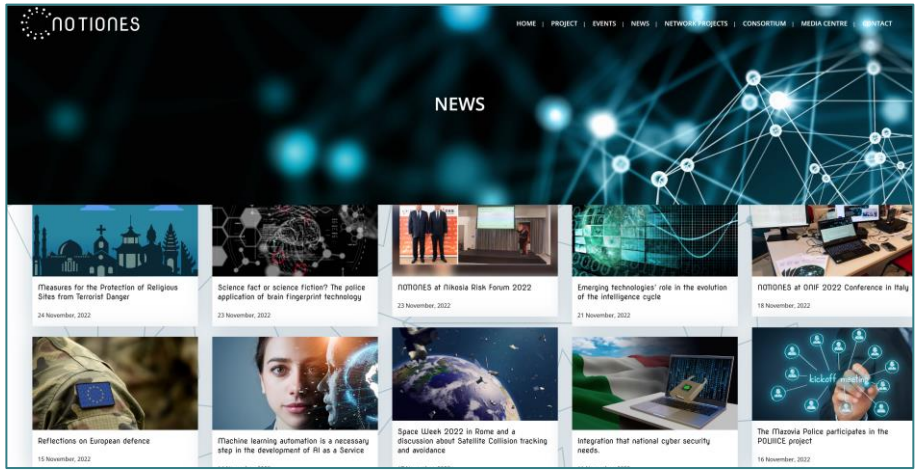
E-mail: m.demasi@ips-intelligence.com

Questions & Answers

DISSIMINATION & COMMUNICATION

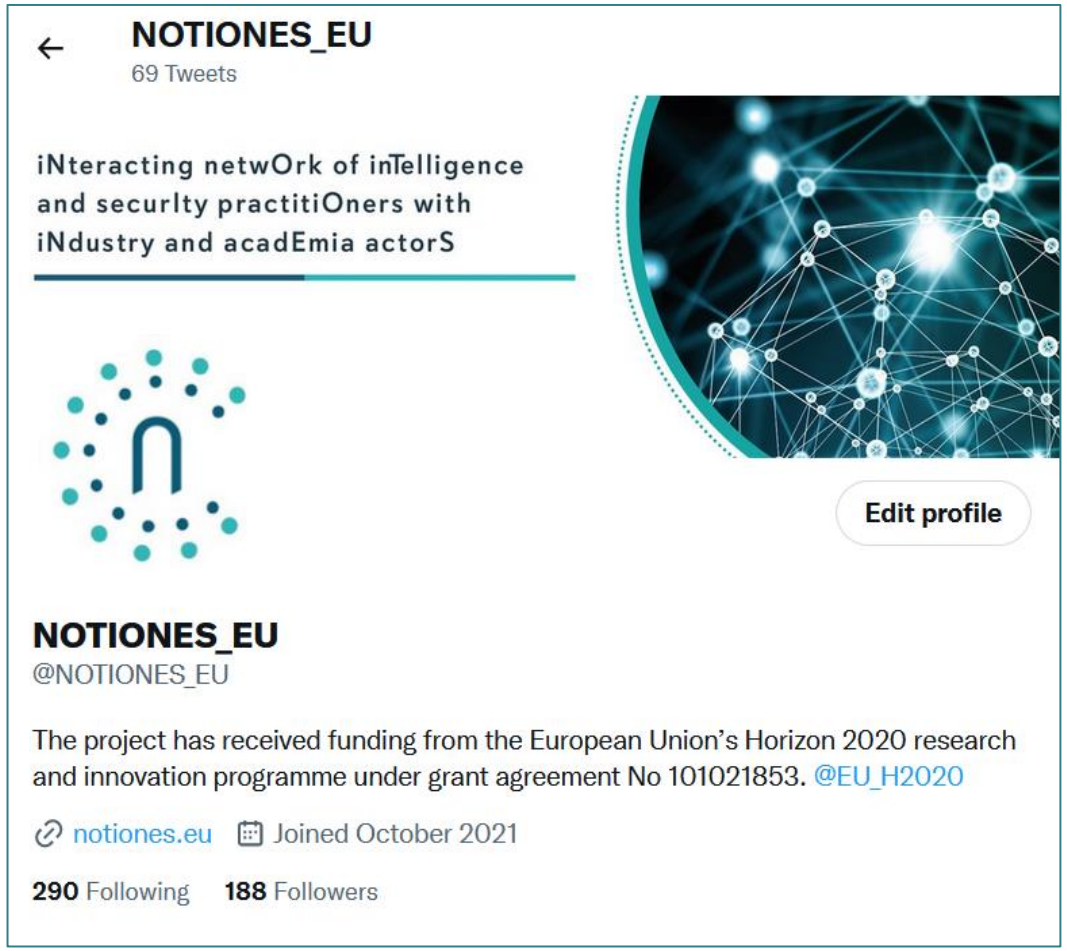
Project website https://www.notiones.eu





DISSIMINATION & COMMUNICATION

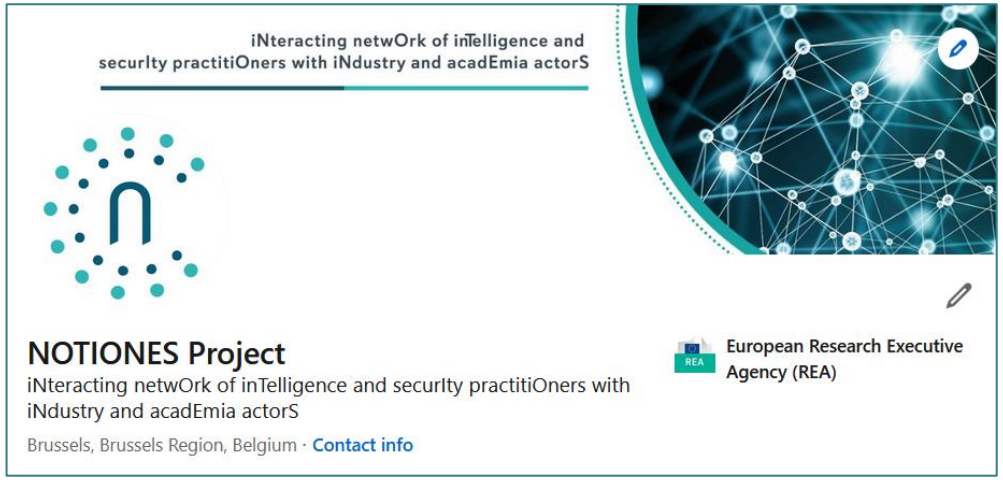
Twitter account | https://twitter.com/NOTIONES_EU



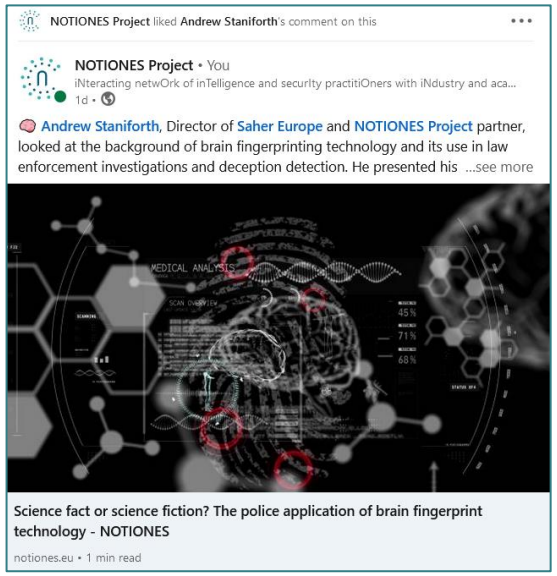
Scan Me

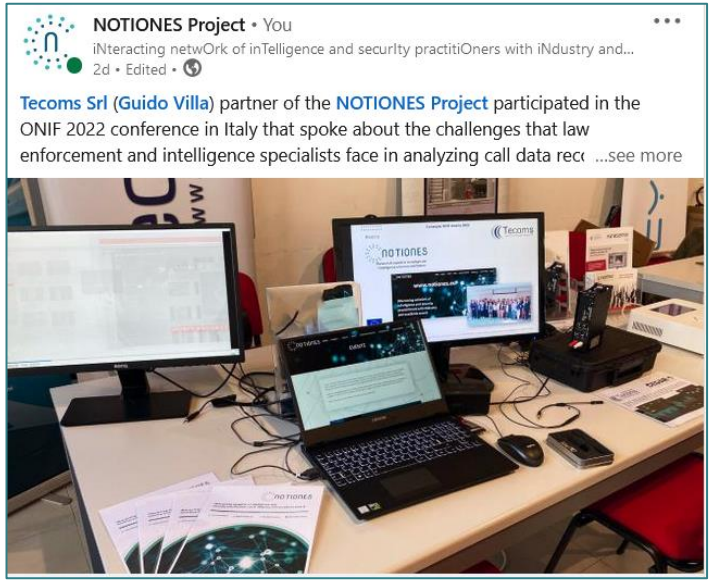
DISSIMINATION & COMMUNICATION

LinkedIn account | https://www.linkedin.com/in/notiones-project-93aa22224/



Scan Me





Thank you for your attention!
Contact us, get involved, stay updated:

office@notiones.eu

www.notiones.eu

@NOTIONES_EU

NOTIONES