NOTIONES

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

D3.1

Technologies for IMINT and SIGINT

-PUBLIC VERSION

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

Project Details

Acronym: **NOTIONES**
Title: **iNteracting netwOrk of inTelligence and securIty practitiOners with iNdustry and acadEmia actorS**

Coordinator: **FUNDACIÓN TECNALIA RESEARCH & INNOVATION** (SPAIN)

Reference: 101021853
Type: Coordination and support action

Program: HORIZON 2020
Theme: Pan-European networks of practitioners and other actors in the field of security
Topic-ID: SU-GM01-2020

Start: 01.09.2021 – 31.08.2026
Duration: 60 months

Consortium:

Id	Participant Name	Short name	Country
1	FUNDACIÓN TECNALIA RESEARCH & INNOVATION	TECNA	Spain
2	ZANASI ALESSANDRO SRL	Z&P	Italy
3	LAUREA UNIVERSITY OF APPLIED SCIENCES LTD	LAU	Finland
4	BULGARIAN DEFENCE INSTITUTE	BDI	Bulgaria
5	DEFENCE RESEARCH INSTITUTE	DRI	France
6	FONDAZIONE ICSA – INTELLIGENCE CULTURE AND STRATEGIC ANALYSIS	ICSA	Italy
7	BAR ILAN UNIVERSITY EUROPE INSTITUTE	BIU	Israel
8	AGENCY FOR THE PROMOTION OF EUROPEAN RESEARCH	APRE	Italy
9	TEKNOLOGIAN TUTKIMUSKESKUS VTT OY	VTT	Finland
10	Expert.AI SPA	EXP.AI	Italy
11	SAHER EUROPE	SAHER	Estonia
12	MARKETSCAPE A/S	MS	Denmark
13	TECOMS SRL	TECOMS	Italy
14	SYNYO GmbH	SYNYO	Austria
15	REGIONAL POLICE HEADQUARTERS IN RADOM	KWPR	Poland
16	BULGARIAN STATE AGENCY FOR NATIONAL SECURITY	DANS	Bulgaria
17	CARABINIERI LT.GENERAL LEONARDO LESO	LESO	Italy
18	FINANCIAL INTELLIGENCE UNIT OF LATVIA	FIU	Latvia
19	BORDER POLICE OF BOSNIA HERZEGOVINA	BHBP	Bosnia & Herzegovina
20	ISEM-INTERNATIONAL SECURITY AND EMERGENCY MANAGEMENT INSTITUTE, n.p.o.	ISEMI	Slovakia
21	KHARKIV NATIONAL UNIVERSITY OF INTERNAL AFFAIRS	KhNUIA	Ukraine
22	POLITSEI.JA PIIRIVALVEAMET	EPBG	Estonia
23	MINISTRY OF INTERIOR OF GEORGIA	MIA	Georgia
24	POLICE SERVICE OF NORTHERN IRELAND	PSNI	UK
25	SWEDISH POLICE AUTHORITY	SPA	Sweden
26	POLICIA JUDICIARIA PORTUGUESE	PJ	Portugal
27	MILITARY ACADEMY "GENERL MIHAILO APOSTOLSKI" – SKOPJE	MAGMA	North Macedonia
28	HOCHSCHULE FÜR DEN ÖFFENTLICHEN DIENST IN BAYERN	HFOED	Germany
29	GOBIERNO VASCO - DEPARTAMENTO SEGURIDAD	ERTZ	Spain

Deliverable Details

Number: **D3.1**

Title: **Technologies for IMINT and SIGINT**

Lead beneficiary: VTT

Work package: WP3

Dissemination level: PU (Public)

Nature: Report (RE)

Due date: 30.04.2022

Submission date: **07.06.2022**

Authors: **Jussi Varis, Matthieu Molinier, Sirra Toivonen, Satu-Marja Mäkelä**, VTT

Reviewers: **Giulia Venturi**, Z&P;
Ciro Caterino, Exp.AI
Erkuden Rios Velasco, TECNA

Version History:

Date	Version No.	Author	Notes	Pages (no.)
17.1.2022	0.1	Erkuden Rios	TOC	All
28.2.2022	0.2	Matthieu Molinier, Jussi Varis	IMINT and SIGINT definitions and scope	All
17.3.2022	0.3	Jussi Varis, Matthieu Molinier	First draft	All
25.4.2022	0.4	Matthieu Molinier, Jussi Varis	Second draft	All
10.5.2022	0.5	Giulia Venturi, Ciro Caterino	First review	Chapter 3
23.5.2022	0.6	Jussi Varis Sirra Toivonen Matthieu Molinier Satu-Marja Mäkelä	Version ready for the final review	All
30.5.2022	0.7	Giulia Venturi, Ciro Caterino Erkuden Rios Velasco	Final review	All
31.5.2022	0.8	Sirra Toivonen, Satu-Marja Mäkelä	Version ready for finalization	All
4.6.2022	1.0	Sirra Toivonen, Matthieu Molinier	Final version	All

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

Table of Content

List of Figures

List of Tables

Acronyms

AI/ML	Artificial Intelligence/Machine Learning
ARTEMIS	Airborne Reconnaissance and Targeting Multi-Mission Intelligence System
COMINT	Communications Intelligence
EO	Earth Observation
ELINT	Electronic Intelligence
EOB	Electronic Order of Battle
ESA	European Space Agency
ETSI	European Telecommunications Standards Institute
EU	European Union
EW	Electronic Warfare
FISINT	Foreign Instrumentation Signals (or Signature) Intelligence
GCHQ	Government Communications Headquarter (UK)
GEE	Google Earth Engine
GEOINT	GEOspatial INTelligence
GSM	Global System for Mobile Communications
HAPS	High-altitude platform systems
HF	High Frequency
HUMINT	HUMan INTelligence
IC	Intelligence Community
IED	Improvised Explosive Device
IMEI	International Mobile Equipment Identity
IMINT	IMagery INTelligence
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
ISR	Intelligence, Surveillance and Reconnaissance
LEA	Law Enforcement Agency
LI	Lawful Interception
LOROP	Long Range Oblique Photography
M2M	Machine-to-Machine
MASINT	Measurement and Signature Intelligence
NASA	National Aeronautics and Space Administration

NATO	North Atlantic Treaty Organization
NSA	National Security Agency (USA)
OSINT	OPen Source INTelligence
RADINT	Radar Intelligence
SAR	Synthetic Aperture Radar
RD	Retained Data
SIGINT	SIGnals INTelligence
SSEUR	SIGINT Seniors Europe
TEP	Thematic Exploitation Platform
TELINT	Telemetry Intelligence
USA	United States of America
UAV	Unmanned Aerial Vehicle
UHF	Ultra High Frequency
UKUSA	United Kingdom - United states of America Agreement
VHF	Very High Frequency
VHR	Very High Resolution

Executive Summary

The present D3.1 Technologies for IMINT and SIGINT report is focused on providing up-to-date information about the latest technological developments in Imagery INTelligence (IMINT) and SIGnal INTelligence (SIGINT). In addition, a brief description of IMINT and SIGINT definitions and integration into the intelligence cycle are provided. The report handles the development of different imagery intelligence technologies, UAVs, HAPS and satellite intelligence, though as the biggest implementation area satellite imagery intelligence is handled the broadest. For Signal intelligence the report shares views of the different areas of this intelligence type. A chapter concerning the legal constraints for acquiring the data is provided as background. In general SIGNAL intelligence technologies are military and therefor detailed information is usually not shared.

The details of the reference methodology followed to conduct the study of the state of the art are described in this deliverable in chapter 1.2. This methodology has been followed also in other tasks of the WP3.

The report also includes information of the projects, publications tools and datasets for both IMINT and SIGINT. Furthermore the most important technology providers worldwide are listed. This information is updated in the separate project CTI-catalogue.

The document also provides a number of discussion points and recommendations focused on the foreseeable development baths, improvements and approaches to tackle different aspects of imagery and signal intelligence, as well as about the necessary holistic approach to be adopted in the intelligence cycle to increase efficiency.

The conclusions summarize the key findings of the report.

1. Introduction

The objective of this deliverable is to provide an overview of IMAgery INTelligence (IMINT) and SIGnals INTelligence (SIGINT) from a technological point of view, as well as insights on the relevance and applicability of these technologies for the Intelligence Community (IC) and Law Enforcement Agencies (LEAs) in the contexts of security or detection of terrorist activities. Since the main target audience of this deliverable is represented by Intelligence and Security practitioners as well as Law Enforcement Agencies (LEAs), care has been taken to present technologies in layman terms.

The state-of-the-art overview of IMINT and SIGINT technologies is presented in sections 2 and 0 respectively, following a similar structure. As an introduction to each section, the intelligence collection discipline is defined, including a short historical context, from the original definition in the military context to its applications for LEAs and recent developments, as well as the connection to other intelligence areas, especially those covered in other WP3 deliverables. Then, the main sources of data acquisition and sensor platforms are listed, with their respective capabilities and limitations relevant for civilian applications. Regarding SIGINT, the reader should note, that it belongs traditionally to the domain of the military and those intelligence agencies, which deal with foreign signals and foreign threats to national security. In this context, the state-of-the-art in SIGINT technology and methodology has always been highly classified. Concerning LEAs, it is not clear at all, which kind of SIGINT technology or methodology they use. This may also be a question of terminology. Intercepting mobile communications or internet communications is often mentioned. It can be argued that the former can be considered SIGINT, whereas the latter is mass surveillance. Due to the lack of LEAs' SIGINT knowledge, the SIGINT sections in this document are dominated by publicly available information about military and intelligence agency related information.

Dedicated subsections describe projects, initiatives and information sources (publications, reports, blog posts or tweet accounts) focused on IMINT or SIGINT approaches or solutions that discuss these technologies (sections 2.8 and 3.4, respectively). Software tools, frameworks and datasets used for conducting IMINT or SIGINT are listed in the Solutions sub-sections (sections 2.9 and 3.5, respectively). Relevant projects, publications, tools, frameworks and datasets for IMINT and SIGINT are also listed in the NOTIONES CTI_catalogue.

The importance of IMINT and SIGINT intelligence collection disciplines has been visible from the start of the war in Ukraine. *"On March 11st, 2022, Ukraine's vice prime minister Mykhailo Fedorov called on eight commercial satellite companies to share SAR satellite imagery, in a plea to help Ukraine's Armed Forces see Russian troop movements."[142]* Also commercial detailed VHR satellite imagery has been released for **media usage**, many of which has then been published on mainstream media (written press, TV) and social media.

1.1 Intelligence cycle

Intelligence cycle is the fundamental cycle of intelligence processing in a civilian or military intelligence agency or in law enforcement as a closed path consisting of repeating nodes [1]. NOTIONES Deliverable 2.3 [2] concentrates specifically on the definitions of the nodes of the intelligence cycle, and on how they have been implemented in various agencies, entities or countries, particularly in the European Union countries.

Depending on the agency or entity, the definitions of the various nodes vary somewhat. For example, Figure 1 shows the cycle definition utilized by EUROPOL [3].

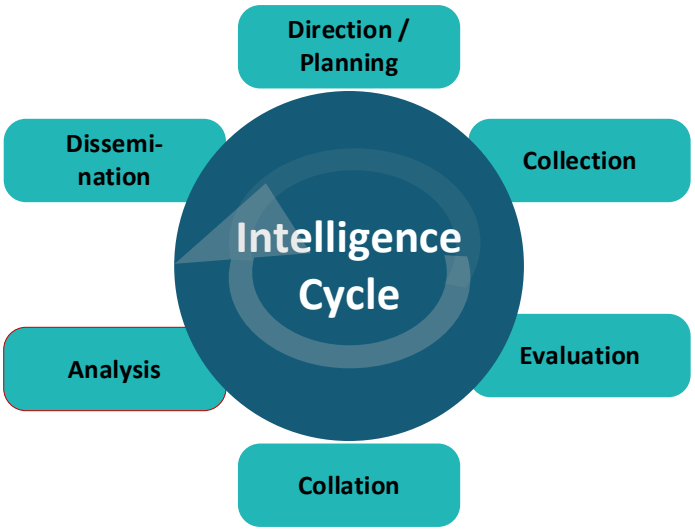

Figure 1. Intelligence cycle by EUROPOL [3].

Imagery Intelligence (IMINT) and Signals Intelligence (SIGINT) have traditionally belonged to the second node of the cycle: *intelligence collection*. Intelligence collection management [4] is the process of managing and organizing the collection of intelligence from various sources. It should be noted, that in its historical definition from the military context, the intelligence collection does not cover analysis of the intelligence or data collected. The collection department of an intelligence organization may attempt basic validation of what it collects, but it is not supposed to render judgement of its significance. However, in the context of civilian applications and with the recent developments in IMINT data availability and value-adding services for a whole range of applications, data collection and analysis are increasingly performed together or not necessarily by separate entities like they used to be in the military context.

1.2 Methodology of the state-of-the-art analysis

The present report fits in the research work of the NOTIONES WP3 *Technologies for Intelligence* whose main objective is to conduct a full review of the technologies and tools used in the intelligence cycle and evaluate their utility in light of the challenges posed by them for intelligence and security applications.

The WP3 reports contribute to the NOTIONES knowledgebase around technologies for intelligence. The analysis performed is documented in seven reports that address a specific intelligence field or a specific supporting technology, namely:

- *D3.1 Technologies for IMINT and SIGINT*, dealing with technologies for IMagery INTelligence and SIgnal INTelligence.
- *D3.2 Technologies for MASINT*, dedicated to Measurement And Signature INTelligence, with a particular focus on Chemical, Biological, Radiological, Nuclear, and explosives (CBRNe) threats.
- *D3.3 Technologies for OSINT and Web Analysis*, which reviews technologies for open source, social media and web analysis as well as the Dark Web analysis.
- *D3.4 Technologies for HUMINT and Support Activities,* covering technologies for HUman INTelligence and Support activities.

- *D3.5 Technologies for Big Data.*
- *D3.6 Technologies for Artificial Intelligence.*
- *D3.7 Technologies for Mass Surveillance.*

The reference methodology for the technology surveys in WP3 was born from the basis of conducting a thorough review of the technologies from multiple angles. In this sense, the deliverables review multiple public information sources, including the EU-funded project and initiatives on the subject, the main publications, peer-reviewed papers, web pages, news, whitepapers, reference documents on best practices and standards, etc. The innovative technology solutions identified from these sources were complemented with other commercial technologies found in the literature and in public webs.

The sources of information reviewed are described in detail in deliverable D5.1 *Methodology for the monitoring of innovation* of WP5, which describes the technology surveillance methodology that will be followed in NOTIONES WP5 to search for new research areas, new technologies and new terrorist threats of interest of NOTIONES practitioners. Beyond these sources, other sources dedicated to the particular focus of WP3 studies were also analysed, as explained in the corresponding deliverables.

The analytical techniques used in WP3 state-of-the-art analysis conform to the set of data analysis techniques described in D5.1. It is worthy to mention that in order to gather and process the huge amounts of sources analysed dedicated web crawlers and scripts have been developed and used as part of the work of the WP3.

Once the relevant sources and data were identified, they were studied and analysed one by one by expert analysts, with the aim to produce classifications, comparative results among the technologies and solutions, clarifications, and comprehensive summaries of the findings.

Following this methodology, the WP3 has produced a set of easily readable reports that establish the common basis for intelligence technology landscape understanding in the project. These reports will be used by NOTIONES partners as reference documents during the project lifetime in different tasks. In WP5 the surveys conducted now in WP3 will be followed up and completed in the future with new tools and products resulting from the continuous monitoring of the identified technologies and solutions. The WP3 reports will also allow clarifying technical aspects when discussing on technology options and drawbacks in WP6 working groups, as well as in conferences and workshops of WP7.

Besides the WP3 reports, the references of the most relevant sources were collected in the “NOTIONES CTI Catalogue” started in WP3 as a common knowledge corpus of Cyber Threat Intelligence (CTI) for NOTIONES participants. Please note that the core of the Catalogue for each of the seven subjects analysed has been documented in the corresponding WP3 deliverable as reference list or as part of the document annexes. Furthermore, the catalogue is also available to all the NOTIONES partners in form of MS Excel file which facilitates a quick access to and fine-grained searching of the references for consultation.

2. The state-of-the-art of IMINT technologies

2.1 Definition of IMINT and its sub-categories

The historical definition of IMINT is in the military context, however recent evolution takes into account for technology evolution especially in satellite imagery capabilities and drones.

Currently e.g. U.S. intelligence Community still defines IMINT as the following: *IMINT—Imagery Intelligence includes representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. Imagery can be derived from visual photography, radar sensors, and electro-optics. NGA is the manager for all imagery intelligence activities, both classified and unclassified, within the government, including requirements, collection, processing, exploitation, dissemination, archiving, and retrieval [5].* It is to be noted that, in this definition, some wording refers to early days of IMINT ("on film", "visual photography") but do not correspond anymore to how data is collected nowadays from satellites or aerial platforms, where data is available digitally soon after collection and transferred automatically to ground segments.

Wikipedia gives a more recent definition of **Imagery intelligence** (**IMINT**), *as an intelligence gathering discipline wherein imagery is analysed (or "exploited") to identify information of intelligence value.[1] Imagery used for defence intelligence purposes is generally collected via **satellite imagery or aerial photography**. As an intelligence gathering discipline, IMINT production depends heavily upon a robust intelligence collection management system.*

In this report, IMINT refers to data collected via satellites or aerial platforms, including airplanes, helicopters, unmanned aerial vehicles (UAV)/drones and High Altitude Platform Systems (HAPS).

Importance of adopting imagery intelligence area in the Intelligence cycle:

Nowadays IMINT often has an ever-increasing role for assessing situations autonomously. On one hand this is due to recent trends in Earth Observation where many military and civil applications push demand for timely monitoring, which in turn favoured development of satellite constellations capable of imaging the entire land surface daily or even several times a day and of the capacity to analyse the data flows by demand. Observations can be divided to surveillance (systematic and permanent) whose coverage area may vary and in reconnaissance (directly related to operations or even precursor to a strike). Depending on the need IMINT can be used for assessing the situation, the evolution of the situation, accurately locate targets ("targeting"), assess the associated risks, and the effectiveness of an action undertaken both for military and civil circumstances. Further, IMINT is a source of decision-making by political power.

The proliferation of imagery systems worldwide including also the relatively inexpensive platforms that are easily transported and operated, such as unmanned aerial vehicles, are becoming available to wide types of users and organisations. The developments in AI and especially for image analysis enable for efficient results according to the intelligence needs.

Connection to other INT areas: Imagery intelligence is closely linked to other intelligence types, like OSINT (Open Source INTelligence), MASINT (Measurement and Signature Intelligence), GEOINT (Geospatial Intelligence) and Mass Surveillance. The following defines shortly the areas that are closely linked to IMINT but within NOTIONES belong to OSINT, MASINT and Mass surveillance, as follows.

- **OSINT** includes open satellite imagery, open platforms displaying satellite imagery (e.g. Google Maps / Google Earth, further information in D3.3)
- **MASINT:** IMINT can be complemented by non-imaging MASINT electro-optical and radar sensors (further information in D3.2).
- **GEOINT** is the analysis and visual representation of security related activities on the earth. It is produced through an integration of imagery, imagery intelligence, and geospatial information. Nowadays usage of IMINT and GEOINT often overlap.

- **Mass surveillance** includes
    - CCTV used for mass surveillance vs CCTV used for security intelligence (e.g. targeting monitoring of someone or count people in a crowd).
    - More widely: "*The Aerospace Corporation of the United States describes a near-future event they call the "GEOINT Singularity" in which everything on the surface of the earth will be monitored at all times and analysed by artificial intelligence systems.*"[6] This is due to recent trends in Earth Observation where many applications push demand for timely monitoring, which in turn favoured development of NewSpace startups launching constellations of small cubesat satellites capable of imaging the entire land surface daily or even several times a day (Planet Labs, ICEYE).
- Please note that NOTIONES D3.7 Mass surveillance will treat the use of CCTV for surveillance, e.g. face recognition, vehicle identification, license plates as means for Mass surveillance, , without going into details about the technology (e.g. models of cameras, transmission of circuit to camera...). Satellite image processing is also part of mass surveillance when it comes to crowd analysis for example.

Imagery intelligence could be collected from different platforms (Table 1), but this state-of-the-art review concentrates on airborne and spaceborne platforms as they are the most important and most versatile. Spaceborne platforms (i.e. imaging satellites) have been historically *government-owned* and have produced highly reliable and secured information (e.g. Landsat program from NASA/USA, or Copernicus Sentinels from ESA/EU). Since the early 2000s, *commercial satellite image providers* have emerged with industry-owned satellites acquiring images at very higher spatial resolution (VHR), providing much more spatial details than government-owned satellites available for civilian applications. The growth of commercial imaging satellites has accelerated over the past few years, with the emergence of *cubesats and satellite constellations* providing more frequent and cost-effective VHR imagery [7]. Airborne platforms consist of manned, unmanned (UAV), fixed wing, and rotary aircrafts, as well as balloons and High-altitude platform systems (HAPS). Sensors and cameras mounted on drones ("hovering type"), balloons or HAPS can provide continuous (known as persistent) coverage of a location or target for a given time, while the sensors are chosen according to the need of the mission and the mission conditions. The pros and cons of the two types of platforms are discussed in the next subsections.

Table 1. Properties and capabilities of main IMINT data sources available for civilian applications (possible applications in green, with restrictions in orange, not possible in red).

Properties	VHR imagery satellites	Aerial imagery & drone/UAV	HAPS High Altitude Aerial Platforms
Spatial resolution	30 cm – 1 m[1] military about 10 cm	1 cm – 30 cm	Few tens of cm
Temporal resolution (revisit frequency)	few days to daily	Irregular, on-demand flights	continuous on defined area, once deployed
Target detection			
Infrastructure changes			
Airplanes Ships Tanks vehicles			
Vehicle tracking	Short time only (1 – 3 mn)		
Licence plate recognition		Close range only	
Crowds			
Single pedestrian detection / counting			
Single pedestrian tracking			
Face recognition		Close range only (< 100m)	
Operational comparison [136]			
Coverage	3 GEO satellites can cover the whole Earth surface. Planet constellation provides daily coverage of the whole globe.	Coverage near the launch area during the mission	Requires tens of thousands of vehicles for global coverage; however, can provide consistent coverage over a specified area
Maintenance and Logistics	Small maintenance and logistics footprint on the ground	Requires pilots, engineers, and supply channels for operations on the ground	Requires pilots, engineers, and supply channels for operations on the ground
Regulation	Flight license not required; requires permission for service provision as per individual country rules (most countries have access)	Requires flight license for UAV/Drones and permission for service provision	Requires flight license and permission for service provision

The main data sources for IMINT are introduced in the next two sections, with a quick overview of data acquisition platforms, data acquisition frequency, capability and limitations, means of procurement (data providers). **Earth observation (EO)** is the general term used to refer to the gathering and analysis of information about planet Earth's physical, chemical and biological systems via remote sensing technologies, usually involving satellites carrying imaging devices [125], as well as aerial platforms (airplanes, helicopters and unmanned aerial platforms). These technologies can also be used for security purposes like border and maritime surveillance or crises management.

2.2 Main sensors used in IMINT and their characteristics

Sensors that can be mounted on aerial platforms or satellites include:

- **Optical sensors:** traditional sensors acquiring visible light, as well as infrared. Optical sensors are widely used as they offer familiar views of the scene of interest, some with high spatial resolution that allows detailed analysis.

[1] 15 cm HD is achieved through a process that intelligently increases the number of pixels in a native 30 cm resolution image, resulting in an improved visual experience to enhance manual and automated feature extraction efforts from satellite imagery. Pub Geo4i Eusi Linkedin PDF

- **SAR** (*Synthetic Aperture Radar*): uses the motion of the radar antenna over a target to provide finer spatial resolution than conventional stationary beam-scanning radars. An active sensor, with different wavelengths in the microwave domain, imaging modes, polarizations or interferometry capability (allowing detection of fine scale motion down to few millimetres) [126].

- **Thermal imaging:** several current satellites (e.g. Landsat) and aerial imaging platforms include thermal imaging capacity although it is not their main sensing objective. The sensor offers night time imaging capacity, but the resolution is lower compared to other optical cameras. Usually the main solutions fields in monitoring of droughts, wildfire, urban heat islands, agriculture, weather and climate. A recent development is to build small-sat constellations with thermal imaging sensors combined with field specific analytics services and tackle the limitations of existing thermal imaging capabilities (low spatial and temporal resolutions).

- **LiDAR** *(Light Detection and Ranging) is a* remote sensing sensor type that emits light from a fast firing laser sensor and collects the reflection to determine points and far distances to map terrain and structures or see through dense forests and build 3D scenes of a target. The sensor is typically aerial or terrestrial, requiring an external platform such as a fixed wing aircraft, helicopter, or UAV (drone) [127]. For this reason LiDAR sensors are often used for geological and climate analysis missions, but use case also include security intelligence missions.[128]

Resolutions in Earth Observation (EO) can refer to several terms:

- **Spatial resolution** is related to pixel size, i.e. the dimension covered in the physical world corresponding to the extents of an image pixel. Ranges of spatial resolutions are often referred to as medium resolution (typically few hundred meters), high resolution (about 10 to 20 meters, down to 1 meter), and very high resolution (VHR) which often refers to sub-metric resolution (less than 1 meter pixel size for spaceborne sensors, down to 30cm for the highest available spatial resolution commercially). The limits between medium and high resolution vary between sources, as there is no absolute definition and any historical definition was made at a time when spatial resolution was overall coarser than it is now. It is however commonly accepted that VHR refers to sub-metric spatial resolution.
- **Spectral resolution** refers to the range of the electromagnetic spectrum that can be observed by sensors. Each spectral band covers a certain range of the electromagnetic spectrum, and in *multispectral sensors*, only a few spectral bands are available (typically 4 for VHR satellites,- 8 to 11 bands for Landsat 7 and 8 satellites respectively, 13 bands for Sentinel-2). Most spaceborne optical sensors include visible channels (Red Green Blue bands, also known as RGB) and one or several infrared bands (some including short-wave infrared SWIR). Some satellites can also include a thermal band, such as Landsat 7 and 8. *Hyperspectral sensors* can contain dozens or hundreds of spectral bands, each band covering a narrower region of the spectrum than typical multispectral bands, and altogether forming a more refined and continuous representation of the spectrum. SAR sensors observe an entirely different part of the electromagnetic spectrum, in the microwave domain.
- **Radiometric resolution**: the radiometric resolution of remote sensing imagery stands for the ability of the sensor to distinguish different intensity values (similarly to grey-scale values in a greyscale digital image). Radiometric resolution is measured in bits. The more bits an image contains, the more grey-scale values can be stored, and, thus, more differences in the reflection on the land surfaces can be spotted [122].

- **Temporal resolution** or **repeat cycle** refers to the minimum interval of time between the acquisitions of two images by the same satellite over the same area under the same orbital conditions. This is also called *revisit frequency*, and is a physical limit of orbiting satellites that is determined almost entirely by the altitude at which the satellite is orbiting, and what type of orbit (e.g. polar, geostationary). Most Earth Observation satellites are polar orbiting satellites, at an altitude of a few hundred kilometres, to provide adequate resolutions to observe targets of interest of different sizes [123]. The trade-off is that the revisit frequency of polar orbiting satellites is usually a few days, depending on the satellite and latitude of the observed area (typically 14-16 days for a Landsat satellite, 2 to 5 days for 2 Sentinel satellites). Nowadays revisit frequency can be increased by using constellation of a number of identical satellites on phased orbits (2 Sentinel-1 or Sentinel-2 satellites, more than a hundred Planet satellites). Geostationary satellites acquire images over the same area of the surface of the Earth, by design, thus temporal resolution is only determined by the capacity of the sensor to acquire and download images to the ground segment. Geostationary satellites can have a very high temporal resolution, useful for weather forecast and modelling, yet have low spatial resolution since the geostationary orbit is located at 36 000 km from the Earth surface.

Each sensor type offers advantages in observing certain types of targets or phenomena, and often a combination of different sensors from different platforms is needed to properly analyse and provide meaningful insights about a given situation on the ground surface. This type of data processing is called data fusion, e.g. the combination of EO data acquired by different sensors which may have different spatial, spectral and temporal resolutions.

2.3 Usual tasks performed in EO image analysis

- **Classification**: can be called also mapping when the target variables are discrete. This is the most common task in remote sensing, as it is common to most application domains – mapping forest, agriculture or any land cover, but also damages due to natural disasters or anthropogenic sources.
- **Regression/continuous variable estimation** refers to the retrieval of intensive variables. Most of the times are not directly observable by sensors and must be modelled (e.g. surface temperature, forest density or percentage of damaged buildings). This can also be called also mapping when target variables are continuous.
- **Object/target detection** refers to the binary detection (presence / absence) of a given object or target in an image, for example detecting vehicles (e.g. cars, buses, airplanes). Object or target detection can be either coarse, returning only a bounding box around each detected target, or more precise by providing the delineation of target boundaries. Object/target detection is usually not concerned with target identification, but can be the first step towards it.
- **Object/target identification** goes further than detection by characterizing of the type or nature of the object/target. This task is similar to classification, but bound to a well delineated object, whereas classification can be done pixel by pixel without the need to detect or delineate objects first. Identification accuracy can be enhanced by intelligent detection tools.
- **Change detection** compares at least two images acquired over the same location at different dates, before and after any phenomenon or event that induces changes on the Earth surface or infrastructures (land, sea or atmosphere), and aims at delineating areas where changed occurred. - e.g. mapping building changes.
- **Time series analysis** goes beyond change detection by using more than 2 images acquired over the same location (often tens or even hundreds of images), to provide a more dense, timely and precise analysis of events or phenomena that induce gradual or subtle changes on the Earth surface. Time series analysis has been used extensively to monitor gradual phenomena of natural

origin (phenology, agricultural crop cycle), long-term impacts of human activities (e.g. pollution incidents, deforestation and forest degradation) as well as recovery after an abrupt event (natural disasters).

2.4 Satellite imagery

Satellite imagery includes acquiring imagery information from military and commercial satellites. The mission of the satellite defines its orbit/bath, capabilities and constellations. This review concentrates on commercial satellite capabilities as very little information is available from military satellite capabilities. According to the recent news US National Reconnaissance Office (NRO) announced a large commercial imagery contract with commercial satellite companies (Planet and ICEYE) to support their capabilities with commercial imaginary (the contract will provide additional 100 million square kilometres imagery weekly). The aim is to enhance information sharing and decision making through unclassified and sharable information to increase mission critical situational awareness. [144]

- **Open and free Earth Observation (EO) / satellite imagery**: The number of commercial satellites is **growing dramatically**. The explosive growth is partly because of the use of larger constellations of smaller satellites (cubesats) by emerging companies (startups), which have used smaller numbers of highly capable satellites [143]. Open and free images captured by Copernicus Sentinels and Landsat have been routinely acquired all over the world for continuous monitoring of the land surface for many years and decades respectively, mostly for land cover and other environment related applications.
- **Commercial imagery**: Very High Resolution (VHR optical : MAXAR; Planet Labs) and Radar/SAR (TerraSAR-X, ICEYE, Capella Space) is available on orders (images are acquired after being ordered) or through archives from previous purchases by other customers. Commercial satellite providers do not perform continuous monitoring, except new space companies such as PlanetLabs (cubesat satellite constellations). One drawback of using commercial satellite imagery for imagery intelligence or surveillance is that satellite orbits are known, they are public and trackable on several live websites and thus predictable. Furthermore, satellite images are usually acquired at a fixed time locally (sun-synchronous orbit, overpass always at same time of the day over any point on Earth).
- **Capability** : the criteria to assess the capability include what can be observed (spatial resolution vs targets / object of interest), how frequently (revisit frequency), imaging capability anywhere in the world (the sky is the limit, satellites are above it) and recently also the video acquisition ability (from very short ones up to 1 to 3 minutes, due to orbital constraints). Satellite imagery is very powerful in detecting phenomena, changes and assets that can be observed at the available resolution.
- Capabilities will be developed also through increasingly powerful development of machine learning and AI capabilities. Recent paper reports of artificial intelligence tools that continue tracking an object on the ground, even after it turns sharply or disappears into a tunnel. The AI algorithm could be uploaded to processors on some of Earth observation satellites already in orbit without any ground assistance. This aims to turn the low-cost commercial satellites already orbiting the Earth into spy platforms capable of tracing moving targets as small as a car size.[145] In addition to imagery intelligence (IMINT) reconnaissance satellite missions can include Measurement and Signature Intelligence (MASINT), Communications eavesdropping (SIGINT), Covert communications. Monitoring of nuclear test ban compliance (see National Technical Means) and Detection of missile launches. VHR Synthetic aperture radar (SAR) and hyperspectral imaging modes, which have mostly been capabilities of military satellites thus far (except

TerraSAR-X for SAR imagery), are also entering the commercial satellites also with improved capacities. Potential capabilities for tasking, cueing, pointing and dwelling are hard to find publicly. [143]

- **Limitations** of satellite imagery are based on the resolution limitations of the current technology, limitations to observe from above (spatial resolution vs targets / object of interest), orbital constraints of the satellites considered, data availability (VHR data is not acquired continuously as open imagery), cloud coverage that limits the usability of optical imagery, geographical extents, difficulty of interpretation of some imagery (especially for SAR), constraints imposed by military for dual use data (for VHR optical imagery). Furthermore, the payload (e.g. instruments on board) cannot be changed once the satellite is in orbit, and if they fail, are rarely repaired or replaced (the satellite is decommissioned).

2.5 Aerial imagery, drones and Unmanned Aerial Vehicles (UAV)

Aerial (or airborne) imagery refers to pictures and videos taken from aerial perspective. Depending on the type of the aerial imagery system (aircraft, UAV or drone) the flight height varies. (Figure 2)

- **Open and free aerial / UAV imagery** do not allow continuous monitoring. Various aerial imagery datasets exist, used as benchmarks to develop methods for object/target detection and recognition, such as planes, tanks, and ships.
- **Commercial UAV imagery** is available on-demand through various local players. This is a more localised market than satellite imagery. End users can fly or operate drones/UAVs themselves.
- **Capability** : as the platform altitude (few hundred meters) is much lower than for the satellites (few hundred kilometres), the spatial resolution is normally much better, though the difference is lowering. The choice for the capability depends on the need: spatial resolution vs targets/object of interest, how frequently information is needed or max payload that can be carried (e.g. instruments on board the UAV/drones are limited in size and weight). Clouds are usually not an issue, if flying below cloud cover.
- **Limitations** : compared to satellites, aerial platforms acquire images over limited geographical extents. There is no regular revisit frequency (costly deployment), as data is not acquired continuously like open satellite imagery. Civilian drones lack furtivity (unlike military ones). On-demand image procurement over a specific area requires a drone pilot or airplane pilot..
- **Legal aspects : a** European wide regulation is in force for unmanned aircraft vehicles (UAV). The regulation concerns e.g. flight areas, altitudes, persons able to fly the aircrafts and areas available for the imagery intelligence.

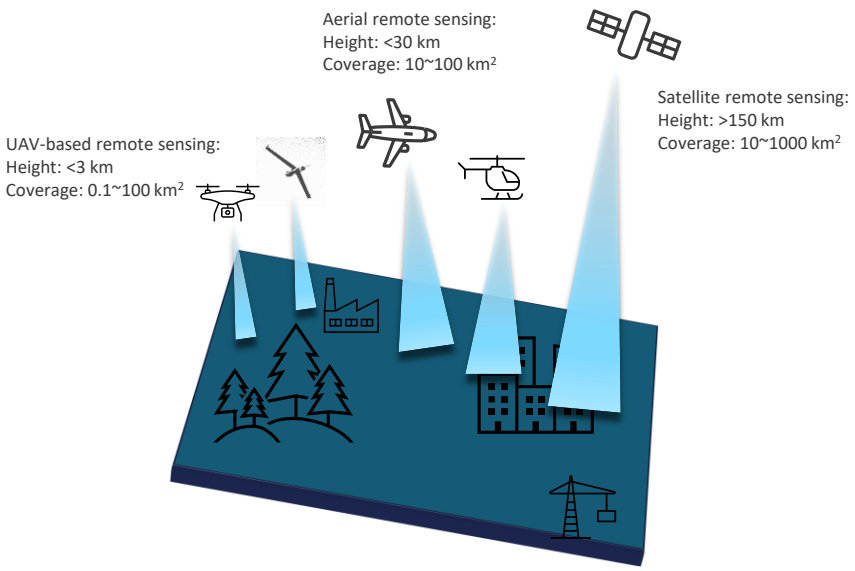

Figure 2. Examples of remote sensing platforms: satellite, manned aviation and low-altitude UAV. Based on [131]

2.6 High-altitude platform systems (HAPS)

"High altitude systems are aircraft that fly or float in the stratosphere, typically at altitudes of around 20km. They can be high-altitude free-floating balloons, airships, or powered fixed-wing aircraft that use either solar power or an on-board energy source. All systems are unmanned and take advantage of weak stratospheric winds and solar energy to operate without interfering with current commercial aviation and with enough endurance to provide long-term services as satellites do."[132] [133]

Figure 3. Example of a HAPS aircraft (NASA Pathfinder Plus – NASA/Nick Galante)

- **Open and free aerial / HAPS imagery :** continuous monitoring during the flight time over the defined area. Assumption that can take advantage of the dataset's development for other aerial platforms
- **Commercial HAPS imagery** : Commercial imagery still missing, but under development.

- **Capability** : as the flight distance is lower than for the satellites, they provide improved high-resolution coverage of specific regions. HAPS can provide long term (up to 2 months) surveillance for a defined area. The choice for the capability depends on the need: spatial resolution vs targets/object of interest, how frequently information is needed or max payload that can be carried (e.g. instruments on board the HAPS). Clouds are an issue as with satellites, since HAPS fly above clouds). In addition to the imagery information, HAPS could provide tactical or emergency communication.
- **Limitations** : structural limitations due to the harsh operational environment in the stratosphere and time, and power consumption issues. A suitable platform is required for different use cases.
- **Legal aspects : a** European wide regulation in force for the unmanned aircraft systems. The regulation concerns e.g. flight areas, altitude and persons able to fly the aircrafts and areas for available for the imagery intelligence.

2.7 Means of IMINT data procurement, visualisation and processing for civilian applications (LEAs)

Ways to access and process EO (from spaceborne or airborne platforms) imagery have greatly evolved several times since the early days of IMINT.

Analysing imagery locally

From the early years of remote sensing up to fairly recently, EO images were first downloaded from data providers (long term public scientific programmes such as MODIS or Landsat, or private imaging satellite operators) then processed locally, either on a standard desktop computer or using a computing cluster for the most demanding processing tasks (such as time series analysis).

Platforms to visualise EO data

- In 2005, Google democratized access to satellite imagery with Google Maps and Google Earth services. Google Maps website offers the possibility to overlay satellite images on top of basemaps to improve user experience for navigation purposes. Google Earth software displays satellite imagery by default as a basemap, that can be augmented with additional layers (street maps and other labels). Google Earth allows smoother and more seamless navigation across the globe, including elevation data for 3D display, as well as the possibility to browse historical images as timelapses, or to import user data or maps. However, images displayed on both Google Earth and Google Maps services are slightly different from those available from EO data providers and come with some limitations: the satellite images displayed on Google Earth and Google Maps are only a subset of all imagery available from EO data providers, e.g. best images usually acquired in summer, selected to contain no clouds or composited/mosaicked to remove clouds (e.g. Landsat imagery displayed on Google Earth basemaps at national/regional scales).

- all VHR images displayed on Google Maps/Google Earth are slightly degraded in spatial resolution (images are less sharp than original images) and spectral resolution (only Red Green Blue bands are displayed, Near Infrared band is not. NB: high/medium resolution images such as Landsat or MODIS contain even more spectral bands in infrared domain, but here again those bands are omitted and only RGB images are shown).

- some VHR images acquired over sensitive sites (such as nuclear powerplants or military bases) are heavily blurred so that the most sensitive details are not visible anymore. However, each VHR image displayed on Google services is also available at full spatial and spectral resolution from the satellite image provider and other resellers. At the cost of a few thousand euros per image, anyone can access them, as there is no border in space or limitation as to what can be imaged [137][138].

These simplifications and degradations in image quality are mainly due to the necessary optimizations for displaying a vast number of images to numerous concurrent users of Google services, to offer a more fluid or seamless browsing experience. Google Maps/Earth services are designed for browsing imagery, not processing or analysing it.

Platforms to process EO imagery / cloud processing:

Instead of downloading images, which is a burden as satellite images take a lot of disk space, a new paradigm was introduced that allows researchers, practitioners and end-users to bring their algorithm to the data. Cloud processing

In 2010, Google introduced the Google Earth Engine, that gives access to original satellite images for processing on the cloud [19]. From 2011 to 2017, Landsat was the most widely used dataset, before Sentinel-2 imagery was introduced to the platform [20]. Landsat data is still a major data source on GEE, with data from the first to the current Landsat series available for use and download.

On-board processing / in orbit processing / edge processing

has been done for years, and recently there has been an increase in interest as both data volumes keep increasing exponentially (in numbers of satellite missions, number of satellites permission or constellation, and size of images) and mainstream methods used to analyse EO images are data-hungry (e.g. machine learning and deep learning). As images acquired by satellites must be downloaded to the ground segment (e.g. network of ground stations receiving images straight from the satellites) for further distribution to all value-adding entities and end users, this introduces delays between data acquisition and its availability to end-users, which can be critical for security and safety applications. Although bandwidth is usually not an issue for traditional imaging satellites acquiring data continuously (e.g. Landsat or Copernicus Sentinels), it can become a limiting factor for large satellite constellations of CubeSats. One of the motivations of on-board processing is to reduce the amount of data to download from the satellite to the ground segment, by analysing raw data and keeping only relevant information for a given application - for example, getting rid first of cloudy pixels, if the targets of interest are located on the ground surface. Another motivation for on-board processing is to increase timeliness of analysis, e.g. provide insights as soon as possible. In this context on-board processing will have a major role to play in safety-critical or near-real time applications related to situational awareness.

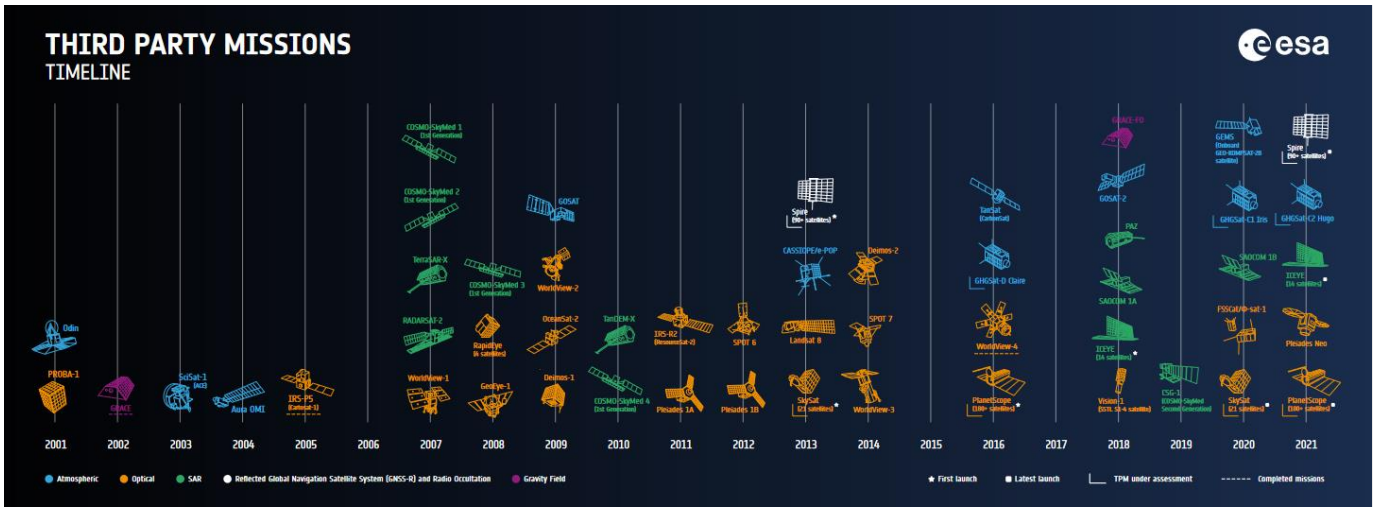

Figure 4. Third Party Missions (TPM) available for free through European Space Agency ESA "Category 1 proposals" for research purposes. Most optical satellites in orange and SAR satellites in green are relevant for IMINT activities related to security or terrorism threats. Source: ESA

2.8 Information sources and Projects for IMINT

2.8.1 Publications

Publications relevant for IMINT were searched on aggregated repositories such on lens.org website. A simple query using the keyword "IMINT" OR "Image intelligence" returned 484 scholarly works since 1970s (Figure 5), mostly authored by Chinese researchers. However, the terms IMINT or Image Intelligence are not widely used in research publications. Using keywords related to the widely used technology terms "satellite image" and "aerial image", refined with complimentary keywords specifying the application areas "security" and "terrorism", returned ten times more publications (4 881, Figure 6) than the basic query using only IMINT.

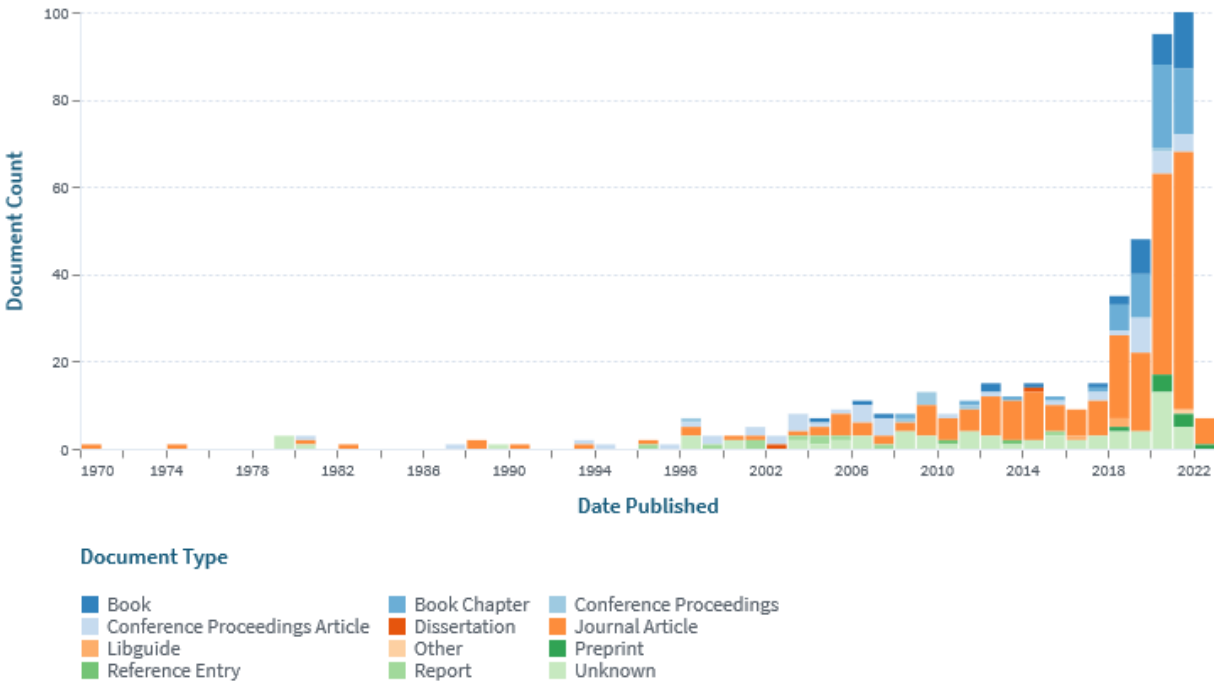

Figure 5. Scholarly works over time on lens-org website, using keywords IMINT" OR "Image intelligence

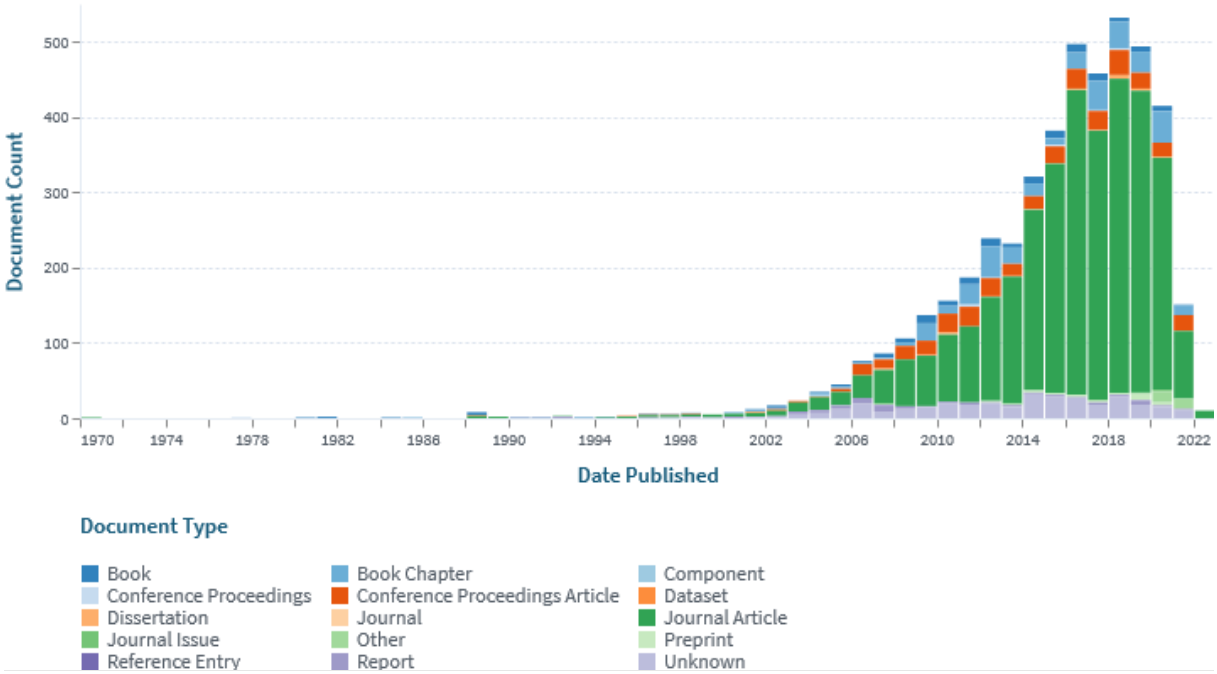

Figure 6. Scholarly works over time on lens-org website, using refined keyword search specifying technology (satellite imagery aerial imagery, Earth Observation) and application areas (security, terrorism)

The vast number of potentially relevant IMINT related publications far exceeds the resources available in NOTIONES to screen them all. Instead, a strategy was defined to narrow down the selection. Priority was given to review articles (spanning a wider scope), recent publications (within the past couple of years) and most cited publications.

Relevant EO reviews for IMINT

ZhiYong, 2021 ([8]). Land cover change detection techniques: Very-high-resolution optical images: A review. IEEE Geoscience and Remote Sensing Magazine.

Molinier, 2021 ([9]). Optical Satellite Image Time Series Analysis for Environment Applications: From Classical Methods to Deep Learning and Beyond. Change Detection and Image Time Series Analysis 2: Supervised Methods, 109-154.

Shimoni, 2019 ([10]). Hyperspectral imaging for military and security applications: Combining myriad processing and sensing techniques. IEEE Geoscience and Remote Sensing Magazine, 7(2), 101-117.

Su, 2021 ([11]). Hyperspectral Anomaly Detection: A Survey. IEEE Geoscience and Remote Sensing Magazine.

Sun, 2021 ([12]). Spaceborne synthetic aperture radar imaging algorithms: An overview. IEEE Geoscience and Remote Sensing Magazine.

Ma, 2021 ([13]). Toward Fine Surveillance: A Review of Multitemporal Interferometric Synthetic Aperture Radar for Infrastructure Health Monitoring. IEEE Geoscience and Remote Sensing Magazine.

Zhu 2017 ([14]). Deep learning in remote sensing: A comprehensive review and list of resources. IEEE Geoscience and Remote Sensing Magazine, 5(4), 8-36.

Xin, 2021 ([15]). Deep Learning for Unmanned Aerial Vehicle-Based Object Detection and Tracking: A Survey. IEEE Geoscience and Remote Sensing Magazine.

Hoeser, 2020 ([16]). Object detection and image segmentation with deep learning on earth observation data: A review-part i: Evolution and recent trends. Remote Sensing, 12(10), 1667.

Hoeser, 2020 ([17]). Object detection and image segmentation with deep learning on Earth observation data: A review—Part II: Applications. Remote Sensing, 12(18)

Gomes, 2020 ([18]). An overview of platforms for big earth observation data management and analysis. Remote Sensing, 12(8), 1253.

EO with Google Earth Engine

Gorelick, 2017 ([19]). Google Earth Engine: Planetary-scale geospatial analysis for everyone. Remote sensing of Environment, 202, 18-27.

Kumar, 2018 ([20]). Google Earth Engine applications since inception: Usage, trends, and potential. Remote Sensing, 10(10), 1509.

Amani, 2020 ([21]). Google earth engine cloud computing platform for remote sensing big data applications: A comprehensive review. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 13, 5326-5350.

Tamiminia, 2020 ([22]). Google Earth Engine for geo-big data applications: A meta-analysis and systematic review. ISPRS Journal of Photogrammetry and Remote Sensing, 164, 152-170.

EO UAV

Shakhatreh, 2019 ([23]). Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges. Ieee Access, 7, 48572-48634.

Yao, 2019 ([24]). Unmanned aerial vehicle for remote sensing applications—A review. Remote Sensing, 11(12), 1443.

Xiang, 2019 ([25]). Mini-unmanned aerial vehicle-based remote sensing: techniques, applications, and prospects. IEEE geoscience and remote sensing magazine, 7(3), 29-63.

EO for counter-terrorism

Zhou, 2009 ([26]). Near real-time orthorectification and mosaic of small UAV video flow for time-critical event response. IEEE Transactions on Geoscience and Remote Sensing, 47(3), 739-747.

Do, 2018 ([27]). Terrorism, geopolitics, and oil security: Using remote sensing to estimate oil production of the Islamic State. Energy research & social science, 44, 411-418.

EO for mapping conflicts

Avtar, 2021 ([28]). Remote sensing for international peace and security: Its role and implications. Remote Sensing, 13(3), 439.

Witmer, 2015 ([29]). Remote sensing of violent conflict: eyes from above. International Journal of Remote Sensing, 36(9), 2326-2352.

EO for crime forensics

Kelly, 2014 ([30]). Validating the remotely sensed geography of crime: A review of emerging issues. Remote Sensing, 6(12), 12723-12751.

Kalacska, 2006 ([31]). Remote sensing as a tool for the detection of clandestine mass graves. Canadian Society of Forensic Science Journal, 39(1), 1-13.

Evers, 2018 ([32]). The application of low-altitude near-infrared aerial photography for detecting clandestine burials using a UAV and low-cost unmodified digital camera. Forensic science international, 289, 408-418.

Blau, 2018 ([33]). Exploring non-invasive approaches to assist in the detection of clandestine human burials: developing a way forward. Forensic Sciences Research, 3(4), 320-342.

Butters, 2021 ([34]). Application of forward-looking infrared (FLIR) imaging from an unmanned aerial platform in the search for decomposing remains. Journal of Forensic Sciences, 66(1), 347-355.

Pensieri, 2020 ([35]). Drones as an integral part of remote sensing technologies to help missing people. Drones, 4(2), 15.

Barone, 2019 ([36]). Forensic geophysics: ground penetrating radar (GPR) techniques and missing persons investigations. Forensic Sciences Research, 4(4), 337-340.

Algahtany, 2016 ([37]). A method for exploring the link between urban area expansion over time and the opportunity for crime in Saudi Arabia. Remote Sensing, 8(10), 863.

EO for border monitoring

Perez, 2017 ([38]). Deep learning for effective detection of excavated soil related to illegal tunnel activities. In 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON) (pp. 626-632). IEEE.

Bassoli, 2019 ([39]). A virtualized border control system based on UAVs: Design and energy efficiency considerations. In 2019 IEEE aerospace conference (pp. 1-11). IEEE.

Coulter, 2012 ([40]). Automated detection of people and vehicles in natural environments using high temporal resolution airborne remote sensing. In Proceedings of the ASPRS Annual Conference (pp. 78-90).

Fytsilis, 2016 ([41]). A methodology for near real-time change detection between Unmanned Aerial Vehicle and wide area satellite images. ISPRS Journal of Photogrammetry and Remote Sensing, 119, 165-186.

Malinowski, 2010 ([42]). Land Border Monitoring with remote sensing technologies. In Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2010 (Vol. 7745, p. 77451V). International Society for Optics and Photonics.

Koslowski, 2018 ([43]). Drones along borders: Border security UAVs in the United States and the European Union. International Studies Perspectives.

Haddal, 2010 ([44]). Homeland security: Unmanned aerial vehicles and border surveillance. Library of Congress Washington DC Congressional Research Service.

U.S. HOUSE OF REPRESENTATIVES, 2010 ([45]) The Role of Unmanned Aerial Systems in Border Security. Hearing before the subcommittee on border, maritime, and global counterterrorism of the committee on homeland security house of representatives, one hundred eleventh congress - second session, July 15, 2010.

EO for mapping slavery

Boyd, 2018 ([46]). Slavery from space: Demonstrating the role for satellite remote sensing to inform evidence-based action related to UN SDG number 8. ISPRS journal of photogrammetry and remote sensing, 142, 380.

LOROP = Long Range Oblique Photography

Thomas Augustyn,(1981) Details of the LOROP camera system.[134]

Petrushevsky V., Tsur (2012) D.Proceedings Volume 8360, Airborne Intelligence, Surveillance, Reconnaissance (ISR) Systems and Applications IX; 836003 [135]

2.8.2 Projects

Below a list of some EU funded research projects from the Cordis database regarding satellite image analysis, aerial surveillance or IMINT related development.

- BorderUAS. https://borderuas.eu/

The project will combine for the first time a lighter-than-air UAV with sophisticated surveillance technology. BorderUAS aims to facilitate effective border surveillance and prevent cross-border criminal activities by supporting search & rescue applications, specifically rough terrain detection, improving the protection of European societies. BorderUAS aims for a holistic UAS surveillance approach integrating aerial and ground components using next generation sensors and technologies and developing a consistent platform used for daily border operations and beyond.

- VIDEO; Video Imaging Demonstrator for Earth Observation. https://video-h2020.eu/

Earth observation images taken by satellites flying into space show the world in so many ways and provide vital information. Satellite images can show environmental changes occurring gradually, like the spread of air pollution over a certain continent. An extra-wide field of view and video observation is the next step. The EU-funded VIDEO project is developing the next instrument generation for Earth observation. It's a novel architecture based on state-of-the-art technologies for mirrors, structures (additive manufacturing), and detection (next generation detector and processing chain). The VIDEO instrument will have the capability to perform high-resolution video monitoring on an extremely wide scene. Partners involved in the project are all from the European space industry value chain.

- BLINK; Satellite Data Acquisition in the Blink of an Eye. https://blink.amphinicy.com/satellite-data-acquisition-blink-eye-blink

It is widely known that key information used in many industries such as meteorology, logistics, navigation, oil and gas, agriculture, ecology and others, comes from space, via Earth observation (EO) satellites. Having this data in a short time frame is becoming essential. Existing ground segment solutions are heavily based on hardware. They are not following technology advances like space hardware do which causes a bottleneck in EO data acquisition: required volume of data is not available quickly or with sufficient value! The objective of this proposal is to provide an innovative, completely software-based data acquisition solution for EO market – Blink, disruptive enough to compete with existing oligopoly in this market segment. The EO market is very interesting as it is being boosted by skyrocketing growth of start-ups in NewSpace industry like SpaceX, OneWeb and Planet, to name a few, and increasing trend of moving from thick hardware solutions towards flexible and dynamic

software solutions as well as moving satellite ground systems and services in the cloud environment. The expected project outcome is a Blink device, a software-based solution for EO ground stations which will enable assembling a full performant ground station at a fraction of time and cost that are usual at a time being. This will bring benefit not just to growing segment of start-up companies, but also to big governmental missions worldwide, including Copernicus – the EU flagship mission for Earth observation. Humanitarian missions will also benefit from Blink. Construction of a larger number of ground stations and a faster GS deployment will significantly reduce time to get satellite images of disaster-struck areas. Therefore, rescue teams will be able to act faster, and hence save thousands of lives and homes. The successful implementation of the project, which already successfully passed Phase 1, with the support of the Horizon 2020 SME Instrument will ensure the company's fast expansion of disruptive innovation for space technology market on EU level and beyond.

- BigEarth; Accurate and Scalable Processing of Big Data in Earth Observation. https://bigearth.eu/

During the last decade, a huge number of earth observation (EO) satellites with optical and Synthetic Aperture Radar sensors onboard have been launched and advances in satellite systems have increased the amount, variety and spatial/spectral resolution of EO data. This has led to massive EO data archives with huge amount of remote sensing (RS) images, from which mining and retrieving useful information are challenging. In view of that, content based image retrieval (CBIR) has attracted great attention in the RS community. However, existing RS CBIR systems have limitations on: i) characterization of high-level semantic content and spectral information present in RS images, and ii) large-scale RS CBIR problems since their search mechanism is time-demanding and not scalable in operational applications. The BigEarth project aims to develop highly innovative feature extraction and content based retrieval methods and tools for RS images, which can significantly improve the state-of-the-art both in the theory and in the tools currently available. To this end, very important scientific and practical problems will be addressed by focusing on the main challenges of Big EO data on RS image characterization, indexing and search from massive archives. In particular, novel methods and tools will be developed, aiming to: 1) characterize and exploit high level semantic content and spectral information present in RS images; 2) extract features directly from the compressed RS images; 3) achieve accurate and scalable RS image indexing and retrieval; and 4) integrate feature representations of different RS image sources into a unified form of feature representation. Moreover, a benchmark archive with high amount of multi-source RS images will be constructed. From an application point of view, the developed methodologies and tools will have a significant impact on many EO data applications, such as accurate and scalable retrieval of: specific man-made structures and burned forest areas.

- MARINE- EO; Bridging Innovative Downstream Earth Observation and Copernicus enabled Services for Integrated maritime environment, surveillance and security. https://marine-eo.eu/

Maritime "Awareness" is currently a top priority for Europe. "Awareness" sought either in regards of maritime security, border control against irregular immigration and safety of navigation while at the same time "awareness" sought in regards of the marine environment and climate change. "Awareness" is sought both for sea-basins of traditional interest like the Mediterranean and the Atlantic as well as for basins currently trending like the Arctic. MARINE-EO teams up a group of 5 maritime authorities (the buyers' group) and a group of 4 prestigious scientific and technical organizations with significant experience in EO and maritime matters (the technical advisors) to

achieve the following objectives: (1) Develop, test and validate two set of demand-driven EO-based services which cover Marine Monitoring and Security Copernicus thematic areas, adopted on open standards, bringing incremental or radical innovations in the field of maritime awareness and leveraging on the existing Copernicus Services and other products from the Copernicus portfolio, (2) Propose a set of "support" / "envelop" services which will better integrate the above mentioned EO and Copernicus-enabled services to the operational logic and code of conduct. Such services shall also bring "closer" the demand side (Public Authorities - PAs) with the EO data providers (Copernicus - contributing missions) and EO data experts and analysts (Service providers/ industry and SMEs) creating a dynamic environment for a single digital market to grow, (3) Strengthen transnational collaboration in maritime awareness sector by facilitating knowledge transfer and optimization of resources for the public authorities which, participate in the buyers group. Pre-Commercial Procurement (PCP) is a powerful tool to tackle these three points under one single joint initiative, and this is why MARINE-EO is in an excellent position to reinforce future capabilities.

- PROMENADE; imPROved Maritime awarENess by means of AI and BD mEthods. https://www.promenade-project.eu/

Marine domain awareness consists of the combination of activities, events and threats that could impact marine activities and the EU territory. The combination of private and public sources of data like the Automatic Identification System or space-related data together with Vessel Traffic Services, Vessel Traffic Management Systems, and Vessel Traffic Monitoring & Information Systems data encourages the development of advanced solutions. The EU-funded PROMENADE project will apply AI and Big Data technologies to improve vessel tracking, behaviour analysis and automatic anomaly detection solutions and promote collaborative exchange of information between surveillance authorities. The project will deliver an open, service-based toolkit with a high-performance computer platform. PROMENADE will improve solutions for the vessel tracking, behaviour analysis and automatic anomaly detection by means of the application Artificial Intelligence (AI) and Big Data (BD) technologies, and to promote collaborative exchange of information between maritime surveillance authorities, shortening the time to market and assuring the compliance with legal and ethical regulations. An open, service-based toolkit implementing "state of art" AI / BD techniques also benefiting of HPC (High Performance Computing) platform is the core activity of the project. The project's developments will be demonstrated and evaluated in 3 operational scenarios and 1 simulated defined by Border Guards Authorities.

- AERIAL-CORE; AERIAL COgnitive integrated multi-task Robotic system with Extended operation range and safety. *https://aerial-core.eu/*

AERIAL-CORE will develop an integrated aerial cognitive robotic system that will have unprecedented capabilities on the operational range and safety in the interaction with aerial co-workers for applications such as the inspection and maintenance of large linear infrastructures. It will implement cognitive capabilities for perception and teaming, aerial morphing to combine long range endurance and hovering for local observations, manipulation involving force interactions, and co-working with humans.

- ALADDIN; Advanced hoListic Adverse Drone Detection, Identification Neutralization. https://aladdin2020.eu/

ALADDIN will study, design, develop, and evaluate, in series of complementary pilots, a counter UAV system as a complete solution to the growing UAV threat problem, building upon a state-of-the-art system and enhancing it by researching on various technologies and functionalities. ALADDIN's sensing arsenal is comprised of a set of custom, innovative, and unique technologies as well as established and standard sensors used for UAV detection and localisation: 1) 2D/3D paired radars; 2) Innovative optro and thermal panoramic imaging; 3) Custom designed acoustic sensors. These will be fused through novel deep learning techniques in order to provide excellent detection accuracy. Further, ALADDIN will study and offer a set of neutralization effectors (jammers, physical and hacking). These sensing and countering capabilities will be operated through an advanced command and control (C2) system. The C2 will achieve great detection and classification accuracy within a large range, by fusing data acquired from all sensors through state-of-the-art deep learning techniques. Operator's efficiency will be enhanced through a novel mixed reality interface with 3D cartographic and situational elements and will be complemented by support to operations like investigation and training.

- FOLDOUT. https://foldout.eu/

Situational Awareness and Alarming is a software component that fuses information from multiple heterogeneous sensors (including ground and airborne), thus reducing cognitive load on the operators. Fusing information from multiple heterogeneous sensors also enables information cross-checking and filtering in order to reduce information overload and hence decrease false alarm rate. For Multi-Altitude Sensor Platforms FOLDOUT technology integrates ground- aerial and satellite data for securing near real-time detection in foliated areas. The technologies provide early and long-distance detection allowing swift alarms or pre-warning to border authorities.

- DARLENE, Deep AR Law Enforcement Ecosystem. https://www.darleneproject.eu/

DARLENE aims to investigate means by which Augmented Reality (AR) can be deployed in real time to aid in LEA decision-making by employing AR capabilities and combining them with powerful ML algorithms, sensor information fusion techniques, 3D reconstruction, wearable technology and personalized context-aware recommendations. Develops image and video processing technologies and capabilities to show the results realtime for LEAs.

- INACHUS, Technological and Methodological Solutions for Integrated Wide Area Situation Awareness and Survivor Localisation to Support Search and Rescue Teams. https://www.inachus.eu/

Crisis incidents may result in difficult working conditions for Urban Search-and-Rescue (USaR) crews. INACHUS aims to achieve a significant time reduction related to Urban Search and Rescue (USaR) phase by providing: 1) Wide-area situational awareness solutions for improved detection and localisation of trapped victim.2) Simulation tools for predicting structural failures. 3) Holistic decision support mechanism aiding in prioritization and mission coordination. Project develops also decision and planning modules for advanced casualty and damage estimation that will be based on input coming from airborne and ground-based laser-scanning and imaging data

- ROCSAFE, Remotely Operated CBRNe Scene Assessment Forensic Examination. https://cordis.europa.eu/project/id/700264

The overall goal of ROCSAFE is to fundamentally change how CBRNe events are assessed, in order to and ensure the safety of crime scene investigators by reducing the need for them to enter high-risk

scenes when they have to determine the nature of threats and gather forensics. For this, ROCSAFE will make use of cost-effective modern remotely-controlled robotic air and ground vehicles (RAVs/RGVs) that are designed for use in rain, wind, and challenging ground surfaces and obstacles. First, RAVs will assess the scene. These will have cameras and can carry an array of innovative new high-performance and rugged miniaturised sensor systems for RN, chemical and biological threats. To reduce the scene commander's cognitive load, ROCSAFE will include new Central Decision Management software and a Command Centre. All images and data will be streamed to this, where it will be analysed and displayed on a sophisticated and intuitive interface with maps and video, showing results of analytics and giving readings geographical context. This will enable the scene commander to assess the nature of threats, develop an Action Plan and an Evidence Plan, supported as needed by the Central Decision Management. It will also assist in coordinating sensors and mobile units. Its data analytics will provide fusion of multiple sensor data sources, to allow probabilistic reasoning about the most likely threats and likely locations of epicentres. After the scene is assessed, RGVs will be dispatched to collect forensic material/evidence, with automatically-optimised routes to avoid hazards. They will have innovative new equipment for forensics collection that will automate best practices. Forensic material will be collected, bagged, tagged, documented, and stored by the RGV. Thus, ROCSAFE will ensure that CBRNe scenes are assessed more rapidly and thoroughly than is currently possible, and that forensic evidence is collected in a manner that stands up in court, without putting personnel at risk.

- SafeShore, System for detection of Threat Agents in Maritime Border Environment. http://safeshore.eu/

Small Remotely Piloted Aircraft Systems (RPAS) are a growing threat to the maritime coast security as they can potentially carry explosives or can be used for smuggling drugs, boats and human intruders onto the sea shore. The mini-RPAS can depart from maritime platforms such as yachts. Their low cost and very small signature makes them a favorite platform for smugglers and terrorists. The mini-RPAS Radar Cross Section (RCS) is too small to be detected by the regular costal radars, which is where SafeShore comes in. Another important maritime threat addressed is low altitude guided parachutes. Due to their low RCS, these parachutes are hard to detect by standard radars. They can be dropped from airplanes far away from the shore and can be used for deploying equipment or explosives. The SafeShore core solution for detecting small targets that are flying at low altitude is to use a 3D LIDAR that scans the sky and creates above the protected area a virtual dome shield. 3D LIDAR will be integrated with passive acoustic sensors, passive radio detection and video analytics. With 3D LIDAR technology, SafeShore will be able to cover a vast area of the coastal border using mobile platforms. Each mobile platform will cover its area with a dome-shaped virtual detection shield with a radius of about 250-300m. There will be approximately 50 meters overlapping between the platforms. The overlapping will create a continuous detection shield along the shoreline.

- Highly Disruptive and Compact Antenna Systems for Small Satellites with Application to Surveillance, Environmental and Crop-Growth Analysis, Enabling European Union Dominance in the Space Industry

Compact satellites are transforming space-based surveillance systems. Typical configurations include a network of small satellites that can offer increased coverage and enhanced data collection rates when compared to conventional large scale systems. Microsatellites can also drastically reduce launching costs and mission development time, thus making remote sensing technologies more cost effective. Applications include vehicle tracking, weather monitoring, maritime surveillance, crop

growth analysis, and climate change observation. However, with satellite miniaturization, new design aspects arise. All satellite components have to be cleverly packaged within a small payload and materials must accommodate the harsh operating environments of space. The objective of the proposed research program is to research, design and test some new and compact antennas with integrated feed systems for such microsatellites.

- Aerial Insights; Aerial Insights: facilitating access to aerial drone imagery services through novel and cost-effective data analytics solutions

Aerial Insights is a software company based in Spain whose main focus is on the development and operation of imaging services with drones. Created in 2015 by a team of experienced and successful entrepreneurs, the company launched its new platform in 2016 to provide drone operators an affordable and innovative solution to extract drone imagery information from aerial data. Drones are becoming more and more popular and rapidly growing throughout the world. Today, they are used in multiple professional environments ranging from agriculture, insurance, mining industry to aerial photography and monitoring. According to recent PWC study, the expected business and services associated to drones will represent 127B USD globally. Among these services, drones equipped with cameras and other sensors (aerial photography) will play the most important role. Processing drone data with existing solutions is today cost-prohibitive. Data processing indeed requires expensive software and hardware as well expertise in multiple highly technical areas. Overall, we estimate an investment of 25K/year is required for physical resources, software and man hours to establish and provide services. Available at an average retail price €29,99 per map since 2016, Aerial Insights is based on a unique cloud platform and set of artificial intelligence algorithms where drone pilots can upload aerial raw imagery (step 1), select the outputs needed depending on the type of sensors onboard (step 2) and receive the relevant information on a secured online account within a few hours (step 3). This new approach is faster, cheaper and more reliable. For example, Aerial Insights reduces the timeframe required to diagnose and pinpoint faulty cells in a solar farm from 2-4 weeks (using traditional solutions) to 1-2 days. Regarding the mining industry, several weeks of work of a land surveyor can be replaced by a 15-minute flight and a couple of hours of processing.

- DroneGrid, Simplifying Aerial Intelligence

The drone industry faces several key challenges that prevent fast adoption of drone technology by mainstream enterprises. Amongst the main challenges are: complex drone regulations, high upfront cost and inadequate drone experience. In general, there is a real need for an end-to-end solution that would enable transforming data collected by drones into actionable aerial intelligence data. DroneGrid is an enterprise platform that enables 2D and 3D aerial inspections of assets using drones, including automated analysis of actionable data. Without needing their own drone fleet, our customers can easily access commercial drone technologies through DroneGrid to gather aerial intelligence and to easily integrate them into their existing processes. We take care of subcontracting the best drone operators for our clients. This enables enterprises to take better decisions, improve staff safety, increase asset efficiency and digitise their field information. DroneGrid consists of an industrial customer app/web platform, backend AI engine and an API layer that integrates with commercial drone software, various third-party services such as weather, regulatory, operational services and enterprise ERPs. On the other side, the platform can be used by certified and pre-approved drone pilots to perform missions on ordered customer operations. DroneGrid is already available in a functional commercial version in several markets: renewable energy (solar inspections), construction

and mining. In order to enter additional industries, we need to improve 3D capabilities (vertical) as well as enhance its intelligence abilities

2.9 Solutions for IMINT

2.9.1 Tools for IMINT

Satellite Imagery

Satellite imaging is growing steadily as the launching of new satellites in made available for growing business community and the need for satellite imaging for national security purposes has increased. Intelligence and defence are an application area of the satellite imagery among others (e.g. geospatial data acquisition and mapping, natural resource management, surveillance and security, construction and development, conservation and research, disaster management). At the moment USA is dominating the market, by having the highest number of researchers and invertors in the area. Key players in the application of satellite imaging for defence purposes are: [139][140]

- **Airbus defence and space** (GER), Airbus has intelligence centres that has various products on multiple intelligence capabilities. IMINT and GEOINT Centres | Fully Packaged IMINT and GEOINT Capabilities (intelligence-airbusds.com)

- **BlackSky** designs, owns and operates one of the industry's leading low earth orbit small satellite constellations, optimized to capture imagery cost-efficiently where and when our customers need it. the company was recently awarded with National Reconnaissance Office (NRO), which includes a comprehensive set of imagery services from current and future satellite capabilities. The award demonstrates the commitment of the U.S. Government to leverage the capabilities of next generation commercial providers in support of its most critical missions. Geospatial Intelligence | Real Time | BlackSky | SmallSat Constellations

- **European Space Imaging** (GER), we provides unparalleled access to critical locations around the globe Through Very High Resolution satellite imagery. Tasking the Maxar WorldView constellation from our multi-mission ground station located at the German Aerospace Center, the economical rapid delivery of 30 cm resolution multispectral imagery. This allows commanders to have a full view during the planning, execution and assessment of any mission. European Space Imaging | Your Satellite Imagery Solution (euspaceimaging.com)

- **Maxar** group has 90 own satellites and imagery intelligence products with over 125+ petabytes of data in the global satellite imagery archive. Maxar's high-definition (HD) technology enhances the visual clarity of the company's high-resolution satellite imagery. HD products are sharper, making information easier to understand and interpret than those in native resolution. https://blog.maxar.com/tech-and-tradecraft/2022/maxars-hd-technology-provides-measurable-improvements-in-machine-learning-applications. DigitalGlobe, is part of the company group.

- **Galileo Group,** specializes in applied hyperspectral imaging technology, for commercial, environmental, industrial, biomedical, and military applications. About Us | (galileo-gp.com)

- **Google Inc** , e.g. Google Earth Pro is free tool for doing OSINT investigations particularly when looking to time-series satellite data for further analysis. e.g. Landsat Algorithms | Google Earth Engine | Google Developers; Google Earth Engine: A Quick Guide for Beginners - GIS Geography

- **ImageSat** Int., Intelligence as a Service line of products provides intelligence insights to customers. Intelligence As A Service™ – ISI (imagesatintl.com)

- **L3Harris Corp**. provides the framework with the SpaceView line of small satellite imaging solutions. Spaceview™ Small Satellite Imaging Solutions | L3Harris™ Fast. Forward.

- **GeoEye Imaging System** (GIS) is optimised for large projects as it can collect over 350,000 square kilometres of VHR satellite imagery every day. Images are collected at 0.41 m panchromatic and 1.65 m 4-band multi-spectral data in 15.2 km swaths.) GeoEye-1 - Earth Online (esa.int)

- **Planet Labs Inc**.'s tools include a imagery catalogue that including daily scenes, quarterly and monthly basemaps and a set of full resolution examples. A limited version is offered for trials: https://www.planet.com/trial/

- **SpaceKnow** Inc. Defence and intelligence solutions offer strategic and operational analysis, classification, detection of changes and monitoring of the activities over the areas of interest. Defense & Intelligence | SpaceKnow

- **Telespazio France**. Currently coordinates the operations European earth observation program. Innovative new SAR-satellite missions. Home (e-geos.it)

- **Urthecast Corp** (Canada) is a Big Data services company specializing in satellite imaging, data services and geo-analytics. Owns and operates two EO satellites. UrtheCast Corp. - Corporate Profile

Further commercial satellite imagery solutions providers include: (some of these have already been presented earlier in the report).

Auduril: *Autonomous air systems that are tasked, connected and controlled by Lattice. Together, they enable a variety of intelligence, surveillance and reconnaissance mission profiles*. https://www.anduril.com/lattice/

ICEYE: manufactures radar imagery satellites and sells satellite-based information. Company's synthetic aperture radar (SAR) images also in cloudy weather, and day or night. It offers analysis through constellation of small satellites to enable persistent monitoring for delivering information of changes at the right time. The analysis comprises of microphase changes within the image pixels, to identify changes in between observations the are beyond human sight. ICEYE - Your Choice for Persistent Monitoring

Preligens: *VHR satellite imagery analysis to assess the activity of strategic areas of interest: ports, airfields, military camps, industrial sites. Detect, classify and identify objects of military interest automatically, and follow the evolution of critical areas, at a glance.* IMINT Capabilities | Strategic Site Surveillance application software. (preligens.com)

Geo4i, a French company that is specialised to combine image analysis and geomatics skills. Cooperation with other imaging companies. Tools include equipment recognition tools. Geo4i - GEOINT - IMINT

Military grade surveillance drones and HAPS:

The list presents only a few examples of drone/UAV solutions as the system must be chosen according to the IMINT needs and requirements assessment. The number of companies that enter the drone market increase every year, as there are no high barriers to entry. The list empasises European companies bit does not include possible rising innovative start-up companies.

- **ARGUS** - provider for Unmanned Aerial Vehicles (UAV's) for surveillance and reconnaissance (S/R) missions. ARGUS-UAV™ is customized to perform various mission profiles: Border and Coastal Control, Homeland Security / Law Enforcement, Ground Surveillance and Monitoring a high def sensor for drone by BAE Systems. 1.8 billion pixels. https://argustech.aero
- **HEIGHT** Technologies. Unmanned drones and UAVs with IMINT capacities. https://heighttechnologies.com/
- Teledyne Flir. Innovative sensing solutions into daily life through our thermal imaging, visible-light imaging, video analytics, measurement and diagnostic, and advanced threat detection systems. https://www.flir.eu/
- **Globhe**, leading EO providers from drones, aggregating from local UAV providers:
    - operationally crowd droning in many countries, and producing data
    - 6000 drone operators in 102 countries
    - Partners : Google, ESRI, DGI, Innova

HAPS Alliance aims to build stratosphere capability specially to enhance connectivity. It aims to research, develop, and launch ecosystem of HAPS technologies. Overview – HAPS Alliance

- **Balloons** (e.g. Google Loon),
- **Fixed wing** (e.g. AeroVironment, SPL, Airbus Zephyr, Softbank HAPSMobile, Skydweller SolarImpulse),
    - Airbus Zephyr: Last test flight in Nov 2020, Holds the current record of 26 days of non-stop flight. Only HAPS to have had a customer—3 sold to the UK Ministry of Defence as Operational Concept Demonstrators. Company aims to launch the Zephyr in 2022–2023.[136]
- **Airships** (e.g Thales Stratobus, Sceye, Altran Ecosat), Hybrid approaches
- **Gorgon stare** : Gorgon Stare is a video capture technology developed by the United States military.[1] It is a spherical array of nine cameras attached to an aerial drone. L3Harris Wide-area motion imagery (WAMI) https://en.wikipedia.org/wiki/Gorgon_Stare

2.9.2 Datasets for IMINT

With the fast-increasing interest in machine learning methods for Earth Observation in the past years, so has the availability of open data benchmark datasets increased significantly. Numerous EO, satellite or aerial imagery datasets are available for developing and comparing methods addressing the main tasks of IMINT as identified in section 2.3, and many more. As it would be neither practical nor possible to list them all in this deliverable, instead we point to several lists of datasets available online and regularly curated.

Hwu, W. (2019, September). Awesome Remote Sensing Change Detection. Github. https://github.com/wenhwu/awesome-remote-sensing-change-detection

Rieke, C. (2020, December). Awesome Satellite Imagery Datasets. Github. https://github.com/chrieke/awesome-satellite-imagery-datasets

Ali Ahmadi, S. (2021, September 14). Awesome Satellite Benchmark Datasets. Github https://github.com/Seyed-Ali-Ahmadi/Awesome_Satellite_Benchmark_Datasets

Schmitt, M., Ahmadi, S. A., & Hänsch, R. (2021, July). There is No Data Like More Data-Current Status of Machine Learning Datasets in Remote Sensing. In 2021 IEEE International Geoscience and Remote Sensing Symposium IGARSS (pp. 1206-1209). IEEE.

Cole, R. (2022, May). Satellite Image Deep Learning. Github. https://github.com/robmarkcole/satellite-image-deep-learning

Microsoft Bing, Airbus Defence and Space - Intelligence & Maxar (2022, April). Global ML Building Footprints. Github. https://github.com/microsoft/GlobalMLBuildingFootprints

NB: 777 million building footprints identified around the world and delineated.

Hammell, B. (2017, September). Planesnet: Planes in Satellite Imagery. Github. https://github.com/rhammell/planesnet

Also as a Kaggle competition related to this dataset: https://www.kaggle.com/datasets/rhammell/planesnet

2.10 Other

SatCen: The European Union Satellite Centre supports the decision making and actions of the European Union in the field of Common Foreign and Security Policy (CFSP), in particular Common Security and Defence Policy (CSDP), including European Union crisis management missions and operations, by providing products and services resulting from the exploitation of relevant space assets and collateral data, including satellite imagery and aerial imagery, and related services. SatCen is referenced also in the new EU Strategic Compass to support EU with situational awareness and decision making in security and defence. SatCen - European Union Satellite Centre (europa.eu)

3. The state-of-the-art of SIGINT technologies

3.1 Definition of SIGINT and its sub-categories

Signals intelligence (or SIGnal INTelligence, SIGINT) is based on sources of information from electromagnetic interceptions coming from various sensors or platforms ([47], [57]). The platforms can be, for example, ground or air platforms. Typically, the intelligence-gathering by interception of signals is divided into two sub-categories (Figure 7) based on, whether it is from communications between people (*COMmunications INTelligence*—COMINT) or from electronic signals not directly used in communication (*ELectronic INTelligence*—ELINT). Signals intelligence is a subset of intelligence collection management.

In most cases SIGINT is defined as interception of enemy or foreign signals. The purpose is to estimate and prevent threats to national security. If this definition is strictly followed, then SIGINT is not part of the methods of the law enforcement (police) agencies (LEAs) focusing on crime prevention and investigations. However, the law enforcement is also increasingly using technological means to carry out their mission. Some of these means fit in with the SIGINT definition of intercepting signals. In EU the country-specific intelligence legislation can be viewed from three perspectives. First there is the national constitution, then the European Convention on Human Rights [48] and European Union law and the case law of the European Court of Justice of the European Union. European case law continues to evolve as the threat of terrorism has risen to a higher level. In several countries, legislation has been refined to be technology-neutral in recent years. Technology-neutral here means that intelligence can be conducted on the same basis in telecommunications and information networks as in the physical world.[49] Well-implemented intelligence legislation combines national security with respect for citizens' fundamental rights. E.g. in Finland the Act on Telecommunications Intelligence in Civil Intelligence defines eleven threats based on which Supo [67] may obtain permission from the Helsinki District Court to initiate data acquisition in data networks.

Because methods to intercept communication signals or data may infringe with privacy rights, there are court cases on the circumstances to use telecommunication or signals interception also discussions on current legislation are regular.[50] The issues of principle at stake can include bulk collection, judicial authorization, notification, and discrimination. In each of these issues, there is some tension between the regional (ECHR, European Court of Human Rights) and sub-regional (EU) human rights standards applicable to signals intelligence. Intelligence methods safeguard the ability to proactively detect and map phenomena, situations and threats. Nowadays, as the national and international operating environment are intertwined, intelligence powers make it possible also to obtain information that is essential and critical to national security from abroad and without co-operation with the state in whose territory the intelligence activities are carried out. Methods of protecting the confidentiality of communications are provided for in telecommunications intelligence legislation.

The powers of foreign intelligence and telecommunications intelligence as methods of civilian intelligence are detailed regulated. The methods only used for military intelligence are radio signal intelligence and foreign information system intelligence. Telecommunication intelligence complements the use of other intelligence methods as a method. Telecommunications intelligence can be considered to include the processing of technical data and the intelligence of governmental and non-governmental operators. The regulation of telecommunications intelligence covers explicit

provisions that it is not a general and untargeted monitoring of telecommunications. e.g. a telecommunications inquiry may not be directed to a message the sender and recipient, in which case the other party must be outside Finland when conducting the telecommunications inquiry. The Act on Military Intelligence provides for the processing of technical data for the acquisition of telecommunications information, which precedes the actual telecommunications intelligence. The provision does not further specify the timeliness of the collection of technical data and the definition is outlined in court. At present, the information obtained from the processing of technical data can only be used to find the part of the communication network that is relevant for telecommunications intelligence. In a globally networked world, intelligence on computer networks is essential.

The European Union issued a Directive 95/46/EC [51] that defines the Lawful Interception[2] of Telecommunications and a Directive 2002/58/EC [52] concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), which together form the framework for telecommunication interception in Europe. Lawful Interception (LI) is a security process in which a service provider or network operator collects and provides law enforcement officials with intercepted communications of private individuals or organizations. The implementation of the directive is supported by ETSI[3] specifications, which regularly update the functionalities of LI (lawful interception) and RD (retained data) specifications. The current mobile communication requires additional capabilities and international cooperation for authorized law enforcement agencies. As an example, the 3GPPTM[4] Technical Specifications [53] on Lawful Interception published by ETSI cover all necessary aspects in a 5G context: requirements, architecture and functions, protocol and procedures. 5G will dramatically increase the amount of data, and this requires modern monitoring centre that allows the law enforcement more capacity, and new tools and analytics to perform successful and fast wading of all data, necessary monitoring, and analysis. [54]

The definition of a handover interface for the delivery of the results of lawful interception should allow the technical facilities to be provided: with reliability; with accuracy; at low cost; with minimum disruption; most speedily; in a secure manner; using standard procedures.[55]

As classified and sensitive information is usually encrypted, signals intelligence in turn involves the use of cryptanalysis to decipher the messages. Traffic analysis—the study of who is signalling whom and in what quantity—is also used to integrate information again.

Figure 7 shows the relation among different types of Intelligence, described below.

[2] interception (lawful interception): action (based on the law), performed by a CSP, of making available certain information and providing that information to an LEMF (Law Enforcement Monitoring Facility)
[3] ETSI is a European Standards Organization (ESO). We are the recognized regional standards body dealing with telecommunications, broadcasting and other electronic communications networks and services. ETSI - Standards, mission, vision, direct member participation
[4] Third Generation Partnership Project (3GPP) is a partnership project bringing together national Standards Development Organizations (SDOs) to develop technical specifications for the 3rd generation of mobile, cellular telecommunications, UMTS. ETSI - THIRD GENERATION PARTNERSHIP PROJECT

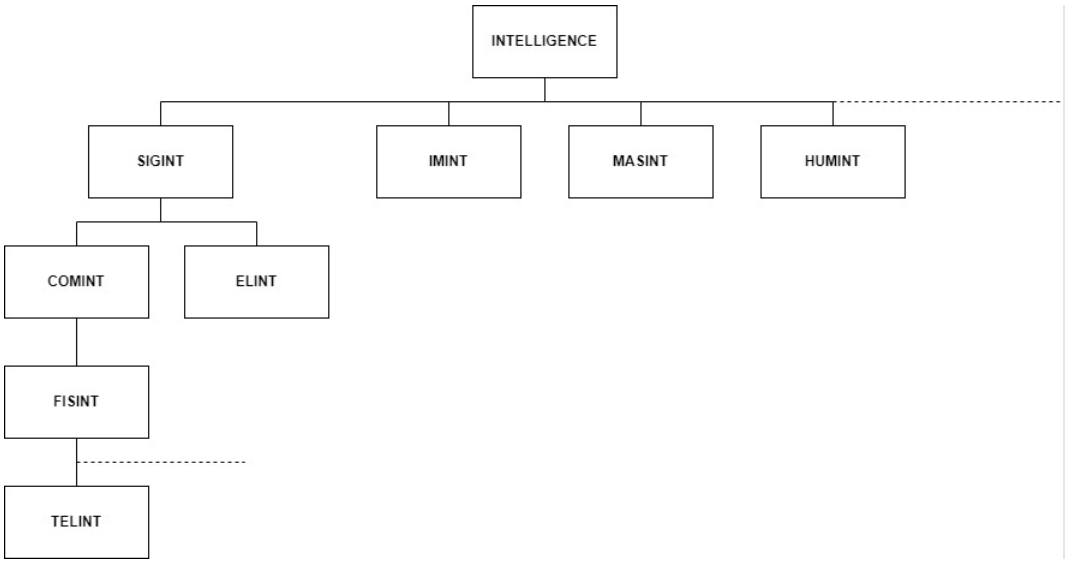

Figure 7. SIGINT and its sub-categories.

SIGINT and *Measurement And Signature INTtelligence* (MASINT) are closely, and sometimes confusingly, related. The signals intelligence disciplines of communications and electronic intelligence focus on the information in those signals themselves, as with COMINT detecting the speech in a voice communication or ELINT measuring the frequency, pulse repetition rate, and other characteristics of a radar. MASINT also works with collected signals but is more of an analysis discipline [47] (defined as a scientific and technical intelligence obtained by the qualitative analysis of technical data associated with any source, emitter or sender [56]). Where COMINT and ELINT focus on the intentionally transmitted part of the signal, MASINT focuses on unintentionally transmitted information. For example, a given radar antenna will have side lobes emanating from a direction other than that in which the main antenna is aimed. The RADINT (*RADar INTelligence*) discipline involves learning to recognize a radar both by its primary signal, captured by ELINT, and its side lobes, perhaps captured by the main ELINT sensor, or, more likely, a sensor aimed at the sides of the radio antenna.

MASINT associated with COMINT might involve the detection of common background sounds expected with human voice communications. If a given radio signal comes from a source or a location, where certain background noise could be expected, the lack of it might prompt MASINT to suggest the intercepted signal is a deception.

Another intelligence collection subset, whose categorization is not clear, is *Foreign Instrumentation Signals (or Signature) INTelligence* (FISINT). In some definitions, it is seen as a subset of COMINT, while in others as part of MASINT. FISINT is the interception of and exploitation of performance and tracking data (usually telemetry) during tests of weapons systems and space vehicles. The sources may include air-, satellite-, ground- and subsurface-based systems.

Unlike COMINT, FISINT concentrates on machine-to-machine (M2M) communications instead of human language or on a combination of instrumentation and human language. Examples include:

- Telemetry data (TELemetry INTelligence, TELINT). Missiles, satellites and other remotely monitored devices often transmit streams of data concerning their location, speed, engine status and other metrics.
- Video data links. These may be from UAVs or from satellites used for reconnaissance.

- Remote access and control transmissions, such as from remote keyless systems and wireless traffic light control systems.
- Command signals used in teleoperation, such as the control of aerial vehicles, missiles and remotely controlled robots.

Figure 8 shows the main steps of a mission to collect SIGINT [57]. The actual intelligence collection takes place in the mission execution step, while the rest involves disciplines from the other nodes of the intelligence cycle.

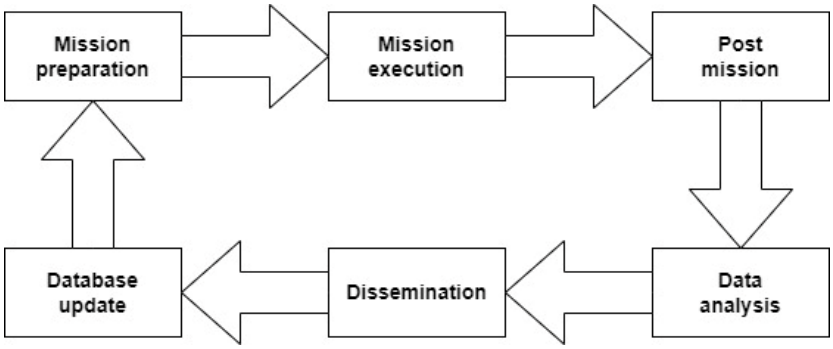

Figure 8. Main steps of a SIGINT mission.

3.2 Application areas of SIGINT

The application areas of SIGINT are military intelligence and civilian intelligence collection with the purpose of estimating and preventing threats to national security. In the strictest sense, the purpose of SIGINT is the interception of enemy or foreign signals. From a military tactical point of view, one of the most important SIGINT tasks is to determine the Electronic Order of Battle (EOB) meaning the localisation and identification of radars and communications nodes associated with enemy weapons systems, and the networks in the enemy territory.

Concerning LEAs, deliverable 2.2 [58] reported results of interviews conducted on 16 practitioners of NOTIONES across the Europe with some of the questions directly related to SIGINT. The report did not identify any technologies or tools for SIGINT, when asked specifically. The few answers received related to SIGINT either did not provide useful or highly relevant information, or the interviewee did not wish to disclose what would be useful. It would seem, that the traditional stance of the military and the intelligence agencies to keep everything concerning SIGINT tools and methods classified, extends itself also to LEAs. To obtain telecommunications data was the only specific application area, which was identified in [58] related to SIGINT intelligence collection.

3.2.1 SIGINT platforms in Europe

Platforms for SIGINT include at least the following:

- ground platforms
- ship platforms
- submarine platforms
- aircraft platforms
- satellite platforms.

On these platforms ELINT focuses its attention on radar systems and to the analysis of their characteristics [76], or more generally RF signals not related to communications. Frequencies vary from 100 MHz to 40 GHz. To do this, the ELINT system needs to detect and locate radars in the specific area of interest and to monitor the full electronic spectrum of interest. This has to be able to be done far away from the enemy installations, and the ELINT system needs to provide detailed information and parameters of the enemy radars. Modern radars utilize a large variety of signal waveforms like pulse, pulse Doppler, frequency hopping, frequency and pulse coded, and so on. Taking into account these factors, the ELINT system needs to have both panoramic, wide band, receivers for monitoring the environment and selective, super heterodyne, receivers for measuring the radar waveforms.

COMINT's purpose is to intercept and analyse radio communications. Today this also includes interception of mobile (3G, 4G, …) and internet communications, which are of interest for LEAs as well. According to [77], COMINT can be divided into the following segments:

1. strategic HF COMINT system (0.5 to 30 MHz)
2. strategic and tactical V/UHF COMINT system (20 MHz to 3 or 6 GHz)
3. GSM COMINT
4. satellite COMINT
5. internet COMINT.

COMINT capabilities are becoming more and more important in detecting, localizing, and analysing the intentions of the source of the threat. Modern weapons systems are interconnected through communication links. They may be "silent" or "stealth", but they still have to use the communication links. Hence, COMINT may be the only way to detect them. In hybrid warfare the internet itself is weaponized in the forms of viruses, denial-of-service methods, intrusion, and sabotage programs, or generally feeding false information in an attempt to sway opinions. Signals-wise COMINT aims to catch both the RF parameters, like carrier frequencies, bandwidths, and modulation types, as well as the information exchanged between the users or terminals.

Concerning the interception of mobile and internet communications, at least the following sub-categories can be identified:

- Internet monitoring with the aim of capturing data in the internet. Technology can be used in any point in the physical and electronic systems of the internet. Tools include both hardware and software.
- Monitoring of mobile telephony with aim of capturing data from the mobile network. Besides capturing, sending of messages to phones is also possible.
- Fixed telephony interception, which requires the capture of public switched telephone networks. Companies provide solutions for the monitoring of such networks.
- Intrusion technologies that allow smuggling of malware to mobile phones and computers. With the malware the operator can take control of the target device.

In both COMINT and ELINT, databases and signature libraries play an important role. This allows quick recognition of sources and their signal types provided that previous intercepted data of them exists. Obviously new intercepts are added to the libraries for future use. A long-standing problem in SIGINT is to recognise new types of signals, like from RF-controlled threats (UAVs, IEDs, etc.). Software-programmable and computer-controlled systems are also very important for providing rapid signal acquisition and data processing with high accuracy. High computing power is required, if cryptanalysis for deciphering messages is needed. Finally, an emerging trend is to combine SIGINT technology with

electronic attack measures to create systems, which are not only able to recognise threats, but also counter them after recognition.

3.2.1.1 Ground platforms

Ground platforms can be generally divided into strategic and tactical. An example of a strategic platform is a site designed for collecting data from one's communications and surveillance satellites. Tactical platforms encompass a wide variety, including directional finders, listening posts, satcom interceptors, cellular monitors, among others. Ground platforms also include transportable or vehicle-mounted systems. An example of a vehicle-mounted SIGINT (COMINT) system is from Rohde&Schwarz [78].

In Europe, at least the following countries have ground platforms for SIGINT [75]: France (DGSE), Germany (BD), Russia and UK (GCHQ). However, it is very likely that practically every European country has at least some tactical SIGINT capabilities.

3.2.1.2 Ship platforms

In Europe, at least the following European countries have ship platforms for SIGINT [75] [79]: Denmark, France, Germany, Italy, Norway, Poland, Russia, Spain and Sweden. Of these, the French Navy ship, Dupuy de Lôme, is perhaps the most advanced SIGINT ship in Europe with extensive COMINT and ELINT capabilities. In general, modern warships equip ELINT-type equipment, like Electronic Support Measures (ESM) or Electronic Counter Measures (ECM), which have a specific tactical warfare purpose.

3.2.1.3 Submarine platforms

In Europe, at least the following countries have submarine platforms for SIGINT [75]: France, Germany, Greece, Italy, the Netherlands, Russia, Sweden, and UK.

Typically, submarines like other modern warships carry radar warning systems. Likewise their ELINT systems have an ESM role, usually with the purpose of missile targeting.

As an interesting side note from LEA perspective, the criminals use submarines or semi-submersible vessels to smuggle drugs. On the Pacific Ocean, these vessels have been used since late 1990's to smuggle drugs to the US. Recently a similar case was reported in Europe (Spain) as well [80]. In US, counter measures have included towed sonar arrays and maritime patrol aircraft. Long range UAVs are becoming feasible as well. Europe may need to develop similar methods.

3.2.1.4 Aircraft platforms

In Europe, at least the following countries have aircraft platforms for SIGINT [75]: France, Germany, Russia, Spain, Sweden, and UK. Most likely other European nations have aircraft SIGINT platforms as well. For example, Finland utilizes a SIGINT package in one of its C-295 aircraft [81]. In Sweden, SAAB has developed the GlobalEye surveillance system mounted on Bombardier Global 6000/6500 aircraft [82]. Among other things this system has ELINT/ESM capabilities.

A reconnaissance aircraft with SIGINT is usually equipped also with other capabilities like COMINT and ELINT systems, communications and positioning systems, and visible, infrared (e.g., LOROP) and Synthetic Aperture Radar (SAR) imaging capabilities. [83]

3.2.1.5 Satellite platforms

In Europe, the following countries at least have satellite platforms for SIGINT [75]: Belgium, France, Germany, Greece, Italy, Russia, and Spain. Additionally, Europe possesses GEOINT capabilities through the European Union Satellite Centre (SatCen, [84]), which is utilized for assessing military infrastructure and military deployment, among other things. An example of this is the forthcoming CERES SIGINT satellite system **¡Error! No se encuentra el origen de la referencia.** being developed by France. Another example involves tracking the entire process of the development of weapons of mass destruction. Figure 9 shows an example of the forthcoming CERES SIGINT satellite system **¡Error! No se encuentra el origen de la referencia.** developed by France.

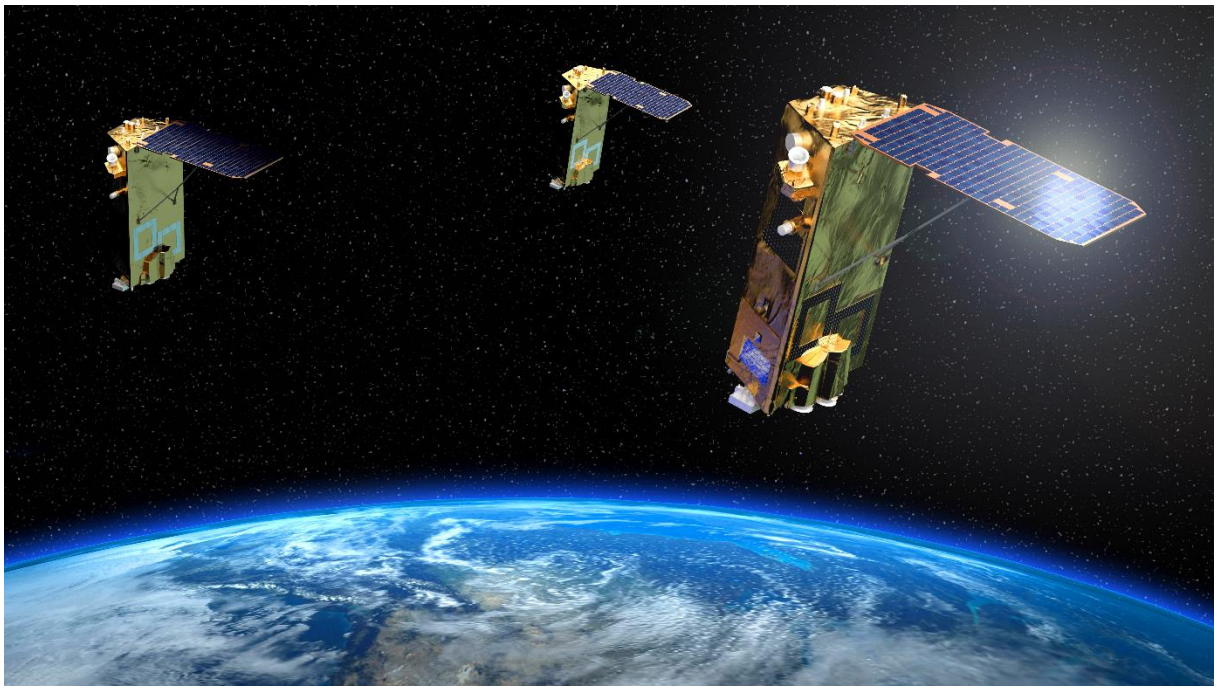

Figure 9. Forthcoming CERES SIGINT satellite system ¡Error! No se encuentra el origen de la referencia.**. @AIRBUS2015**

3.2.1.6 Intercepting mobile and internet communications

As mentioned earlier, today COMINT collection includes mobile and internet communications intercepts as well. Phone monitoring can be divided into two categories: the physical and the mobile [86]. The physical runs on the Public Switched Telephone Network (PSTN, “landline”). The mobile runs on wireless radio networks, which are the mainstream these days. Perhaps the most well-known is the Global System for Mobile Communications (GSM), which is sometimes referred to belong to the second generation (2G) of mobile communications systems. After 2G, the following generations (3G, 4G, …) have added more and more data transmitting solutions besides the actual phone communications. The world is currently implementing the 5G, which will in future include IoT and massive sensor networks. Companies manufacturing the base stations and other hardware for the mobile radio networks also sell systems for monitoring the mobile traffic for the network operators. LEAs (and intelligence agencies) can obtain this data in some cases (lawful interception [87]). Depending on the legal system of a given country, this may, for example, require the LEA to provide a probable cause of criminal activity to obtain a warrant from a court to request the mobile telecommunications data from a network operator or getting access to a legal interception gateway or node.

Mobile telecommunications can also be intercepted passively in between the mobile device and the base station it is communicating with. The intercepting system tunes into the base station and receives the uplink signal from the mobile device and the downlink signal from the base station. The uplink signal contains the content of a call or a message. The downlink signal is the reply to the call or the message. By simply tuning the intercepting system's receiver to the correct uplink/downlink frequencies, the system can gain access to the information being transmitted between the mobile device and the base station. The information is encrypted, but in the case of GSM the ciphers were reverse engineered already in the 90's making the GSM very prone to interception. Real time GSM interceptor kits are commercially available [88]. The following generations have made improvements to the security, and for example with the 5G it is a major topic worldwide.

A well-known interception tool is called the Stingray or the GSM interceptor or the IMSI catcher. An IMSI catcher presents itself as the most powerful base station among others in the mobile network. The mobile device is always looking for the base station, to which it has the strongest connection. This leads to a situation, where the mobile devices in the area connect to the IMSI catcher. Once this happens the catcher has the mobile device to provide its IMSI (International Mobile Subscriber Identity) and IMEI (International Mobile Equipment Identity), after which the catcher can monitor the voice calls taking place in the mobile device, the messages being sent and the location of the device. Concerning the newer generations, it is not well-known what intercepting techniques are available, or what the intelligence agencies use. A lot of unconfirmed theories relating, for example, to ECHELON circulate the internet.

Intercepting internet communications can be physical, or software based. The physical involves installing interception hardware ("wire taps", fibre optic splices, etc.) in the fibre optic network or the routers, repeaters, and the like in the network. There has been plans in Europe to require the network operators to install "interception interfaces" for lawful interception [89]. This is similar to the case, in which in some countries the law requires the mobile network operators to install legal interception gateways or nodes. These kinds of methods relate usually to dragnet-type mass surveillance scenarios.

An example of the software-based internet interception is to intercept the encrypted web traffic between the web browser and the website with an interceptor software [90]. This can be done either locally or remotely. The first requires installing the interceptor software to a user's computer by some means. The second requires inserting the interceptor on the network path connecting the user's computer to the requested site. In both cases, the interceptor software pretends to be the requested website and directs the web connection to itself rather than the requested site. It then opens a new encrypted connection to the requested website and proxies the data back and forth between the connections. The interceptor has now access to the unencrypted data in the connection and can read, change, or block it.

3.3 SIGINT organisations and capabilities in Europe

3.3.1 Intelligence alliances

The United Kingdom - United States of America Agreement (UKUSA, also called the "five eyes") is a multilateral agreement for SIGINT co-operation between the UK, the USA, Canada, Australia, and New Zealand [59]. One of the major SIGINT activities, that the five countries are co-operating on, is code named ECHELON [60]. There is no unclassified definition of what ECHELON does, and unofficial reports

on its capabilities and operations are conflicting. General agreement seems to be, that ECHELON is a surveillance program run by the USA (and the National Security Agency, NSA) with the aid of the countries in the UKUSA partnership.

The North Atlantic Treaty Organization (NATO, [61]) is a political and military defence co-operation, which purpose is to guarantee the freedom and security of its members. The members of NATO have access to a wide range of SIGINT equipment and techniques. The NATO doctrine for SIGINT is classified. The European NATO members are Albania, Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Montenegro, the Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and the United Kingdom.

Like ECHELON, a part of the Snowden-related publication revelations was that the intelligence agencies of nine European countries are 3rd party partners of the NSA and the UKUSA countries. The countries are France, Germany, Spain, Italy, Belgium, the Netherlands, Denmark, Norway and Sweden, which form a group called SIGINT Seniors Europe (SSEUR, [62]), which together with the UKUSA partners is also called the “fourteen eyes”.

3.3.2 National organisations

Collection of SIGINT in a given country is usually handled by the military forces, specialised intelligence agencies (like e.g. NSA in the USA) or in co-operation between the two. Neither military forces nor the intelligence agencies disclose any details of their methodology, technology or targets. On the military side ground, air and naval forces have their own platforms, and the members of NATO have access to a wide range of SIGINT equipment and techniques. The specialised intelligence agencies may have their own ground stations and satellite platforms, for example, or have access to the military platforms. The following information per European nation is on a very general level obtained from www-based articles [63], home pages of the agencies and so on. The following list covers only countries, where information relating specifically to the SIGINT role was able to be found.

In **Belgium**, the SIGINT operations [64] are handled by the Belgian military intelligence ADIV/SGRS (Algemene Dienst Inlichting en Veiligheid/ Service Général du Renseignement et de la Sécurité), which operates under the ministry of defence. Its main role is to provide security to Army’s military operations. The State Security Service (VSSE) is the Belgian civilian intelligence and security agency operating under the ministry of justice. The VSSE concentrates on counterespionage and counterterrorism, and it has a variety of surveillance techniques including communications intercepts (COMINT) at its disposal. The VSSE takes part in a number of international intelligence cooperative relationships. Belgium is a member of NATO.

Denmark’s national level SIGINT operations are carried out by the Intelligence Regiment of the Royal Danish Army (Efterretningsregimentet), which co-operates with the Danish Defence Intelligence Service (Forsvarets Efterretningstjeneste, FE) and the Danish Security and Intelligence Service (Politiets Efterretningstjeneste, PET), which is the intelligence arm of the Danish police. Denmark is a member of NATO.

In **Finland**, SIGINT belongs to the domain of Finnish Defence Intelligence Agency (PV TIEDL, [65], [66]). This agency is organic to the Intelligence Division of Defence Command of the Finnish Defence Forces. The organizational structure, the manpower, the targets of intelligence collection and the methods of

the agency are not public knowledge. Besides SIGINT, this agency has IMINT and Geospatial Intelligence (GEOINT) capabilities. In addition, the Finnish Security Intelligence Service (SUPO, [67]) has intelligence collection capabilities, some of which are technological in nature like interception of telecommunications, intelligence collection in lieu of interception of telecommunications, network traffic intelligence, etc.

The national-level SIGINT in **France** is the responsibility of DGSE (General Directorate of External Security [68]), which is French equivalent for the British Secret Intelligence Service (SIS/MI6) or the CIA of US. The DGSE operates under the direction of the French Military Forces, and it has ship, aircraft and land-based platforms at its disposal. France is a member of NATO.

In **Germany**: SIGINT operations belong to the domain of the Foreign Intelligence Service (Bundesnachrichtendienst, BND [69]), which operates several ground platforms. German military has additional aerospace, naval, etc., platforms with SIGINT capabilities. Germany is a NATO country.

In **Ireland**, SIGINT (as well as cyber surveillance) is the responsibility of the Irish Defence Forces Communications and Information Services Corps (CIS [70]) and the Directorate of Military Intelligence.

In **the Netherlands**, the Dutch government organisation handling SIGINT collection is the Joint Sigint Cyber Unit (JSCU). This is a joint team from the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD). The JSCU co-operates closely with the allied foreign intelligence agencies. The Netherlands are a member of NATO.

National SIGINT operations in **Norway** belong to the domain of the Norwegian Intelligence Agency (NIS or Etterretningstjenesten [71]), which is the Norwegian military intelligence agency operating under the Ministry of Defence. NIS runs about half a dozen stations with SIGINT capabilities. In addition, the Norwegian navy has an ELINT collection vessel. Norway is a member of NATO.

Intelligence collection in **Spain**, including SIGINT, is handled by the National Intelligence Centre (Centro Nacional de Inteligencia, CNI [72]). The Spanish Armed Forces have also aerospace, naval, etc., SIGINT platforms. Spain is a NATO member.

In **Sweden**, SIGINT operations are handled by the National Defence Radio Establishment (FRA, [73]). However, the FRA cannot operate independently. The assignment has to come from the Government or its Offices, the Armed Forces, the Swedish Security Service (SÄPO) or the Swedish National Police Board. A part of the latter is the Swedish Criminal Police, which has among other units a surveillance unit and a cyber-crime unit.

United Kingdom has divided its SIGINT operations between the Government Communications Headquarters (GCHQ [74], strategic SIGINT), the military (tactical SIGINT) and the Security Service (MI5) (specialized SIGINT for counter espionage). UK is a NATO member.

In **Italy**, SIGINT and the other types of Intelligence are entrusted to the Department of Information for Security (DIS), whose Director General is appointed directly by the President of the Council of Ministers, and to the two operational agencies that deal with internal (AISI) and external (AISE) dimensions of national security. Italy is a NATO member.

In **Russia,** the sixth directorate of the Main Intelligence Directorate (GRU) is responsible for SIGINT collection on the military side. It has in its use a large variety of different types of aircraft, naval vessels,

satellites, and ground stations to collect signals intelligence. Russia's counterpart for the NSA in the United States is the Special Communications Service of Russia, which is a cryptologic agency of the Federal Protective Service of Russia (FSO). This unit is responsible for the collection and analysis of foreign communications and foreign signals intelligence.

Companies

There are several companies, including for example Boeing, EADS, General Dynamics, Horizon Technologies, L3 Harris, SIGINT Systems, Northrop Grumman, Raytheon, Rohde&Schwartz, SAAB and Thales, who provide SIGINT equipment and solutions (see Section 3.5 further). In addition, there are companies (Anritsu, Keysight, Rohde&Schwartz, etc.) providing signal sources, analysers, etc., which can be used as building blocks of SIGINT systems, but which are commercially available to anybody for general signal generation and analysis purposes. The various military forces and intelligence agencies tend to have strong in-house prototyping activities as well. The contents of these activities are generally not public knowledge.

3.4 Projects, Initiatives, and Information sources for SIGINT

EU HERCULE programme and CORDIS databases were searched using SIGINT, COMINT, ELINT and related key words. The following paragraphs give the results.

HERCULE:

4G-INTERCEPT (Investigation tools, HERCULE-TA-2017-01) is a project that aims at enhancing the technical capacity of Romanian Police to intercept data communications, with the purpose of increasing the efficiency of investigations in the cases of fraud, trafficking and other types of economic crimes. The action will consist of the procurement of an electronic surveillance system and the training of police staff for the use of the system.

ACIPC (Investigation tools and methods, HERCULE-TA-2018-01) aims at building and advancing an effective holistic big data analytics system, which is able to process different types of intelligence data (HUMINT, FININT, OSINT, SIGINT, CYBINT, GEOINT) and large amounts of data, uncovering hidden patterns, correlations and producing other insights, is essential for the successful implementation of the main strategic and operational objectives of the Special Investigation Service of the Republic of Lithuania (STT) focusing on preventing, combating and eliminating the causes of large-scale systemic corruption, fraud, and similar financial crimes which are detrimental to the protection of both national and EU's financial interests. In order to counter new fraud schemes against EU budget anti-corruption tools need to enable to detect and manage risks before they turn into fraudulent activities.

HELM OF HADES project (Specialised training sessions, HERCULE-TC-2020-01) aims to provide the Operational Central Unit of the Guardia Civil n Spain, with advanced technical surveillance skills, by the implementation of a training programme, led by the best experts in the EU, which will enhance its capacity to prevent and combat fraud, corruption and, specially, tobacco smuggling organised crime groups. Covert surveillance is a legitimate and very powerful LEA tool used by these agencies in criminal investigations to collect intelligence and evidence and to support operational activity. The Guardia Civil has special units dedicated to the exploitation of advanced technological skills to fight criminal groups, but these skills need to be enhanced continuously to stay a step ahead of criminals.

CORDIS:

CORDIS search did not recognise projects that have direct relevance to or goals to advance specifically SIGINT. However, the search results provided a large number of research projects that develop and utilise radars, wireless radio telecommunications systems, telemetry, and related electronics and semiconductor technologies applied in a large variety of disciplines ranging from Earth Observation and astrophysics to archaeology, to health care and even biology. Among the disciplines are threat assessment technologies, where, for example, radar sensors are used for detecting concealed explosives, guns and knives, or for detecting flying threats to aeroplanes, like birds and drones. In many cases, the utilised frequencies are much higher (in the mm-wave range) than what have been traditionally used in SIGINT. The leading edge of the research is currently at these high frequencies, because the upcoming 5G/6G telecommunications and IoT technologies are expected to use them. The technology development will, no doubt, benefit SIGINT applications as well in future.

SCIENTIFIC PUBLICATIONS:

In searching scientific publications databases, keywords SIGINT, COMINT and ELINT did produce thousands of results, but for the most part they did not relate to modern or recent SIGINT technologies or methods. Most books and journal articles seem to concentrate on reviewing the history of SIGINT between the First World War and the Cold War, or in general before the introduction of spy satellites. The publications may discuss the intelligence alliances (UKUSA, etc.) to some extent. However, information about the state-of-the-art hardware, software, tools or methods are not available, or it is speculative in nature. In any case, screening thousands of publications is outside the scope of NOTIONES.

The searches relating to intercepting mobile or internet communications again produced tens of thousands of results. A lot of them concern mostly the lawful interception or the known interception tools like the IMSI catcher (see Section 3.2.1.6). The lawful interception papers concentrate on the legal or societal ramifications (privacy issues) of the lawful interception. There are technical papers as well, especially since cybercrime (and ways to combat it) have massive public interest. However, again, screening thousands of papers is outside the scope of NOTIONES.

3.5 Solutions for SIGINT

The following lists SIGINT frameworks, software, tools and solutions. In the NOTIONES practitioners' interviews' results in [58], no SIGINT software and/or tools were identified. Adding artificial intelligence (AI) / machine learning (ML) tools to existing collection methods was mentioned as a technological need by practitioners.

Frameworks (see Section 3.3.1):

- UKUSA
- ECHELON
- NATO
- SSEUR

The following lists companies, who provide commercially available SIGINT software and tools. Many of the products may be aimed at military needs, but nothing indicates that they would not be available

to everybody. One exception is the Pegasus software, which the NSO group sells only to governments. List of providers:

- COMINT Consulting [91]
- Memento Labs [92]
- NSO Group [93]
- Ubuntu-based SIGINT Linux distribution (SigintOS, [94]), operating system with diagnostic tools for SIGINT systems installation
- Southwest Research Institute [95]
- SRC, Inc. SIGINT and Electronic Warfare (EW) tools [96]
- Stingray/GSM interceptor/IMSI catcher [97]
- thinkRF [98]
- Valley Tech Systems [99]

Many companies produce SIGINT systems and solutions. Many of these companies are well known to subcontract to military forces, which is quite clear from their web pages. Whether LEAs could also obtain solutions from them is not known. List of providers:

- Airbus [100][101]
- Avantix SAS [102]
- BAE Systems [103]
- Black River Systems [104]
- Boeing [105]
- General Dynamics [106]
- Horizon Technologies [107]
- IAI [108]
- L3Harris [109]
- Leonardo SPA [110]
- Northrop Grumman [111]
- Raytheon [112]
- Rohde&Schwartz [78]
- SAAB [82]
- TCI International [113]
- Thales [114]
- Unseenlabs [115][5]

3.6 A current SIGINT and IMINT use case: conflict in Ukraine, 2022

The current crisis in Ukraine is a very recent example, in which NATO and Europe are using reconnaissance aircraft to monitor the situation. Prior to the Russian invasion, Ukraine had given permission to these aircraft to be used in the Ukrainian air space. According to [116], NATO member air forces and alliance assets flew unprecedented, and almost continuous, intelligence, surveillance, and reconnaissance (ISR) flights over Ukraine itself. The media reported that at least the Rivet Joint (RC-135W) aircraft used by US and UK were flying in Ukraine prior to the start of hostilities [117]. The Rivet Joint is an aircraft dedicated to SIGINT. [116] also mentions US Army Bombardier Challenger 650-

[5] operates a unique satellite-based technology to identify, recognize and track a broad range of radio emitters and collects & processes proprietary data for maritime surveillance, contributing to maritime situational awareness. The technology relies on RF ELINT/SIGINT and serves both military and civilian applications.

based ARTEMIS aircraft, which have both COMINT and ELINT capabilities. Another report based on publicly available flight-tracking software and data suggest that quite a large number of aircraft types have been used in Ukraine and areas nearby it [118]. Also Unmanned Aerial Vehicles (UAVs), like the RQ-4 Global Hawk, have been mentioned in this context [116]. This UAV has among its many systems also ELINT capabilities. It is unclear, to which extent, if any, the ISR flights have been able to continue since the start of the hostilities. According to [116], this has not been possible at all, because Russia closed the Ukrainian air space as part of the invasion. However, continuous news streams from Ukraine for the past two months have repeatedly reported that Russia has not been able to achieve air superiority.

Relating to COMINT, several mainstream news organisations have reported interceptions of Russian military communications by Ukrainian amateur radio operators (for example [119]). According to the reports, the Russians were broadcasting in the clear particularly in the shortwave frequencies. Many sources and their frequencies have been identified and reported [120].

Finally, it has been reported (for example [121]), that the Ukrainian forces have managed to capture an advanced Russian electronic warfare (EW) system (so called Krasukha-4). This system is designed to jam low orbit satellites, drones, and missiles. It is also believed that the system can track NATO and alliance aircraft. The analysis of the system may bring insight how to detect (ELINT) and neutralize it in the battlefield.

Regarding IMINT the commercial satellite pictures have been shared in news media regularly to report on the progress of the war and of the invasion of the Russia groups. The shared pictures have been especially reporting on the areas that are of public interest: development of the invasion, destruction, casualties and e.g. shipping of Ukrainian corps to a Russian ship. The satellite imagery has not shared any highly critical or tactical information on. However commercial satellites have been following the area carefully and they can be used as vital evidence of the phases of the war and the destruction caused by the Russian. Already in 2015, after Russia annexed Crimea, Ukraine asked the Canadian government for access to RADARSAT-2 SAR imagery. RADARSAT-2 satellite is operated by the Canadian Space Agency and operated by MDA. Spatial resolution 1 m to 100 m, revisit frequency 24 days.

4. Discussion and recommendations

Role of SIGINT and European co-operation: Concerning the intelligence cycle, SIGINT is fundamentally about collection of intelligence. Depending on how various organisations define their intelligence cycles, SIGINT may also contain analysis of the collected data. There are also areas in which SIGIT overlaps with other forms of intelligence collection, or the definitions are not clear. MASINT and FISINT are examples of such. SIGINT has traditionally been defined as interception of foreign or enemy signals. Hence, it has been the domain of the military intelligence and those civilian intelligence agencies, which deal with foreign threats. With LEAs, this definition is flawed, but COMINT or ELINT type technical means can be applied for crime prevention and investigations. For such purposes, many European countries have lawful interception (such as intercepting mobile communications) degreed in their laws. Based on the study and references in this document, no clear picture could be formed on how LEAs utilize (or will utilize) SIGINT, or how LEAs co-operate to carry out SIGINT operations or share SIGINT information. On the military side, European NATO members have access to NATO SIGINT, while non-NATO members have to rely only to their national capabilities. It is not clear, for example in the current crisis in Ukraine, to which extent intelligence is exchanged between NATO and the alliance states. Concerning the civilian intelligence operators, nine European countries are rumoured to have formed an alliance, the so called SSEUR, with the UKUSA countries. Again, to which extent these countries exchange information with other European countries is not known. Such exchange may, for example, happen for combatting terrorism, but not necessarily in other areas.

Future needs of SIGINT: Concerning SIGINT, it is difficult to say, what are the future needs in terms of technologies, software and tools for countering enemy threats to national security or countering crime. The military and the specialised intelligence agencies do not discuss these issues publicly. LEAs seem to say very little as well. A long-standing problem in SIGINT is to recognise new types of signals, like from RF-controlled threats. UAVs and IEDs are examples of such. One recognised future trend is to combine SIGINT technology with electronic attack measures to create systems, which are not only able to recognise threats, but also counter them after recognition. From the perspective of LEAs, [58] identified the need to obtain telecommunications data as the only specific application area, which the interviewees recognised. Concerning tools or software, no highly relevant input was obtained, or the interviewees did not want to disclose their views on the matter.

Sensor / data fusion: within each INT, sensor or data fusion is usually performed to increase detection and identification capabilities, combining characteristics of several sensors (e.g. optical sensors for interpretable results and SAR imagery for all-weather capability)AI/ML tools was mentioned on the wish list in [58] for SIGINT, which is something that is becoming desirable in any technology area. However, it should be realised, that AI/ML solutions are tailor-made to a specific task, for example for canvasing specific type of details from specific type of intelligence. One aspect, where AI/ML could be very powerful is sensor data fusion, or fusion of different types of collected intelligence to form a more complete situational awareness. With the upcoming 5G (and 6G), mobile telecommunication networks will be combined with IoT and massive sensor networks. Sensor fusion is an obvious step to take both in commercial use and intelligence work.

Situational awareness: with a wide combination of various sensors and platforms, acquiring imagery and signals at different scales, spatial, spectral and temporal resolutions, the combined IMINT and SIGINT can provide a more complete situational awareness. AI/ML is a potential new methodology to

bring this about. Satellite constellations revisit and cover ever increasing area of the Earth surface and in addition UAV, HAPS platforms are developed to cover ares of key interest providing a precise situational awareness of the areas needed. In addition to military interests the EO applications have been developed to number of security and civilian applications that benefit from clear objectives of the imagery mission.

Artificial intelligence / machine learning for IMINT and SIGINT: For IMINT, AI / ML solutions are needed not only to process and analyse the ever-increasing amount of openly available data, but also simply to access, sift through and select relevant data. Because of the swift development the challenge is to keep up with the progress. It is argued with EO data that the unprecedented amount of data and its variability, velocity, and other Vs require more than calculation capacity, but rather disruptive innovations in big data management and production of information.[123] New reporting of the AI tools that can follow moving objects can change the use of commercial platforms to serve more intelligence purposes. Cloud processing will enable analysis results in near real time if needed. For SIGINT, "there is no silver bullet for AI in SIGINT", solutions need to be tailor-made for specific signals and applications. Although the need and the benefits for AI are visible the resources are often the bottleneck. Systems must always be built for the specific case, including training the models, which can be slow. ESA has initiatives to bridge the Artificial Intelligence for Earth Observation (AI4EO) [124] AI for intelligence has been discussed in detail in D3.6.

The advanced analysis of imagery intelligence to detect patterns, man-made changes and objects that we want to detect is becoming very precise while taking into account the resolution limits of the imagery. **Automated change detection**: has been developed for decades, but there is still the need for improvement especially for automatic identification of changes and unsupervised multi-sensor approaches.

Platform for data processing / thematic applications for security: One option to solve capacity challenges could include shared platforms for data processing and thematic applications for intelligence and security. One example from the other implementation area is the ESA Forestry TEP. This idea and possible implementation possibilities in European scale could be further discussed in the NOTIONES working groups. TO establish this kind of platforms common view should be built on various data management, AI ethics, platform development and ownership issues. The sharing of knowledge and common learning of detections could benefit all.

The increase of the **cooperation** with military and intelligence with commercial satellite community (what is seen now in USA) is expected to provide new approaches for IMINT and SIGINT products, for the development and for handling the satellite platforms and constellations. Taken together, the civilian, commercial, defence, and intelligence uses of space provide a vast and often interconnected matrix of essential capabilities. The new cooperation for collecting imagery and signals intelligence will provide additional support other agencies' intelligence products and services. Those current cooperation contracts are providing weekly about 100 million square kilometers of commercial imagery. The increasing number of satellites in the space and aerial platforms will enable monitoring of larger areas, in more detail, detecting deviations and changes, recognising shapes and tracking objects in more detail. The development of additional capabilities of COMSAT can also blur the line between military and commercial satellites. The increased number of aerial assets will probably also shift the development also to handling of the swarms of satellites to increase situational awareness and real time management of situations.

EO specialists that use imagery-based intelligence solutions can evolve exclusive versions for military users so that the solutions can be integrated with the overall domain awareness capability controlled by the users. Those with diverse sensing capabilities (EO/SAR/IR/RF monitoring) can consider the use of integrated solutions wherein multiple datasets are brought together for enhanced near-real-time domain awareness in support of space forces. [146]

In Europe the EU Satellite Centre (EU SatCen) plays an important role in creating the EU's indigenous intelligence capability to analyse satellite imagery and collateral data, including aerial imagery and related services.

Market analysis of the IMINT and space platform development report huge development during the last five years. The predicted further development on several technology areas will continue promptly. Therefore it is important that stakeholders and intelligence community participants periodically **update their knowledge** about the industry.

As a result of the high image quality and accurate data, IMINT data (UAV, HAPS, satellite) is a reliable source of information for different intelligence authorities or the military, which helps to achieve required security objectives. Information extracted from IMINT imagery will help authorities assess real situations, develop programs protect humans and infrastructures and improve future security and financial stability of communities. The current threat of terrorism or attacks on critical infrastructure can be monitored through IMINT and SIGINT products and preventive measures. Therefore, the government and the defence sector remain the main drivers of growth in the market. Aerial imagery streamlines decision-making and prediction of future developments.

As problems and datasets grow, modern computing systems have had to scale with them. Open-source frameworks can offer solutions e.g. Data Cube is a framework in which satellite imagery datasets are organized for a geographic area over a specified time period. Users can inspect changes to any area over any timespan covered by the ingested datasets. On the other hand quantum computing will offer a totally new and potentially disruptive computing paradigm that may be one solution for optimizing satellite constellation optimization and data analysis management.

Preliminary results on this problem using heterogeneous classical/quantum solutions are promising. Future intelligence will rely on technology, data fusion and analysis and of multiple intelligence sources where IMINT and SIGINT technologies provide important baseline for collection of data and information of the relevant targets and missions.

Intelligence acquisition systems are being developed in all operating environments. Due to rapid technological development, maintaining performance requires continuous significant new investments in. Technology trends, as well as the significant increase in the amount of information, including irrelevant information, and the complexity of analysis, place demands on the development of intelligence processes and systems to provide end-to-end information that is relevant and useful to the user. The **long-term development of staff skills** is also important.

5. Conclusion

This report presents the state of the art of IMINT and SIGINT technologies at the time when the Ukrainian war started. Due to this, the usage and benefits of both IMINT and SIGINT technologies have been reported largely in the normal news media though keeping of course the most strategic intelligence capabilities and information obscured. The war has shown that the capabilities of both intelligence types are huge in assessing the situation at hand, assessing the capabilities of both sides and projecting the possible future baths of the war. Furthermore both IMINT and SIGINT provide important sources of intelligence information in Multi-INT platforms. With the aid of current and future AI capabilities these platforms will conceptually transformation and impact traditional methods to process intelligence. The released from imagery intelligence has shown that the spatial resolution of also commercial IMINT has increased. The released commercial footages use AI based tools that provide very accurate results.

The different IMINT platforms and solutions differ according to resolution and operational time. However the common development path for all is that they all benefit from advancements in all areas of the solution e.g. hardware and AI. Future platforms, including HAPS, have high development opportunities as they may combine both IMINT and SIGINT needs. The technological challenges have diminished during the recent years making the solutions more economical and technically feasible. General digitalization and the additional use cases of HAPS for communication and surveillance may be the driving forces for the development. Regarding SIGINT Frost &Sullivan estimates that HAPS are well suited for peace time signal intelligence monitoring by employing a variety of communication and electronic payloads and that they could offer persistent resource that could build an electronic order of battle (EOB) picture 24/7 in peacetime and during hostilities.

Data processing capabilities, that allows users to transform imagery into e.g. common geospatial data, feeding map products and intelligence workflows is a critical component of IMINT.. As sources of data continue to grow exponentially machine learning and AI processes must be embedded to further automate tasks such as object and change detection on the imagery, and even the qualification of point cloud data. For this reason the data management and decisions on processing solutions may have significant importance. It must also be taken into account if the access to the native data without unadulterated pixels and information is provided e.g. to the decision-makers.

Based on the collected SIGINT information in this document, it is unclear, how and what SIGINT technologies and methods LEAs currently use, or what their needs for the future are. It is also unclear to what extent LEAs and intelligence agencies exchange information on a national level. On international level there are frameworks, within which intelligence agencies co-operate, but these do not include LEAs. Intercepting mobile communication or data, or intercepting internet communications or data, are most often mentioned. The former could be considered COMINT, but the latter is more in the area of mass surveillance. There are companies, who offer SIGINT systems and solutions. A large number of these companies are well known to produce these systems to the military forces. It is not known whether these companies have provided solutions to LEAs. Commercial SIGINT software and tools are also available, and it seems that anybody can acquire these with some exceptions. In conclusion, the role of SIGINT in LEA operations needs a lot of further work, which should be considered to take place in the Working Groups of WP6.

References

Literature:

[1] https://en.wikipedia.org/wiki/Intelligence_cycle

[2] NOTIONES Deliverable 2.3 report: The intelligence cycle.

[3] B. De Buck, (2014) “Role of Europol in International Police Cooperation after Lisbon”, ECLAN Summer School (12th Ed.), Brussels, June 29th - July 3rd.

[4] https://en.wikipedia.org/wiki/Intelligence_collection_management

[5] Office of the Director of National Intelligence (2018). What is Intelligence? [online] Dni.gov. Available at: https://www.dni.gov/index.php/what-we-do/what-is-intelligence.

[6] Wikipedia on Mass surveillance: https://en.wikipedia.org/wiki/Mass_surveillance and ref [10] from the Wikipedia article: Vinci, Anthony (August 31, 2020). "The Coming Revolution in Intelligence Affairs: How Artificial Intelligence and Autonomous Systems Will Transform Espionage". Foreign Affairs. Vol. 99, no. 5. ISSN 0015-7120.

[7] Anon, (n.d.). Image Intelligence, white paper. [online] Available at: https://sky-watch.com/media/1537/sky-watch-white-paper-image-intelligence_rev2.pdf.

[8] ZhiYong, L., Liu, T., Benediktsson, J. A., & Falco, N. (2021). Land cover change detection techniques: Very-high-resolution optical images: A review. IEEE Geoscience and Remote Sensing Magazine. https://doi.org/10.1109/MGRS.2021.3088865

[9] Molinier, M., Miettinen, J., Ienco, D., Qiu, S., & Zhu, Z. (2021). Optical Satellite Image Time Series Analysis for Environment Applications: From Classical Methods to Deep Learning and Beyond. Change Detection and Image Time Series Analysis 2: Supervised Methods, 109-154. https://doi.org/10.1002/9781119882299.ch4

[10] Shimoni, M., Haelterman, R., & Perneel, C. (2019). Hypersectral imaging for military and security applications: Combining myriad processing and sensing techniques. IEEE Geoscience and Remote Sensing Magazine, 7(2), 101-117. https://doi.org/10.1109/MGRS.2019.2902525

[11] Su, H., Wu, Z., Zhang, H., & Du, Q. (2021). Hyperspectral Anomaly Detection: A Survey. IEEE Geoscience and Remote Sensing Magazine. https://doi.org/10.1109/MGRS.2021.3105440

[12] Sun, G. C., Liu, Y., Liu, W., & Chen, J. (2021). Spaceborne synthetic aperture radar imaging algorithms: An overview. IEEE Geoscience and Remote Sensing Magazine. https://doi.org/10.1109/MGRS.2021.3097894

[13] Ma, P., Lin, H., Wang, W., Yu, H., Chen, F., Jiang, L., Zhou, L., Zhang, Z., Shi, G.& Wang, J. (2021). Toward Fine Surveillance: A Review of Multitemporal Interferometric Synthetic Aperture Radar for Infrastructure Health Monitoring. IEEE Geoscience and Remote Sensing Magazine. https://doi.org/10.1109/MGRS.2021.3098182

[14] Zhu, X. X., Tuia, D., Mou, L., Xia, G. S., Zhang, L., Xu, F., & Fraundorfer, F. (2017). Deep learning in remote sensing: A comprehensive review and list of resources. IEEE Geoscience and Remote Sensing Magazine, 5(4), 8-36. https://doi.org/10.1109/MGRS.2017.2762307

[15] Xin, W., Li, W., Danfeng, H., Ran, T., & Du, Q. (2021). Deep Learning for Unmanned Aerial Vehicle-Based Object Detection and Tracking: A Survey. IEEE Geoscience and Remote Sensing Magazine. https://doi.org/10.1109/MGRS.2021.3115137

[16] Hoeser, T., & Kuenzer, C. (2020). Object detection and image segmentation with deep learning on earth observation data: A review-part I: Evolution and recent trends. Remote Sensing, 12(10), 1667. https://doi.org/10.3390/rs12101667

[17] Hoeser, T., Bachofer, F., & Kuenzer, C. (2020). Object detection and image segmentation with deep learning on Earth observation data: A review—Part II: Applications. Remote Sensing, 12(18), https://doi.org/10.3390/rs12183053

[18] Gomes, V. C., Queiroz, G. R., & Ferreira, K. R. (2020). An overview of platforms for big earth observation data management and analysis. Remote Sensing, 12(8), 1253. https://doi.org/10.3390/rs12081253

[19] Gorelick, N., Hancher, M., Dixon, M., Ilyushchenko, S., Thau, D., & Moore, R. (2017). Google Earth Engine: Planetary-scale geospatial analysis for everyone. Remote sensing of Environment, 202, 18-27. https://doi.org/10.1016/j.rse.2017.06.031

[20] Kumar, L., & Mutanga, O. (2018). Google Earth Engine applications since inception: Usage, trends, and potential. Remote Sensing, 10(10), 1509. https://doi.org/10.3390/rs10101509

[21] Amani, M., Ghorbanian, A., Ahmadi, S. A., Kakooei, M., Moghimi, A., Mirmazloumi, S. M., Moghaddam, S.H.A., Mahdavi, S., Ghahremanlo, M., Parsian, S., Wu, Q. & Brisco, B. (2020). Google earth engine cloud computing platform for remote sensing big data applications: A comprehensive review. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 13, 5326-5350. https://doi.org/10.1109/JSTARS.2020.3021052

[22] Tamiminia, H., Salehi, B., Mahdianpari, M., Quackenbush, L., Adeli, S., & Brisco, B. (2020). Google Earth Engine for geo-big data applications: A meta-analysis and systematic review. ISPRS Journal of Photogrammetry and Remote Sensing, 164, 152-170. https://doi.org/10.1016/j.isprsjprs.2020.04.001

[23] Shakhatreh, H., Sawalmeh, A. H., Al-Fuqaha, A., Dou, Z., Almaita, E., Khalil, I., Noor, S., Khreishah, A. & Guizani, M. (2019). Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges. IEEE Access, 7, 48572-48634. https://doi.org/10.1109/ACCESS.2019.2909530

[24] Yao, H., Qin, R., & Chen, X. (2019). Unmanned aerial vehicle for remote sensing applications—A review. Remote Sensing, 11(12), 1443. https://doi.org/10.3390/rs11121443

[25] Xiang, T. Z., Xia, G. S., & Zhang, L. (2019). Mini-unmanned aerial vehicle-based remote sensing: techniques, applications, and prospects. IEEE geoscience and remote sensing magazine, 7(3), 29-63. https://doi.org/10.1109/MGRS.2019.2918840

[26] Zhou, G. (2009). Near real-time orthorectification and mosaic of small UAV video flow for time-critical event response. IEEE Transactions on Geoscience and Remote Sensing, 47(3), 739-747. https://doi.org/10.1109/TGRS.2008.2006505

[27] Do, Q. T., Shapiro, J. N., Elvidge, C. D., Abdel-Jelil, M., Ahn, D. P., Baugh, K., Hansen-Lewis, J., Zhizhin, M & Bazilian, M. D. (2018). Terrorism, geopolitics, and oil security: Using remote sensing to estimate oil production of the Islamic State. Energy research & social science, 44, 411-418. https://dx.doi.org/10.1016%2Fj.erss.2018.03.013

[28] Avtar, R., Kouser, A., Kumar, A., Singh, D., Misra, P., Gupta, A., Yunus, A.P. Kumar, P., Johnson, B.A., Dasgupta, R., Sahu, N., & Besse Rimba, A. (2021). Remote sensing for international peace and security: Its role and implications. Remote Sensing, 13(3), 439. https://doi.org/10.3390/rs13030439

[29] Witmer, F. D. (2015). Remote sensing of violent conflict: eyes from above. International Journal of Remote Sensing, 36(9), 2326-2352. https://doi.org/10.1080/01431161.2015.1035412

[30] Kelly, A. B., & Kelly, N. M. (2014). Validating the remotely sensed geography of crime: A review of emerging issues. Remote Sensing, 6(12), 12723-12751. https://doi.org/10.3390/rs61212723

[31] Kalacska, M., & Bell, L. S. (2006). Remote sensing as a tool for the detection of clandestine mass graves. Canadian Society of Forensic Science Journal, 39(1), 1-13. https://doi.org/10.1080/00085030.2006.10757132

[32] Evers, R., & Masters, P. (2018). The application of low-altitude near-infrared aerial photography for detecting clandestine burials using a UAV and low-cost unmodified digital camera. Forensic science international, 289, 408-418. https://doi.org/10.1016/j.forsciint.2018.06.020

[33] Blau, S., Sterenberg, J., Weeden, P., Urzedo, F., Wright, R., & Watson, C. (2018). Exploring non-invasive approaches to assist in the detection of clandestine human burials: developing a way forward. Forensic Sciences Research, 3(4), 320-342. https://doi.org/10.1080/20961790.2018.1493809

[34] Butters, O., Krosch, M. N., Roberts, M., & MacGregor, D. (2021). Application of forward-looking infrared (FLIR) imaging from an unmanned aerial platform in the search for decomposing remains. Journal of Forensic Sciences, 66(1), 347-355. https://doi.org/10.1111/1556-4029.14581

[35] Pensieri, M. G., Garau, M., & Barone, P. M. (2020). Drones as an integral part of remote sensing technologies to help missing people. Drones, 4(2), 15. https://doi.org/10.3390/drones4020015

[36] Barone, P. M., & Di Maggio, R. M. (2019). Forensic geophysics: ground penetrating radar (GPR) techniques and missing persons investigations. Forensic Sciences Research, 4(4), 337-340. https://doi.org/10.1080/20961790.2019.1675353

[37] Algahtany, M., & Kumar, L. (2016). A method for exploring the link between urban area expansion over time and the opportunity for crime in Saudi Arabia. Remote Sensing, 8(10), 863. https://doi.org/10.3390/rs8100863

[38] Perez, D., Banerjee, D., Kwan, C., Dao, M., Shen, Y., Koperski, K., Marchisio, G., & Li, J. (2017, October). Deep learning for effective detection of excavated soil related to illegal tunnel activities. In 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON) (pp. 626-632). IEEE. https://doi.org/10.1109/UEMCON.2017.8249062

[39] Bassoli, R., Sacchi, C., Granelli, F., & Ashkenazi, I. (2019, March). A virtualized border control system based on UAVs: Design and energy efficiency considerations. In 2019 IEEE aerospace conference (pp. 1-11). IEEE. https://doi.org/10.1109/AERO.2019.8742142

[40] Coulter, L., Stow, D., Tsai, Y. H., Chavis, C., Lippitt, C., Fraley, G., & McCreight, R. (2012, March). Automated detection of people and vehicles in natural environments using high temporal resolution airborne remote sensing. In Proceedings of the ASPRS Annual Conference (pp. 78-90). https://geog.sdsu.edu/People/Pages/lcoulter/DARPA/files/Coulter_et_al_2012b.pdf

[41] Fytsilis, A. L., Prokos, A., Koutroumbas, K. D., Michail, D., & Kontoes, C. C. (2016). A methodology for near real-time change detection between Unmanned Aerial Vehicle and wide area satellite images. ISPRS Journal of Photogrammetry and Remote Sensing, 119, 165-186. https://doi.org/10.1016/j.isprsjprs.2016.06.001

[42] Malinowski, R. (2010, September). Land Border Monitoring with remote sensing technologies. In Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2010 (Vol. 7745, p. 77451V). International Society for Optics and Photonics. https://doi.org/10.1117/12.871930

[43] Koslowski, R., & Schulzke, M. (2018). Drones along borders: Border security UAVs in the United States and the European Union. International Studies Perspectives. https://doi.org/10.1093/isp/eky002

[44] Haddal, C. C., & Gertler, J. (2010, July). Homeland security: Unmanned aerial vehicles and border surveillance. Library of Congress Washington DC Congressional Research Service. https://apps.dtic.mil/sti/citations/ADA524297 | https://apps.dtic.mil/sti/pdfs/ADA524297.pdf

[45] U.S. HOUSE OF REPRESENTATIVES (2010) The Role of Unmanned Aerial Systems in Border Security. HEARING BEFORE THE SUBCOMMITTEE ON BORDER, MARITIME, AND GLOBAL COUNTERTERRORISM OF THE COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES, ONE HUNDRED ELEVENTH CONGRESS - SECOND SESSION, JULY 15, 2010. https://www.govinfo.gov/content/pkg/CHRG-111hhrg64701/pdf/CHRG-111hhrg64701.pdf

[46] Boyd, D. S., Jackson, B., Wardlaw, J., Foody, G. M., Marsh, S., & Bales, K. (2018). Slavery from space: Demonstrating the role for satellite remote sensing to inform evidence-based action related to UN SDG number 8. ISPRS journal of photogrammetry and remote sensing, 142, 380. https://doi.org/10.1016/j.isprsjprs.2018.02.012

[47] https://en.wikipedia.org/wiki/Signals_intelligence

[48] European Convention on Human Rights. (2013). https://www.echr.coe.int/documents/convention_eng.pdf

[49] Nortio, J. (2019). Tiedustelulait muuttavat oikeuskäyntäntöä. Lakimiesuutiset. https://lakimiesuutiset.fi/tiedustelulait-muuttavat-oikeuskaytantoa/

[50] Cameron, I. (2020). REGULATING SIGNALS INTELLIGENCE. Strassbourg Observers. https://strasbourgobservers.com/2020/07/13/regulating-signals-intelligence/

[51] Council Resolution of 17 January 1995 on the lawful interception of telecommunications. (1996). Official Journal C 329. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31996G1104

[52] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). (2009). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

[53] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security; Lawful Interception requirements (Release 17). (2022). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3181

[54] Managing & Analyzing Huge Datasets for Law Enforcement Investigations. (2020). Managing & Analyzing Huge Datasets for Law Enforcement Investigations. https://ss8.com/managing-analyzing-huge-datasets-for-law-enforcement-investigations/

[55] Lawful Interception (LI); Requirements of Law Enforcement Agencies. (2021). ETSI TS 101 331 V1.8.1. https://www.etsi.org/deliver/etsi_ts/101300_101399/101331/01.08.01_60/ts_101331v010801p.pdf

[56] Eng Seng, A. C. (2007). MASINT the Intelligence of the Future. https://www.dsta.gov.sg/docs/default-source/dsta-about/dh2007_chapter_10.pdf?sfvrsn=2

[57] https://www.emsopedia.org/entries/signal-intelligence-sigint/

[58] NOTIONES Deliverable 2.2 report: Synthesis of the interviews' results.

[59] https://military-history.fandom.com/wiki/UKUSA_Agreement

[60] https://en.wikipedia.org/wiki/ECHELON

[61] https://www.nato.int/

[62] https://www.electrospaces.net/2013/12/14-eyes-are-3rd-party-partners-forming.html

[63] https://en.wikipedia.org/wiki/List_of_intelligence_agencies

[64] K. L. Lasoen (2019), "Belgian Intelligence SIGINT Operations", *International Journal of Intelligence and CounterIntelligence* **32** (1), pp. 1-29.

[65] https://en.wikipedia.org/wiki/Finnish_Defence_Intelligence_Agency

[66] https://puolustusvoimat.fi/tietoa-meista/tiedustelulaitos (in Finnish)

[67] https://supo.fi/en/intelligence-gathering

[68] https://www.defense.gouv.fr/english/dgse/tout-le-site/who-we-are

[69] https://www.bnd.bund.de/EN/What-we-do/Collecting-Information/collecting_node.html;jsessionid=68D278919D1BE4ABD8C2CA0C6131EF7A.2_cid386

[70] https://www.military.ie/en/who-we-are/army/army-corps/cis-corps/
[71] https://www.forsvaret.no/en/organisation/norwegian-intelligence-service
[72] https://www.cni.es/en/intelligence/collection
[73] https://www.fra.se/system/engelska/english.4.6a76c4041614726b25ae4.html
[74] https://www.gchq.gov.uk/
[75] https://en.wikipedia.org/wiki/Signals_intelligence_operational_platforms_by_nation
[76] https://www.emsopedia.org/entries/electronic-intelligence-elint/
[77] https://www.emsopedia.org/entries/acoustic-intelligence-acint-2/
[78] https://www.rohde-schwarz.com/fi/solutions/aerospace-defense-security/defense/signal-intelligence-electronic-warfare/overview/signal-intelligence-systems_91497.html
[79] https://www.navalanalyses.com/2015/01/naval-forces-5-signals-intelligence.html
[80] https://insightcrime.org/news/tides-turning-first-narco-sub-built-europe-seized-spain/
[81] https://corporalfrisk.com/2019/06/14/finnish-maritime-patrol/
[82] https://www.saab.com/products/globaleye
[83] https://www.emsopedia.org/entries/tactical-surveillance/
[84] https://www.satcen.europa.eu/
[85] AIRBUS Media Centre. CERES. @AIRBUS 2015. https://mediacentre.airbus.com/element?id=598168
[86] https://privacyinternational.org/explainer/1640/phone-monitoring
[87] https://en.wikipedia.org/wiki/Lawful_interception
[88] https://iicybersecurity.wordpress.com/2015/05/11/how-to-intercept-mobile-communications-calls-and-messages-easily-without-hacking/
[89] https://www.theguardian.com/technology/1999/apr/29/onlinesupplement3
[90] https://elie.net/blog/security/understanding-the-prevalence-of-web-traffic-interception/
[91] https://www.comintconsulting.com/
[92] https://www.mem3nt0.com/en/
[93] https://www.nsogroup.com/
[94] https://www.sigintos.com/about/
[95] https://www.swri.org/industries/signals-intelligence-solutions
[96] https://www.srcinc.com/services/intel-analysis-and-production/sigint-tool-development-and-ew-modernization.aspx
[97] https://www.securitynewspaper.com/2018/02/19/intercept-mobile-communications-calls-messages-easily-without-hacking/
[98] https://thinkrf.com/solutions/signals-intelligence-sigint/
[99] https://vts-i.com/signals-intelligence-surveillance-and-reconnaissance-isr/
[100] https://www.airbus.com/en/newsroom/press-releases/2021-11-ceres-reconnaissance-space-system-designed-by-airbus-and-thales
[101] https://www.intelligence-airbusds.com/newsroom/press-releases/thales-airbus-selected-by-dga-to-upgrade-frances-joint-electronic-warfare-capabilities/
[102] https://avantix.net/
[103] https://www.baesystems.com/en-us/productfamily/adaptive-sensors
[104] https://www.blackriversystems.com/
[105] https://www.boeing.com/
[106] https://gdmissionsystems.com/intelligence-systems/signals-intelligence

[107] https://horizontechnologies.eu/
[108] https://www.iai.co.il/defense/air/airborne-sigint-electronic-warfare-ew
[109] https://www.l3harris.com/all-capabilities/signals-intelligence-sigint-systems
[110] https://www.leonardo.com/en/web/electronics/products/sage-1
[111] https://www.northropgrumman.com/
[112] https://www.raytheon.com/capabilities/products/ast
[113] https://www.tcibr.com/signals-intelligence-elint-comint-systems/
[114] https://www.thalesgroup.com/en/markets/defence-and-security
[115] https://unseenlabs.space/technology/
[116] https://www.janes.com/defence-news/news-detail/nato-loses-isr-capability-over-ukraine-as-putin-closes-airspace
[117] https://ukdefencejournal.org.uk/british-aircraft-continue-to-monitor-russian-forces-near-ukraine/
[118] https://www.thedrive.com/the-war-zone/44337/these-are-the-planes-keeping-watch-on-russian-forces-around-ukraine
[119] https://www.youtube.com/watch?v=gOmYi96cU1M
[120] https://k0lwc.com/monitoring-the-airwaves-during-ukrainian-conflict/
[121] https://www.businessinsider.com/russian-hi-tech-warfare-system-seized-ukraine-hold-military-secrets-2022-3?r=US&IR=T
[122] https://www.euronews.com/next/2021/07/20/what-is-pegasus-the-israeli-mobile-phone-spyware-used-by-governments-around-the-world
[123] Sudmanns, M., Tiede, D., Lang, S., Bergstedt, H., Trost, G., Augustin, H., Baraldi, A., & Blaschke, T. (2019). Big Earth data: disruptive changes in Earth observation data management and analysis? International Journal of Digital Earth, 13(7), 832–850. https://doi.org/10.1080/17538947.2019.1585976
[124] https://ai4eo.eu/
[125] https://joint-research-centre.ec.europa.eu/scientific-activities-z/earth-observation_en
[126] https://earthdata.nasa.gov/learn/backgrounders/what-is-sar
[127] Satellite vs LiDAR: Which is the future of Vegetation Management?. (2021). Www.tdworld.com. from https://www.tdworld.com/vegetation-management/whitepaper/21168494/satellite-vs-lidar-which-is-the-future-of-vegetation-management
[128] Shedd, D. R. (2021). It's time for a tactical LiDAR satellite. Retrieved May 24, 2022, from Defense Systems website: https://defensesystems.com/2021/01/its-time-for-a-tactical-lidar-satellite/195114/
[129] Radiometric Resolution | fis.uni-bonn.de. (n.d.). Retrieved from www.fis.uni-bonn.de website: https://www.fis.uni-bonn.de/en/recherchetools/infobox/professionals/resolution/radiometric-resolution
[130] Temporal Resolution | fis.uni-bonn.de. (n.d.). Retrieved from www.fis.uni-bonn.de website: https://www.fis.uni-bonn.de/en/recherchetools/infobox/professionals/resolution/temporal-resolution
[131] Xiang, Tian-Zhu & Xia, Gui-Song & Zhang, Liangpei. (2018). Mini-UAV-based Remote Sensing: Techniques, Applications and Prospectives. IEEE Geoscience and Remote Sensing Magazine, 2019, Vol. 7, No. 3, pp. 29-63. https://doi.org/10.1109/MGRS.2019.2918840
[132] GSMA. (2021). High Altitude Platform Systems. Towers in the Skies. Retrieved from https://www.gsma.com/futurenetworks/wp-content/uploads/2021/06/GSMA-HAPS-Towers-in-the-skies-Whitepaper-2021.pdf

[133] AeroVironment, Inc. | Unmanned Aircraft Systems (UAS), Tactical Missile Systems, Unmanned Ground Vehicles. (n.d.). Retrieved May 24, 2022, from AeroVironment, Inc. website: https://www.avinc.com/

[134] Thomas Augustyn, "The KS-146A Long Range Oblique Photography (LOROP) Camera System," Proc. SPIE 0309, Airborne Reconnaissance V, (12 December 1981); https://doi.org/10.1117/12.932761

[135] Proceedings Volume 8360, Airborne Intelligence, Surveillance, Reconnaissance (ISR) Systems and Applications IX; 836003 (2012) https://doi.org/10.1117/12.917684 . Event: SPIE Defense, Security, and Sensing, 2012, Baltimore, Maryland, United States

[136] Global High altitude Pseudo Satellites (HAPS) Growth Opportunities. New Technology Strategies Will Move the Market from the Development Stage to Early Adoption by 2026. (2021) PBDA-59. Frost&Sullivan.

[137] Deutche Welle (www.dw.com), (n.d.). Satellite imagery becomes big business | DW | 12.04.2022. https://www.dw.com/en/satellite-imagery-becomes-big-business/av-61448697

[138] Get your own satellite in orbit in just 10 months. (n.d.). Www.esa.int. https://www.esa.int/Applications/Technology_Transfer/Get_your_own_satellite_in_orbit_in_just_10_months

[139] Satellite Imaging Market Size, Share, Industry Analysis by application, by End-Use and by regional forecast 2022-2029. Summary. (n.d.). Www.fortunebusinessinsights.com. https://www.fortunebusinessinsights.com/satellite-imaging-market-103372

[140] Commercial Satellite Imaging Market Size, Trends, Analysis 2030. (n.d.). Allied Market Research. Retrieved May 30, 2022, from https://www.alliedmarketresearch.com/commercial-satellite-imaging-market

[141] Maxar's HD Technology Provides Measurable Improvements in Machine…. (n.d.). Maxar Blog. Retrieved May 31, 2022, from https://blog.maxar.com/tech-and-tradecraft/2022/maxars-hd-technology-provides-measurable-improvements-in-machine-learning-applications

[142] Meaker, M. (2022). High Above Ukraine, Satellites Get Embroiled in the War. Wired. https://www.wired.com/story/ukraine-russia-satellites/

[143] Yonekura, E., Dolan, B., Kim, M., Romita, K., Raza Khan, G. and Kim, Y. (2022). Commercial Space Capabilities and Market Overview The Relationship Between Commercial Space Developments and the U.S. Department of Defense. [online] RAND. Available at: https://www.rand.org/pubs/research_reports/RRA578-2.html.

[144] NRO's Largest Award Of Commercial Imagery Contracts Worth Billions To Three Companies – SatNews. (n.d.). News.satnews.com. Retrieved May 31, 2022, from https://news.satnews.com/2022/05/26/nros-largest-award-of-commercial-imagery-contracts-worth-billions-to-three-companies/

[145] Chinese AI turns commercial satellite into precise spy tracker: paper. (2022). South China Morning Post. https://www.scmp.com/news/china/science/article/3173285/chinese-ai-turns-commercial-satellite-spy-tracker-able-follow

[146] Global Military Satellite-based ISR Growth Opportunities. Growth Opportunities are Evolving to Engage NewSpace Start-ups Driven by Innovation Culture.(2022) Global Aerospace & Defense Research Team at Frost & Sullivan K643-66 Frost&Sullivan.