Earth Observation for Security and Defense 38

Ferdinando Dolce, Davide Di Domizio, Denis Bruckert,
Alvaro Rodríguez, and Andrea Patrono

Contents

Introduction 706
Earth Observation Security and Defense Application Landscape 706
Earth Observation Missions and Applications for Security and Defense 710
Security and Defense EO Application 713
Examples of EO Operational Tasks and Services for Security and Defense 717
Examples of EO Operational Tasks 717
Copernicus SEA 719
Evolution of EO Services and Application at EU SatCen and Copernicus SEA 724
SatCen Service Evolution: Artificial Intelligence/Machine Learning 724
Copernicus SEA Service Evolution 726
Conclusion 728
References 729

Abstract

The contents reported in this chapter reflect the opinions of the authors and do not necessarily reflect the opinions of the respective Agency/Institutions

Space-based Earth Observation is a consolidated capability providing added value to reach information superiority, a crucial enabler for operations in both security and defense domains. The availability and responsiveness of satellite payloads, together with exploitation capacity, allow to plan, monitor, and inform security and defense forces with performance not available with other means.

F. Dolce (✉) · D. Di Domizio
European Defence Agency (EDA), Brussels, Belgium
e-mail: ferdinando.dolce@aeronautica.difesa.it; davide.didomizio@eda.europa.eu

D. Bruckert · A. Rodríguez · A. Patrono
EU Satellite Centre (EUSC), Madrid, Spain
e-mail: Denis.Bruckert@satcen.europa.eu; Alvaro.Rodriguez@satcen.europa.eu; Andrea.Patrono@satcen.europa.eu

K.-U. Schrogl (ed.), *Handbook of Space Security*,
https://doi.org/10.1007/978-3-030-23210-8_106

This chapter describes how the gap between security and defense domains is increasingly blurred and the capacity to exploit the "big data" made available by the satellite systems and other contributing missions is becoming a common technological and operational challenge.

Introduction

Space-based Earth Observation (SBEO) capabilities are one of the main data providers to imagery intelligence (IMINT) and geospatial intelligence (GEOINT) communities, since the technical and geographic information that can be derived from satellite systems through the interpretation or analysis of imagery is nowadays essential. However, SBEO products, including exploitation of imagery data derived from several categories of sensors, electro-optical, radar, infrared (IR), multi-spectral, or laser, can go well beyond IMINT/GEOINT domains and are used for both security and defense users for several purposes. Future SBEO satellites are providing big data from space and are building situation awareness, enabling the possibility to analyze the collected information, delivering products that will require strong optimization and improving in terms of delays in processing, interpreting, and disseminating to final customers. SBEO data/products, however, support also the monitoring phase, which relies on intelligence and is composed of two complementary functions: the early warning and the strategic surveillance. Furthermore, military planning, as well as geospatial support, also represents additional needs that can be accomplished through Space-based Earth Observation (SBEO) satellites' data and products at both political, strategic, and operational level.

In recent years, there has been an increase in the development of tools and techniques to improve the exploitation of collected imagery data also to face the proliferation of SBEO assets. However, it is judged that the security and defense communities have not fully benefitted from this development, and they will need tools and procedures to fully take advantage of these technologies and to increase the trust in such kind of future supporting capabilities. One of the main difficulties will be the need to better balance and leverage the skills of analysts and operators within effective and efficient operational workflows and trusted data exploitation algorithms.

This chapter is mainly focused on the analysis of current and future applications to support security and defense missions using Space-based Earth Observation sources.

Earth Observation Security and Defense Application Landscape

Earth Observation (EO) sensors mounted on space-borne platforms have now almost 50 years' life – successful – story. Three systems which represent the founding pillars of EO commercial satellites era: (1) Landsat-1 (1972), the first EO satellite to be launched to study and monitor the whole Earth's surface; (2) SPOT-1 (1986) that used a revolutionary commercial model for image distribution; (3) Ikonos (1999), the first commercial EO system capable to collect images with a ground sampling distance below 1 m (0.82 m) at Nadir (Denis et al. 2017). Meanwhile, US policy shift favored rapid market adoption for high-resolution satellite imagery anticipating a significant short- and long-term growth. Shortly after, DigitalGlobe launched QuickBird (2001).

In the last few years, there has been a proliferation of SBEO systems (archival, current, and planned – over 100 s of sensors (Committee on Earth Observation Satellites www.ceos.org)) and others are now planned up to 2030 and beyond. Performance of sensors and mission technology has progressed over the last two decades. Overall, missions experimented longer endurance than expected and both optical and SAR sensors meliorated their design increasing, e.g., sensing performance, positional accuracy, and platforms' agility. Moreover, satellite systems progressively moved from the single-sensor model to the constellation approach. Performances have been boosted as well by the progressive implementation of the "dual-use" systems concept that allow different user communities to manage and exploit them taking advantage of a synergetic approach (despite configurations and rules may vary from mission to mission). The most recent development is the launch of nano- and micro-satellites (with constellations that can reach 100+). Lowering the cost of access to SBEO, they are becoming increasingly more attractive than conventional satellites. As an overall consequence, availability and access to data obtained by space-borne missions are increasing – and will continue to – in an exponential way, offering better and truly affordable observation capabilities at a greater range of spatial, spectral, and temporal resolutions (Belward and Skøien 2015; Denis et al. 2016; Toth and Jóźków 2016).

Image analysis production based and organized as a sequential series of human interventions in a pipe way may soon get overwhelmed in the new scenario shaped by huge observation data handiness and increasing computing capability. Providers sitting on massive amounts of exploitable data and user communities progressively expanding their analytical appetite for new products and services need faster and further interactive production modalities. The increasing development of web-based solutions and cloud-based services has allowed better quality of online functionality and performance without having necessarily to host and manage the data. Fast access to extensive archives of data, integration of diverse workflows user-specific, qualification of providers and users to work in diverse but interconnected environments to consume data, provide services, generate information and distribute products, are step by step leading the way of EO exploitation and derived value-added production. Any implementation can/shall be adapted for ad hoc security environments, without implying different design but with enforcement of specific security protocols and restrictions – no misuse or free outflow (Holmes et al. 2018). As an example, NGA (former) Director Robert Cardillo, during his keynote at the 2018 GEOINT Symposium in Tampa, announced a new online platform for open collaboration and development of geospatial solutions.

An important component of EO in supporting the primary aims of the space and security and defense domain is the provision of image and geospatial intelligence products and services resulting from the exploitation of remotely sensed data acquired by sensors mounted on space-borne assets. The reflections or emissions measured by the different types of sensors are depicted in images that need to be converted into meaningful information. Observation data are currently showing a new unique scenario in terms of variety, volume, velocity, veracity, and value. Geospatial information and EO, together with modern data processing and big data analytics, offer unprecedented opportunities (Lee and Kang 2015; Nativi et al. 2015; Câmara et al. 2016). There are different application approaches to face this challenge and they mainly depend on the type of sensor used and the sort of information that needs to be extracted.

Historically, in the security-defense environment, information is derived through a subjective analytical approach principally based on the experience and the skills of the analyst who visually interprets the image(s). The spatial and contextual way to proceed varies and depends on the objective of the study. Spatial, pattern, texture, and, in general, spectral information is most of the time improved by standard image processing technics (i.e., image enhancement) for increasing the visual distinction between features. Different collateral/ancillary data, spatially and temporally correlated with the imagery, made available through different sources, may complement the analytical process providing worthwhile information, essential in helping, confirming, etc. the interpretation course and its inferences (Campbell and Wynne 2011).

When the analysis needs to cover large areas, perform quantitative investigation, implement complex monitoring, rapidly highlight features not detectable at first view, (semi)automation of the analytical process may facilitate the interpretation process, e.g., decreasing the analysis time span and the risk of poor detection rates when compared to only human, lengthy, scrutiny approaches.

The application of robust algorithms/models to transform spectral into “meaningful” information offers an invaluable support. Nevertheless, deterministic models have to be accurately parameterized according to the sensor performance, the nature of the analyzed variables, and the information to infer for a specific task (Adams and Gillespie 2006). Since this approach needs an exhaustive knowledge, testing, and repeatable conditions to establish firm physical relations (that not necessarily exist and that ideally should be supported by an extensive fieldwork activity that most of the time – in the security-defense domain – is unfeasible for the nature of the requests and/or its location), alternative ways to proceed are used to facilitate the analytical process.

The statistical analysis of the spectral information and its supposed relationship with the phenomena to be assessed is used to reduce or transform the dimensionality of the data and to increase either the computational efficiency of, e.g., an image classification or the understating and manual extraction of the analyzed features (Lillesand et al. 2014).

Spectral rationing with adequately chosen spectral areas and appropriate wavebands or combinations of wavebands may as well facilitate the depiction of specific information. They can be used to better reflect the image content and, as well, to further improve the performance of any of the hereby mentioned methods, including image fusion such as pan-sharpening techniques (Ghassemian 2016).

As temporal resolution of EO systems and constellations increased, multi-temporal data merging and change detection computing capacities augmented as well in terms of applicability and efficiency in supporting (semi)automatic monitoring of surface changes over varying time span intervals – including detection, estimation, and/or comparison of trends and dynamics (Fulcher et al. 2013; Hussain et al. 2013; Bovolo and Bruzzone 2015). This also simplifies the handling of the increasing load of imagery data, the controlling of alarms, and a better management of direct human involvement.

Where subjective, deterministic or statistical classic analysis become insufficient to identify relationships between the different pieces of available information – or simply are unknown or too lengthy, approximate, etc. to be established. Artificial Intelligence (AI) methods are progressively demonstrating the potential to get information out faster with more thorough and complete analysis. In recent years, neural network applications increasingly demonstrated better capability to automatically discover relevant contextual features in remotely sensed images (Arel et al. 2010; Long et al. 2017; Maggiori et al. 2017). Data volume and computational capacity increased exponentially, boosting precisely the application of neural network computing to satellite image (when compared to studies performed in the 1990s such as (Hepner et al. 1990) or (Atkinson and Tatnall 1997)). However, one of the major problems associated with precise recognition and extraction of objects from remotely sensed data is still the time and cost of wide-ranging training of algorithms, requiring experienced analysts (Ball et al. 2017), particularly when tasks to be undertaken are context specific and imply constant tailoring and precise knowledge, background, etc. as in the security-defense domain.

Collateral information gathered from social media are both worthy in supporting imagery analysis, and progressively more complex to use (i.e., floods of data, abundant, rapid, and accessible implying fast and qualified reactivity to provide the required situational awareness of relevant information) (Li et al. 2017). AI is as well improving the speed and accuracy of identifying enlightening evidences, allowing analysts to expand capacity, create new analytic products, etc. Reliable information gleaning has definitely progressed thanks to AI; nevertheless, it is still *in fieri* and constant adaptation and tailoring is often necessary to build up and maintain a knowledge data base, requiring expert interpretation processes to cope with uncertainty and/or incomplete information extraction.

The choice of analytic approach depends on the available data, the degree of understanding of the processes under examination, and the possible relationship between the EO data inputs and the goal of the analysis. In the security-defense domain, when the rather heterogeneous portfolio of possible EO-based services is considered, there is no rigid predefined approach to tackle any specific task. Experience, to be read as knowledge, understanding, mastering, etc., is at the core of any study and will guide the analyst to choose and combine, in an optimized way, any of the above-mentioned approaches, according to the context and the data availability. While operational use of EO keeps growing, gaps and opportunities for further development to tackle increasingly complex operational applications still exist and will always need adequate experienced human supervision throughout the entire analytical process.

Earth Observation Missions and Applications for Security and Defense

Space-based Earth Observation is now able to satisfy the growing needs of both security and defense entities and private customers coming worldwide since space systems are now becoming more and more numerous. Nowadays, it is expected that almost an infinite amount of information will be available, creating a high level of common awareness, while just a few years ago the prediction of a future information age was providing a different outlook. As matter of fact, the US commercial approach, known as “new space,” is moving the market in the clear direction of an easier and cheaper access to space, reducing the life and dimensions of space missions and increasing the number of systems in orbit (Space Strategy for Europe – European Commission COM 2016). Governmental institutions and small countries can see micro-satellites’ capabilities as the only opportunity to reach an independent, confidential, and trusted space-based capability due to the lower cost in development and launch phases they are promising.

On the other hand, in addition to real information, there is a lot of misleading information that can become a threat in modern warfare scenarios. In the past, such kind of information was not considered a relevant threat since they were limited to few numbers of potential events, while today it represents one of the most challenging threats to face. Criminal organizations can express their soft power generating misleading information, e.g., in the cyber domain. From this prospective, space-based information and communication services can represent a reservoir in terms of reliability and trustiness of the information more than other alternate sources.

In this congested and competitive space environment, EO products can certainly be derived by different platforms and the integration of the information coming from several sensor classes will represent the new bottleneck. With the availability of big data coming from space, such a huge offer of space imageries could move the equilibrium from the space to the ground segment. If yesterday access to space was the real challenge, and possibility to get access to space capabilities was the key enabling factor, now this is not anymore the case: the challenge will be the capability to acquire, store, manage, process, and deliver reliable and timely information, to be extracted by all essential data. Military will continue to define SBEO requirements in terms of accuracy and spectrum band; however, data fusion and integrated products merging different EO data, Positioning Navigation and Timing (PNT), and communication capabilities will be the key to deliver effective recognized pictures for defense operations.

Even considering that, the Ministries of Defences (MoDs) cannot certainly rely on commercial application to accomplish their task, especially if the data are provided by foreign companies, that are able to exercise a shutter control in certain specific time and area of interest (AoI). It is then easy to understand that space institutional flagship programs turn to be strategic as they provide not only a full set of information but also the control of the data acquisition, flow, policy, and security.

Space-based data moreover solve a key issue in terms of autonomy to the MoDs. In fact, one of the biggest strengths of the SBEO systems is that they are not affected by sovereign rights of States "overflown" by spacecrafts (United Nations Treaties and Principles on Outer Space 2002). This makes possible to obtain information about the area of interest through means regulated by agreed international laws, without any engagement of the States overflown by the spacecraft.

Even if the difference between defense and security domains is not easy to identify and both concepts could lead to misinterpretation, it could be summarized as the following: security's main task has to face with Member State's internal risks without a prerecognized enemy or attack to face, e.g., terrorism; on the other hand, defense's main task has to face with Member State's threats against an external identified enemy (Britz and Eriksson 2005; French white paper on Defence and National Security 2013). From this simple, but of course not exhaustive definition, it is clear that the capabilities required to deal with these two different scenarios are not necessarily equal. Nevertheless, the evolution of the global international scenario is generating boundaries that are quite often not clearly defined. The power's global model, in fact, is evolving quite rapidly moving from a clear unipolar international system after the end of Cold War, when some distinguished authors declared "The End of History" (Fukuyama 1989) to a more global and fragmented multipolar model, where the symmetry of previous scenarios is not anymore applicable. This asymmetry is certainly reflected into military operations, coping with a hybrid warfare scenario and threats that cannot be easily identified. In such conditions, the evolution of guerrilla environments led to an unclear definition and delineation of geospatial limits. The time when the Greek arena's competition model was applicable looks today as an ancient memory, while strategic models based on oriental philosophies, referring mainly to Sun Tzu's doctrine (Tzu 2007) where the art of camouflage is a key capability, are becoming more applicable to modern terroristic threats.

As a direct consequence of these new scenarios, the boundaries between internal and external activities are clearly not well identified, calling for an increasing application of defense capabilities for homeland security. Defense techniques, procedures, and expertise are now finding a great demand in the civilian and the security world (European External Acton Service 2016).

Nevertheless, there are still specific tasks related to defense domain that mainly stick with military operations and this is true also in the case of SBEO applications. In EU dimension, the taxonomy developed in the framework of the European Defence Agency, the "Generic Military Task List" (GMTL) clearly define some tasks that are not applicable to security dimensions. The GMTL, for example, refers to the conduct and synchronization of joint precision strike aimed to conduct efficient application of joint precision firepower. For such kind of tasks, SBEO data and products can play a key role. High-accurate weapons, in fact, are based on such kind of information that, if properly elaborated and ingested in the weapon system, produce a high added value. With the increase of revisit time and with the decreasing of processing time, also battle damage assessment (BDA), a typical military task could be supported by SBEO capabilities on top of more tactical vehicles, and a potential link between automatic change detection algorithms and tactical operational commanders could produce effective information (https://www.eda.europa.eu/what-we-do/activities/activities-search/persistent-surveillance-long-term-analysis-(sultan) 2019).

Furthermore, military planning is underpinned by a continuous process of information collection, military assessment, and analysis. The strategic planning, in particular, relies on information to be collected in conditions where forces are not yet deployed and the "expeditionary" characteristic of satellite systems, able to reach faraway points on the planet in a few hours and in the next future will be able to provide near-real time information with global coverage, are fundamental. On the other hand, geospatial support is a key enabler also for the planning and execution of military and civilian missions and operations, training, and exercises, and it is based on imageries also coming from space domain, supporting, in this case, tactical functions. Nowadays, geospatial support is essential in everyday life and hence it is even more necessary in security and defense operations (EU Capability Development Plan 2018). SBEO data are the pillars and the first layer to build on further information and to derive multiple products for multidomain assessments and to provide effective tools for decision making and military or mission commanders.

In addition to these specific military missions, in the domain of SBEO, there are three fundamental general requirements driving and steering the development of military space systems: availability, confidentiality, and integrity.

Starting from the integrity requirement and keeping in mind the disinformation threats are world-scale threats; it can be stated that only with an independent, well-defined, and verified information source, it is possible to implement armament control, confidence-building, and treaty monitoring, in particular in a framework of a common defense and security policy. To achieve this goal, MoDs shall have a reliable information source to reach a common situational awareness; otherwise, it will be difficult to set up a room to agree on a common foreign policy and to deal with common threats as well as to verify information accuracy. The point is, how such kind of requirement can influence the developments of future space-based reconnaissance systems.

In addition, SBEO applications present governance, data security, service continuity, and business model criticalities. For instance, the use of open-source applications not only involves criticality about the services themselves, but also allows to the service provider to gather and store key information about uses and users. The confidentiality is a general key issue for the future of information technology and this is particularly true for defense users, as revealed by recent application cases such as the application able to collect military positions around the globe through the use of connected fitness trackers (Fitness tracking app Strava gives away location of secret US army bases 2019). The same problem can be applied to commercial SBEO providers, where even only the information about the area and time of interest could represent an intelligence information, pointing out the importance of the confidentiality requirement. These issues have a direct impact in terms of SBEO needs for military missions. It raises the problem not only of the production and the availability of the information, but also the question of the control and the security of the data provided for the MoDs use. When imagery is obtained through commercial companies directly contracted by local MoD, the integrity of the information could not be guaranteed. Technically speaking, imagery data can be manipulated, even if such kind of theoretical operations could require some delay in providing the requested service. By building up its own fleet of satellites or strong restricted commercial licenses, including ground segments and processing, these potential concerns are not in place anymore.

Finally, also based on recent military operations' experience, where a coalition of States is involved, the same data might be needed by all of them at the same time, implying the requirements of the availability of the data. For this kind of issue, data exchange agreements must be addressed accordingly, leading in some cases to considerable additional costs and delays, while a broader and structured pooling and sharing approach would probably lead to more effective benefits for the coalition.

Security and Defense EO Application

Earth Observation from space in the defense sector was largely used historically for intelligence purposes, being considered as an extension of the capacity of spy aircrafts. In particular, the branch of intelligence dealing with imagery is known as IMINT.

IMINT is the technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials. It includes exploitation of imagery data derived from several categories of sensors: electro-optical, radar, infrared (IR), multispectral, or laser (US Joint Publication 2013).

The use of SBEO systems was initially devoted to specific strategic tasks (e.g., nuclear sites discovery). The current improvement of sensors' performance, the agility of the satellite platforms, and the possibility to integrate different datasets are important enablers allowing the use of SBEO also for more specific and repetitive tasks, even in direct support to missions and operations.

In this regard, system design parameters may however impose constraints on the ability to use SBEO satellites in military operations. The architecture of the mission and the choice of the orbit is one example of these constraints.

Traditionally, SBEO missions have been conceived with the use of low Earth sun-synchronous orbits. In this case, the complexity of system design was manageable thanks to the advantages of orbit stability, global coverage, constant sunlight on the platform, and of advantageous geometries for imagery collection. This type of orbit however limits the capacity of continuous observation (e.g., areas at equatorial latitudes are visited only twice a day), and moreover the satellite passes on target locations always at the same local time, reducing the possibility of discretional imaging. Constellations including several satellites, although improving the performance of continuous observation, would hardly be considered as sole source of information in the case of military operations.

Indeed, IMINT can be collected via satellites, but also with other assets: unmanned aerial vehicles, reconnaissance aircraft, and ground systems. These assets are not interchangeable and should be used in combination. A recent study conducted by the European Defence Agency evaluated the potential options to enhance collection capabilities in the area of IMINT through innovative and technologically feasible solutions, to meet the need of persistent surveillance of wide areas in defense and security operations (https://www.eda.europa.eu/what-we-do/activities/activities-search/persistent-surveillance-long-term-analysis-(sultan) 2019). To this extent, the analysis based on operational scenarios provided the respective merits of assets/systems based on geostationary earth observation satellite systems, constellations of optical and radar small/mini satellites in low earth orbit, High Altitude Pseudo-Satellite Systems (HAPS), and Remotely Piloted Aircraft Systems (RPAS). The quantitative analysis performed, while showing that the performance in resolution of geostationary EO satellites seems yet to meet the requirements of military operations, demonstrated a real complementarity between the LEO constellations and other technologies which are likely to be used concurrently or successively in order to achieve the objectives pertaining to a given phase of operations.

The intelligence communities are used to develop their activities on the basis of the so-called intelligence cycle. The IMINT cycle mirrors the intelligence cycle. The steps in this cycle define a sequential, interdependent process for developing IMINT. The management of operations of SBEO systems used to produce IMINT is typically harmonized with the steps of the IMINT cycle: tasking, collection, processing, exploitation, and dissemination processes (MCRP 2-10B.5 Imagery Intelligence – US Marine Corps).

Concerning the exploitation of imagery information, imagery analysts have a central role in this domain, especially taking into account the traditional approach mostly built on visual interpretation of satellite imagery.

In the above described framework of big data environment, the traditional analysts' task of building situation awareness and producing actionable intelligence is changing and needs to be supported by modern tools to obtain the promising enormous added value coming from such numerous amounts of data. In several cases, current tools are not able to adequately support analysis, producing delays in the processing and in the interpretation or not allowing to take advantage of the real potential of big data.

In the defense domain, the use of modern technologies might be hampered by the need to comply with security rules, to work on "closed" classified systems to protect the data and the information, not relying on the support of distributed resources normally available in large private networks or on the Internet.

In the last years indeed, we witnessed a large development of tools and techniques reaching a good level of maturity in providing useful information by exploiting collected imagery data. However, the military operational communities have not benefitted in full of this technology growth. For instance, although new techniques recently presented in the domain of big data analytics can provide added value for the security domain (Popescu et al.), a direct implementation in the defense applications needs to be properly addressed duly taking into account the still existing difficulties to put together the architectural elements of a cloud-based processing and the security constraints of classified systems. This does not mean however that defense imagery analysts are condemned to work with archaic tools.

As described previously, an important area of development is represented for instance by the future development of application of deep learning and artificial neural networks for imagery analysis. These capabilities will help to identify and refine the behavioral models by parsing and correlating the voluminous data streams available from space assets. Anomaly detection tools based on this concept are already available in Europe for the maritime domain with dual-use applications, valid both in defense (maritime situational awareness) and in security scenarios. Combining satellite radar imagery with Automatic Identification System (AIS) (IAC-14-B1.5.4 Cosmo-Skymed data utilization and applications), Vessel Monitoring System (VMS), coastal radars, and any available intelligence data provide useful information to build a database of normal behaviors concerning the vessel tracks in specific area. Any deviation from recognized track patterns might be considered as an anomaly to be further investigated.

This is one practical example of the use of Synthetic Aperture Radar (SAR) satellite imagery. This technology has become a consolidated asset of military SBEO in Europe, thanks to important satellite programs (ref. COSMO-SkyMed, SAR-Lupe, COSMO-SkyMed Second Generation, SARah). The evolution from the first generation of the years 2000–2010 to the one under development in these years is making available considerably larger amounts of data, thanks to the improved resolutions, larger swaths, and more imagery per orbit.

In this case, the challenges deriving from the increased amount of data are complicated by the inherent complexity of SAR data and by the preponderance of historically well-established procedures that make use of electro-optical images to support military operations and the decision-making process, relegating in several cases SAR imagery to a secondary source of information.

On the contrary, a thorough exploitation of SAR imagery strengths would enlarge the use of SAR imagery alone and/or in combined use with electro-optical images, thus taking full advantage of its unique 24/7 and all-weather characteristics, therefore raising the effectiveness of investments made by several European Ministries of Defence on SAR satellites.

Ongoing studies are investigating new techniques aimed at developing solid procedures in support of SAR imagery analysts, overcoming the inherent difficulties of interpretation of "salt and pepper" images and with the objective to reach high automation levels (https://www.eda.europa.eu/docs/default-source/eda-factsheets/2017-04-03-factsheet_react 2019).

The tasks can be performed by skilled analysts or by operators that might use tools developed for that purpose. In this regard, software exploitation tools for SAR images are available; however, the drawback is that those are not always able to extract and present the information that makes SAR images a product "easy and ready to use." In addition to this, the intrinsic peculiarities linked to the programming cycle of an SAR product and the lack of proper tools to assist the preparation of a task constitute an additional hurdle that limits the use of SAR images at operational level.

The procedures to analyses data are based on operational workflows. Those are defined as a series of activities that typically encompass several tasks: e.g., data preparation, data processing, visual interpretation. Operational workflows can be tailored on the basis of operational scenarios (ports, airfields, urban, lines of communications, industrial compound, etc.).

Data preparation are normally executed, thanks to the most common software functionalities already available in the market, e.g., co-registration, phase coherence extraction, geocoding, ortho-rectification.

Data processing would benefit from algorithms and tools available in the market or developed on purpose, according to the need of users, e.g., layover analysis, change detection (amplitude, coherent, or incoherent), edge detection and feature extraction.

The definition of workflows has a twofold advantage. First of all, the workflows become a guided process for imagery analysts through the complex applied physics of the SAR imagery interpretation. Secondly, in the near future, with application of deep learning techniques, it would be possible to train semiautomated systems to execute the workflows, requesting the intervention of the imagery analysts only in case of abnormal behaviors.

Military applications already investigated falls in the domain of damage assessment (Fig. 1), target analysis, monitoring, and military planning.

Significant elements characterizing defense-related SBEO applications have been described, also providing information on more recent developments in this domain.

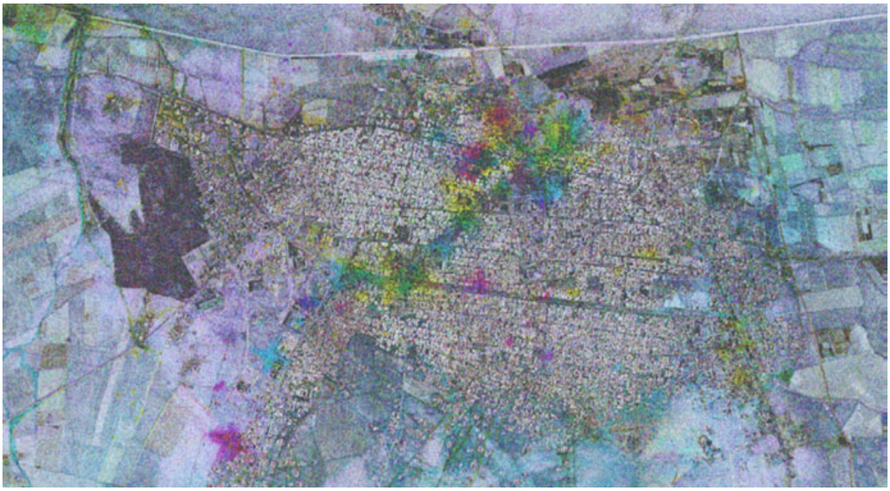


Fig. 1 Multicoherence product from the execution of a workflow for damage assessment COSMO-SkyMed image © ASI 2017

The use of adequate satellite constellations with suitable architectural characteristics and possibly in combination with other collection sources is an important enabler. Furthermore, in order to be effective in current operational scenarios, military SBEO applications need to find the proper balance to use modern exploitation and analysis capacities and flexible dissemination chains with the constraints of secure environments typically set up to protect classified information.

Examples of EO Operational Tasks and Services for Security and Defense

Examples of EO Operational Tasks

The public domain has the perception of how SBEO works based on what they have seen in the movies rather than in the actual orbital dynamics that govern the movement of the satellites. The inescapable truth is that, once a satellite has been inserted into its orbit, there is not much we can do to control the moment at which it overflies our target of interest other than wait. This introduces a number of caveats that need to be carefully considered when using such systems for security and defense applications. Hence, the expression commonly used by image analysts who say that “when you need an image of a certain location the satellite is usually on the other side of the Earth; and when it finally reaches the desired coordinates, they are always cloud covered.”

Fortunately, while this was usually the case two decades ago, the proliferation of satellite platforms that we have seen in recent years has somehow alleviated this limitation, increasing dramatically the number of passes/day over any given location. However, despite the efforts of some companies that claim to be able to provide imagery every 3 h, we cannot ignore the fact that a satellite does not and will not (for the time being) provide the same live feed as other systems such as RPAS or potentially HAPS, already mentioned above. Thus, although these are increasingly frequent, the views that they provide are still limited to particular instants in time. Thus, the image analysts have developed a series of skills over time that allow make assessments based on hypotheses developed using these views. It would be equivalent to try to understand a movie while only being able to see certain frames.

Image analysts call certain features that they use to elaborate these hypotheses “indicators.” For instance, the sudden appearance of inflatable rubber boats at a makeshift illegal migrant camp located on a specific coastline is an indicator that, even if there are no departures visible on the image yet, there is a very high probability that launches will soon be taking place. Of course, the presence of indicators is very strongly associated to the identification of “patterns of life” or “patterns of behavior.” And these, in turn, are associated with the continuous observation of a location of interest, or what is called “monitoring.” Monitoring allows the analyst to establish a baseline, a visual understanding of the type and level of activity that is common at a certain location. When the analyst sees an event that departs from this usual activity, something that may be called an “anomaly,” an alert can immediately be triggered and the level of surveillance be increased to identify the causes and possible consequences of such change. Of course, the reliability of the assessment is directly correlated with the duration of the monitoring period, meaning that longer baselines provide better results.

Some examples of this application are the monitoring of military installations, such as ports and airfields, that serve as a baseline for the detection of the deployment of certain types of weapons systems, troops, aircrafts, and vessels that may have strategic implications for the region: arrival/departure of aircrafts and vessels, deployment of SAM or SSM systems, improvement of facilities, development of new infrastructures, identification of the level readiness of the different units occupying the military installations, assessment of their operational status, estimation of their capability, etc.

Another example very commonly related to SBEO monitoring for defense is the field of treaty verification. This was in fact the origin of Open Skies, an initiative signed between the USA and the former USSR at the peak of the Cold War to guarantee support to the mutual assured destruction (MAD) doctrine by providing means to each of the parts to ascertain what the other was doing. Today, satellite imagery is used to monitor the development of nuclear weapons by measuring the level of activity taking place at well-known uranium mines, or monitoring the status of certain processing and enrichment plants or gauging the performance of certain nuclear reactors where plutonium is known to be produced, or assessing the results of nuclear detonations carried out at carefully concealed underground test sites. Monitoring is also the basis for the assessment of a country’s strategic outreach in terms of its capacity to project power, either through the deployment of forces or the use of weapons of mass destruction (WMD) and their means of delivery. Other additional requested information, for example, are the capacity and status of their naval units: how many cruiser vessels do they have available; if they are building aircraft carriers: how many, when they will be operational; if they have ballistic missiles: how far they can go, from where are they launched; if it is likely to be another launch test soon: how accurate they are; where are their strategic bombers deployed; and so on.

Monitoring tasks generally account for a significant portion of SBEO applications for security and defense. There are other uses, however, for which intelligence derived from satellite imagery is also critical. One of this use is obviously military planning, an activity which occurs generally before actual events take place. The term coined for this in military parlance is “intelligence preparation of the battlefield (IPB).” There are numerous instances where products derived from images may support the IPB process: terrain reconnaissance, multicriteria cross-country mobility analysis (CCM), identification of Go/No Go areas, visibility analysis, analysis of critical infrastructures, route analysis, contingency planning, training, etc.

Other uses involve the assessment of a situation on the ground after a certain event has taken place, like an airstrike (BDA). Another very frequent post-event application of SBEO is the validation of intelligence obtained through other sources. In this regard, there is an increase of demands that deal with the investigation of illegal activities, including cross-border crime (CBC). A significant amount of these have to do with the trafficking of drugs or weapons, which pose an important security threat to

EU Member States. Most of them are related to the existence of vessels, aircraft, trucks, and other means of transportation and the need to confirm their presence at certain locations such as ports, airfields, or border crossing points (Figs. 2, 3, and 4).

The list of examples is obviously nonexhaustive and it leaves out some other plausible uses of SBEO for security and defense. However, we cannot close this section without mentioning one important security application which is the management of the crisis following natural disasters such as earthquakes, wildfires, or floods. In these cases, it is critical to have immediately after the event updated maps and spatial datasets of the theaters of operation which will most likely have changed significantly due to the unfolding of the disaster itself. These datasets will provide the rescue teams with the necessary information to establish priorities and make informed decisions on the ground as soon as possible even before arriving at the disaster area.

Security and defense operations and information managers will face a wide range of situations involving different requirements and end users. Industry and technological innovation are developing at such a pace that the offer of SBEO services available is increasing exponentially. Now, more than ever, the GEOINT professional needs to amplify his/her domain of knowledge in order to incorporate an understating of the different options available in order to choose that which better satisfies the needs of his/her customers. In most cases, the solution will consist of a mix of different tools, platforms, and sensors that, properly combined, will cover all the aspects of any given situation and provide the most efficient answer.

Copernicus SEA

Cooperation between the EU Satellite Centre and the European Commission (EC) is a key enabler for SatCen EO applications development. Such cooperation started more than 10 years ago with a strong involvement of SatCen in the EC research

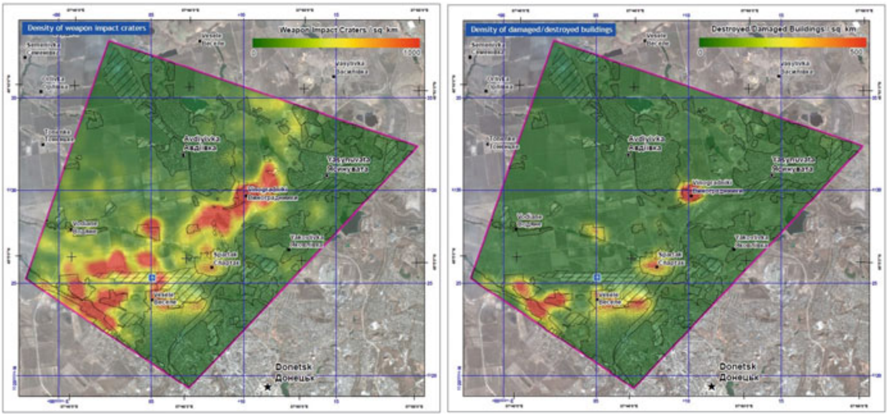

Density of weapon impact craters
Weapon Impact Craters / sq. km
0
1000
Density of damaged/destroyed buildings
Destroyed Damaged Buildings / sq. km
0
500
Avdiivka
Авдіївка
Yasynuvata
Ясинувата
Spartak
Спартак
Veselе
Веселе
Donetsk
Донецьк

Fig. 2 Density maps comparing the weapon impacts visible on the image with the damage to buildings and infrastructures

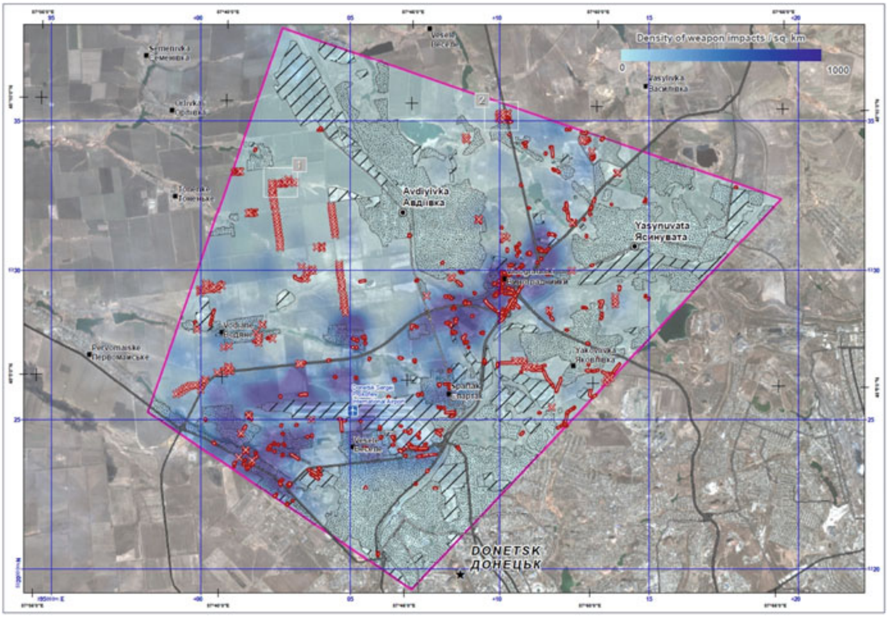


Fig. 3 Density map representing weapon impacts overlaid with the different military positions and equipment observed on the image

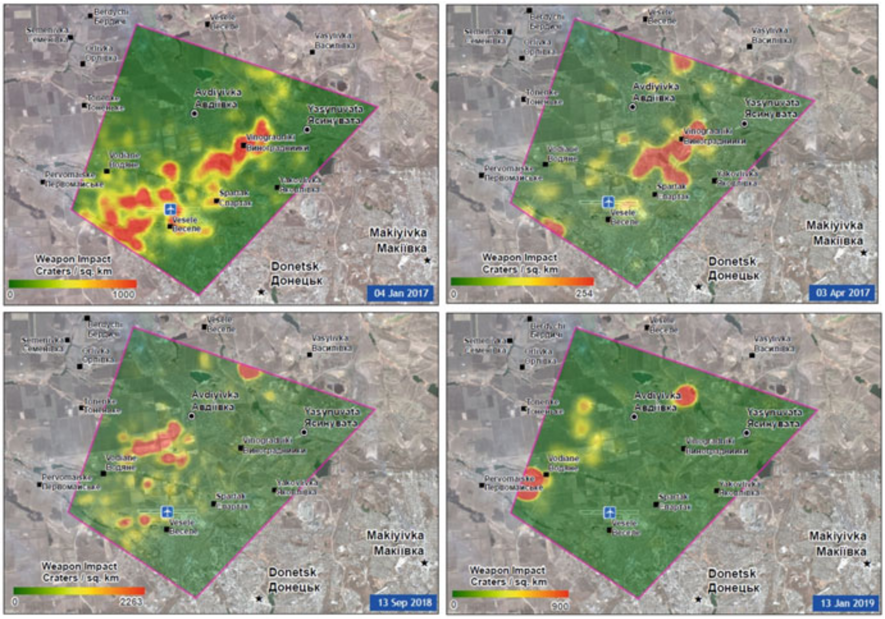


Fig. 4 A temporal series representing the evolution of the weapon impacts over the duration of the conflict

projects mainly in the areas of space and security and, in particular, through the FP6, FP7, and finally the H2020 Framework Programme.

The main element of this cooperation has been, and remains, Copernicus and several projects such as LIMES, GMOSAIC, G-NEXT, and BRIDGES that prepared the future operational role of SatCen in Copernicus, setting up the preoperational framework for the services that started in 2017.

Thus, Copernicus Support to EU External Action (SEA) is the result of many years of research and development by SatCen in partnership with the Industry under the European Union's Framework Programme for Research and Technological Development materialized by the transition of SEA from research and development and preoperational service provision to a fully operational mode.

Copernicus SEA is embedded in the Copernicus programme security component, therefore part of "*the world's largest single programme for observing and monitoring the Earth, for the ultimate benefit of all European citizens*" (Copernicus Support to Eu External Action Website) (Fig. 5).

Copernicus is composed of three components:

- *The space component*. This includes two types of satellite missions: Copernicus dedicated Sentinels and commercial or other space agencies' missions, called Contributing Missions (including very high-resolution satellite missions critical for security applications)
- In situ measurements (mainly ground-based providing information on oceans, continental surface, and atmosphere)
- Six services offered to authorized users and public

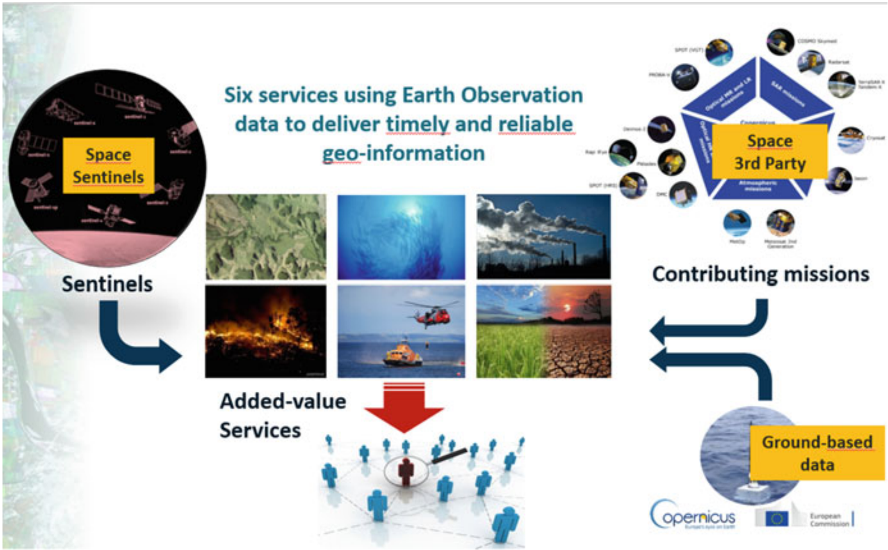


Fig. 5 Copernicus Programme structure – Source Commission DG-GROW (Presentation at SEA User Workshop – Paris)

The six services are land, marine, atmosphere, emergency, climate change, and security. Each service is delegated to different "entrusted entities."

Regarding the Governance, the EC has the overall responsibility of the program, and it is assisted by the Copernicus Committee including Member States, a Security Board (specific configuration of Committee), and a User Forum, as a working group to advise the Copernicus Committee on user requirements aspects (Regulation (EU) No 377/2014 of the European Parliament 2010).

The Security Board is involved in the management of information security for Copernicus and addresses issues such as the cyber security of the space and service infrastructures (Fig. 6).

Copernicus Security Services

The security service is to provide information in support of the civil security challenges of Europe improving crisis prevention, preparedness, and response capacities, in particular for border and maritime surveillance, but also support for the Union's external action, without prejudice to cooperation arrangements which may be concluded between the Commission and various Common Foreign and Security Policy bodies, in particular the European Union Satellite Centre (Regulation (EU) No 377/2014 of the European Parliament 2010).

In three key areas, i.e., Support to EU External Action, Border Surveillance and Maritime Surveillance, the security service is being implemented by the following entrusted entities: SatCen, FRONTEX, and EMSA. The operations started in 2016 for the Border Surveillance and Maritime Surveillance components of the security service and in May 2017 for the Support to External Action component.

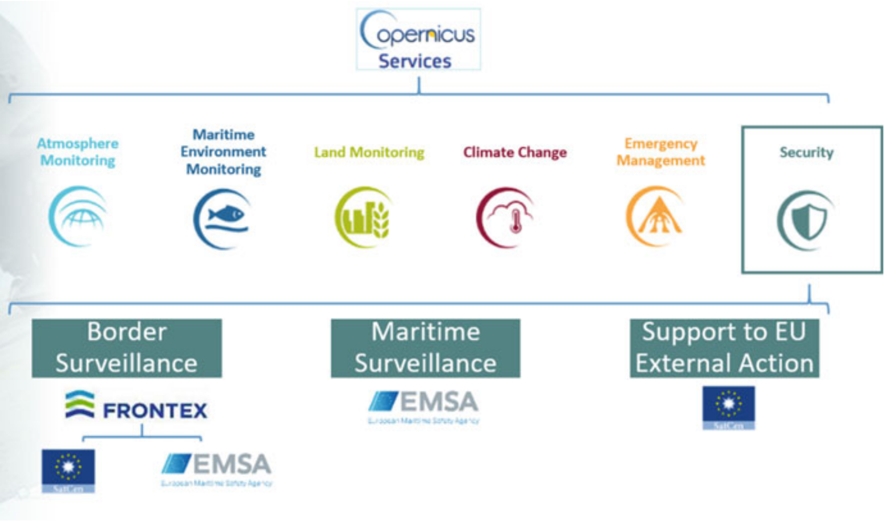


Fig. 6 Copernicus services (and components in security). (Source Commission DG-GROW)o

SatCen's main contribution is materialized by the role of entrusted entity for the operations of the Copernicus service in Support to EU External Action (SEA); SatCen also supports Border Surveillance through a Service Level Agreement with FRONTEX.

SatCen is thereby entrusted with the operational management of the Copernicus SEA service. Today, SEA addresses service production mainly through issuing and management of industrial service contracts such as a Framework Contract for "Geospatial production" but also the production of sensitive layers of information by image analysts and quality checks at SatCen. In addition, SEA implements user uptake activities mainly for the enlargement of the user base as well as service evolution activities taking benefit of state of the art in research and technological developments. For user uptake activities at least two workshops are organized per year. SatCen also implements a focal point for service's "Authorised Users" in the "SatCen Brussels Office." Security consideration regarding the requests is fully taken into account as each request is evaluated by the SatCen Tasking Authority (EEAS) from the sensitivity point of view. As Copernicus SEA does not currently manage EU Classified Information (EUCI) (2013/488/EU 2013), if a request is considered too sensitive and needs to be classified, it could be managed, if relevant, outside the perimeter of Copernicus as a SatCen classified task.

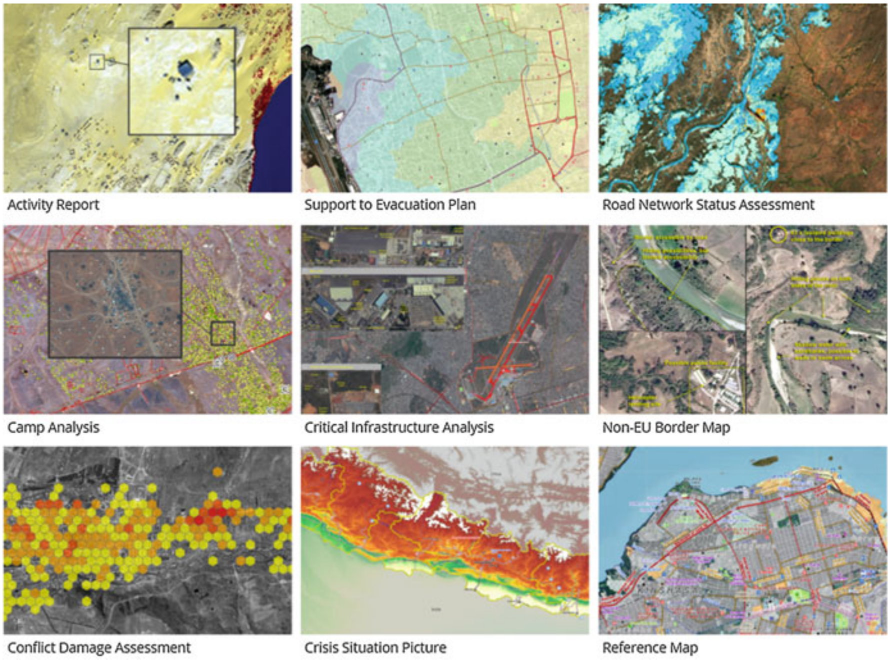
SEA's objective is to assist the EU and its Member States in civilian missions, military operations, and interests outside EU territory. It is designed to support the EU by improving the situational awareness of European Commission, European External Action Service, and Common Security and Defence Policy stakeholders including the Member States. The service can be activated to respond within very short timescales, as is necessary in cases of responses to crises such as political or armed conflicts. On the other hand, it is possible for the service to carry out monitoring campaigns over longer periods of time in order to develop a picture of how phenomena on the ground are changing. The primary target users are European entities, the EU, and Member State Ministries of Defence and Foreign Affairs as well as key international stakeholders, as appropriate under EU international cooperation agreements such as United Nations.

SEA Service Portfolio

After a ramping up of the service, SEA reached its full operational state in 2018 with, as mid-2019, more than 140 activations received from authorized users from EU Institutions, in particular EEAS and Member States. SEA products were built using mainly Copernicus Contributing missions as well as Sentinels satellites data as complementary sources (Fig. 7).

Mid-2019, the SEA service is mainly activated by the EU External Action Service: from the nine services of the portfolio, seven have been used so far (Fig. 8).

Analysis of EO data based on different techniques is used to identify patterns of illegal activity in an area of interest. Optical very high resolution (VHR) imageries are used to identify vehicles and infrastructure potentially suspicious. Radar Sentinel imagery interferometry techniques are used to identify the use of paths and roads during a time lapse.



Activity Report

Support to Evacuation Plan

Road Network Status Assessment

Camp Analysis

Critical Infrastructure Analysis

Non-EU Border Map

Conflict Damage Assessment

Crisis Situation Picture

Reference Map

Fig. 7 SEA service portfolio. (Source SatCen (European Defence Action Plan – COM 2016))

Evolution of EO Services and Application at EU SatCen and Copernicus SEA

SatCen Service Evolution: Artificial Intelligence/Machine Learning

The concept of artificial neural networks and the theory of how these could be applied to a number of different applications, particularly in the field of EO and remote sensing, have been deeply described in the previous paragraphs. The development of the computing power necessary to drive this major breakthrough has reached critical mass, thanks to the continuous increase of chip capacity. Moreover, big data must be carefully stored over years of increasing generation and ingestion of information. But big data in itself is not useful. It only acquires a meaning if we are able to exploit it in such a way that it allows us to identify patterns, understand behaviors, bring to the surface the hidden structure of a certain phenomenon, and even predict what is going to happen next. It is particularly important in the field of Artificial Intelligence and Machine Learning (AI/ML) because for the first time SBEO service providers such as EU SatCen have accumulated enough data to train the algorithms to such an extent that they will provide meaningful, reliable, and actionable results. And once they are trained, the expectations are that these

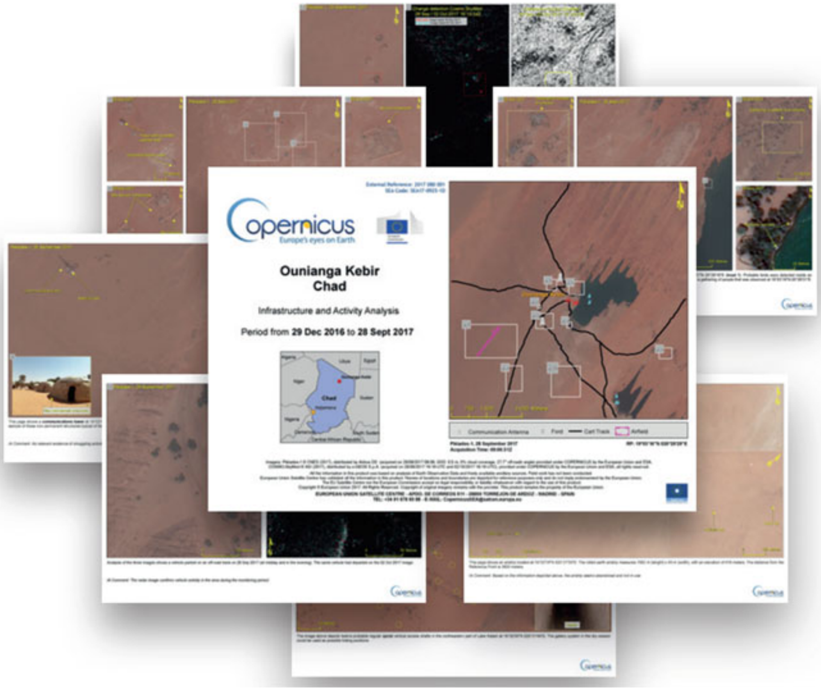

Copernicus
Europe's eyes on Earth
Ounianga Kebir
Chad
Infrastructure and Activity Analysis
Period from 29 Dec 2016 to 28 Sept 2017
Chad

Fig. 8 Example of an SEA activity analysis product for detecting smuggling and other illegal activity. (Source SatCen – SEA product portfolio (Copernicus website www.copernicus.eu))

algorithms will be able to breeze through the data and draw conclusions that would otherwise take an unfeasible amount of time for a human to reach.

There are numerous situations in the field of SBEO where AI/ML is already being used. Experience has shown that the algorithms are particularly efficient at performing repetitive tasks that may seem pretty straightforward in terms of complexity but often excruciatingly tedious for an analyst, such as scanning an image in search of changes or looking for certain objects like armored vehicles, aircraft, air defense sites, or other sorts of military equipment. At the EU SatCen, for example, it is not considered a future scenario in which the machine will eventually end up substituting the human analyst. There is a strong belief that certain traits which are common in successful image analysts, such as the capacity to unveil causal associations between elements on the image, or the ability to understand spatial relationships, or the facility to elaborate probable hypotheses to explain what is being observed, will very hardly, if ever, be outperformed by a machine. Thus, what is envisaged as a more likely scenario is one where the image analyst takes full advantage of the power of AI/ML to automate tasks such as automatic change detection and automatic feature detection and only intervene when the algorithms flag an alert, to alert that some relevant event has been found. This idea, which is sometimes known as a “tip and cue” approach, may fit surprisingly well with a hybrid SBEO collection plan which could include a mix of different sensors with complementary capabilities. As an example, to illustrate this, consider a situation where access is guaranteed to a constellation of microsatellites that provides fresh imagery at a medium spatial resolution but very high cadence, e.g., 3 m pixels every 2–3 h. The precision given by a 3 m pixel may not be enough to identify the type of equipment present on the ground, but if you know already what you are dealing with because of higher resolution imagery acquired at an earlier date, the medium resolution-high cadence imagery may be more than enough to highlight a change in the level of activity and trigger an alert. The analyst can then use the awareness of this event to tip off another constellation with higher precision sensors and program an acquisition with a better spatial resolution, and then may confirm the assessment. If the identification of the changes that triggers this mechanism can be done automatically by an AI/ML neural network, the analyst can significantly increase the area of surveillance and wait for these alerts to pop up, thus covering a larger surface and using his skills more wisely.

Copernicus SEA Service Evolution

Within the Copernicus Security Service component, the service evolution aims at promoting changes to the Service, aligned with the overall Copernicus strategy. The goal is to improve the existing portfolio of services by adding or modifying existing products or by implementing changes within the production or activation and delivery systems that improve the overall service experience to the users.

First, Copernicus SEA service is constantly adapting its response to the upcoming applicable policies, in particular those policies governing the EU External Action such as the EU Global Strategy for the European Union's Foreign and Security Policy and the Space Strategy for Europe, both issued in 2016. Any other relevant EU Policy will be considered as well.

Space Strategy for Europe (Space Strategy for Europe – European Commission COM 2016) states that *"Additional services will be considered to meet emerging needs in specific priority areas, including . . . (ii) Security and Defence to improve the EU's capacity to respond to evolving challenges related to border control and maritime surveillance with Copernicus and Galileo/EGNOS. This expansion will take account of new technological developments in the sector, the need to ensure adequate level of Security of the infrastructure and services, the availability of different data sources, and the long-term capacity of the private sector to deliver appropriate solutions."*

European Defence Action Plan (European Defence Action Plan – COM 2016): *"The Commission shall explore how Copernicus could cover further Security needs, including Defence. It shall strengthen Security requirements and will reinforce synergies with non-space observation capabilities in 2018."*

In the Space Strategy for Europe, additional services are considered in the area of security and defense. To some extent, the Copernicus SEA service could be considered as already implementing new services for defense and security, and therefore in line with the EDAP orientations (Member States defense users and CSDP military operations being part of the SEA users whenever they request to access the service within the context of the Common Foreign and Security Policy). The EDAP provides guidance on possible future evolution, in particular regarding the strengthening of security requirements and re-enforcing synergies with nonspace observation capabilities; this guidance shall be taken into account for the evolution of the Copernicus SEA service.

Nevertheless, SEA shall also be made available to new users having a bearing on the EU External Action. Copernicus SEA workshops, in particular the workshop organized in Paris at CNES (Centre National d'Études Spatiales) in December 2018, clearly highlighted that there are many potential new users in areas such as Ministry of Interior, Ministry of Foreign Affairs, maritime security actors, and agencies such as EFCA and EUROPOL that could get benefit from the service. Those users would need an easy access to the service, and this will have to be taken into account for its evolution. Regarding maritime security, it is worth mentioning the "European Union Maritime Security Strategy" (On 24 June 2014 the General Affairs Council of the European Union approved the "European Union Maritime Security Strategy" (EUMSS) 2018) endorsed by the EU Council. Its action plan revised in June 2018 specifically target *Support the conduct of CSDP missions and operations in the global maritime domain with EU maritime surveillance assets.* (*"In line with CISE* (Common Information Sharing Environment (A common information-sharing environment (CISE))), *ensure consistency and strengthen coordination between the existing and planned maritime surveillance initiatives on the basis of existing programs and initiatives by EDA, EFCA, EMSA, EUSC, FRONTEX, and other European agencies (*e.g. *ESA) as well as the Earth Observation programme (Copernicus), GALILEO/EGNOS (European Geostationary Navigation Overlay Service), and other relevant projects and initiatives. [MS/COM/EEAS/EDA]").*

Second, Copernicus SEA is strongly user driven and their requirements are fully taken into account both regarding the access to the service as well as the extension of the service portfolio.

Considering the rationale behind the Copernicus SEA, a set of predefined products has been defined and compiled in the Copernicus SEA portfolio, offering EU and international actors an initial pool of services that aim to tackle their needs in crisis situations or emerging crisis.

Service evolution is to bring new products to the users by extending SEA portfolio of services. Emerging requirements have been expressed, for example, in the areas of cultural heritage, illegal crop monitoring, security of EU/international events.

New products are achieved by finding new methods to exploit existing sensors by retrieving new types of information as well as exploiting new sensors and data. SEA service evolution demonstrated, for example, that the use of Copernicus Sentinels satellites was useful as complementary data based, for example, on the following capabilities: the revisit time of Sentinel-2, interferometry with Sentinel 1 to detect small changes in specific areas such as deserts, sea, etc.

Interagency cooperation is also a driver of innovation in this context, and it is worth mentioning the SatCen/EDA GeoHub project that is building a geo-spatial portal as well as the REACT project (briefly described previously (IAC-14-B1.5.4 Cosmo-Skymed data utilization and applications)) on the exploitation of SAR data. Both projects could be beneficial for SEA service evolution, as synergies are already well established.

Regarding the access to the service, SEA is currently benefiting from the infrastructure already in place at EU SatCen. The new developments planned for the infrastructure are aimed to provide the necessary hardware/software infrastructure to enable and optimize the management of the Copernicus SEA service, including activation workflow; seamless production and publishing; easier request and access to the products by the users. In the future, this infrastructure will need to be adapted to a considerable increase in data sources and volume, both for Earth observation and additional data, such as in situ, open source, etc. Additionally, the mentioned infrastructure must adapt to the need to "strengthen security requirements" and to "cover further security needs, including defense" (c.f. EDAP (European Defence Action Plan – COM 2016)) which might have an impact on the infrastructure in terms of the reinforcement of the capacity to process sensitive data.

Service evolution of this first phase of Copernicus SEA for the period 2014–2020 is currently extending the user community, the service portfolio, and is facilitating the access to the service.

SatCen is currently preparing with its partners the next phase of SEA within addressing "Copernicus 2.0" for the period 2021–2027, taking benefit of the results and lessons learned of service evolution during the first phase. A particular attention will be given to common requirements, interagency cooperation, interactive access through geo-portal, innovative tools such as artificial intelligence, and the availability of new space and nonspace sensors.

Conclusion

This chapter identified the current and future trend in the domain of Space-based Earth Observation (SBEO) from a security and defense perspective. Starting from a high-level state of the art, the current security and defense general needs have been described, pointing out how the future SBEO capabilities will be changed by the current new military scenario as well as the new space economy. In particular, the center of gravity will be more and more moved to the ground segment, always keeping in mind the specific military requirement of confidentiality, integrity, and availability of IMINT information.

Any SBEO capability shall be adapted for ad hoc security and defense environments, without necessarily implying different design but with enforcement of specific security standard protocols and restrictions, aiming to the interoperability and integration of different sources. The use of commercial and unsecured outflows can in any case represent a valid contribution that indeed needs to be properly balanced.

Considering the duality and increasing synergies between homeland security and external actions, the challenge will be in the implementation of a coordinated and holistic approach avoiding unnecessary duplication.

Some example of SBEO tasks and applications have been described, showing how the management of Artificial Intelligence and Machine Learning services will need to be properly customized to improve the inalienable analysts' skills, expensive, and precious resources that can be increased exponentially with tailored tools and related services.

Security domain, based on the experience of Copernicus Programme and EU SatCen services, nowadays is working with a cooperative model, delivering effective results in many applications.

This cooperative model has not yet reached the same level of maturity in the defense domain. However, significant efforts are conducted by national MoDs to cooperate on specific needs and activities. A further step forward might be a "pooling and sharing" model's application.

Furthermore, more support and contribution from EU institutions, eventually taking advantage of the security domain experience, tools, and facilities, might provide added value and cost benefit in the challenge of implementing a more structured and coordinated approach even in the defense domain.

The development of new common SBEO platforms/services could represent a first example (or the second one if we consider Galileo Public Regulated Service) of a European system to support defense needs of EU Member States.

References

2013/488/EU: Council Decision of 23 September 2013 on the Security rules for protecting EU classified information – Article 2: 'EU classified information' (EUCI) means any information or material designated by a EU Security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States'

A common information-sharing environment (CISE) is currently being developed jointly by the European Commission and EU/EEA members with the support of relevant agencies such as the EFCA. It will integrate existing surveillance systems and networks and give all those authorities concerned access to the information they need for their missions at sea. (Source: https://www.efca.europa.eu/en/content/common-information-sharing-environment-cise)

Adams J, Gillespie A (2006) Extracting information from spectral images. In: Remote sensing of landscapes with spectral images: a physical modeling approach. Cambridge University Press, Cambridge, pp 1–38

Arel I, Rose DC, Karnowski TP (2010) Deep machine learning – a new frontier in artificial intelligence research. Comput Intell Mag IEEE 5:13–18

Atkinson PM, Tatnall ARL (1997) Introduction neural networks in remote sensing. Int J Remote Sens 18(4):699–709

Ball JE, Anderson DT, Chan CS (2017) Comprehensive survey of deep learning in remote sensing: theories, tools, and challenges for the community. J Appl Remote Sens 11(4):042609-1–042609-54

Belward AS, Skøien JO (2015) Who launched what, when and why; trends in global land-cover observation capacity from civilian earth observation satellites. ISPRS J Photogramm Remote Sens 103:115–128

Bovolo F, Bruzzone L (2015) The time variable in data fusion: a change detection perspective. IEEE Geosci Remote Sens Mag 3(3):8–26

Britz M, Eriksson A (2005) The European security and defence policy: a fourth system of European foreign policy? Polit europeenne 3(17):35

Câmara G, Ferreira Gomes de Assis LF, Queiroz G, Reis Ferreira K, Llapa E, Vinhas L, Maus V, Sanchez A, Cartaxo Modesto de Souza R (2016) Big Earth Observation data analytics: matching requirements to system architectures. BigSpatial16, Oct 31–Nov 03 2016, Burlingname. https://doi.org/10.1145/3006386.3006393

Campbell JB, Wynne RH (2011) Introduction to remote sensing. Guilford Press; 5th edition (June 21, 2011). ISBN-10: 160918176X ISBN-13: 978-1609181765. p 667

Committee on Earth Observation Satellites www.ceos.org

Copernicus Support to Eu External Action Website. https://sea.security.copernicus.eu/

Copernicus website. www.copernicus.eu

Denis G, de Boissezon H, Hosford S, Pasco X, Montfort B, Ranera F (2016) The evolution of Earth Observation satellites in Europe and its impact on the performance of emergency response services. Acta Astronaut 127:619–633

Denis G, Claverie A, Pasco X, Darnis J-P, de Maupeou B, Lafaye M, Morel E (2017) Towards disruptions in Earth observation? New Earth Observation systems and markets evolution: possible scenarios and impacts. Acta Astronaut 137:415–433

EU Capability Development Plan 2018

European Defence Action Plan – COM (2016) 950 final – Nov 2016

European External Acton Service – A Global Strategy for the European Union's Foreign and Security Policy, Jun 2016

Fitness tracking app Strava gives away location of secret US army bases. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases. Last access Apr 2019

French white paper on Defence and National Security – 2013

Fukuyama F (1989) The end of history? Natl Interest (16):3–18, Summer

Fulcher BD, Little MA, Jones NS (2013) Highly comparative time-series analysis: the empirical structure of time series and their methods. J R Soc Interface 10:20130048

Ghassemian H (2016) A review of remote sensing image fusion methods. Inf Fusion 32:75–89

Hepner GF, Logan T, Pitter N, Bryant N (1990) Artificial neural network classification using a minimal training set: comparison to conventional supervised classification. Photogramm Eng Remote Sens 56(4):469–473

Holmes C, Tucker C, Tuttle B (2018) GEOINT at platform scale. In: The state and future of GEOINT 2018. Published by The United States Geospatial Intelligence Foundation USGIF, Herndon, pp 1–38

https://www.eda.europa.eu/docs/default-source/eda-factsheets/2017-04-03-factsheet_react. Last visit Mar 2019

https://www.eda.europa.eu/what-we-do/activities/activities-search/persistent-surveillance-long-term-analysis-(sultan) Last visit Mar 2019

Hussain M, Chen D, Cheng A, Wei H, Stanley D (2013) Change detection from remotely sensed images: from pixel-based to object-based approaches. ISPRS J Photogramm Remote Sens 80:91–106

IAC-14-B1.5.4 Cosmo-Skymed data utilization and applications

Lee J-G, Kang M (2015) Geospatial Big Data: challenges and opportunities. Big Data Res 2 (2):74–81

Li J, He Z, Plaza J, Li S, Chen J, Wu H, Wang Y, Liu Y (2017) Social media: new perspectives to improve remote sensing for emergency response. Proc IEEE 105(10):1900–1912

Lillesand T, Kiefer RW, Chipman J (2014) Remote sensing and image interpretation. Wiley, Hoboken, p 704

Long Y, Gong Y, Xiao Z, Liu Q (2017) Accurate object localization in remote sensing images based on convolutional neural networks. IEEE Trans Geosci Remote Sens 55(5):2486–2498

Maggiori E, Tarabalka Y, Charpiat G, Alliez P (2017) Convolutional Neural Networks for Large-Scale Remote-Sensing Image Classification IEEE Transactions on Geoscience and Remote Sensing 55(2):645–657

MCRP 2-10B.5 Imagery Intelligence – US Marine Corps

Nativi S, Mazzetti P, Santoro M, Papeschi F, Ochiai O (2015) Big Data challenges in building the Global Earth Observation System of systems. Environ Model Softw 68:1–26

On 24 June 2014 the General Affairs Council of the European Union approved the "European Union Maritime Security Strategy" (EUMSS), Following the mandate by EU heads of state or government. The EUMSS action plan was recently revised (26 June 2018). This document provides guidelines regarding COM, EEAS and agencies (including SatCen) cooperation in the EUMSS framework. https://ec.europa.eu/maritimeaffairs/policy/maritime-security_en

Popescu et al. Cloud computing case studies and applications for the space and security domain. European Union Satellite Centre

Regulation (EU) No 377/2014 of the European Parliament and of the Council of 3 April 2014 establishing the Copernicus Programme and repealing Regulation (EU) No 911/2010

Space Strategy for Europe – European Commission COM (2016) 705 final – October 2016

Toth C, Jóźków G (2016) Remote sensing platforms and sensors: a survey. ISPRS J Photogramm Remote Sens 115:22–36

Tzu S (2007) The art of war. Filiquarian, First Thus edition. ISBN-10: 1599869772

United Nations Treaties and Principles on Outer Space (2002) United Nations, New York. United Nations publication, Sales no. E.02.I.20. ISBN 92-1-100900-6

US Joint Publication – Joint Intelligence – 22 October 2013