

This is an electronic reprint of the original article. This reprint may differ from the original in pagination and typographic detail.

Please cite the original version: Sarlio-Siintola, S. & Tammilehto, T. (2019) Societally Acceptable and Ethically Sustainable Way of Performing Maritime Surveillance. RAdars for loNG distance maritime surveillancE and Search and Rescue operations.

URL: <https://cordis.europa.eu/project/id/700478/results>



H2020-700478

RAAdars for loNG distance maritime surveillancE and Search and Rescue opeRations

**SOCIETALLY ACCEPTABLE AND ETHICALLY SUSTAINABLE WAY OF PERFORMING
MARITIME SURVEILLANCE**

Deliverable Identifier: D3.2
Delivery Date: December 31th, 2019
Classification: Dissemination Level *PUBLIC*
Editor(s): Sari Sarlio-Siintola (LAUREA), Tuomas Tammilehto (LAUREA)
Document version: 1.0

Contract Start Date: May 1st, 2016
Duration: 44 months
Project coordinator: EXUS Software Ltd. (UK)
EXUS (UK), DXT (FR), ICCS (GR), TUD (DE), LAU (FI), FNM (IT), TEL (GR), NATO (BE), HMOD (GR), DMA (FR)

This work was performed within the RANGER Project, with the support of the European Commission and the Horizon 2020 Programme, under Grant Agreement No.700478



Document Control Page

Title	Societally Acceptable and Ethically Sustainable Way of Performing Maritime Surveillance	
Editors	Sari Sarlio-Siintola	LAUREA
	Tuomas Tammilehto	LAUREA
Contributors	Saara Siintola	LAUREA
	Jyri Rajamäki	LAUREA
	Markko Kallonen (to the initial version D3.1)	LAUREA
	Jaakko Tyni (to the initial version D3.1)	LAUREA
	Dimitris Katsaros (to the initial version D3.1)	EXUS
	Vincent Lassourd (to the initial version D3.1)	DMA
	Giovanni Soldi (to the initial version D3.1)	NATO
Peer Reviewers	Name	Partner
	Vincent Lassourd	DMA
		HMOD
Security Assessment	<input checked="" type="checkbox"/> passed <input type="checkbox"/> rejected Comments:	
Format	Text - Ms Word	
Language	en-UK	
Work-Package	WP3	
Deliverable number	D3.2	
Due Date of Delivery	31/12/2019	
Actual Date of Delivery	28/12/2019	
Dissemination Level	Public	
Rights	RANGER Consortium	
Audience	<input checked="" type="checkbox"/> public <input type="checkbox"/> restricted <input type="checkbox"/> internal	
Date	9/12/2019	
Revision	None	
Version	1.0	
Edited by	Sari Sarlio-Siintola, Tuomas Tammilehto	
Status	<input type="checkbox"/> draft <input checked="" type="checkbox"/> Consortium reviewed <input checked="" type="checkbox"/> WP leader accepted <input checked="" type="checkbox"/> Project coordinator accepted	

Revision History

Version	Date	Description and comments	Edited by
0.1	7/10/2016	Version D3.1	Sari Sarlio-Siintola
0.2	20/11/2019	Updated sections 3-6	Saara Siintola
0.3	26/11/2019	Full version (excl. chapter 6 updates)	Sari Sarlio-Siintola
0.4	2/12/2019	Final editions for internal review	Sari Sarlio-Siintola Tuomas Tammilehto
0.9	9/12/2019	Version for the Peer Review	Sari Sarlio-Siintola Tuomas Tammilehto
2.0	19/12/2019	Feedback from the reviewers taken into account (minor corrections, e.g. fixing links etc.)	Tuomas Tammilehto
1.0	19/12/2019	Annexes added	Tuomas Tammilehto

Executive summary

The purpose of this deliverable is to aid maritime surveillance experts, end-users, “commercialisers” and further developers of the RANGER solutions to understand and take into consideration the ethical and societal dimensions of the RANGER solutions created during the RANGER project.

The ethical and societal dimensions of the RANGER solution encompass research, the technology itself, its use in diverse maritime surveillance activities, as well as the RANGER business, procurement and adoption models. The topics discussed in this deliverable include for instance border control, safety and security, customs, fisheries control and environment.

The biggest ethical and societal challenges are related to the use of RANGER in the border control. The tension between humanitarian values and duties and security (internal and external) in particular is also a politically sensitive topic and concerns the right of both EU citizens and migrants. However, this is not a challenge specific to RANGER, but has to do with the whole EU maritime surveillance policy. In the context of RANGER, the potential effects of the technology on irregular immigration and the illegal trafficking of humans and goods are important issues to be investigated during each implementation to ensure the effective fulfilment of human rights and other international obligations. The use of novel, advanced technology such as over the horizon (OTH) radars and advanced data fusion services makes the challenges even more pronounced.

Another central challenge for all maritime surveillance activities is related to data management and security. Although the current radar technologies are neither capable of or intending to directly capture information relating to natural persons, privacy and data protection under EU law are still to be taken into consideration in the RANGER development, use, and business model. Both the possibility to use RANGER data in combination with other data to identify natural persons, and possible future advancements in radar technology and data use mean that the compliance with relevant data protection legislation is central to ensure the long-term sustainability of the solution. The implementation of proper data security architecture and a Data Protection by Design/Default -approach to the development and use has thus been essential during the development of the RANGER solution. From the ethical and societal viewpoint, the importance of ethically and socially sustainable utilising of the data and the protection of the data from leakage and misuse (including to military tracks) cannot be overstated.

A third central ethical challenge is RANGER’s impact on the wildlife and humans. This theme emerged already during the initial societal impact assessment workshops in the beginning of the project. Regardless of whether negative impacts of RANGER on wildlife and humans are likely to take place or not, the concerns are real, and such need to be investigated and duly addressed. The problems have potential implications on at least the concern the design of the RANGER technology, the location and installation of the radars, as well as the use of the technology in various maritime surveillance activities. These concerns have also been addressed in a specific deliverable touching regulations and environmental standards (D3.11). Further, a specific botanical survey was carried out relating to the French pilots (on the Cap Bear site), as a specific requirement.

The structure of this deliverable is as follows. We begin by a short recap of the RANGER project and the maritime surveillance activities relevant to it. After that, we shed light on the international value basis of maritime surveillance in general and discuss the central ethical challenges of RANGER. In the following chapter, we provide a Societal Impact Assessment for the RANGER Solution. Finally based on these contents we will provide the Code of Conduct for RANGER that ensures the ethical use and further development of the solutions after the project.

Table of Contents

Executive summary	4
1 Introduction	7
2 Background	9
2.1 The Ranger Platform	9
2.1.1 RANGER in a Nutshell.....	9
2.1.2 RANGER, CISE, and EUROSUR.....	10
2.2 The RANGER User Communities	11
2.2 The Ethics of Maritime Surveillance.....	12
3 Norms in Maritime Security – The Big Picture.....	15
3.1 International Law	15
3.1.1. Overview.....	15
3.1.2. The European Convention on Human Rights	15
3.1.2 United Nations Convention on the Law at the Sea	16
3.1.4 International Convention for the Safety of Life at the Sea.....	16
3.1.5 The International Convention on Maritime Search and Rescue.....	17
3.1.5 The Convention Relating to the Status of Refugees	17
3.2 European Union Law	18
3.2.1 The European Council.....	18
3.2.2 The Charter of Fundamental Rights of the European Union.....	21
3.2.3 Privacy, Data Protection and Data Security	23
4 The Ethical and Societal Challenges of RANGER	26
4.1 Search and Rescue, and the Duty to Render Assistance	26
4.2 Irregular Immigration and Border Control.....	27
4.3 The Displacement Effect	28
4.4 Misuse and Dual Use	29
4.4.1 Misuse and Dual Use of RANGER Research	29
4.4.2 Misuse and Dual Use of the RANGER Solutions	30
4.5 Tensions in International Relationships	31
5 Societal Impact Assessment (SIA)	32
5.1 What is a Social Impact Assessment?.....	32
5.2. The Mitigation of Ethical and Legal Barriers.....	34
5.3 The Benefits of RANGER	42
6 RANGER Code of Conduct.....	43
Summary	46
Final note:.....	46
Annex A - References & Relevant Readings	47
Annex B – The Review of the Ethical Experts.....	50
Annex C – Ethical & Societal Compliance Check –table (of this D3.2 deliverable)	52
Annex D – Ethical & Societal Compliance Check –table (template)	56
Annex E – The Privacy Impact Assessment.....	60

List of Figures

Figure: 1 Ethical Dimensions of RANGER..... 7
 Figure 2: RANGER platform 10

List of Tables

Table 1: Different aspects of Maritime Surveillance and RANGER 12
 Table 2: Ethics and RANGER’s various compositions 14
 Table 3: EC priority areas and RANGER surveillance 20
 Table : 4 The Fundamental Rights of the EU 22
 Table 5: The EU Fundamental Rights in the Maritime Surveillance Context 23
 Table 6: RANGER use cases 34
 Table 7: The Mitigation of Ethical and Legal Barriers..... 41
 Table 8: Benefits the RANGER provides 42
 Table 9: RANGER Code of Conduct..... 45

1 Introduction

The purpose of this deliverable is to help maritime surveillance experts, end-users, commercializers and developers of the RANGER solutions to understand and take into consideration the ethical and societal dimensions of the RANGER solutions created during the RANGER project. By ensuring the ethical and social sustainability of RANGER, we have been aiming to maximise its benefits for society in combating the illegal trafficking of humans and goods, through enhanced search and rescue activities to save lives, and by increased situational awareness. In a similar manner, we have been aiming to make the RANGER solution itself, including its governance and business models, such that any ethical harms and risks for either humans or wildlife are minimised. The themes discussed in this deliverable include, for instance, border control, safety and security, customs, fisheries control and the environment.

EU Maritime Surveillance aims at an effective understanding of activities taking place at the sea that could impact the security, safety, economy or environment of the European Union and its Member States. The main purpose of RANGER is to advance these interests by combining innovative radar technologies with novel technological solutions for early warning, and by integrating them into the EU maritime surveillance ecosystem, including CISE and EUROSUR. The use of RANGER is not limited to the EU, however; the solution is developed to enable its commercialisation and implementation even in third countries.

The ethical and societal dimensions of the RANGER solution encompass research, the technology itself, its use in diverse maritime surveillance activities, as well as the RANGER business model/procurement as part of the European Maritime Surveillance ecosystem. However, since the solution is meant to be commercialised also outside of the EU, the ethical requirements of the stand-alone version of RANGER need to be specified separately; their content and implementation could differ from that of the RANGER-As-Part-Of-CISE-Environment.

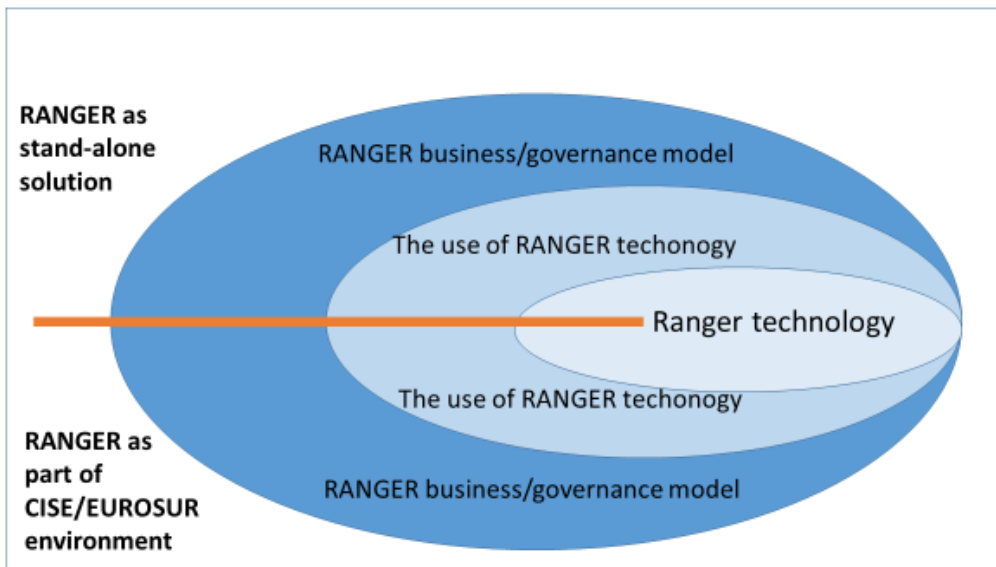


Figure: 1 Ethical Dimensions of RANGER

The biggest ethical challenge concerns the use of RANGER in the border control. This is related to the tensions between humanitarianism and security, and the human rights of both EU citizens and migrants. On the other hand, this is not only a challenge for RANGER, but for the whole EU maritime surveillance policy and practices which - according to several scholars - are more focused

on safety, technology and security businesses than on human rights and saving lives. In addition, and especially in the RANGER context, any displacement effects on irregular immigration traffic are important issues to be investigated.

Data protection is a central ethical issue for nearly all maritime surveillance activities, be it border control, SAR, fisheries, or environment control. Privacy and protection of personal data are a concern with the use of RANGER although the current radar technology cannot capture sensitive or personal information. However, since the RANGER data combined with other data can violate privacy and personal data protection, the adaptation the Privacy by Design/Default –approach anticipated in the General Data Protection Regulation (GDPR), and the Data Protection Law Enforcement Directive (LED), as well as proper data security architecture have been essential in the development of the RANGER solution during RANGER project. Even more relevant issue from the ethical and societal viewpoint is the data security: the right way of utilizing the data, and the avoidance leakage and misuse of that data, which includes also military tracks.

RANGER's impact on the wildlife and humans is the third ethical concern, which emerged already during the initial societal impact assessment workshops organized in the beginning of the RANGER project. Regardless of how probable different the feared impacts on wildlife and humans are, it is ethically and societally important to address these problems and worries. Tackling of the concerns both the design of the RANGER technology, the location and installation of the radars, as well as the use of the technology in various maritime surveillance activities. These concerns have also been addressed in a specific deliverable touching regulations and environmental standards (D3.11). Further, a specific botanical survey was carried out relating to the French pilots (on the Cap Bear site), as a specific requirement.

This deliverable D3.2 has been produced in the last period of RANGER project. The starting point for the work have been both the initial version D3.1 of this RANGER ethics deliverable, as well the MARISA D2.13 Ethics deliverable. The deliverable has been designed to be quite short (including several tables and pictures) and without too many academic arguments because of a practical reason: Based on our experiences the partners in technology projects may not be very familiar with ethical issues. Therefore, the deliverable has to be interesting to the point and easy to read – and to give incentives to consider ethical and societal issues further during the project and after the project as part of the business/adaption activities.

In this deliverable and after the introduction, we will first describe the RANGER project and the maritime surveillance activities it supports. After that, we will shed light on the basic values of the maritime surveillance operations and discuss the most relevant ethical challenges of RANGER. In the fifth chapter, we will provide initial societal impact assessment on the RANGER. Finally based on these contents we will provide the Code of Conduct for RANGER.

2 Background

The purpose of this chapter is to provide the reader with an orientation base for understanding the more detailed ethical and societal discussion of this deliverable. We begin with a presentation of the main features of RANGER. After that, we describe the central maritime surveillance activities which RANGER aims to bring value to. Finally, we provide a short summary of the current academic discussion concerning maritime surveillance and the technology it employs.

2.1 The Ranger Platform

2.1.1 RANGER in a Nutshell

The objective of RANGER project was to provide a complete solution for traffic surveillance and search and rescue (SAR) operations. The RANGER solution created during the RANGER project offers vessel detection, recognition and identification capacities far beyond existing radar in terms of both targets size and distance, ranging over-the-horizon. The OTH radar stands out for detecting targets at large distances compared to the state-of-the-art radar systems, whereas MIMO radars as part of the RANGER solution stand out for achieving extremely high resolution, detect small, fast manoeuvring objects with line of sight ranging limitations.

The RANGER architecture is designed to be both scalable and modular in terms of its components and outputs. In this way RANGER can easily perform any necessary adaptation steps that need to be followed so as such a platform to be deployed on European “hotspots” of expected illicit activity. Further, the RANGER platform is developed in a way to achieve sustainable integration with the CISE framework of services and EUROSUR framework, while being also available as standalone version. For the time being we foresee three distinct RANGER CISE-compliant services: the OTH radar track service, the PA-MIMO radar track service and the RANGER EWS service.

The RANGER Advanced User Interface is a component specifically designed to provide multiple categories of users (e.g. radar designers, operational users, result stream subscribers) with the functionalities required to operate and exploit the results of both the OTH and MIMO radars, according to their needs and without requiring extensive training. This has been a rather challenging objective as, for instance the operation of OTH radars require a solid expertise in particular to change in real-time the radar configuration in order, for instance, to better interpret results, focus processing on uncertain cases, and filter out false positives and noise.

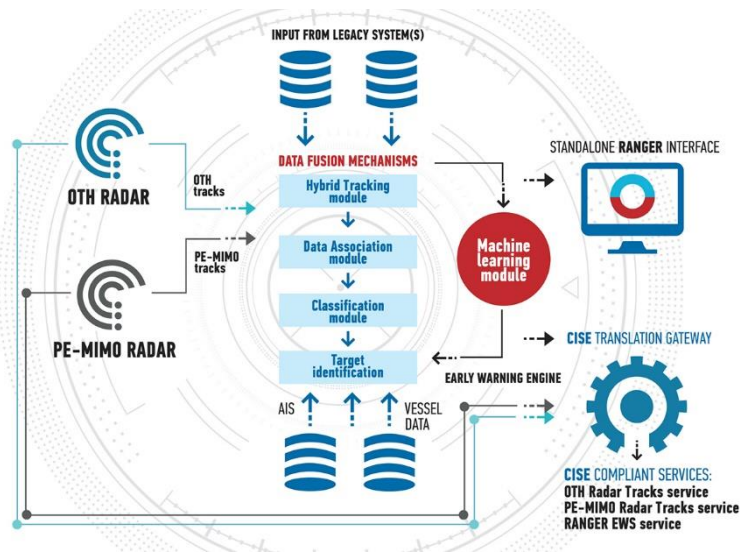


Figure 2: RANGER platform

The substantial advantages provided by the two ground-breaking radar technologies developed in RANGER project are the enormous detection range that extends over the horizon and the unprecedented high resolution that allows for the accurate detection of small, fast manoeuvring vessels. RANGER project leveraged the combination of these two complementary to each other technologies, to take a step further towards the design, implementation and provision of a system that not only detects targets but has the ability to identify and track vessels within the range limits of its sensors detection capability. Thus, RANGER project developed a platform that supports maritime surveillance operators and consequently maritime security operations, by providing early warnings, alerts and recommendations to its users.

RANGER EWS collects data from a variety of sensors (OTH and PA-MIMO radars), legacy systems (mainly AIS, and legacy radars) as well as databases information to correlate data and present it into an intuitive and understandable advanced visualization module. Technologically, EWS is built upon advanced Data fusion algorithms and architectures as well as novel deep machine learning structures to provide:

- a) A threat classification of all simultaneously detected targets based on AIS data, historical data in available databases as well as manoeuvring patterns of detected and tracked vessels.
- b) Automatic Target Recognition (ATR) through cross correlation of Radar and AIS data.
- c) Target Continuous Tracking, especially valuable for high-threat vessels.
- d) Alarms including collision warning, boundary violation and proximity alerts.
- e) Recommendations on required interventions based on risk assessment and self-training of threat detection models.

2.1.2 RANGER, CISE, and EUROSUR

RANGER platform is developed in a way to achieve sustainable integration with the CISE framework of services and the current EUROSUR framework, while being also available as standalone version. On both, RANGER has produced separate deliverables (D3.5, D3.6, D3.7, and D3.8).

CISE is an information sharing platform among EU member states' maritime authorities. The idea of CISE is to gather together maritime domain's surveillance data from numerous national and independent surveillance systems in order to picturise and to maintain the best possible situational

awareness, readiness and cost effectiveness from the European sea borders, sea territories and areas related (e.g. *Search and Rescue Regions*). The user communities of CISE represent maritime safety, maritime security and prevention of pollution caused by ships, Border control & surveillance, Fisheries control, Customs, Environment, General law enforcement and Defence. (EU 2010). Currently, CISE is ongoing as a prototype, it is planned to be operative by 2020.

EUROSUR (launched in 2008) is a common framework for the exchange of information and for the cooperation of Member States among themselves and with Frontex. The main purpose of EUROSUR is to improve the “situational awareness” and reaction capability to prevent irregular migration and cross-border crime at the EU’s external land and maritime borders. It provides Frontex and ‘national’ border control authorities with the infrastructure and tools for detecting, preventing and combatting cross-border crime, detecting and preventing irregular migration and protecting and saving the lives of migrants at sea. Frontex coordinates the use of these tools and contributes to coordinated reaction capacity as a main possible operational priority. It is supported by a communication network.

2.2 The RANGER User Communities

“The sea is valuable source of growth and prosperity for the European Union and its citizen. The EU depends on open, protected and secure seas and oceans for economic development, free trade, transport, energy security, tourism and good status for marine environment”. (EC 2014)

“European citizens expect effective and cost-efficient responses to the protection of the maritime domain, including borders, ports and offshore installation, in order to secure sea borne trade, address potential threats from unlawful and illicit activities at sea, as well as to make optimal use of the sea’s potential for growth and jobs, whilst safeguarding the marine environment.” (EC 2014)

As stated above, the sea is both a valuable source of growth and prosperity, a domain to be protected from unlawful and illicit activities, and an environment to be protected. Both the growth and prosperity, security and safety and ethically important issues which have societal impact on society. (COM 2014). Maritime surveillance in turn is essential for creating maritime awareness, “knowing what is happening at sea”. This awareness assists the authorities responsible for monitoring and surveillance activities in preventing and managing in a comprehensive way all situations, events and actions related to the EU maritime domain. (COM 2009)

Maritime surveillance includes various aspects and different kind of user communities. The categorization of maritime surveillance presented in the table below is used to further study the ethical and societal issues of the proposed RANGER solution. The user-groups defined in the left column of the table are the same as the CISE user communities¹ (see COM 2010). The activities where RANGER is intended to be used are described in the right-side column of the table.

¹ The defense and military activities are excluded from the table since RANGER is not aimed to serve military purposes.

Aspects of Maritime Surveillance	Why RANGER’s Vessel Tracking?
Maritime safety, maritime security and prevention of pollution caused by ships	Vessel traffic management Search and rescue (SAR) early warning/identification Piracy early warning/identification Terrorism early warning/identification Port security
Border control & surveillance	Early warning/identification of Irregular immigration (both asylum seekers and illegal immigration) Early warning/identification of Human trafficking
Fisheries control & Other economic activities	Early warning/identification of Illegal, un-reported/-regulated fishing (>wrong area, wrong time, wrong equipment, exceeding fishing quotas) Monitoring fish nets/fish traps Exploration and exploitation of seabed (oil and gas platforms) Off-shore wind power
Customs	Early warning/identification of vessels smuggling illegal goods Early warning/identification of vessels smuggling legal goods
Environment	Early warning/identification of vessels causing oil spills and/or unleashing wastewater Monitoring of protected areas
General law enforcement	Monitoring of compliance with applicable legislation in sea areas, where there is a policing competence and support to enforcement and/or response operations.

Table 1: Different aspects of Maritime Surveillance and RANGER

2.2 The Ethics of Maritime Surveillance

From ethical, social and political point-of-view surveillance can be understood as “the process of watching, monitoring, recording, and processing the behaviour of people, objects and events in order to govern activity”. This mean that surveillance is not strictly confined to the act of watching and observing, but also the process of recording and processing what is being seen, where the finality is to know better in order to govern the observed activity.

TCT-mediated surveillance increases the speed of control practices and the differential between the legal borders of rights and of policing, which casts a doubt over the pertinence of the latter claim. Critically engaging with the notion that Europe is “under treat” ... should thus go together with asking whether the Europe that is shaped by current border control and surveillance practices, has not itself become a threat.’ (Jeandesboz 2011)

‘Data Mining enables large amounts of personal data from disparate sources to be organised and analysed, facilitating the discovery of previously unknown relationships amongst the data. Knowledge Discovery in Databases (KDD) is a heuristic process of data mining which has evolved from the convergence of machine learning, database systems, statistics and artificial Intelligence. KDD is a multi-step process that facilitates the conversion of large data to valid, novel, potentially useful, and ultimately understandable information.’ (European Group of Ethics 2014)

The ethics of Maritime Surveillance in general has been discussed a lot in academia and in various reports and statements, both from the philosophical viewpoint as well as from more practical point of view, especially concerning the privacy and its trade off with security, freedom and other human rights. Privacy and data protection is a special concern e.g. when using drones and surveillance

cameras, with automated border control, and when collecting and analysing big data. In addition, the impact of the new surveillance technologies on the fundamental rights of asylum seekers and refugees, as well the increased responsibility this more effective situational awareness brings (under international refugee law and the Search and Rescue regime) , have been deliberated by several scholars. (see Marin 2012, Jaendesboz 2011, European Group of Ethics 2014, Crepeau 2013, Meijers Committee 2012). The Meijers Committee, the Standing Committee of Experts on International, Immigration and Refugee Law, has for example noted the following:

“Assessing the content of the current proposal for a Regulation establishing the European Border Surveillance System, the Meijers Committee not only has doubts with regard to the necessity and efficiency of the proposed measures (also considering the high permanent costs involved), but is also very concerned with regard to the effects of Eurosur for the fundamental rights of asylum seekers and refugees, including the right to privacy and data protection. In particular, the Meijers Committee warns against the risks of increased surveillance as this might also increase the human costs of undocumented migration: border surveillance indeed will have an impact on migration routes but not on the root causes of migration.” (Meijers Committee 2012)

Further, Francois Crepeau (2013), the UN Special Rapporteur on the Human Rights of Migrants, has raised a number of questions regarding the actual user processes of the new system:

“The Special Rapporteur regrets that the proposal does not, however, lay down any procedures, guidelines, or systems for ensuring that rescue at sea is implemented effectively as a paramount objective. Moreover, the proposed Regulation fails to define how exactly this will be done, nor are there any procedures laid down for what should be done with those “rescued”. In this context, the Special Rapporteur fears that EUROSUR is destined to become just another tool that will be at the disposal of member States in order to secure borders and prevent arrivals, rather than a genuine life-saving tool.

Many of the ethical/societal challenges and opportunities of RANGER are those of maritime surveillance in general and discussed above, including the rights of asylum seekers and increasing responsibilities, the impact of surveillance on the migration routes, and privacy and data protection. However RANGER’s more efficient and effective capacity in vessel tracking emphasizes the importance of taking these challenges and opportunities more seriously into consideration not only when designing the RANGER technology, but also in its user processes and business modelling - either we have RANGER as a stand-alone version, or as part of the EUROSUR/CISE environment.

In the table below there are illustrated ethical aspects of RANGER in its various compositions: the stronger the red colour is, the more challenging are the ethical and societal issues.

These ethical and societal issues are further discussed in detail in the chapters 3-5.

RANGER as stand-alone system (in Europe and/or outside)	Insufficient data security and information leakages, the misuse of the data and the violation of privacy.	Unethical ways of using RANGER data in decision making, Information leakages	Misuse, dual use other unethical aims of the use of RANGER (especially outside Europe)
RANGER as part of EUROSUR/CISE	Insufficient data security and information leakages, the misuse of the data and the violation of privacy	Unethical ways of using RANGER data in decision making, Information leakages	Unethical aims of using RANGER in maritime surveillance
	RANGER technology	RANGER user processes and training	RANGER business/governance model

Table 2: Ethics and RANGER's various compositions

3 Norms in Maritime Security – The Big Picture

In this chapter, we shed light on the international and European values and norms behind the maritime surveillance and search and rescue (SAR) at sea. We will take International Law and especially *Human Rights*, *Convention on the Law of the Sea*, and *Conventions of Search and Rescue at Sea* as the starting point for this work.

3.1 International Law

3.1.1. Overview

International Law is a network of legal rules, principles and practices generally regarded and accepted as binding among states. The lack of a single, overarching authority from which the law emanates is perhaps the most noticeable characteristic of international law: its sources consist of bilateral or multilateral treaties that sovereign states voluntarily bind themselves to (the dominant source of international law), as well as customary law (general, established practice accepted as law). International law can thus be said to be a largely consent-based system.

The scope of subjects addressed by international law ranges from traditional topics such as war and peace and diplomacy to human rights, rules on trade, protection of the environment, maritime law, international criminal law and the protection of refugees. International agreements are often developed and negotiated within the framework of international organizations such as the United Nations (UN) or the Council of Europe. Also disputes relating to international law are typically solved with the help of such organizations. The International Court of Justice is the principal judicial organ of the UN that settles, in accordance with international law, legal disputes submitted to it by states

3.1.2. The European Convention on Human Rights

The idea that individuals can be subjects of international law with specific rights is new. For centuries, states were seen as eligible to treat their citizens as they pleased. The Universal Declaration of Human Rights in 1948 by the United Nations (UN) marks a breakthrough for human rights thinking. The declaration contains a collection of rights, with their underlying philosophy being that all individuals, by virtue of human dignity, enjoy certain rights and should be protected against their governments. Though not a legally binding document, the declaration's influence has been huge and at least some of the provisions can be argued to form a part of international customary law (Klabbers 2013).

It is, however, one thing to declare human rights, and quite another to actually put the rights specified in them into practice. Perhaps the most practically successful system for the protection of human rights is the Council of Europe's 1953 Convention for the Protection of Human Rights and Fundamental Freedoms, better known as the European Convention on Human Rights (ECHR). The convention offers protection for diverse individual rights such as the right to life, the right to liberty and safety, and the right to a fair trial.

What makes the convention so effective is that joining it, as almost 50 European states (including all EU member states) have done, entails acceptance of the jurisdiction of the European Court of Human Rights (ECtHR), a supranational court established by the convention. The ECtHR rules on complaints by individuals, organizations or states alleging on violations of rights set out in the convention and its protocols. It is worth noting that the applicant does not have to be a citizen of a contracting state. The court's judgements are binding and have led to numerous changes in legislation and administrative practices in the contracting states, in a wide range of areas (ECHR 2010).

Since its adoption in 1950 the Convention has been amended several times and supplemented with many rights in addition to those set forth in the original text.

3.1.2 United Nations Convention on the Law at the Sea

The general international law of the sea was long heavily dependent on customary international law. Nowadays a great deal of it is found in the United Nations Convention on the Law of the SEA (UNCLOS) - a treaty that was concluded in 1982 but entered into force as late as 1994, replacing several smaller but relatively outdated treaties. The UNCLOS defines the rights and responsibilities of states in their use of the world's oceans and establishes a framework for the conduct of maritime commerce, the environment, and the management of marine natural resources. Importantly from the perspective of RANGER, UNCLOS also sets the geographical limits of maritime zones (e.g. the territorial seas over which each state has sovereignty) and establishes rights and discretionary and non-discretionary responsibilities of coastal States (UNCLOS 1994).

For the purposes of maritime surveillance and security, the most important provision in the UNCLOS is the article 98 on duty to render assistance. It obliges for every master of a ship flying the flag of a contracting state, so long as this does not put their own ship in danger:

- 1) To render assistance to any person found at the sea in danger of being lost
- 2) To proceed with all possible speed to the rescue of persons in distress
- 3) After a collision, to render assistance to the other ship

In addition to this, every coastal state shall promote the establishment, operation and maintenance of an adequate and effective search and rescue service regarding safety on and over the sea and, where circumstances so require, by way of mutual regional arrangements cooperate with neighbouring states for this purpose (UNCLOS 1994).

3.1.4 International Convention for the Safety of Life at the Sea

The 1974 International Convention for the Safety of Life at Sea (SOLAS Convention) in its successive forms is perhaps the most important treaty concerning the safety of merchant ships. Its fifth chapter, Safety of Navigation, however, generally applies to all ships, including yachts and other private ships, on all voyages, including local ones.

From the perspective of maritime surveillance and security, two provisions stand out. The first one is a general obligation for ship masters to render assistance, similar to the provision found in UNCLOS: *'The master of a ship at sea which is in a position to be able to provide assistance, on receiving information from any source that persons are in distress at sea, is bound to proceed with all speed to their assistance, if possible, informing them or the search and rescue service that the ship is doing so.'* Should the ship be unable to provide help or consider it unnecessary (e.g. if they are aware that help is already being provided), they are required to enter in the log-book the reason for failing to proceed to the assistance, taking into account the said recommendation to inform the appropriate SAR service. In addition to this, ships can be requisitioned by the master of a ship in distress or the SAR authorities to render assistance (SOLAS 1974).

The provision has later been amended with a few clarifications: the duty to provide assistance applies regardless of the nationality or status of the persons in distress or the circumstances in which they are found. Once rescued, they shall be treated humanely and delivered to a place of safety (IMO WB).

SOLAS also contains a provision on search and rescue services: each state undertakes to ensure that necessary arrangements are made for distress communication and coordination for the

rescue of persons in distress at sea around its costs. These arrangements shall include the establishment, operation and maintenance of SAR facilities that are necessary and practicable with regard to the density of the seagoing traffic and the navigational dangers. Adequate means of locating and rescuing shall be provided (SOLAS 1974).

3.1.5 The International Convention on Maritime Search and Rescue

Even though both custom and treaties such as SOLAS oblige ships to provide help for those in distress, it was only after the 1979 International Convention on Maritime Search and Rescue (SAR Convention) that an international system for SAR operations was established. The SAR Convention is aimed at developing an international SAR plan so that no matter where an accident occurs, their rescue would be coordinated by a SAR organization or, when applicable, several SAR organizations in cooperation. The SAR convention obliges the contracting states to, individually or in cooperation with other states, develop SAR services to ensure that assistance is rendered to anyone in distress at sea. On receiving information about such a situation, urgent steps to endorse the necessary assistance shall be taken. The treaty has been ratified by 113 countries (SAR Convention 1979).

Following the adoption of the SAR Convention, IMO's Maritime Safety Committee divided the world's oceans into 13 search and rescue areas, in each of which the countries concerned have delimited search and rescue regions for which they are responsible (IMO 2005).

The participating states to the SAR Convention are obliged to establish certain basic elements of a SAR service: a legal framework, assignment of a responsible authority, organization of available resources, communication facilities, coordination and operational functions, and processes to improve the service (including planning, domestic and international cooperative relationships and training). The Convention also regulates the establishment of preparatory measures, including SAR coordination centres and sub-centres. The convention outlines operating procedures to be followed in the event of emergencies or alerts and during SAR operations (SAR Convention 1979).

The SAR Convention includes several provisions on information management and system design for SAR services. These instructions can be followed in RANGER, so that they are well suited for rescue purposes, too:

- 1) Each rescue co-ordination centre and rescue sub-centre shall have available up-to-date information relevant to search and rescue operations in its area. (SAR Convention 1979, chapter 4.1.1.).
- 2) 'Each rescue co-ordination centre and rescue sub-centre should have *ready access to information* regarding the position, course, and speed of vessels within its area which may be able to provide assistance to persons, vessels or other craft in distress at sea, and regarding how to contact them. This information should either be kept in the rescue co-ordination centre or be readily obtainable when necessary' (SAR Convention 1979, chapter 4.1.2.).

3.1.5 The Convention Relating to the Status of Refugees

The **Convention Relating to the Status of Refugees**, also known as the **1951 Refugee Convention**, is a United Nations multilateral treaty which recognises the right of person to seek asylum from persecution in other countries, sets out the rights of the displaced, and the legal responsibilities of states to protect them (UN 1951). It is grounded in Article 14 of the UN declaration of human rights ('everyone has the right to seek and to enjoy in other countries asylum from persecution') and has been ratified by 145 states.

A refugee is defined as a person who, owing to a well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group, or political opinion, is outside the country of his nationality, and is unable to or, owing to such fear, is unwilling to avail himself of the protection of that country.

The convention is built upon a number of fundamental principles, the most notable of which are the principles of non-refoulement and non-penalisation. Non-refoulement is perhaps the most central one, providing that no contracting state shall expel or return a refugee in any manner whatsoever to the frontiers of territories where his or her life or freedom would be threatened on account of his or her race, religion, nationality, membership of a particular social group or political opinion. Both the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) have consolidated the application of the principle of non-refoulement in their judgements. In cases of so called indirect refoulement or ‘chain refoulement’ (when one country returns a refugee to an allegedly ‘safe’ third country, which then returns them to an unsafe country), both countries may bear responsibility.

The principle of non-penalisation entails the recognition that the displaced may be and often are required to breach immigration rules to exercise their right to seek asylum, and should not be penalised for their illegal entry or stay. A refugee has a right to same treatment and economic and social help as any foreigner who is a legal resident.

3.2 European Union Law

The European Union (EU) is a political and economic union with 28 member states who have decided to act as one to achieve mutual peace and prosperity. The driving forces behind its development were originally related to the perseverance of peace and liberty as well as mutually beneficial economic integration, but in the recent decades the range of goals has expanded also to areas such as social progress and environmental protection.

The EU is based on the rule of law: each action taken by the EU is founded on treaties voluntarily and democratically approved by all member states. The EU is not a typical international organization, however. First of all, most of its acts are based on majority opinion (not consensus), and are adopted by EU: s own institutions, not the member states themselves (even if both member states and individual citizens have good representation in different EU organs). Secondly, as the member states have conferred to the EU competences to legislate and adopt legally binding acts – regulations, directives and decisions – in certain areas, no national ratification processes are needed for such acts to become binding for them.

In addition to this – and in order to ensure that the system can function in practice - EU law takes precedence over national law: the member states cannot adopt legislation that conflicts with EU law. Should such legislation nevertheless exist, it must be either given an interpretation that removes the conflict or be outright ignored. This is a fundamental principle in the EU law, as it is necessary for uniform and consistent application of the EU law.

3.2.1 The European Council

The European Council is an EU institution that comprises the heads of government/state of the EU member states together with its president and the president of the Commission. Its task is to define the overall political directions and priorities of the Union. It is not one of the EU's legislating institutions, however, so it does not exercise legislative functions. Instead, it sets the EU's policy agenda by adopting 'conclusions' that identify issues of concern and actions to take.

In June 2019, the European Council agreed on a **new strategic agenda for the EU for the next five years**. This agenda provides an overall framework and direction to respond to any challenged and opportunities that the Union faces, to promote the interests of EU citizens and to guide the work of union institutions in the next five years.

The Agenda comprises four priority areas: protecting citizens and freedoms; developing a strong and vibrant economic base; building a climate-neutral, green, fair, and social Europe; and promoting European interests and values on the global scale. From the viewpoint of RANGER and maritime surveillance in general, two priority areas are particularly important: ‘protecting citizens and freedoms’, and ‘promoting European interests and values on the global scale’. In the following part, we will take a closer look at them both.

‘Protecting citizens and freedoms’ deals with the freedom, security and prosperity of the EU itself, and as such is of importance to RANGER first and foremost the European use context (for instance in border control, SaR, and migration-related issues). The agenda underlines the integrity of the EU territory and the effective control of external borders is as absolute prerequisites for upholding security, law, and order, and for ensuring that EU policies function properly. However, this cannot happen at the expense of European values and principles, such as fundamental and human rights. Most of the specific objectives under this priority area are directly relevant for RANGER. It is also noteworthy that these objectives look different from those of the previous, 2014 strategic agenda: a heavy emphasis has been put on effective border control and migration policies and practices, and the issues relating to SaR are named specifically.

Since RANGER is developed to be implemented also outside of the EU context, and as its use within the EU has implications in the international setting, even ‘promoting European interests and values on the global scale’ is of relevance to ranger. The key message of this priority area could be summed up as increasing the unity, efficiency, and assertiveness of the EU to ensure effective and comprehensive influence in the unions global relationships, be it about the promotion of democracy and human rights, trade, or security and defence.

Priority area	Contents	Maritime Surveillance Aspects
<p>1) Protecting Citizens and Freedoms</p> <p><i>‘Europe must be a place where people feel free and safe. The EU shall defend the fundamental rights and freedoms of its citizens, as recognised in the Treaties, and protect them against existing and emerging threats.’</i></p> <p><i>‘We must ensure the integrity of our territory. We need to know and be the ones to decide who enters the EU.’</i></p> <p><i>Effective control of the external borders is an absolute prerequisite for guaranteeing security, upholding law and order, and ensuring properly functioning EU policies, in line with our principles and values.’</i></p>	<p>Developing a comprehensive migration policy.</p> <p>Deepening cooperation with countries of origin and transit.</p> <p>Fighting illegal migration and human trafficking and ensuring effective returns.</p> <p>An effective internal migration and asylum policy; a reform of the Dublin Regulation based on a balance of responsibility and solidarity, taking into account the persons disembarked following Search and Rescue operations.</p> <p>Enhancing the proper functioning of Schengen.</p> <p>Increasing EU’s resilience against natural and man-made disasters through active solidarity and pooling of resources.</p> <p>Protecting the EU from malicious cyber activities, hybrid threats and disinformation.</p>	<p>Increased control and security measures are justified with the need to protect Europe against cross-border crime, such as illegal trafficking and smuggling. The European maritime border is however not only a security issue for the EU, but also for those seeking to enter Europe by sea.</p> <p>Protecting the European seas and borders should be aimed at both creating a secure maritime environment, but also protecting the lives and physical and moral integrity of those at the sea.</p> <p>The lack of accountability and clear lines of responsibility between EU member states and their different actors has been a persistent problem. Also, the diverging interpretations of international law hindered the cooperation between Member States in maritime surveillance and SAR.</p>
<p>2) Promoting European interests and values on the global scale</p> <p><i>‘In a world of increasing uncertainty, complexity and change, the EU needs to pursue a strategic course of action and increase its capacity to act autonomously to safeguard its interests, uphold its values and way of life, and help shape the global future.’</i></p> <p><i>‘The EU will remain a driving force behind multilateralism and the global rules-based international order, ensuring openness and fairness and the necessary reforms. It will support the UN and key multilateral organisations.’</i></p>	<p>Leading the response to global challenges in the fight against climate change, promoting sustainable development, implementing the 2030 Agenda, cooperating with partner countries on migration.</p> <p>Pursuing an ambitious neighbourhood policy and developing a comprehensive partnership with Africa.</p> <p>Working towards global peace and stability, promoting democracy and human rights.</p> <p>Taking greater responsibility for EU’s own security and defence; enhancing defence investment, capability development, and operational readiness; cooperating closely with NATO.</p> <p>More synergies between the EU and the bilateral levels; the EU needs to present a united front and avoid a piecemeal approach in order to have a robust foreign policy.</p>	<p>Third countries must be taken seriously as stakeholders, partners, and potential users of information when developing RANGER and its future business/adoption models.</p> <p>The solution, in all of its dimensions, must be designed in such a way that the specific needs of each implementation context can be taken into account.</p> <p>The tensions between different rights, freedoms, and interests, such as those between European security interests on the one hand, and humanitarian values and obligations on the other, must be taken seriously when developing RANGER and its future adoption/business models.</p> <p>In addition to border control, both SAR, fisheries control and environment control are relevant aspects of maritime surveillance in the context of RANGER development and future use.</p>

Table 3: EC priority areas and RANGER surveillance

3.2.2 The Charter of Fundamental Rights of the European Union

The earliest EU treaties were thought of as more or less purely economic and did not include any references to fundamental rights. This fact, taken together with the doctrine concerning EU law’s precedence over national law, eventually led to worries about the protection of fundamental rights granted in the member states’ national constitutions.

In 1970, The Court of Justice of the European Union argued that respect for fundamental rights forms an integral part of the general principles of EU law. The EU’s Charter of Fundamental Rights is a document established in 2000 to bring consistency and clarity to the fundamental rights protected in the EU. The Charter became legally binding in 2009 when the Treaty of Lisbon was ratified and has the same legal weight as the EU treaties (EU 2007).

According to the Societal Impact Expert Working Group Report (SIEWG2012), the respect for fundamental rights must be a necessary requirement in determining the boundaries on what is and what is not acceptable in EC funded security research initiatives.

The EU Charter of Fundamental Rights is consistent with the ECHR that was described earlier: when the Charter contains rights that stem from this Convention, their meaning and scope are the same (http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm).

Dignity
1 Human dignity
2 Right to life
3 Right to the integrity of the person
4 Prohibition of torture and inhuman or degrading treatment or punishment
5 Prohibition of slavery and forced labour
Freedoms
6 Right to liberty and security
7 Respect for private and family life
8 Protection of personal data
9 Right to marry and right to found a family
10 Freedom of thought, conscience and religion
11 Freedom of expression and information
12 Freedom of assembly and association
13 Freedom of the arts and sciences
14 Right to education
15 Freedom to choose an occupation and right to engage in work
16 Freedom to conduct business
17 Right to property
18 Right to asylum
19 Protection in the event of removal, expulsion or extradition
Equality
20 Equality before the law
21 Non-Discrimination
22 Cultural, religious and linguistic diversity
23 Equality between women and men

24 The rights of the child
25 The rights of the elderly
26 Integration of persons with disabilities
Solidarity
27 Workers’ right to information and consultation within the undertaking
28 Right of collective bargaining and action
29 Right of access to placement services
30 Protection in the event of unjustified dismissal
31 Fair and just working conditions
32 Prohibition of child labour and protection of young people at work
33 Family and professional life
34 Social security and social assistance
35 Health care
36 Access to services of general economic interest
37 Environmental protection
38 Consumer protection
Citizens’ rights
39 Right to vote and to stand as a candidate at elections to the European parliament
40 Right to vote and to stand as a candidate at municipal elections
41 Right to good administration
42 Right to access to documents
43 Right to access the European Ombudsman
44 Right to petition
45 Freedom of movement and residence
46 Diplomatic and consular protection
Justice
47 Right to an effective remedy and to a fair trial
48 Presumption of innocence and right to defence
49 Principles of legality and proportionality of criminal offences and penalties
50 Right not to be tried or punished twice in criminal proceedings for the same criminal offence

Table : 4 The Fundamental Rights of the EU

In the RANGER use contexts, it is important to remember that human rights and the EU fundamental rights concern not only Europeans, but all the people - including those attempting to reach Europe through the sea. Important is also to note that these rights are not just about about setting restrictions on activities – ethics have the potential to bring active, positive value to the RANGER development. There are various fundamental rights which RANGER can be used to promote, most obviously in border control and SAR, but also in the domains of fisheries control, environment and customs, for instance. Ethics is shall not be seen as a burden, but also as a possibility to create value in society – and to justify (morally, politically, socially..) the existence of RANGER despite the challenges present.

Aspect of maritime surveillance	Related Rights
Search and Rescue	Article 3: Right to liberty and security (more efficient SAR operations) Responsibility for search and rescue remains valid no matter how one receives information about a vessel in distress. (e.g. RANGER-technology, surveillance for illegal immigration)
Border control	Article 3: Right to life, liberty, and security. Border control operations should not prevent individuals from the right to leave their country. Article 14: Right to seek asylum from persecution. Border control operations should not prevent asylum seekers from having their demands examined.
Fisheries control	Article 7: Right to property (better surveillance of fish tracks) The increased radar control can also reveal details related to fishery. The improved radar control might help to reveal irregular fishing. Moreover, it could indicate precise timing and areas of fishing which might be information that currently is not being spread around. Article 16: Freedom to conduct business (diminished need to aid in SAR) Article 31: Fair and just working conditions. (> not so much need for patrolling boats)
Customs	Article 16: Freedom to conduct business (the avoidance of pirate goods in the market) Article 38: Consumer protection Improved maritime surveillance technology can help customs to protect EU citizens from illegal and pirate goods
Environment	Article 17: Environment protection Improved radar system can help to fight environmental pollution by offering a better control over the vessels and their whereabouts

Table 5: The EU Fundamental Rights in the Maritime Surveillance Context

3.2.3 Privacy, Data Protection and Data Security

EU Surveillance systems have raised concerns regarding privacy, the protection of personal data, and the potential misuse of such data.² Privacy and data protection are of importance also for RANGER. Even though the processing of personal data is not central for the project objectives, and current radar technologies generally cannot capture personal data, these things could change with technological advancements. Also, even originally non-personal data could turn into personal data when ranger data is combined with other data on the RANGER platform (e.g. AIS data on vessels), risks for violations of privacy and data protection rights increase significantly.

The importance of data protection has grown massively alongside with technological advancements and increased processing of personal data in all areas of life and society. The right to the protection of personal data has gained the status of a fundamental right and receives protection in the EU on the level of primary legislation. Any organisation, company, or public sector actor that in any way processes personal data must be able to demonstrate compliance with

² See e.g. Hayes and Vermeulen 2012, Frontex 2010, especially regarding the use of drones and other means of aerial surveillance.

the legislation. The magnitude of sanctions for failure to comply (up to 20 000 000 EUR or 4% of the association’s worldwide annual turnover) clearly reflects the seriousness of the new European approach to data protection. Data protection has, thus, been turned into a major compliance risk area, and as such should be taken seriously even by actors not explicitly focusing on personal data management.

The two most important pieces of EU legislation concerning data protection, also from the perspective of RANGER, are the General Data Protection Regulation (“GDPR”) and the Data Protection Law Enforcement Directive (“LED”). They have both been enforceable since May 2018.

The LED applies to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Its purpose is to ensure that the data of victims, witnesses, and suspects of crimes, are duly protected in the context of a criminal investigation or a law enforcement action, and to harmonise the legislation to facilitate cross-border cooperation of the relevant authorities to combat crime, terrorism, and other threats more effectively across Europe.

The GDPR has a broader scope, applying to virtually all other processing of personal data by controllers or processors in the Union (regardless of whether the processing itself takes place in the Union), and if the data subjects are located in the Union. This means that all organisations, companies, and public sector actors outside of law enforcement generally need to comply with the GDPR. The GDPR has two main purposes: to enhance the protection of fundamental rights by giving people better control over their personal data, and to unify and modernise the legislation to promote an effective Digital Single Market by cutting red tape and reinforcing consumer trust.

What this means is that different pieces of legislation are apply to different RANGER user communities. The LED will be applicable to the law enforcement actors, whereas the activities many other users, such as SAR groups, fall under the scope of the GDPR. Therefore, the starting point for the design of the RANGER technology, its user processes and business/governance model from the data protection perspective has been in both pieces of legislation.

More detailed information regarding the exact rules and principles concerning the processing of personal data in the RANGER context are found in RANGER Privacy and Data Protection Impact Assessment (DPIA). In order to be able to identify the situations where ethical challenges concerning personal data can rise, however, it is important to understand what exactly is meant by ‘processing’ of ‘personal data’. The definitions given in the EU legislation are as follows:

- 1) *‘Personal data’ means any information relating to an **identified or identifiable** natural person (‘data subject’); an identifiable natural person is one who can be identified, **directly or indirectly**, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*
- 2) *‘Processing’ means **any operation or set of operations which is performed on personal data or on sets of personal data**, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction...*” (EU2016, article 4)

It is, thus, of importance for RANGER further developers and users to be aware that the scope of activities that legally fall under ‘processing of personal data’ is very broad: any data that could help

identify a person even indirectly is categorised as personal data, and even passive storage of such data counts as processing. If, for instance, a vessel is tracked, data regarding its ownership, operations, passengers, crew, agents etc. is more or less likely to be processed – in which case the data protection legislation applies.

Adopting the Privacy by Design/Default –approach and a proper data security (including e.g. anonymisation, pseudonymisation and encryption) is essential, and this is sufficiently covered in the RANGER technical platform. However, in the context of each implementation and configuration of RANGER platform also administrative tasks has to be performed in order be compliant with GDPR and/or LED. As it is stated in the article 25

“The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons” (EU 2016).

The use of RANGER as part CISE environment does not free us from these requirements, as CISE is meant to be only a transmission tool between different user communities' systems. CISE does not store the exchangeable data, but only transfers it in the commonly agreed form for commonly agreed users. Therefore, each user community remains responsible for gathering and storing its data by means of its own sectoral systems and security standards. Both when an actor transfers data for common use through the CISE environment, and when receiving any data inside the CISE network, the transferring must live up to commonly agreed trustworthy security standards while receiving its present classification level (COM(2010)).

The activities needed to safeguard the privacy and data protection of RANGER solution are as follows:

- 1) RANGER technical solutions and user processes are designed based on the privacy by design approach, including needed security mechanisms, access rights etc. The current technical capabilities are described in the RANGER Privacy and Data Protection Impact Assessment (PIA) based on the RANGER technology piloted during the 2. phase trials.
- 2) RANGER governance and business models of each future implementation must take into account the organizational arrangements defined in the GDPR and LED and to fulfil the basic information security requirements issues related to the IT management system in General, to the Configuration management system and to the Privacy management systems.
- 3) Finally, there is a need to conduct PIA on each new RANGER implementation. There are several tools available for this work, including the PIA tool developed by the French Supervisory Authority (“CNIL”). see <https://www.cnil.fr/en/home>

4 The Ethical and Societal Challenges of RANGER

In this section, we shed light on the ethical and societal dimensions of maritime surveillance operations aided by technology such as RANGER.³ The purpose is to give the reader an overall picture of the current value base for operations from the viewpoint of fundamental and human rights, as well as other principles and norms discussed in the previous section. The main emphasis is on the maritime surveillance operations, which are currently most ethically laden, namely border control, search and rescue, and the operations around irregular immigration.

4.1 Search and Rescue, and the Duty to Render Assistance

Search and Rescue (SAR) organisations exist to assist people in distress or danger at sea: to prevent accidents, to assist vessels in distress, to search and rescue those in distress at the sea and to provide medical consultations and patient transport. SAR organisations can be either public or private/voluntary bases. The statutory basis for the minimum level of SAR services is set out in both international treaties, EU legislation and national laws and regulations.⁴

The Right to Life is one of the most fundamental rights enshrined in the EU Charter of Fundamental Rights (article 2) and the European Convention on Human Rights (article 3). In the maritime context, it has been codified by the duty to render assistance to persons in distress at sea and by the duty to establish and maintain search and rescue services (European Union Agency for Fundamental Rights 2013). RANGER will increase the probability of finding out about any ships in distress at the sea, thus playing a role in saving the lives of people on board. Additionally, it can help reduce the volume of sea vessels which are not seaworthy and thus save lives of migrants at sea.

The Duty to Render Assistance to those in distress at sea is found in multiple international treaties: at least UNCLOS (1982), SOLAS (1974), and the SAR Convention (1979). The duty applies to all vessels public and private, including private yachts and other non-commercial ships. Additionally, it poses responsibilities for coastal states to promote the establishment, operation and maintenance of SAR services, also in collaboration with neighbouring states. The European Agency for Fundamental Rights has in a 2013 paper stated the following: 'When the EU and its Member States provide assets, equipment and other maritime border management facilities to neighbouring third countries, priority should be given to assets and equipment that can be used to enhance their search and rescue capacities.'

Improved technological capabilities raise questions also concerning international responsibilities. Currently, states are responsible for carrying out maritime rescue operations within their designated regions. It is, however, possible that a state is for one reason or another either unable to detect a situation of distress or to react to it in a timely and effective manner. The recent political turbulence in certain Mediterranean countries is a good example of a situation that poses risks for effective SAR operations. If another state with increased radar coverage is able to observe and monitor such an event, what legal and moral responsibilities can and should be invested on said state? Would it be sufficient to inform the relevant local authorities of the situation, or should said state also take action themselves? If so, how could such actions outside of the designated SAR area be organised, and how can permissions to operate on foreign waters be granted so that no legal or political conflicts arise?

³ See also separate deliverable d3.3 on the Legal Framework.

⁴ See separate deliverable on RANGER legal framework D3.3. and D3.4.

Another dilemma for SAR is created by the improved awareness and control is related to the potential displacement of irregular migration, for instance across the Mediterranean to Europe. Improved border control and coast surveillance is likely to influence the flows and routes of migrants, but the exact changes in movement patterns can be hard to predict. One undesired scenario is that technological solutions such as RANGER that were intended to increase safety and security actually result in the closing off of old routes, causing migrants to resort to more dangerous routes. This creates challenges for the development and use of surveillance technology; EU's commitment to the fundamental and human rights call for well-balanced actions to minimise the inadvertent harm caused by the adoption of new technology.

Both the duty to render assistance and the obligations of states related to SAR have implications for the development of RANGER. At least the following issues are to be deliberated:

- 1) How could we deliver the long distance information provided by RANGER to third countries so that they can also improve their SAR activities, but without any unwanted negative consequences?
- 2) What should the division of labour between different actors be in situations where information is received about distress situations outside of a country's designated SAR-region? Could Frontex be active in the coordination of such situations?

4.2 Irregular Immigration and Border Control

The **RANGER OTH radar** enables tracking vessels not only on their own sea territories, but also in the high seas and the territorial waters of third countries. It is therefore technically possible to use RANGER to organise border control outside countries' own borders and to redirect intercepted migrants to the coasts of third states. Several ethical challenges raised by the RANGER technology relate to border control activities.

Both the protection of the migrants' rights, and the EU principles of solidarity and burden-sharing are constantly through the arrival of new migrant boats. Obligations stemming from both international and European law prohibit European border authorities from turning back, escorting back, preventing the continuation of a journey, towing back or transferring vessels to non-EU coastal regions in the case of any person in potential need of protection. This obligation is extraterritorial in nature and applies in all sea areas. European authorities are similarly responsible for ensuring that the non-refoulement principle of refugee law is respected by any third parties involved in European surveillance and SAR operations. Since returning refugees to African transit countries is not in line with the principle of non-refoulement, and the determining of a person's refugee status happens through specific administrative processes that cannot be done on the spot, in practice the principle of non-refoulement has to be applied to anyone wishing to come to Europe to apply for asylum (Fischer-Lescano et al. 2009).

However, as countries face increasing migratory pressures, they often try to interpret their international obligations more restrictively: appeals to Article 33(2) of the refugee convention, which provides that *the benefit of non-refoulement may not be claimed by a refugee whom there are reasonable grounds for regarding as a danger to the security of the country in which she is, or who, having been convicted by a final judgment of a particularly serious crime, constitutes a danger to the community of that country*, has gotten more and more common in line with the raising migratory pressures.

Also EU's integrated maritime surveillance and border control, EUROSUR, and CISE have been subject to criticism and concerns that bear relevance to RANGER. Despite the clarity of the

legislation, in some SAR operations the vessels in distress rescued by border patrols have been brought back to their port of origin. These operations have been criticised as concealed push-back operations that violate both the rights and the needs of migrants. For instance Human Rights Watch and several scholars⁵ have brought attention to the EU has funded sophisticated surveillance systems, given financial support to member states such as Bulgaria and Greece to fortify their borders, and created an agency to coordinate a Europe-wide team of border guards to patrol EU frontiers. From the viewpoint of the migrants, these kind of activities can pose severe threats to the fulfilment of human rights and various rights guaranteed in international conventions such as the refugee convention.

In addition to the above challenges, certain diplomatic aspects of enhanced border control need to be considered. The use of RANGER could be considered as intrusive if it is used to monitor third state's territorial waters without prior agreement. Any state is sovereign within its territorial waters, and surveillance that reaches these waters should be carried out in the framework of agreements with the concerned third states.

Ensuring that the rights of the already vulnerable refugees and other migrants are not further compromised for the interests of the more well-off European citizens is, thus, a key concern for RANGER. The following issues must be taken into account in the development:

- 1) EUROSUR and CISE are likely to have already taken into account the above criticism. It is crucial that RANGER's interoperability and compliance with EUROSUR and CISE covers also these ethical issues (not only technology). This concerns especially the fulfilment of the non-refoulement principle, and the use of RANGER radars to detect vessels on the high seas and on the territorial waters of third countries.
- 2) RANGER as a stand-alone solution - especially its user processes and business/governance models - needs to be designed carefully. These include also the designing of user training and selling/procurement strategy. Collaboration with non-governmental organizations is essential to create a sustainable action model.

4.3 The Displacement Effect

It is to be expected that the use of RANGER in border control and customs (either as a stand-alone solution or as part of the integrated CICE/EUROSUR solution) may cause situations in which one route of unregulated immigration and/or smuggling of goods closes, while another opens. In the context of 'the war on drugs', this type of displacement has been given an illustrating name: 'the balloon effect': squeeze a balloon in one place, and it expands somewhere else. Something similar is happening with efforts to crack down on irregular migration. The balloon effect can put the supposed success of certain migration control operations in a questionable light (Andersson 2015). As the new routes can be even more dangerous than the old ones, an increase of threat for the fulfilment of human rights, such as right to live and security occurs.

We can take the year 2010-2011 in Greece and Bulgaria as an example. In summer 2010, a sudden increase in irregular migration, mostly from Iraq and Afghanistan, took place along a 12km stretch of the River Evros, which marks the land border between Greece and Turkey. Diverse actions to

⁵ See e.g. Hayes and Vermeulen 2012; Rijpma and Vermeulen (2015); HRW 2009.

battle this development were implemented in Greece, including measures such as erecting a 12km long fence in Orestiada, but the numbers climbed again in 2011, with a total of 57 000 irregular border crossings taking place: the Greek response had produced a displacement effect to the Bulgarian land border. The choice of sea routes also became innovative. Some smugglers even took the passage from Turkey to Italy. The smuggling of migrants has developed into an important industry in for instance in Turkey, with active networks in various cities, such as Istanbul, Izmir, Edirne and Ankara. The nationalities of the smugglers vary, frequently mirroring the nationality of their customers. The relaxation of Turkey's visa rules towards many African countries has created another pull factor for migrants from this continent, who arrive in Turkey by plane before attempting entry into the EU. (see <http://frontex.europa.eu/trends-and-routes/eastern-mediterranean-route>).

It is likely that the smuggling of humans and goods will resort to new routes after the current Mediterranean routes will be closed. Ensuring that the rights of the already vulnerable refugees and other migrants are not further compromised for the interests of the more well-off European citizens is, thus, a key concern for RANGER. The following issues must be considered in the development:

- 1) Challenges relating to the ways new technologies such as RANGER could impact migration routes must be solved in cooperation with other key actors in the domain of maritime surveillance (e.g. CISE, EUROSUR).
- 2) Before the implementation of RANGER in a new setting, it is crucial to conduct a feasibility study and a Societal Impact Assessment, and to take action to eliminate any undesirable consequences beforehand. The role of both governmental and non-governmental organizations is essential to find sustainable solutions. Consider that the requirements based on the SIA are likely to be considerably more extensive when RANGER is implemented as a stand-alone solution.
- 3) After implementation, follow-up evaluations of the consequences are to be carried out for the purposes of e.g. risk analyses. In cases RANGER is sold stand-alone system instead of as part of the CISE ecosystem, this information sharing must be designed separately.

4.4 Misuse and Dual Use

4.4.1 Misuse and Dual Use of RANGER Research

The term **misuse** refers to research involving or generating materials, methods, technologies or knowledge that could be misused for unethical purposes. Despite the fact that such research is usually carried out with benign intentions, it has the potential to harm humans, animals or the environment. The main areas of concern regarding potential misuse could be:

- 1) research providing knowledge, materials and technologies that could be adapted for criminal/terrorist activities;
- 2) research that could result in the development of chemical, biological, radiological or nuclear (CBRN) weapons and the means for their delivery;
- 3) research involving the development of surveillance technologies that could result in negative impacts on human rights and civil liberties;
- 4) research on minority or vulnerable groups and research involving the development of social, behavioural or genetic profiling technologies that could be misapplied for stigmatisation, discrimination, harassment or intimidation.

If we investigate RANGER from the misuse point of view, the only point in common with RANGER is the point number three. RANGER does not develop technologies that could be adapted for criminal or terrorist activities, neither CBRN weapons nor means for their delivery. It does not involve research on minority or vulnerable groups, or profiling technologies. It does develop a surveillance technology, but this work does not have the risk of negative impacts on human rights and civil liberties. RANGER innovates by combining novel Radar technologies with supporting technological solutions for early warning, with the scope of delivering a surveillance platform that will offer detection, recognition, and identification as well as tracking of suspicious vessels capabilities beyond existing legacy radar systems. Therefore, the main objective of RANGER is to enhance the already existing maritime surveillance framework to prevent threats coming from non-cooperating vessels. The proposed technologies will be developed and integrated into the already existing maritime surveillance frameworks such as EUROSUR and CISE, by following the already well-established ethical guidelines. Following these considerations, RANGER does not include any risk of misuse, in European context or elsewhere.

The term **dual use** could be used in association with products or services that can have both a military and civilian application, that is to say generally intended for civilian purposes, for example in industry, but also for developing weapons and military equipment. As such, their export is not prohibited in principle, but is subject to restrictive controls, generally in the form of a required licence. Certain dual-use goods and technologies may have a conventional military use, while others may serve to manufacture weapons of mass destruction, such as chemical and biological nuclear weapons, as well as missiles capable of carrying such weapons.

As already mentioned earlier, RANGER project is concerned with the development of efficient radars for long-distance surveillance in order to enhance the already available European maritime surveillance framework such as EUROSUR and CISE.

Although, the project aims to develop new technologies in strict relation with military purposes in particular to prevent potential threats coming from sea, the development of such a technology does not require the use of goods that could be used to manufacture weapons or other military equipment for which particular care should be taken of.

Following these considerations, RANGER does not include any aspect of the potential ethical considerations in relation to dual use, in European context or elsewhere.

4.4.2 Misuse and Dual Use of the RANGER Solutions

We can separate the following risks to the misuse of the RANGER solution:

- a) The misuse/dual use of the data RANGER provides (including also military tracks)
- b) The use of the RANGER solution for purposes which are classified as misuse/dual use

The misuse and/or dual use of the RANGER data are possible if persons with malicious intents can gain access to the RANGER data. There are three principal ways in which this could happen: a) by capturing the RANGER data when it is transformed from the antennas to the RANGER platform, b) by hacking the RANGER platform and its data bases, c) due to the human information leakage when somebody having access right to the RANGER data will intentionally or unintentionally leak data to third parties. To avoid data leaks, a strong focus on safety has been adopted in the designing of both technology and data transfers, user processes and access rights, as well as the governance model.

Concerns regarding potential misuse or dual use of the complete RANGER solution are strongly linked to the business/governance models, especially those of the stand-alone version of the solution. The key question is how to make it sure that the solution is used only for agreed purposes after that it had been sold to third parties. Thus, it is imperative to follow e.g. embargos and bans of export imposed by European authorities.

4.5 Tensions in International Relationships

The improved radar coverage can create challenges for international relations. In a case of conflict escalation between states, the radar data could be used for military purposes. Apart from interstate conflict, the data provided by the radars could be utilized by different actors in intrastate conflicts.⁶ This could further complicate and destabilize a region. On the other angle, enhanced radar control accessible for a large number of states could also yield hard evidence that up until now has provided certain room for manoeuvring in power politics. In international politics, it has been sometimes better to offer the ‘villain’ state possibility to withdraw without losing its face. Occasionally, this has seen as a better pragmatic option. A state, region, political leaders who are pushed into corner might feel that they have very few alternatives and might, therefore, resort to extreme even desperate measures (Let me give you an example, yet it is a clumsy, it will illustrate the essence of this point. Malaysian Airlines flight MH17 was shot down over separatist controlled airspace in eastern Ukraine on 17 July 2014.⁷ Ever since, different parties have come up with different theories over the culprits of the incident. One of the versions states that the US has flight control data which can be used to identify the perpetrator. This information is, however, not released. The reason for this is, according to some, that releasing the data would place the perpetrator in such a bad light that it would back-fire; lead to unwanted escalation of the situation and diminish the possibilities to find a diplomatic solution. All these would increase human suffering and prolong the conflict.

The developed technology can be utilized in much larger maritime areas than only in Mediterranean. This can create other type of ethical questions linked to the complex political and societal realities. A few examples are provided in the following.

The activities of the Russian Federation in the Arctic sea and close to North Pole have increased recently. The explanation for this is twofold. Firstly, the exploitation of the natural resources in arctic areas has become more attractive. Secondly, the Arctic Sea has an importance both strategically and for the trade. The heightened tensions between the US (and indirectly with its NATO allied) and Russian Federation can in one scenario lead to military confrontation in Arctic sea area. In a situation like this, the new developed technology might be used for military purposes (already because out of 28 member states 22 belong to NATO).⁸

The complexity of crisis and related turmoil can also create changing unintended consequences. The EU Common Security Defence Policy operation Atalanta has been successful in diminishing

6 An example of the role radar data can have in a case of complex crisis entailing elements both from interstate and intra-state conflict, http://uk.mfa.gov.ge/index.php?lang_id=GEO&sec_id=595&info_id=450

7 <http://www.bbc.com/news/world-europe-28357880>

8 Padrtova, Barbora, *Russian Approach Towards the Arctic Region*, Center for European and North Atlantic Affairs, the article is available at: <http://cenaa.org/analysis/russian-approach-towards-the-arctic-region/> Nicholas de Larrinaga, London - IHS Jane's Defence Weekly, *Russian submarine activity topping Cold War levels*, 02 February 2016, the article is available at: <http://www.janes.com/article/57650/russian-submarine-activity-topping-cold-war-levels>

the pirate activities along the Somalian coast. Allegedly, after the waters had been cleared from the pirates, unregulated fishing boats arrived from other countries to conduct uncontrolled fishing with the only aim to make as much economic profit as possible without taking ecological aspects into account. The EU operation was not able to effectively interfere on this development as it was not part of the operation mandate (only monitoring task). Against this backdrop, it can be concluded that the increased operational abilities (potentially generated by improved radar technologies) need to be combined with coordinated cooperation between different authorities and comprehensive mandates.⁹

5 Societal Impact Assessment (SIA)

This chapter contains a Societal Impact Assessment (SIA) for RANGER. We begin with a short explanation about what a SIA is, before moving on to describing use cases/scenarios that are relevant to RANGER. After that, we identify specific ethical and legal challenges that might affect RANGER and give suggestions for strategies to mitigate them. Finally, we investigate the benefits of RANGER from the viewpoint of key stakeholders.

5.1 What is a Social Impact Assessment?

The term ‘Social Impact Assessment’ (SIA) refers to the processes of analysing, monitoring and managing the intended and unintended social consequences of planned interventions (policies, programs, plans, and projects) and social changes invoked by these interventions. Its primary purpose is to ensure that the ecological, socio-cultural, and economical sustainability of projects and policies can be maximised.

SIA can best be understood as an umbrella framework that embodies the evaluation of all impacts on humans and on all the ways in which people and communities interact with their socio-cultural, economic and biophysical surroundings. SIA has strong links with a wide range of specialist sub-fields involved in the assessment of areas such as: aesthetic impacts, archaeological and cultural heritage impacts, community impacts, cultural impacts, demographic impacts, development impacts, economic and fiscal impacts, gender impacts, health and mental health impacts, impacts on indigenous rights, infrastructural impacts, institutional impacts, leisure and tourism impacts, political impacts, poverty, psychological impacts, resource issues, impacts on social and human capital, and other impacts on societies. This means that a comprehensive SIA cannot normally be undertaken by a single person but requires a multidisciplinary team approach (International Association for Impact Assessment n.d.).

It is central to note that a Social Impact Assessment is not just about predicting impacts in a regulatory context; it is an active process of managing the social aspects of development. Assisting stakeholders to identify development goals and ensuring the maximisation of positive outcomes can be more important than minimising harm from negative ones. By identifying impacts in advance, better quality decisions can be made regarding which interventions should proceed and how they should proceed. Following this, mitigation measures can be implemented to minimise

⁹ The European Union Naval Force ATALANTA (EU NAVFOR), for more information, see: <http://eunavfor.eu/>; Alexandru Voicu, Ruxandra-Laura Bosilca, Centre for European Studies, *Maritime Security Governance in the Fight Against Piracy off the Coast of Somalia: a Focus on the EU response*, available at: http://cse.uaic.ro/eurint/proceedings/index_htm_files/EURINT2015_VOI.pdf

the harm and maximise the benefits from a specific planned intervention or related activity. Respect for human rights should underpin all actions (Vancley and Esteves 2011:3).

The contents of the social Impacts concern the following aspects in society (Vancley and Esteves 2011):

- 1) **Way of life, fears and aspirations** (how people live and interact with each other on a daily basis, their perceptions about their safety and that of their communities, and their aspirations for the future, including that of their children);
- 2) **Culture and community** (peoples’ shared beliefs, customs, values and languages, as well as the cohesion, stability and character of their communities);
- 3) **Political systems** (participation in the decisions and processes that affect peoples’ lives, the nature and functioning of democratic processes, and the resources available to support peoples’ involvement in these);
- 4) **Environment** (access to clean air, water, and other natural resources, as well as the level of exposure to pollutants and harmful substances and the adequacy of sanitation);
- 5) **Health & well-being** (physical and mental well-being, not just an absence of infirmity);
- 6) **Personal and property rights** (economic effects, civil rights and liberties, personal disadvantages)

We formulated the first SIA contents for this deliverable in 2017 with contributions from RANGER project partners, stakeholders in the LAUREA networks, and LAUREA master students. These contents were then updated in Autumn 2019 with the help of both project partners, Laurea students and well as participant in the NATO’s and RANGER’s MSAW 2019 workshop in Lerici. In addition impacts defined in the EUCISE d.22. and in the MARISA d2.13 are incorporated in the final SIA. The starting point for the discussions has been the following aspects of the maritime surveillance and the use of RANGER in them (see table below).

Aspects of maritime surveillance	Use Cases/Scenarios
Border control & surveillance	<p>The maritime border surveillance is difficult with current coastal resources. The range of radar and the speed of vessels do not provide a reasonable time limit for detection and identification. Unidentified vessels reach the coast only 2 hours after detection.</p> <p>France experienced two cases of unidentified ship that could not be stopped due to short notice, particularly at night.</p> <p>The way to counter these constraints is to ensure a presence at sea with patrol boat or aircraft.</p> <p>RANGER, by the warning provided by OTH data, should strengthen the capacity of detection. It would allow to save the means used for monitoring to identify a detected target.</p>
Maritime Safety and security	<p>The search and rescue at sea require real-time knowledge of the position of vessels likely to be able to assist. Furthermore, it is necessary to detect or track the maritime event, even-if the ship involved has no AIS, LRIT or VMS.</p> <p>Being able to have a system capable of correlating all sensors and information sources would offer the operator a comprehensive tactical situation.</p>

		<p>RANGER by the multiplicity of different types of sensors and correlation of available information should strengthen action and reaction capabilities for maritime safety.</p>
Fisheries control		<p>Fishing vessels are submitted to European legislation in the European EEZ. Ships have to transmit position by AIS or VMS, they have to register all catches on a logbook for each area.</p> <p>In case of a transshipment at long range from shore, it is not able to detect this kind of unreported action.</p> <p>RANGER intends to have the capability to track and detect all abnormal behaviours between ships, even if they shut down their tracking system as AIS or VMS by mixing raw video from radar and data.</p> <p>In case of incursion of unauthorized foreign fishing vessels in European EEZ RANGER could be a solution to detect and track this illegal fisheries.</p> <p>RANGER could be an alternative to aircraft and patrol boat.</p>
Customs		<p>Customs control operations at sea can only be achieved on the ships previously identified as suspect by intelligence elements but also by randomly checking and opportunities' cases.</p> <p>The fight against smuggling and counterfeiting requires the ability to monitor maritime traffic, identify routes and who leaving them, but also to cross dynamic information with historical data to generate relevant alarms.</p> <p>RANGER could provide an opportunity to detect abnormal situations or generate alarms based on behavioural analysis of vessels of interest or ships from ports known for their absence of systematic controls.</p>
Environment		<p>AIS data and satellite images are not considered as evidence by the judicial authorities in order to unmask suspected polluters.</p> <p>In this way by continuous tracking from shore to high sea, RANGER could be a means to demonstrate that the ship suspected is the ship involved.</p> <p>RANGER is the first step to mix all kind of data to build a common operational picture in EEZ, combining coastal systems and satellite's means.</p>
General enforcement	law	<p>Strengthening the law enforcement at sea is based on knowledge of what happens in real time in order to identify criminal behaviour and provides an appropriate response.</p> <p>RANGER should strengthen the knowledge of what is happening at sea by the fusion and correlation of data. If the level of confidence in the system increases, RANGER could become a tool for targeting ships and intervention areas and therefore should reduce the time devoted to the achievement of air or maritime patrol.</p>

Table 6: RANGER use cases

5.2. The Mitigation of Ethical and Legal Barriers

The table below lists the identified legal, ethical and societal problems, which RANGER and its use may cause, as well as the activities to mitigate/eliminate them. In the third column of the table, we have reported the activities taken in order to mitigate the challenge. Finally, in the fourth column

there are identified activities still need to be performed in the context of RANGER future implementations and developments. The focus of the problems is on the expected outcome (RANGER solution) rather than on the problems of the research ethics (such as plagiarism). In turn, mitigating and eliminating the problems concern not only the R&D work and features of the RANGER technology, but also how the user guidance should be, as well as requirements for the RANGER business modelling and dissemination.

The table is not exhaustive. The idea of it is to catalyse constant deliberations on ethical issues and challenges and provide an overview of the strategies on how to cope with them inside each work-package's R&D work. For the same reason, all problems presented by the people attending the workshops have been included in the table, although some of them may turn out to not be problems in the end.

<i>Identified ethical risks and problems</i>	<i>Planned Activities to Mitigate/Eliminate Problems</i>	<i>Activities performed during the project in order to mitigate/eliminate problems</i>
Tension between human values, security and business		
<p>In times of austerity, why put money to this?</p> <p>RANGER fails to address the impact of the proposed radar solution on fundamental rights and freedoms and politics, solely focusing on technical issues and overall efficiency of maritime surveillance operations.</p> <p>Ranger will be used for the border control and building up boarders at the expense of saving lives of migrants.</p>	<p>Good PR and communication.</p> <p>Make communities understand both the benefits and disadvantages of RANGER. Lower the costs of platform and maintenance</p> <p>The proper involvement of end-users and non-governmental organizations in the RANGER project.</p> <p>SAR criterion, human rights and other ethical guidelines should be taken into account when developing the RADAR technology, its processes and business model. Laws of the sea (UNCLOS, SOLAS and SAR conventions shall be respected.</p> <p>The language and terminology of the user interface should serve each aspect of maritime surveillance (e.g. by taking into account the status of the user logged in)</p>	<p>RANGER solutions and their benefits to societies have been presented to end-users and stakeholders in several maritime events during the project.</p> <p>The ethicalness of the solutions have been stressed in several presentations and published as article (see, Sarlio-Siintola, Tammilehto & Siintola 2019)</p>
<p>The use of RANGER radar to enable border control at high seas may violate the principle of non-refoulement</p>	<p>Issue to be discussed with CISE/EUROSUR. While there are no specific regulations on surveillance on the high seas, this should be carried out with respect for relevant international laws and especially the laws of the sea (UNCLOS; SOLAS and SAR).</p>	<p>RANGER solution is focused on SaR operations and on the creation of warnings/alerts. The actions that follow are responsibility of the border control authorities and should be according to the EU regulations</p>
<p>Attention will not necessarily be paid on people in distress if they are located outside country's SAR responsibility areas.</p> <p>Due to the richer information RANGER provides e.g. from high seas, following "Duty to render assistance"</p>	<p>When implementing RANGER, points of contact/national coordination centres ¹⁰in the area RANGER covers are to be defined, In addition a joint</p>	<p>RANGER solution has been tested and validated in the interconnection with CISE world. RANGER as a compatible solution with CISE framework can assist on the common operations among different countries.</p>

¹⁰ See, European Commission 2014 about the points of contacts.

<p>principle may bring more work the SAR organizations using RANGER.</p>	<p>operation plan with all the third countries¹¹ in the area is to be done before starting use RANGER</p> <p>Third countries in the Mediterranean sea should be seen as end-users of the RANGER information, as well as real partners solving the joint problem with new technology.</p> <p>The extension of cooperation towards third countries must be respectful of these countries' sovereignty and right to decide over own territory.</p>	
<p>RANGER together with EUROSUR/CISE may enforce a conflation of asylum with illegal immigration and thus foster an extension of asylum seekers¹².</p>	<p>It is necessary in the RANGER dissemination and communication use the terms “irregular” “asylum” and “illegal” in a logical and informative way¹³.</p>	<p>The differences of the terms have been well communicated during the project.</p>
<p>Using RANGER e.g. in the Mediterranean will probably cause a displacement of the irregular immigration. The people may even use more dangerous routes or even smaller boats to avoid being detected by RANGER.</p> <p>Both human trafficking and smuggling (illegal and legal) goods are big businesses. In case one route is closed, other (even more dangerous) will be used.</p>	<p>The information sharing to boarder management authorities (FRONTEX) is essential to figure out the big picture of the situation.</p> <p>In case RANGER is sold as stand-alone solution outside EUROSUR/CISE, the information sharing is to be organized properly.</p>	<p>RANGER technical capabilities have been tested with different kind of vessels (from small rib boats to big metallic vessels). In addition, the results and capabilities of such a solution should be classified.</p>

11 According to the European Agency for fundamental rights (2013) “When the EU and its Member States provide assets, equipment and other maritime border management facilities to neighboring third countries, priority should be given to assets and equipment that can be used to enhance their search and rescue capacities.” See also European Commission 2015 about the partnership with third countries.

12 About this problem, see Sombetzki & Quicker 2016.

13 See also Sunny 2014 p. 8.

The quality of our maritime surveillance system in the long run		
<p>How can we make it sure that RANGER will be developed continuously based on end-user requirements and ethical/legal requirements after the project ends? Is there a risk that current technology providers will attain a monopoly in the area of radar surveillance, and thus may not be interested to put money on R&D activities?</p> <p>Since the deployment of RANGER is voluntary for the countries - and if the quality of the solution is not satisfactory – this can lead in a situation where the penetration of RANGER remains in a low level.</p>	<p>Continuous development of the RANGER should be embedded in the RANGER business model from the early beginning.</p>	<p>The most potential buyers/users of the solutions are large organisations and/or states, all following ethical principles and legalities.</p>
<p>Due to the capacity of RANGER to cover long distances there is a risk that some countries choose to be free riders. They will leave the costly surveillance work and investments for other countries. This may be the case both in Europe and outside in the third countries.</p>	<p>Responsibilities and the moral division of labour in maritime surveillance is to be discussed. This can include e.g. the bigger role of FRONTEX in situations where the responsibilities and the amount of inputs are not in balance.</p>	<p>RANGER has disseminated its capabilities to specific authorities that are responsible to balance the effort of the maritime surveillance.</p>
Misuse of RANGER and/or its data		
<p>Technical Information leakage: The data RANGER collects will be captured and misused e.g. for spying, military or terrorist purposes.</p>	<p>Specific security standards are to be followed.</p>	<p>RANGER used the following security mechanisms: Use of VPN connection for legacy systems, use of firewalls, use of network segmentation for isolating internal components from public internet, use of TLS/SSL encryption/ authentication.</p>
<p>Human information leakage: RANGER data will be delivered to someone who should not have it.</p>	<p>User logs as part of the system. Check and balance approach. Any information put into the system and shared through it should be traceable, in order to verify sources and their reliability when necessary.</p>	<p>All RANGER components log all user activities.</p>
<p>Exchange of information with third countries: Possible misuse of personal data.</p>	<p>Any data that in some way relates to an identifiable individual leaving one's country should not be shared with third countries, as these can be used against them if they are returned.</p>	<p>Its CISE node has the responsibility what kind of data will be exchanged and in which country. RANGER can share data only with a specific CISE node.</p>

	Collaboration with third countries (in the framework of CISE or EUROSUR) should only be possible via separate flow of information, where no personal data is allowed to be entered.	
The RANGER will be available for organizations and persons not allowed to use such systems.	Limit the access to the ranger data only to relevant authorities (access rights, ranger business modelling)	RANGER has been demonstrated only to authorized persons and to specific authorities (EU Border Control Authorities)
Diplomacy issue: how to use the radar data that inevitably include also military tracks?	Rules & regulation on the use of data.	RANGER is a civil protection oriented project
Dual roles of the users		
Difficulties to share between civilian and military services (>different regulation) in case the user serves both.	<p>To define the need to share, the need to know and the final aspect concerning low level data.</p> <p>Rules & regulation on the use of data (Are to be defined as part of the D3.2. in the end of the project?).</p> <p>Training as part of the RADAR implementation on necessary also from this point of view.</p>	RANGER is a civil protection oriented project.
Privacy and data protection		
Fundamental rights privacy and data protection should be maintained. Although the data processing of the current RANGER technology doesn't process any identifiable personal data, the situation may change in the future.	Apply "privacy by design" and other requirements (anonymizing etc) defined in the coming new Data Protection legislation (Act + Directive) coming in the effect 2018.	<p>RANGER has been developed by following the Privacy By Design –approach and by implementing several data protection and security features. See the separate document RANGER Privacy and Data Protection Impact assessment (DPIA). DPIA shows that RANGER has sufficient technical capabilities from the viewpoint of LED and GDPR.</p> <p>In the future, each RANGER installation has to 1) take into consideration various organizational arrangements in order to be compliant with LED and GDPR. 2) conduct a DPIA based on these organizational arrangements and on the actual configuration & data sources to be used.</p>

<p>The promotion of “control society”, you cannot even sail at the sea without somebody monitoring you.</p>	<p>Good PR and communication about the justification and advantages of the system</p>	<p>This has been communicated in several events and especially stressed during the demonstration pilots.</p>
<p>Harm to environment and wellbeing</p>		
<p>The electromagnetic pollution and the use of RANGER will disturb wildlife, both animals and plants, including also movements of migratory birds.</p> <p>The use of OTH radar crates the ethical problem of human exposure in high power radiation which is needed for long wave detection</p> <p>Radiation at nearby villages and also to neighbouring countries</p> <p>People may be afraid of the radar and its impact on the nature and human lives.</p>	<p>Follow both EU and local legislation and standards (radiation, environment, NATURA2000 etc.) from the design phase of the radars. Be especially aware of the changing legislation.</p> <p>Choose the right location for the radar that doesn’t cause problems to the nature, archaeological sites or tourism. To mitigate human exposure in radiation, the OTH radars can be located in unpopulated areas. Further minimize the power levels by improving the directivity of the radar.</p> <p>Have agreements from local/national authorities to install and use HF waves.</p> <p>Safety instructions are also needed for installing radars and doing maintenance work.</p> <p>Good PR and information with local communities. Make communities understand both the benefits are disadvantages.</p>	<p>A specific botanical survey was conducted for the French pilots (the site in Cap Béar).</p> <p>A dedicated deliverable was produced address these challenges (D3.11).</p>
<p>Aesthetic footprint</p>		
<p>Size of radar e.g. in Greek islands with traditional architecture will be an ugly landmark in an otherwise beautiful coastline. Local people may complain about it.</p> <p>(on the other hand, people in Aegean islands are already used to military bases and radars.)</p> <p>Local residents’ hostility because of tourism values.</p> <p>A lot of space is needed to install the radars.</p>	<p>Hire industrial designer etc. to create beautiful antennas and radars.</p> <p>Good PR and information with local communities. Make communities understand both the benefits are disadvantages.</p>	<p>Installation sites has been selected in touristic zones. In any case the system respects and complies with environmental regulations. For example, in France the OTH and the PE-MIMO radars has been installed in a NATURA 2000 site. In addition, in Greece we used the deployable versions of the radars in order to reduce the needed space for the installations.</p>

OTM antennas could be awful for neighbours.		
Cases of finding ancient monuments while installing radars?	Consider environmental studies when installing the antenna. Be in contact with archaeological experts before installing the system.	The systems have been installed in end users premises.
Property rights		
The use of public soil to install radar and the impacts on the private property nearby the radar may be unfair. Tourists and local people will be kept away from areas where ranger radars are installed. This may affect local businesses such as hotels, restaurants and other tourism-based business.	Installing the radars in locations which are already being used for similar activities (e.g. military bases).	The demonstration pilots were conducted in military bases and/or using areas already dedicated for this kind of action. Both are potential permanent sites for the solutions.
Ownership of RANGER data, can it be a problem?		
Dual Use		
Fear about the military use (Ranger technology should not have dual use) E.g. if radars are installed nearby military areas.	Good communication. Avoidance of the installation on sensitive areas.	RANGER is a civil protection oriented project.
Other issues (new issues during the second round of the SIA)		
Ethical challenges with machine learning? -The risk for “False Positive” and False Negative” decisions made with the help of RANGER services.	Transparency of the system for the end-users. Triangulation of the data. (the use of several data sources)	No Ethical issues have been raised during the pilot demonstrations.
Interference with other (military) radar systems?		The frequencies are certified for radar purposes by the national authorities.
The policy to share data between administration in several countries (outside CISE as a stand-alone system).		This is an action that will be defined per case. In any case RANGER consortium is going to follow the EU regulations

Table 7: The Mitigation of Ethical and Legal Barriers

5.3 The Benefits of RANGER

The table below identifies the various positive impacts RANGER may have on the fulfilment of fundamental/human rights as well as on other ethical and social values (way of life, fears, culture and community, political systems, environment, health and safety, property and personal rights).

Target group	Benefits
Maritime surveillance in general	<p>Cost savings (investment + maintenance).</p> <p>Surveillance 24H/7days instead of patrols.</p> <p>Better coverage with less money (acquisition and maintenance).</p> <p>The responsibilities of e.g. fishing boats for SAR operations will diminish (>not so much economic losses because of the time spent in those operations).</p> <p>Improvements and effectiveness in operational level in tracking ships</p> <ul style="list-style-type: none"> -early warning alarms with more accuracy -international collaboration -faster identification of threats. <p>Better working environment (compared with patrol boats).</p> <p>Benefits in the logistics (e.g. estimating times of arrivals to ports).</p>
Irregular immigrants	<p>Security and saving lives by preventing illegal and/or inappropriate sea traffic.</p> <p>Diminishing human trafficking.</p>
European citizen's	<p>Way of life and security: less pirates, less terrorism at sea, less smuggling of both drugs and arms, less illegal immigration, less losses of life at sea.</p> <p>Health and well-being: less smuggling of drugs and other illegal goods.</p> <p>Culture and community: Better controlled illegal immigration.</p> <p>Environment and healthier sea areas: less emissions in sea surveillance and more effective detection of oil spilling. This will benefit environment itself, but also tourism businesses and even people's health (because of less polluted sea fauna).</p> <p>Personal and property rights and economic benefits: new technology businesses, less pirate products diminishing fair businesses and destroying brands, more tax revenues thanks to more effective customs, less ships accidents and even lower insurance costs, lower business costs in transporting due to diminished risk to susceptible to piracy, prevention of accidents at the sea, less illegal fishing and therefore better fair fishing business and jobs.</p>
Research and business in general	<p>Innovative techniques to process data (data fusion, machine learning).</p> <p>Industry: new markets and businesses, also side uses e.g. in meteorology.</p> <p>Provides general user requirements beyond what ranger can actually cover.</p> <p>Creating jobs during the Research.</p>
Other issues	<p>European integration and increased collaboration.</p> <p>Shows that the country is involved in project to increase its capabilities for SAR, against smuggling and illegal immigration.</p> <p>International security.</p>

Table 8: Benefits the RANGER provides

6 RANGER Code of Conduct

This Code of Conduct is designed based on the contents of the previous sections. It establishes seven points of principles which should be taken into consideration when developing, implementing and using the RANGER-technology. These principles are to be further integrated to the other Codes of Conducts of the RANGER end-users. In addition it is essential to remember that Code is a living document.

RANGER code of conduct

1 The Justification of RANGER is Based on Ethical Grounds

The adoption of new Maritime Surveillance technologies in border control and other such activities easily gives rise to tension concerning fundamental and human rights such as the rights to freedom, security and justice. RANGER is no exception to this. It is therefore vital that its use can be justified on ethical grounds: RANGER must respect fundamental rights and other applicable legislations, regulations and values. An ethically conscious approach is important also to enable the sustainable competitiveness of RANGER and its various components.

The challenges – but also opportunities - stemming from numerous ethical, societal and legal viewpoints have implications on both the technology and user processes of RANGER, as well as on decision making and the future governance and business models of RANGER. Establishment of a dynamic review process of the system in order to take into account the evolving technologies in this area as well as future changes in the legal and ethical framework is essential.

RANGER does not endorse any operations not strictly adhering to regulations. It is also required that a context-specific Societal Impact Assessment (SIA) is conducted as part of each implementation of the solution, and the use of sunset provisions (3-5 years) is recommended.

2 Humanitarian imperative and rights of the people at sea

Duty to Render Assistance is the hallmark of SAR regulation.

The most important contribution of RANGER will be to significantly progress the accuracy and long-distance detection, identification and recognition capacity for small boats, thus drastically improving the response and intervention capacity of European SaR services and personnel, severely reducing the expected number of casualties in the Mediterranean basin. Furthermore, early detection of vessels with unusual behaviour allows interventions to occur before any incident occurs that would require a SaR operation. This will save lives at sea.

The human rights and dignity of the people at sea need to be respected, regardless of their origin or nationality. The information RANGER collects (combined with other data) people's age, race, gender, religion, physical condition etc. should not be used for discrimination or other unethical purposes.

Non-refoulement is a core principle of international refugee law which means that a refugee should never be returned to a country where they face threats to their life or freedom. RANGER enables an effective identification vessel on high seas and even on the territorial waters of third countries. It is therefore technically possible that RANGER will be used to enable to organise border control outside countries' own borders and to redirect intercepted migrants to the coasts of third states. One key challenge for RANGER is to prevent the creation of such processes.

3 Privacy, data protection and data management

“**The privacy** of those who navigate at the sea (especially those in vulnerable position, e.g. refugees, victims of human trafficking) **must be protected** wherever the RANGER technology and information is used and available. Sensitive RANGER data shall not be used for media purposes.

It must be kept in mind, **that non-personal data may become personal data**, and non-sensitive data may become sensitive following their transmission to another user, as this user may hold other relevant information that is combined with the exchanged data (for example information combined with different data layers in CISE).

Privacy and data protection measures must be embedded in the RANGER technology **to achieve compliance** with both the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED). RANGER Procurement Strategies/Adoption Models and Training materials **must be provided to give guidance in** organizational arrangements to ensure data protection. **The conducting of a** Data Protection Impact Assessment (PIA) is a compulsory part of each RANGER configuration and business model, including establishment of clear lines of responsibility, where each agent dealing with data is responsible for ensuring appropriate levels of protection.

In addition to privacy and data protection, even other legal and ethical aspects, such as IPR’s, must be considered in data management and organizational arrangements.

4 Involvement of end-users

RANGER will provide an improved maritime awareness picture and give authorities more time to plan and act more proactively. This means changes to the daily work of different end-user groups, e.g. coast guards, search and rescue team. It is important that end users are involved in the RANGER development throughout the project. Furthermore, end users should also represent different levels of maritime surveillance and other actors (search and rescue, border control, fisheries control, customs, environment, general law enforcement).

The training of the operational personnel is a necessary part of the implementation of RANGER-technology.

5 Moral division of labour and respecting of sovereignty

RANGER will provide an improved detection range compared to the current radar systems. It will be possible that new technology will affect the division of labour between EU member states. Some states might become free riders regarding with surveillance activities and costly investments. Responsibilities between member states and the moral division of labour in maritime surveillance should be discussed.

Third states are sovereign in their coastal waters and using RANGER-technology in such third states’ coastal waters should be carried out in the framework of cooperation agreements with these states and in conformity with international law and regulations.

Third countries in the Mediterranean should be seen as RANGER end-users, as well as real partners solving the joint problem with new technology.

6 Transparency, Robustness and Accountability

Systems using Machine Learning and Artificial Intelligence can be used to empower human beings, allowing them to make informed decisions. At the same time, mindfulness of the associated risks is to be emphasised and proper oversight mechanisms must be established. This

can be achieved through human-in-the-loop, human-on-the-loop, and human-in-command approaches.

Machine Learning (and Artificial Intelligence) systems like RANGER must be resilient, secure accurate, reliable and reproducible.

Mechanisms to ensure responsibility and accountability for RANGER Machine Learning systems and their outcomes must be established. Accountability and learning must be embedded in the functionalities, and proper user guidelines of RANGER shall be provided. Transparency and on the accountability of RANGER and its information management and use must be prioritised.

Table 9: RANGER Code of Conduct

Summary

When it comes to ethics, a question is often more important than the answer. This is because for someone to raise a question, he or she had to ponder it first in his or her mind, thus ethical thinking had to happen. And only when thinking first, ethics can materialise into action, into a project and end-results (including practices and processes) that are both societally acceptable and ethically sustainable.

Therefore, on one hand, this deliverable (and the ethical work done throughout during the project) aims to help ask questions. During the RANGER project, all involved were kept interested, if not forced, and encouraged questioning the ethical aspects of both performing the project's activities but also about the end-results, ultimately: will RANGER produce results that are suitable for the market also from ethical point-of-view.

During the RANGER project, two deliverables of the same titled were produced (D3.1 and D3.2). In the initial version deliverable (D3.1) one major aim was to gather the possible ethical requirements for RANGER's end-results. In this latter version (D3.2) the work is project work is practically done, and thus this deliverable is more reflecting to the tasks performed, and giving more general recommendations for the future. This deliverable is thus for all interested in maritime surveillance.

Therefore, this deliverable described the contexts (in plural): RANGER solutions and the maritime security and surveillance ethics and legalities. In this deliverable were examined and presents the various challenges from SaR to immigration, and to different tensions that affects RANGER, too. Then, the “tools” for analysing ethical and other problems were presented, and the results are shown. Finally, the RANGER Code of Conduct is set out. This code contains of ethical and moral principles according which RANGER, both the project and the results, were done, but it sets the principles according which the results should be developed further. It is the ethical legacy of RANGER (not to be confused with legacy systems).

In short, this deliverable ensures that RANGER's justification was based on ethical grounds, the project followed humanitarian imperative, took into account the moral division of labour, stressed the importance of value creation, aimed to ensure transparency, liability, and human decision making, protected privacy, emphasised data management and quality, and last but not least respects the rights of people and European values.

Final note:

In addition to this work visible in this deliverable, here in the summary must be acknowledged some additional work that was done but did not materialised as individual and separate deliverables to be reported to the EC. These were the Privacy Impact Assessments that RANGER performed for the four demonstration pilots. Therefore, it is our pleasure to present the PIA for an interested reader, who can find them in the attachments: in short, privacy concerns were not an issue in RANGER. (Annex C)

Also, in the attachment reader can find the review of RANGER's Ethical Experts about the ethical work done in RANGER. (Annex B)

Annex A - References & Relevant Readings

- Amnesty International (2014) *The Human Cost of Fortress Europe*. London. Available online at <https://www.amnesty.org/download/Documents/8000/eur050012014en.pdf> (Accessed 9.12.2019).
- ASSERT (2014): *ASSERT Toolkit for Societal Impact Assessment in Security Research*. ASSERT project. Retrieved from: <http://assert.maisondx.com/>(Accessed 9.12.2019).
- Bellanova et al. (2012). *Supporting fundamental rights, privacy and ethics in surveillance technologies* (SAPIENT). Deliverable 1.1. Smart surveillance – Stated of the Art, 23 January 2011.
- Council of Europe (2010). *European convention on Human Rights*. Retrieved from: http://www.echr.coe.int/Documents/Convention_ENG.pdf (Accessed 9.12.2019).
- European Agency for Fundamental Rights (2013). *Fundamental Rights at Europe's Southern Sea Borders*, Luxembourg.
- European Commission (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Retrieved from: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> (Accessed 9.12.2019).
- European Commission (2011). Commission Staff working document. Accompanying Document to the communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of Regions. Examining the Creation of a European Border Surveillance System (EUROSUR). Impact Assessment. Brussels: European Commission. (COM 2011)
- European Commission (2014). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Better situational awareness by enhanced cooperation across maritime surveillance authorities: next steps within the Common Information Sharing Environment for the EU maritime domain
- European Commission (2015). A Europa Agenda on Migration. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels: European Commission.
- European Commission (2016) TIETOSUOJAUDISTUS (ACT JA DIRECTIIVI)
- European Group on Ethics in science and new technologies (2014). Ethics of Security and surveillance Technologies. Opinion 28. European Commission, Brussels.
- European Parliament and European Council (2014) REGULATION (EU) No 656/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing rules for the surveillance of the external sea borders in the context of operational cooperation coordinated by the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union. (EU 2014)
- François Crépeau (2013). Regional study: management of the external borders of the European Union and its impact on the human rights of migrants, 24 April 2013
- Frontex (201) Ethics of Border Surveillance –report.

- Hayes B and Vermeulen M (2012). Borderline The EU's new Border Surveillance Initiatives. Assessing the costs and fundamental rights implications of EUROSUR and the smart borders proposals. Heinrich Boll Stiftung.
- High-Level Expert Group on AI (AI HLEG) (2019). *Ethics Guidelines for trustworthy AI*. European Commission: Brussels. Available online at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419 (Accessed 9.12.2019).
- Hojtink M (2014). Capitalizing on emergence: The “new” civil security market in Europe. Security Dialogue. Vol 45(5), p. 458-475.
- Human Rights Watch (HRW) (2009). *Pushed Back, Pushed Around. Italy's Forced Return of Boat Migrants and Asylum Seekers, Libya's Mistreatment of Migrants and Asylum Seekers*. Available online at: <https://www.hrw.org/report/2009/09/21/pushed-back-pushed-around/italys-forced-return-boat-migrants-and-asylum-seekers> (Accessed 9.12.2019).
- International Association for Impact Assessment (n.d.) Social Impact Assessment. Overview & History. Retrieved from <https://www.iaia.org/wiki-details.php?ID=23> (Accessed 9.12.2019).
- Jeandesboz J (2011). Beyond the Tartar steppe: EUROSUR and the ethics of European border control practices. In Burgess J and Gutwirths S. (eds.) Migration and Integration. Institute for European Studies Series.
- M Jimenez (2013) European border surveillance system: humanitarianism and (in)security for sale? Master thesis. University of Amsterdam.
- Marin L (2013) Protecting the EU's borders from ...fundamental rights? In R Holzhaecker & P Luif (eds.) Freedom, Security and justice after Lisbon. New York: Springer.
- Meijers Committee (2012). Note of the Meijers Committee on the proposal for a Regulation establishing the European Border Surveillance System 12.9.2012
- RANGER project (2016) Grant Agreement. European Commission, Directorate General for Migration and Home Affairs, “Grant Agreement number 700748 ‘RANGER’”, Annex 1 (part B).
- Report of the United Nations Special Rapporteur on the human rights of migrants, François Crépeau - Regional study: management of the external borders of the European Union and its impact on the human rights of migrants, 24 April 2013, A/HRC/23/46.
- Rijpma J and Vermeulen M (2015). EUROSUR: saving lives of building borders? European security vol. 24 nr. 3, 454-472.
- Societal Impact Expert Working Group (2012). *Societal Impact Expert Working Group EC DG ENTR Report*. CIES. Retrieved from: <http://cies.ie/wp-content/uploads/2014/05/Report-of-the-Societal-Impact-Expert-Working-Group.pdf>
- Sombetzki P and Quicker J (2016). European border surveillance system running a self-fulfilling circle. MarRBLE research papers. Vol. III.
- Sunny project (2014) Deliverable 1.4: Surveillance societal and Ethical Aspects. Project co-funded by the European Commission within the Seventh Framework Programme.




D3.2 – SOCIETALLY ACCEPTABLE AND ETHICALLY
SUSTAINABLE WAY OF PERFORMING MARITIME
SURVEILLANCE

United Nations (1982). The United Nations Convention on the Law of the Sea.

Vanclay, F., and Esteves, A.M (Eds.) (2011). *New directions in Social Impact Assessment. Conceptual and Methodological Advances*. Cheltenham (UK).

Annex B – The Review of the Ethical Experts

- 1) Feedback from Prof. Lilian Mitrou after the 2nd pilot in Greece (two pages extract, relevant to ethics):



Handbook 2nd Greek Pilot

Ethics and Data protection


Consent forms and data protection of pilot participants

1. Consent forms will be collected from end-users and other stakeholders taking part in the RANGER pilots.
2. The contact information of the participants (including name, organisation, email or other contact information) will be kept in separate files, which are accessible only for the party responsible for the organisation of the pilot. The files will be destroyed after the project.
3. The signed consent forms will be archived by Laurea University of Applied Science / Ethics management, and destroyed after the project.
4. The pictures and/or videos taken for the dissemination purposes will be used only in the dissemination material of the RANGER project. The active sharing/promoting/posting will be terminated once the project ends. This dissemination channels includes RANGER webpages, LinkedIn, Twitter and Newsletter.

RANGER platform and processing of personal data

1. The only RANGER data from which persons could be identified indirectly when combined with other external data sources outside the RANGER platform, is the AIS data including vessel identification number. In addition user credentials are collected in order to manage RANGER access rights.
2. AIS and radar tracks data are used in phase 2 pilots, but the pilots report only info related to vessel characteristics, position, speed, and course. Persons cannot be identified directly or indirectly from this reported data. AIS data, including vessel identification

17



Handbook 2nd Greek Pilot

information, will be stored only for each trial and will be destroyed after the project.

3. Privacy Impact Assessment (PIA) including more detailed information on privacy and data protection of the RANGER platform will be finalized as part of the second phase pilot and its validation.

RANGER code of conduct

RANGER Code of Conduct is designed for the developers and for the various end-users of the RANGER. It establishes 7 points of principle which should be taken into consideration when developing and using the RANGER-technology

- 1) Feedback from Prof. Jean-Guy Fontaine after the 2nd pilot in Greece (two pages extract, relevant to ethics):

RANGER
H2020-700478
RAAdars for loNG distance maritime surveillancE and Search and Rescue operations

2nd GREEK PILOT and Workshop

19th-20th November 2019 CHANIA (Greece)

Report from
Jean-Guy FONTAINE
Ethics Independent Expert

The 2nd Greek pilot was held in Chania and took place at “Maleme” military Airport and the workshop in 115CW AB in Chania Crete.

The 2nd Greek pilot was set in 7 steps during that day.
With these 7 steps, a complete global view of the different scenario was demonstrated in real time at sea. During this pilot, it has to be noted the great interest of the audience for the demonstration. This clear presentation included questions and answers. Very precise details were addressed and explained.

I noted the full commitment of all the partners to the presentations. The Ethics and Data protection has been clearly stated from the very beginning. All participants were invited to fill a consent form. Information are clearly stated and kept in a separate file.

All documents are kept separately by one partner of the project: LAUREA. Files are to be destroyed (not simply delayed!) by the end of the project. Dissemination related to the project are considered for the future with the same protecting goal.

An interesting point, in this project, is that Ethics and Data protection are included from the very beginning of the project. It is a fundamental asset and this project has shown its full compliance. Indeed, such an approach is a key of the success: Ethics and Data protection are part of the project and not addressed on top of the project. It is included by essence and by design.

Two major outputs should be pointed out: an early awareness of the consortium of such a sensitive subject on one hand and on the other hand, a broader view already set for any final user. In such

a way, Ethics and Data protection encapsulate sensitive matters like AIS identification, vessel identification, credential as well as radar’s identification. It is clear that: “persons cannot be identified directly or indirectly from reported data including vessel identification”.

In a nutshell RANGER is not only the demonstration of different kind of sensors but a platform sufficiently open to different technologies. It is an early warning system with a uniform communication gateway delivering information to a user interface and CISE interoperability. Within the detection of anomalies, search and rescue operations are very well addressed.

Annex C – Ethical & Societal Compliance Check –table (of this D3.2 deliverable)

In this table there are summarized the ethical and societal guidelines for the RANGER solution. The table is originally defined in the D3.1. “*SOCIETALLY ACCEPTABLE AND ETHICALLY SUSTAINABLE WAY OF PERFORMING MARITIME SURVEILLANCE*”. Please make this ethical compliance check of each of RANGER deliverable with the help of this table and fill in the needed information in the column “How are the guidelines applied?”. Finally attach the table as an annex in the deliverable in case.

Deliverable		D3.2
Activity	Main Responsibility	How are the guidelines applied?
1	<p>Development of RANGER Code of Conduct and follow-up of the current discussion on maritime surveillance</p> <p>The initial RANGER Code of Conduct provided in chapter 4 is to be developed and specified more in detail during the RANGER project. Separate versions of the Code of Conduct are needed for RANGER as stand-alone version and for RANGER as part of EUROSUR/CISE.</p>	<p>Project management and ethics committee working.</p> <p>Updated Code of Conduct is provided in chapter 6.</p>
2	<p>Legal framework follow-up regarding maritime surveillance and its technology</p> <ul style="list-style-type: none"> Especially since RANGER may change the moral division of labor in maritime surveillance (e.g. in SAR where much more information will be available), it may even be a mean to change to the legislation (or how it will be interpreted) Follow both EU and local legislation and standards (radiation, environment, NATURA2000 etc.) from the design phase of the radars. Be especially aware of the changing legislation. 	<p>Each WP in case.</p> <p>These challenges are discussed in this deliverable in chapter 4. In addition RANGER Code of Conduct highlights the need for ethical and legal follow up (point 1).</p>
3	<p>Proper understanding of maritime surveillance operations & involvement of end-users</p> <ul style="list-style-type: none"> End-users are to be involved in the project during its <u>whole life span</u>. End-users should come from various levels of maritime surveillance and from various operations in EU and member states (search and rescue, border control, fisheries control, customs, environment). Representatives from the third countries from Mediterranean coast site also to be involved in project, as well as various non-government organizations. <p>In addition make it sure that in the research work with the end-users consent forms are always collected and the collection & processing of personal data is avoided</p>	<p>All the work-packages working with end-users.</p> <p>The importance of the end-user involvement also after the RANGER project is emphasized in the RANGER Code of Conduct (point 4).</p>

4	<p>EUROSUR/CISE collaboration in ethics work</p> <p>Since EUROSUR and CISE probably has already taken into account the critics of forgetting humanities in favour of security and new businesses, it is crucial that RANGER’s interoperability and compliance with EUROSUR and CISE covers also these ethical issues (not only technology). This includes especially the following issues:</p> <ul style="list-style-type: none"> • Non-refoulement and the use of RANGER radar to detect vessels on high sea and on the water territories of third counties. • Seeking for the solution how we will deliver the long-distance information RANGER provides also to neighbouring third counties so that they can also enhance their SAR activities. • Seeking for the fair moral division of labour in providing assistance in a situation in which we constantly get distress information outside country’s own SAR –regions. 	<p>Project management team (with the help of ethics committee)</p>	<p>These issues are discussed in this deliverable in chapter 4. In addition Ranger Code of Conduct highlights these issues (point 2 and 5).</p>
5	<p>RANGER business/governance modelling</p> <ul style="list-style-type: none"> - RANGER as stand-alone solution, and especially its user processes and business/business model need to be designed carefully, including the user training and selling/procurement strategy which avoids the biased use of RANGER in border control and SAR. - Productizing a feasibility study and societal impact assessment about RANGER and its use in the proposed area before the implementation as part of the “RANGER package”, including needed activities to eliminate undesirable consequences beforehand. - When selling RANGER as stand-alone solution, follow up of the consequences of the use of RANGER technology is needed to provide as part of the “RANGER service package”. - Selling RANGER only for the use of municipalities or other authorized bodies (>the avoidance of the misuse and dual-use) - Licensing 	<p>WP 8</p>	<p>These issues are highlighted in Code of Conduct (point 1).</p>
6	<p>Design of the RANGER technology/Data management and security</p> <ul style="list-style-type: none"> - “Privacy by design” and other requirements (anonymizing etc.) defined in the coming new Data Protection legislation (Act + Directive). - Specific Data security standards are to be followed - User logs as part of the system. - Check and balance approach 	<p>Technical partners</p>	<p>Fundamental rights and data protection issues are discussed as part of the deliverable in chapter 3. In addition these are highlighted in Code of Conduct (points 3 and 8).</p>

	<ul style="list-style-type: none"> - Limit the access to the RANGER data only to relevant authorities (access rights, ranger business modelling) - Rules & regulation on the use of data 		
7	<p>Design of the RANGER technology/ The modifications of the user interface according the users background/maritime surveillance aspect</p> <ul style="list-style-type: none"> - SAR criterion, human rights and other ethical guidelines should be taken into account when developing the RADAR technology, its processes and business model. - The language and terminology of the user interface should serve each aspect of maritime surveillance (by taking into account the status of the user logged in) 	Ethics committee and technical partners	The importance of SAR and the importance of end-user collaboration also after the RANGER project is emphasized in the Code of Conduct (points 1 and 4).
8	<p>Design of the RANGER technology/Physical design of the radar antennas</p> <p>Hire industrial designer etc. to create beautiful antennas and radars.</p>	WP 4	N/A
9	<p>Continuous societal impact assessment of RANGER during the project</p> <ul style="list-style-type: none"> • Joint societal impact assessment with all the work packages will be done in the mid and end of the project under the work of ethics committee and documented in D3.2. This concern especially the Mediterranean area where the system is to be piloted. Also expertise from other areas than maritime surveillance are needed in order to figure out the impacts on society (e.g. irregular immigration) • In addition each wp is expected to conduct SIA among their own stakeholders 	Ethics committee and each work-package	Updated SIA is provided in the deliverable in chapter 5.
10	<p>Communication and dissemination</p> <ul style="list-style-type: none"> - Good PR and information with local communities. Make communities understand both the benefits are disadvantages - It is necessary in the RANGER dissemination and communication use the terms “irregular” “asylum” and “illegal” in a logical and informative way. 	WP 8	N/A
11	<p>Guidelines for the installation and use of the system</p> <ul style="list-style-type: none"> - Rules & regulation on the use of data. Training as part of the RADAR implementation on necessary also from this point of view. - Consider environmental studies when installing the antenna, and be in contact with archaeological experts before installing the system. Have agreements from local/national authorities to install and use HF waves 	WP 7 + trials	N/A

	<ul style="list-style-type: none"> - The installation of the radars in a places which are already occupied for same kind of activities (e.g. military bases) - Choose the right location for the radar that doesn't cause problems to the nature, archaeological sites, tourism. To mitigate human exposure in radiation, the OTH radars can be located in unpopulated areas. Further minimize the power levels by improving the directivity of the radar. - Safety instructions are also needed for installing radars and doing maintenance work. 		
12	<p>Follow-up of the implementation of these guidelines</p> <p>Work Packages (WPs) and their deliverables (in which an ethical and societal compliance check is to be added as an annex of each deliverable).</p>	Each WP	done

Annex D – Ethical & Societal Compliance Check –table (template)

In this table there are summarized the ethical and societal guidelines for the RANGER solution. The table is originally defined in the D3.1. “*SOCIETALLY ACCEPTABLE AND ETHICALLY SUSTAINABLE WAY OF PERFORMING MARITIME SURVEILLANCE*”. Please make this ethical compliance check of each of RANGER deliverable with the help of this table and fill in the needed information in the column “How are the guidelines applied?”. Finally attach the table as an annex in the deliverable in case.

Deliverable		Dx.x	
Activity		Main Responsibility	How are the guidelines applied?
1	<p>Development of RANGER Code of Conduct and follow-up of the current discussion on maritime surveillance</p> <p>The initial RANGER Code of Conduct provided in chapter 4 is to be developed and specified more in detail during the RANGER project. Separate versions of the Code of Conduct are needed for RANGER as stand-alone version and for RANGER as part of EUROSUR/CISE.</p>		
2	<p>Legal framework follow-up regarding maritime surveillance and its technology</p> <ul style="list-style-type: none"> Especially since RANGER may change the moral division of labor in maritime surveillance (e.g. in SAR where much more information will be available), it may even be a mean to change to the legislation (or how it will be interpreted) Follow both EU and local legislation and standards (radiation, environment, NATURA2000 etc.) from the design phase of the radars. Be especially aware of the changing legislation. 		
3	<p>Proper understanding of maritime surveillance operations & involvement of end-users</p> <ul style="list-style-type: none"> End-users are to be involved in the project during its <u>whole life span</u>. End-users should come from various levels of maritime surveillance and from various operations in EU and member states (search and rescue, border control, fisheries control, customs, environment). Representatives from the third countries from Mediterranean coast site also to be involved in project, as well as various non-government organizations. <p>In addition make it sure that in the research work with the end-users consent forms are always collected and the collection & processing of personal data is avoided</p>		
4	<p>EUROSUR/CISE collaboration in ethics work</p>		

	<p>Since EUROSUR and CISE probably has already taken into account the critics of forgetting humanities in favour of security and new businesses, it is crucial that RANGER's interoperability and compliance with EUROSUR and CISE covers also these ethical issues (not only technology). This includes especially the following issues:</p> <ul style="list-style-type: none"> • Non-refoulement and the use of RANGER radar to detect vessels on high sea and on the water territories of third counties. • Seeking for the solution how we will deliver the long-distance information RANGER provides also to neighbouring third counties so that they can also enhance their SAR activities. • Seeking for the fair moral division of labour in providing assistance in a situation in which we constantly get distress information outside country's own SAR –regions. 		
5	<p>RANGER business/governance modelling</p> <ul style="list-style-type: none"> - RANGER as stand-alone solution, and especially its user processes and business/business model need to be designed carefully, including the user training and selling/procurement strategy which avoids the biased use of RANGER in border control and SAR. - Productizing a feasibility study and societal impact assessment about RANGER and its use in the proposed area before the implementation as part of the “RANGER package”, including needed activities to eliminate undesirable consequences beforehand. - When selling RANGER as stand-alone solution, follow up of the consequences of the use of RANGER technology is needed to provide as part of the “RANGER service package”. - Selling RANGER only for the use of municipalities or other authorized bodies (>the avoidance of the misuse and dual-use) - Licensing 		
6	<p>Design of the RANGER technology/Data management and security</p> <ul style="list-style-type: none"> - “Privacy by design” and other requirements (anonymizing etc.) defined in the coming new Data Protection legislation (Act + Directive). - Specific Data security standards are to be followed - User logs as part of the system. - Check and balance approach - Limit the access to the RANGER data only to relevant authorities (access rights, ranger business modelling) - Rules & regulation on the use of data 		

7	<p>Design of the RANGER technology/ The modifications of the user interface according the users background/maritime surveillance aspect</p> <ul style="list-style-type: none"> - SAR criterion, human rights and other ethical guidelines should be taken into account when developing the RADAR technology, its processes and business model. - The language and terminology of the user interface should serve each aspect of maritime surveillance (by taking into account the status of the user logged in) 		
8	<p>Design of the RANGER technology/Physical design of the radar antennas</p> <p>Hire industrial designer etc. to create beautiful antennas and radars.</p>		
9	<p>Continuous societal impact assessment of RANGER during the project</p> <ul style="list-style-type: none"> • Joint societal impact assessment with all the work packages will be done in the mid and end of the project under the work of ethics committee and documented in D3.2. This concern especially the Mediterranean area where the system is to be piloted. Also expertise from other areas than maritime surveillance are needed in order to figure out the impacts on society (e.g. irregular immigration) • In addition each wp is expected to conduct SIA among their own stakeholders 		
10	<p>Communication and dissemination</p> <ul style="list-style-type: none"> - Good PR and information with local communities. Make communities understand both the benefits are disadvantages - It is necessary in the RANGER dissemination and communication use the terms “irregular” “asylum” and “illegal” in a logical and informative way. 		
11	<p>Guidelines for the installation and use of the system</p> <ul style="list-style-type: none"> - Rules & regulation on the use of data. Training as part of the RADAR implementation on necessary also from this point of view. - Consider environmental studies when installing the antenna, and be in contact with archaeological experts before installing the system. Have agreements from local/national authorities to install and use HF waves - The installation of the radars in a places which are already occupied for same kind of activities (e.g. military bases) 		

	<ul style="list-style-type: none"> - Choose the right location for the radar that doesn't cause problems to the nature, archaeological sites, tourism. To mitigate human exposure in radiation, the OTH radars can be located in unpopulated areas. Further minimize the power levels by improving the directivity of the radar. - Safety instructions are also needed for installing radars and doing maintenance work. 		
12	<p>Follow-up of the implementation of these guidelines</p> <p>Work Packages (WPs) and their deliverables (in which an ethical and societal compliance check is to be added as an annex of each deliverable).</p>		



*D3.2 – SOCIETALLY ACCEPTABLE AND ETHICALLY
SUSTAINABLE WAY OF PERFORMING MARITIME
SURVEILLANCE*

Annex E – The Privacy Impact Assessment



H2020-700478

RAAdars for loNG distance maritime surveillanceE and Search and
Rescue opERations

1ST GREEK PILOT – PRIVACY IMPACT ASSESSMENT (PIA)

Date:	19 th September 2019
Location:	Maleme - Chania (Greece)
Classification:	Restricted
Editor(s):	LAU - ICCS
Contract start date:	May 1 st , 2016
Duration:	42 months
Project coordinator:	EXUS SOFTWARE LTD. (UK)
Partners:	EXUS (UK), DXT (FR), ICCS (GR), TUD (DE), LAU (FI), FNM (IT), TEL (GR), NATO (BE), HMOD (GR), DMA (FR)

This work was performed within the RANGER Project, with the support of the European Commission and the Horizon 2020 Programme, under Grant Agreement No.700478.





Table of Contents

<i>About RANGER</i>	1
<i>RANGER Privacy Impact Assessment (PIA)</i>	2
<i>Context</i>	3
Overview	3
Data, processes and supporting assets	5
<i>Fundamental principles</i>	10
Proportionality and necessity	10
Controls to protect the personal rights of data subjects	14
<i>Risks</i>	17
Planned or existing measures	17
Illegitimate access to data	22
Unwanted modification of data	23
Data disappearance	24
<i>Action plan</i>	28



PIA 1st Greek Pilot

About RANGER

RAAdars for loNG distance maritime surveillancE and Search and Rescue opeRations

RANGER is a European project, co-funded by the European Union's Horizon 2020 research and innovation programme. RANGER combines innovative Radar technologies with novel technological solutions for early warning, in view of delivering a surveillance platform offering detection, recognition, identification and tracking of vessels, beyond current radar systems' capabilities, thus drastically improving the response and intervention capacity of European Search and Rescue services.

Today, sea-border surveillance and the monitoring of maritime traffic within the Exclusive Economic Zone (EEZ) are of critical importance, especially for the Mediterranean Sea. Widespread irregular immigration, criminal trafficking, piracy and terrorism threats needs to be addressed in order to ensure maritime security. However, while Europe needs to have the capability to act in response to the numerous crises occurring within its maritime environment, current maritime surveillance is no longer adequate to cope with these challenges.

RANGER RAAdars for loNG distance maritime surveillancE and SaR operations European project is designed to address these issues by providing novel technologies that enable more effective Search and Rescue operations and crime confrontation in maritime environment.

RANGER solution will contribute to the enhancement of maritime border security, Search and Rescue operations, and crime prevention capabilities (irregular immigration, human trafficking, smuggling, illegal fishing and other illegal activities) through radar systems capable of detecting small vessels over the horizon in different Mediterranean sites supported by data fusion and machine learning mechanisms that provide more accurate early warning alerts to coast guards or other authorities responsible for maritime security.



PIA 1st Greek Pilot

RANGER Privacy Impact Assessment (PIA)

Author's names

Karagiannidis, Lazaros (ICCS)
Rajamäki, Jyri (LAU)
Sarlio-Siintola, Sari (LAU)
Siintola, Saara (LAU)
Tammilehto, Tuomas (LAU)

Assessor's name

nn

Validator's name

nn

(Initial) Creation date

11/05/2019



Context

Overview

Which is the processing under consideration?

RANGER project will provide solution for vessel detection, recognition and identification capacities for marine traffic surveillance and search and rescue (SAR) operations.

Its Early Warning System (EWS) collects data from OTH and PE-MIMO radars, legacy systems, Automatic Identification System (AIS) and other available data sets.

This PIA concerns on the RANGER solution/platform to be created and piloted during the project. Thus, this PIA describes the technical preparedness that has been developed to ensure that the GDPR and LED compliance.

Processing of personal data in which persons can be identified directly or indirectly includes AIS data on vessels (> indirect identification) and personal data on RANGER developers, end-users and other stakeholders (> direct identification). When AIS data is linked to crew lists, location of persons will be exposed, and this is private data covered by the GDPR. In addition, the other available data sets connected to EWS can include personal data, or anonymized personal data. The RANGER solution includes a Machine Learning module, and via machine learning anonymized data can be de-anonymized. In case that in the future, new legacy systems, or other data from sensors (for example data of high definition cameras), are added to RANGER, those can include personal data. This must then be taken into account.

In addition to the RANGER solution and its development and piloting, personal data is processed as part of the following activities:



PIA 1st Greek Pilot

- RANGER websites collecting contact information for dissemination
- Contact information and pictures from research participants
- These are, however, excluded in this PIA. Their privacy and data protection is described in a separate Privacy and data protection policy.

What are the responsibilities linked to the processing?

The processor of RANGER personal data is the RANGER consortium jointly, based on the RANGER Grant Agreement.

Are there standards applicable to the processing?

AIS is a maritime technical standard developed by the International Maritime Organization (IMO). It is a radio technology combining GPS, VHF and data processing technologies to enable the exchange of relevant information in a strictly defined format between different entities.

Evaluation: Acceptable



Data, processes and supporting assets

What are the data processed?

RANGER processes multiple types of data. Below is shortly described all the data types in order to create an overall picture about the system in which also personal data (AIS, end-user data) is processed as part of various RANGER services.

OTH Radar tracks

Type of data: Location, speed and course of detected vessels.

Storage: AUI temporary storage (up to 2 hours). EWE storage (up to 2 days)

Recipients: UCG, EWE, AUI, Data Fusion, Machine Learning, CISE translation gateway

French AIS and Greek AIS data

Type of data: Maritime Mobile Service Identity (MMSI), location, speed, course etc. based on international AIS data regulations.

Storage: Storage: AUI temporary storage (up to 2 hours). EWE storage (up to 2 days)

Recipients: UCG, EWE, AUI, Data Fusion, Machine Learning, CISE translation gateway

French and Greek legacy radar tracks

Type of data: Location, speed and course of detected vessels.

Storage: AUI temporary storage (up to 2 hours). EWE storage (up to 2 days)

Recipients: UCG, EWE, AUI, Data Fusion, Machine Learning, CISE translation gateway

PE-MIMO Radar tracks

Type of data: Location, speed and course of detected vessels.



Storage: AUI temporary storage (up to 2 hours). EWE storage (up to 2 days)

Recipients: UCG, EWE, AUI, Data Fusion, Machine Learning, CISE translation gateway

Advanced User Interface (AUI) data

Type of data: (a) track data from OTH, PE-MIMO, and French and Greek legacy radar (Location, speed and course of detected vessels) (b) AIS data (Maritime Mobile Service Identity (MMSI), location, speed, course etc. based on international AIS data regulations.) (c) early warnings on detected anomalies (e.g. suspicious course changes, merged tracks etc.) (d) cartographic data.

Storage: AUI temporary storage (up to 2 hours). EWE storage (up to 2 days)

Recipients: AUI operator

Data Fusion data

Type of data: (a) track data from OTH, PE-MIMO, and French and Greek legacy radar (Location, speed and course of detected vessels) (b) AIS data (Maritime Mobile Service Identity (MMSI), location, speed, course etc. based on international AIS data regulations.)

Storage: AUI temporary storage (up to 2 hours). EWE storage (up to 2 days)

Recipients: UCG, EWE, AUI, Machine Learning, CISE translation gateway

Machine Learning data

Type of data: (a) track data from OTH, PE-MIMO, and French and Greek legacy radar (Location, speed and course of detected vessels) (b) AIS data (Maritime Mobile Service Identity (MMSI), location, speed, course etc. based on international AIS data regulations.)



(c) anomaly detections (e.g. suspicious course changes, merged tracks etc.)

Storage: AUI temporary storage (up to 2 hours). EWE storage (up to 2 days)

Recipients: EWE, AUI, CISE translation gateway

Uniform Communication Gateway (UCG) data

Type of data: (a) track data from OTH, PE-MIMO, and French and Greek legacy radar (Location, speed and course of detected vessels) (b) AIS data (Maritime Mobile Service Identity (MMSI), location, speed, course etc. based on international AIS data regulations.)

Storage: AUI temporary storage (up to 2 hours). EWE storage (up to 2 days)

Recipients: EWE, AUI

Early Warning Engine (EWE)

Type of data: (a) track data from OTH, PE-MIMO, and French and Greek legacy radar (Location, speed and course of detected vessels) (b) AIS data (Maritime Mobile Service Identity (MMSI), location, speed, course etc. based on international AIS data regulations.), (c) fused track data (e) early warnings on anomaly detections (e.g. suspicious course changes, merged tracks etc.)

Storage: AUI temporary storage (up to 2 hours). EWE storage (up to 2 days)

Recipients: Data Fusion, AUI, Machine Learning, UCG, CISE translation gateway

CISE translation gateway

Type of data: (a) track data from OTH, PE-MIMO tracks (Location, speed and course of detected vessels) (b) AIS data (Maritime Mobile Service Identity (MMSI), location, speed, course etc. based on international AIS data regulations.), (c) fused track data (e) early warnings on anomaly detections (e.g. suspicious course changes, merged tracks etc.)



PIA 1st Greek Pilot

Storage: AUI temporary storage (up to 2 hours). EWE storage (up to 2 days)

Recipients: CISE connected node

How does the life cycle of data and processes work?

The data flow diagram of Early Warning System is as an attachment. The EWE Data Storage stores at least indirect personal data! With regard to the EWE Data Storage, data destruction is not described.

All data consumed by UCG are streamed through the translation process (in case of AIS/Legacy), and merged into an aggregated message queue. This queue is served by the IVEF service to AUI and EWE IVEF clients. The streaming pipeline of processes uses small temporary buffers and no data history is saved permanently. Each message is instantly sent from the input queues to the output service as fast as possible.

What are the data supporting assets?

Uniform Communication Gateway (UCG) is the connecting link between RANGER project's Radar sensors, Legacy systems and AIS Systems with the Early Warning Engine (EWE) and the Advanced User Interface (AUI).

Operating system: Linux Debian

Protocols: TCP/IP, IVEF, SSL

Early Warning Engine (EWE) constitutes the back-end of the RANGER system, and is responsible for early detection of events, data storage and provision of warnings and alerts. It is the core element which is closely interdependent with the data fusion and machine learning module of the RANGER platform.

According to the protocols chosen for both internal and external EWE communication, the appropriate authentication and authorization methods will be chosen alongside with user management tools.



Data Fusion module main role is to take all the available measurements at a particular time step , that could be detections from different sensors (OTH radar, MIMO radar, detections from existing legacy systems, AIS data), and fuse them in order to obtain a set of tracks (routes), which are related to the existing targets in the current maritime scedata fusion module main role is to take all the available measurements at a particular time step , that could be detections from different sensors (OTH radar, MIMO radar, detections from existing legacy systems, AIS data), and fuse them in order to obtain a set of tracks (routes), which are related to the existing targets in the current maritime scene.

Machine Learning module will take input measurements from available sensors (OTH radar data, MIMO radar data, AIS data, legacy systems data) through the Data Fusion module, and employ machine learning methods to derive conclusions about the characteristics of the detected/tracked vessels and their behaviour.

The front-end of the Ranger system consists of the **Advanced User Interface (AUI)**. This interface is used in the standalone version of RANGER. The main goals of the AUI are to display the different tracks from RANGER providers (OTH, PE-MIMO, AIS, Legacy system, fused tracks)), to display early warnings related to marine incidents (abnormal behaviours etc. based on EWE Alerting Component), and to give the possibility at an operation to see RANGER information/data and early warnings/alerts on a selected tracks.

CISE translation gateway is a component that will allow the integration of the RANGER platform with the CISE network. In CISE terminology the “RANGER CISE translation gateway” will be an “Adaptor” between the CISE network and the RANGER platform.

Evaluation: Acceptable

Fundamental principles

Proportionality and necessity

Are the processing purposes specified, explicit and legitimate?

Maritime surveillance and SAR operations in EU are based on various international legislation, EU-level legislation and local legislation, including *United Nations Convention on the Law of the Sea (UNCLOS)*, *International Maritime Organization (IMO)* and *International Convention for the Safety of Life at Sea (SOLAS)*. As regards surveillance activities, a coastal State has the exclusive right to undertake monitoring and surveillance within its territory including territorial sea. A coastal State also has the exclusive right to undertake monitoring and surveillance in connection with the economic exploitation and exploration of its Exclusive Economic Zone. Furthermore, all states have the implied right to undertake monitoring and surveillance in the high seas, but not to the extent of interfering with the exercise of the freedom of the high seas by ships flying a foreign flag.

Processing personal data as part of the maritime surveillance and SAR operations is regulated in *General Data Protection Regulation (GDPR)* and the *Directive 2016/680 'on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data'* which both applies in RANGER context. GDPR applies during the development of RANGER platform and its piloting. Whereas in the operational use of RANGER in the future either Directive 2016/680 or GDPR applies based on the authority and the purpose for which RANGER is used. Therefore, both GDPR and Directive 2016/680 are to be taken into account in the development of RANGER.

Evaluation: Acceptable



What are the legal basis making the processing lawful?

Data processing during the pilot is done in order to test RANGER in maritime operations.

The lawfulness of processing personal data in maritime operations is based on A) Directive 2016/680 (article 1 and 8) and corresponding local laws when operations are related to crime prevention by competent authorities. B) General Data Protection Regulation (article 1 and 6) when operations are related to other activities (e.g. SAR).

GDPR applies during the pilots since controller is the RANGER consortium developing the RANGER solution. The lawfulness defined in GDPR article 6 includes the following:

- processing is necessary for compliance with a legal obligation to which the controller is subject
- processing is necessary in order to protect the vital interests of the data subjects or of another natural person
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Evaluation: Acceptable

Are the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')?

1) AIS data is needed in the following data fusion algorithms, such as:

- Threat classification based on AIS data, historical data and manoeuvring patterns of detected and tracked vessels.
- Automatic Target Recognition (ATR) through cross correlation of Radar and AIS data.
- *AIS is also collected and forwarded by UCG (ICCS) and EWE (also stored), and consumed by CISE (fused tracks).*
- ***AUI displays the AIS data without processing.***

2) Personal data on RANGER end-users is needed in order to manage RANGER access rights and accountability.

3) Personal data on RANGER developers and stakeholders that participate pilots is needed in order to manage RANGER access rights and accountability during the trials.

Evaluation: Acceptable



Are the data accurate and kept up to date?

AIS data: Quality of data is ensured by the AIS data providers: the French Navy and Greek Ministry of Defence. Furthermore, the AIS data collected and processed by the RANGER components is filtered within the Data Fusion module (need to ask NATO), so as to remove any erroneous or outdated data entries. No other post processing of the AIS data is performed by the other RANGER system components.

Radar track data (OTH and PE-MIMO radar tracks): The average OTH data accuracy is around 300m. The OTH data are updated continuously (with the period of 60 and 90 sec.) The OTH data are transferred to ULG based on IVEF format.

Legacy radar tracks: Quality of data is ensured by the legacy radar track providers, the French Navy and Greek Ministry of Defence, which have an internal filtering process to remove erroneous or outdated data entries.

UCG: UCG collects, translates and forwards AIS data, OTH and PE-MIMO radar tracks, and legacy radar tracks. AIS and legacy radar tracks quality of data: UCG validates the quality of data using checksums and content validation during data translation

OTH and PE-MIMO tracks: UCG validates the data based on XML schema and content inspection.

Evaluation: Acceptable



What are the storage duration of the data?

Storage time/Destroying of data from EWE Storage Database as well as from UCG and AUI temporary storage is un-defined in current MARISA technical documents.

Evaluation: Acceptable

Controls to protect the personal rights of data subjects

How are the data subjects informed on the processing?

The purposes for which RANGER controller processes AIS data do not require the identification of a data subject by the controller (see the GDPR article 11).

Pilot plan documents should describe what personal data is collected from participants during pilots, and how the data will be controlled.

Evaluation: Acceptable



If applicable, how is the consent of data subjects obtained?

n/a

Evaluation: Acceptable

How can data subjects exercise their rights of access and to data portability?

n/a

Evaluation: Acceptable

How can data subjects exercise their rights to rectification and erasure?

n/a

Evaluation: Acceptable

How can data subjects exercise their rights to restriction and to object?

n/a

Evaluation: Acceptable



Are the obligations of the processors clearly identified and governed by a contract?

According to GA, Plenary Board (PB) is the ultimate decision making body and has the highest level of authority in the project. The PB is chaired by the Project Coordinator.

Evaluation: Acceptable

In the case of data transfer outside the European Union, are the data adequately protected?

n/a

Evaluation: Acceptable

Risks

Planned or existing measures

Policy

RANGER guidelines on data protection are based not only on General Data Protection Regulation (GDPR), but also on Directive 2016/680, since Maritime Surveillance includes also operations related to crime prevention.

During the pilots GDPR is applied.

Evaluation: Acceptable

Encryption

From D4.2 VPN and TSL/SSL

Evaluation: Acceptable

Logical access control

From D4.2

Evaluation: Acceptable

Traceability (logging)

Session initiation logs (UCG) - Log in Management. **Similar Log management is installed with the AUI.** VPN connection logs.



PIA 1st Greek Pilot

Evaluation: Acceptable



Managing workstations

Workstations have no internet access. Periodically and controlled updates operating systems are planned, providing limited time internet access. Automatic locking of workstations is configured.

Evaluation: Acceptable

Maintenance

Maintenance is performed locally. Remote maintenance of SW and applications is allowed only using RANGER secure VPN solution.

Evaluation: Acceptable

Processing contracts

Partner must obtain the approval of the Contracting Authority before beginning negotiations with a view to subcontract (GA, Part B, p. 134).

Evaluation: Acceptable

Network security

From D4.2 firewalls, VLANs (network segmentation), VPN

Evaluation: Acceptable

Physical access control

During French pilot the RANGER platform will be installed in the Diginext premises which have a fence, an access control at entrance, and an electronic access at the main buildings. The Diginext premises have authorization for classified data processing.



PIA 1st Greek Pilot

During the Greek pilot the RANGER platform will be installed in the HMOD premises which have a fence, an access control at entrance, and an electronic access at the main buildings. The HMOD premises have authorization for classified data processing.

Evaluation: Acceptable

Hardware security

Need to ask all partners (if and what hardware security solution are available or planned?)

For the OTH

- 1) in the French pilots, the OTH servers are in the DXT premises with specific access authorization.
- 2) in the Greek pilots, the OTH servers are in the HMOD premises (Maleme air base) with specific access authorization.
- 3) in the French pilots the Rx site are located in private sites and installed in closed buildings or closed it cabinet.
- 4) in the Greek pilots the Rx site are located in HMOD premises (Heraklion) with specific access authorization.

Evaluation: Acceptable

Avoiding sources of risk

The main risk is to send data on a public network. The only link towards the outside is the CISE gateway. Risk mitigation with a VPN until CISE node.

Evaluation: Acceptable

Protecting against non-human sources of risks



PIA 1st Greek Pilot

The access to OTH sites are unauthorized. The electronic ports on the OTH systems on site are protected against other network.

Evaluation: Acceptable

Organisation

Ethics Manager is responsible to monitor the compliance of the project activities in respect to e.g. privacy and data protection norms, in cooperation with the Ethics Committee (GA Part B, p 50).

Evaluation: Acceptable

Illegitimate access to data

What could be the main impacts on the data subjects if the risk were to occur?

Unethical surveillance on individuals is illegitimate access to data manage to catch up the vessel id and connect it to other data sources.

What are the main threats that could lead to the risk?

Terrorism, Internal attack, External attack via CISE

What are the risk sources?

External human source, internal human source, Non-human source (e.g. a computer virus).

Which of the identified planned controls contribute to addressing the risk?

Physical access control, Traceability (logging), Encryption, Network security, Logical access control, Processing contracts.

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Limited, Hard to imagine very serious risks for the captain and personnel on the vessel

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Limited, AIS is publicly available information. RANGER itself does not necessary increase the risk for external attacks (only for internal). Or, does it with the sophisticated data fusions etc.?

Evaluation: Acceptable

Unwanted modification of data

What could be the main impacts on the data subjects if the risk were to occur?

Anonymised data becomes de-anonymised, Data subject mis-information

What are the main threats that could lead to the risk?

External attack via CISE, Internal attack, Terrorism?, Hacking

What are the risk sources?

External human source, Criminal elements, State-level operators, i.e. foreign intelligence services

Which of the identified controls contribute to addressing the risk?

Encryption, Logical access control, Maintenance, Network security

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Negligible

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Negligible, What could even be the interest of someone to modify the AIS data in RANGER?

Evaluation: Pending

Data disappearance

What could be the main impacts on the data subjects if the risk were to occur?

No risk for privacy.

What are the main threats that could lead to the risk?

External attack via CISE, Hacking, Internal attack, Terrorism

What are the risk sources?

Non-human source (e.g. a computer virus), Criminal elements, State-level operators, i.e. foreign intelligence services

Which of the identified controls contribute to addressing the risk?

Logical access control, Maintenance, Physical access control, Network security

How do you estimate the risk severity, especially according to potential impacts and planned controls?

























Negligible, This risk is related to the quality of RANGER (AIS processing), not to data protection as such.

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Limited

Overview







Fundamental principles

Purposes		
Legal basis		
Adequate data		
Data accuracy		
Storage duration		
Information for the data subjects		
Obtaining consent		
Right of access and to data portability		
Right to rectification and erasure		
Right to restriction and to object		
Subcontracting		
Transfers		

Planned or existing measures

		Policy
		Encryption
		Logical access control
		Traceability (logging)
		Managing workstations
		Maintenance
		Processing contracts
		Network security
		Physical access control
		Hardware security
		Avoiding sources of risk
		Protecting against non-human sources of risks
		Organisation

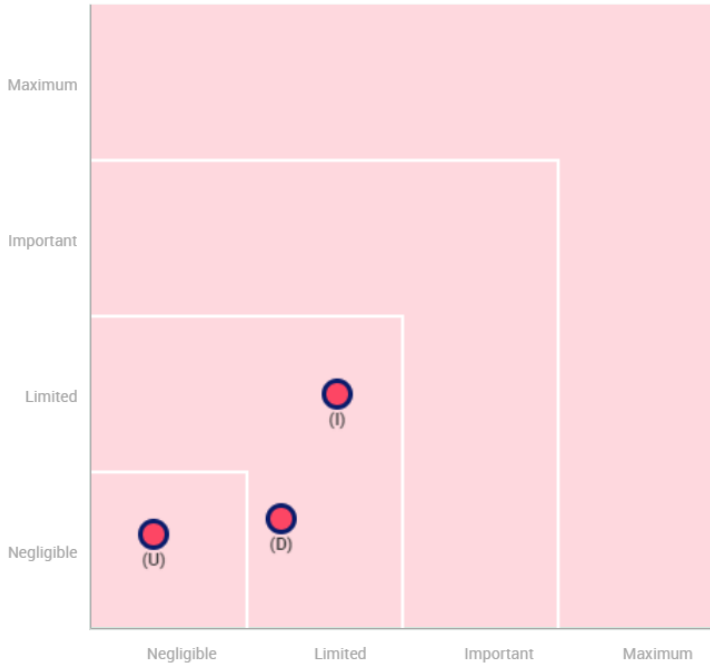
Risks

		Illegitimate access to data
		Unwanted modification of data
		Data disappearance

Improvable Measures

Acceptable Measures

Risk seriousness



- Planned or existing measures
- With the corrective measures implemented
- (I)illegitimate access to data
- (U)nwanted modification of data
- (D)ata disappearance

Risk likelihood

Potential impacts

- Unethical surveillance on i.
- Anonymised data becomes
- Data subject mis-informati
- No risk for privacy

Threats

- Terrorism?
- Internal attack
- External attack via CISE
- Hacking

Sources

- External human source
- Internal human source
- Non human source
- Criminal elements
- State-level operators, i.e....
- non-human source

Measures

- Physical access control
- Traceability (logging)
- Encryption
- Network security
- Logical access control
- Processing contracts
- Maintenance

Illegitimate access to data

Severity : Limited
 Likelihood : Limited

Unwanted modification of data

Severity : Negligible
 Likelihood : Negligible

Data disappearance

Severity : Negligible
 Likelihood : Limited



Action plan

The risk during the pilots are so small that there is no need for a specific action plan.

Therefore:

Fundamental principles

No action plan recorded.

Existing or planned measures

No action plan recorded.

Risks

No action plan recorded.