FORESIGHT

ADVANCED CYBER-SECURITY SIMULATION PLATFORM FOR PREPAREDNESS TRAINING IN AVIATION, NAVAL AND POWER-GRID ENVIRONMENTS

Grant Agreement: 833673

D3.3

Overall Legal and Ethical Framework

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 833673.

Document Information

Deliverable number:	**D3.3**
Deliverable title:	Overall Legal and Ethical Framework
Deliverable version:	1
Work Package number:	WP3
Work Package title:	Ethical, Legal and Societal Aspects
Due Date of delivery:	M13
Actual date of delivery:	M13
Dissemination level:	Public (PU)
Type	Ethics (ETHICS)
Editor(s):	Prof Dr M.Gercke (CRI), Dr. L. Gercke (CRI), U. Gasper (CRI)
Contributor(s):	Prof Dr Marco Gercke (CRI), Ulrich Gasper (CRI), KEMEA, ACS, CYB
Reviewer(s):	CEZ, KEMEA, FORESIGHT Ethics Board
Project name:	Advanced cyber-security simulation platform for preparedness training in Aviation, Naval and Power-grid environments
Project Acronym	FORESIGHT
Project starting date:	1/10/2019
Project duration:	36 months
Rights:	FORESIGHT Consortium

Document history

Version	Date	Beneficiary	Description
0.1	10.10.2020	CRI	ToC
0.2	23.10.2020	CRI	1st version
0.3	28.10.2020	KEMEA, CYB, ACS	Input provided
0.4	29.10.2020	CRI	Final version for review
0.5	30.10.2020	Ethics board	Review and feedback
0.5	30.10.2020	KEMEA	Review feedback
0.6	04.11.2020	CEZ	Review feedback
0.7	05.11.2020	CRI	Final version for submission
1	06.11.2020	KEMEA	Quality assurance review and submission

Acknowledgement: This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 833673.

Executive Summary

FORESIGHT aims to develop a cyber-range solution to enhance the preparedness of cyber-security professionals at all levels and advance their skills towards preventing, detecting, reacting and mitigating sophisticated cyber-attacks. This is achieved by delivering an ecosystem of networked realistic training and simulation platforms that brings together unique cyber-security aspects in three domains, aviation, smart grid and naval. The FORESIGHT platform will extend the capabilities of existing cyber-ranges and will allow the creation of complex cross-domain/hybrid scenarios to be built jointly with the IoT domain.

This Deliverable is the third deliverable of WP3. It is related to T3.3 that is described as follows: “Based upon the work carried out under T3.1 the overall legal and ethical framework will be developed. The framework will include concrete recommendations for the project with regard to the issues identified in the aforementioned tasks and thereby provide guidance with regard to the overall project, the development of the Cyber Range.”

The idea is not to produce another extensive scientific deliverable. D3.1 provides a solid scientific basis that addresses various ethical, legal and societal issues that are relevant for this project. The focus of D3.3 is to provide practical and actionable information to guide those Consortium members, that are developing the FORESIGHT solution.

Contents

Acronyms & Abbreviations

Term	Description
CERTs	Computer Emergency Support Teams
CSIRTs	Computer Security Incident Support Teams
COE	Council of Europe
D	Deliverable
DPIA	Data Protection Impact Assessment
EU	European Union
GDPR	General Data Protection Regulation
LEA	Law Enforcement Agency
T	Task
WP	Work Package

1 Introduction

1.1 Overview

The purpose of this deliverable is to provide a concrete, actionable framework related to legal and ethical issues that are relevant for the project. FORESIGHT aims to develop novel methods and tools to train security practitioners to deal with highly sophisticated attacks as well as to prevent, detect, and respond to these attacks. In this regard, the FORESIGHT project will develop advanced tools that aim to automatically identify trends and developments that can be used for developing plots in simulations. The awareness of and respect for legal, ethical and societal concerns and boundaries is vital for all members of the Consortium during the project. This deliverable aims to provide them with actionable orientation.

1.2 Legal issues in the Context of Collecting Threat Intelligence as identified in D3.1

One of the advantages of FORESIGHT is the availability of advanced cyber-reasoning systems to automatically identify (unknown) cyber threats and include them into simulations. The advantage is obvious – trends can not only be detected at an early stage, but also be included in the simulations so that professionals going through this simulation-based training are exposed to up-to-date realistic scenarios which prepare them as soon as the trends emerge instead of weeks or months after they have spread. However, the legal assessment revealed that the process of collecting the necessary threat intelligence is going along with significant legal challenges ranging from possible licensing issues and copyright violations to potential collection of illegal content during the search for unknown cyber threats.

1.3 Ethical issues identified in D3.1

While binding legal standards are largely missing in simulated environments, ethical and societal considerations remain applicable. The assessment in the context of FORESIGHT revealed that the FORESIGHT platform might qualify as AI system within the meaning of the AI H-LEG's definition of AI provided for the application of the Ethics Guidelines on Trustworthy AI and identified four ethical principles and their correlated values founded on the fundamental rights and freedoms guaranteed in the European Union as base layer of guidance for the development of software tools in FORESIGHT. Already because of this common base layer it seems appropriate to draw on the recent AI H-LEG's Assessment List for Trustworthy AI (ALTAI)[1] for the ethical framework in this Deliverable. The Assessment List for Trustworthy AI (ALTAI) is intended for self-evaluation purposes and aimed at provoking appropriate action and nurturing an organizational culture committed to the protection of fundamental rights as enshrined in the EU Treaties and the EU Charter.[2]

[1] High-Level Expert Group on Artificial Intelligence (AI H-LEG), Assessment List for Trustworthy Artificial Intelligence (ALTAI), 17 July 2020.

[2] High-Level Expert Group on Artificial Intelligence (AI H-LEG), Assessment List for Trustworthy Artificial Intelligence (ALTAI), 17 July 2020, p. 3-4.

The ALTIA's relevance beyond actual artificial intelligence is supported by a recent resolution of the European Parliament. On 20 October 2020, the European Parliament adopted the Resolution suggested in its Report with recommendations to the European Commission on a framework of ethical aspects of AI, robotics and related technologies.[3]Annex B of this Report contains a rough draft proposal for a Regulation on ethical principles "for the development, deployment and use of artificial intelligence, robotics and related technologies" indicating the European Parliament's legislative priorities and regulatory approach.[4] According to Art. 5(1) of this rough draft proposal, "any artificial intelligence, robotics and related technologies … shall be developed, deployed and used in accordance with Union law and in full respect of human dignity, autonomy and safety and other fundamental rights set out in the Charter."[5] Read together with the list of definitions in Art. 4 of this rough draft proposal, the qualification of a technological system as "artificial intelligence" appears to become less relevant and the focus seems to shift towards a system's autonomy.

1.4 Societal Aspects for Responsible Research and Innovation as identified in D3.1

It is essential to reflect on how to improve societal engagement with aspects of cybersecurity. Although the FORESIGHT federated platform will be for cybersecurity specialists in specific domains such as the naval, aviation or the energy sectors, it is vital to create public awareness concerning the positive contributions of the FORESIGHT project to critical infrastructure security. Therefore, this deliverable also includes an analysis of potential social issues concerning the project's societal impact in areas that go beyond the development of a successful federated cybersecurity training platform. Drawing on the framework for Responsible Research and Innovation offered by the European Commission as fundamental guidance, the areas of public engagement, gender equality, science education, open science/open access and social justice & inclusion revealed valuable recommendations for the activities of FORESIGHT project.

1.5 Disclaimer

The legal considerations in the following deliverable are based on the information available to the authors at the time this deliverable was written. They are not conclusive. It might be necessary to carry out an additional review process once the project reached prototype status. In addition, it is important to point out that the legal considerations in this deliverable largely focus on EU legislation. Member States may however have implemented legal and regulatory standards that go beyond EU standards. When carrying out an additional review, national laws (especially laws of the country where a specific tool is operated) should, therefore, be taken into consideration.

[3]European Parliament, Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)), A9-0186/2020, 8 October 2020.
[4]European Parliament, Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)), A9-0186/2020, 8 October 2020, p. 37-61.
[5]European Parliament, Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)), A9-0186/2020, 8 October 2020, p. 50.

1.6 Relation to other tasks and deliverables

This deliverable is related to the following other FORESIGHT tasks and deliverables:

Receives inputs from:

Table 1. Inputs from other Deliverables

Deliverable Number	Deliverable Title	Relation
D3.1	Social, Ethical and Legal Report	Based on the scientific exploration of all potential legal, ethical and societal concerns related to the FORESIGHT in D3.1, Deliverable D3.3 develops the analytical considerations into an actionable orientation for every individual participant of the FORESIGHT project. This orientation creates an awareness of and respect for legal, ethical and societal concerns and boundaries and nurtures an organisational culture committed to create legal as well as ethically sound software solutions and tools.

Provides outputs to:

Table 2. Output from other Deliverables

Deliverable Number	Deliverable Title	Relation
D3.4	Development of the Review Mechanism	D3.4 will develop a review mechanism to ensure that the orientation developed in Deliverable D3.3 is adhered to and implemented in within the development process. The review mechanism is envisioned to assess and ensure that the future operation of the (federated) Cyber Ranges will be compliant with the orientation provided in D3.3 and in line with legal and ethical requirements and values defined in D3.1.
D3.5	Review Report	In the final phase of the FORESIGHT project, the review mechanism developed in D3.4 will be applied to the pilot applications developed in the entire project. The documentation of this review's findings will summarised in the Report of D3.5.

1.7 Structure of the deliverable

This deliverable is divided in four sections, as follows:

- The fist section is the introductory part of this report
- The second section provides the legal framework
- The third section provides the ethical framework
- The fourth section concludes this deliverable

2 The Legal Framework

2.1 Data Protection

Various tasks carried out within FORESIGHT will include interaction with personal data. The Data Management Plan[6] provides an overview about the different categories of data that are processed as well as protection measures. As the consequence this overall framework focuses on one specific aspect: the information gathering module.

Personal data might be collected via the 'Information Gathering Module' of Task 9.4. As the operation of the crawler is not limited to specific data, processing of personal data related to individuals is likely to take place. Since the collection process is automatic and personal data might exist in the sources of interest, any kind of personal data could be collected, even special categories.

D3.1 highlights that the collection of personal data with the 'Information Gathering Module' takes place in a challenging legal environment. As a consequence, legal considerations will need to be taken into account when developing the FORESIGHT solution. In addition, there are other deliverables that address the issue of data protection and that should be consulted prior to implementing solutions that interact with personal data and could potentially lead to a violation of data protection laws. Examples are D 13.5 (especially the need of conducting a DPIA prior to information gathering activities) and D 13.7.

Actionable Recommendations	
1.	**Keep Data Protection in Mind**
	Be mindful about the fact that interacting with personal data – even if only as side aspect of the project – requires a legal basis. The General Data Protection Regulation[7] (GDPR) as well as national data protection frameworks provide strong protections for personal data. It is essential that protections are respected when developing solutions.
2.	**Involve your DPO and the FORESIGHT DPO**
	When developing any component of the FORESIGHT solution where personal data will be processed, consult your data protection officer (DPO) as well as the project's DPO.
3.	**Protect Personal Data**
	If possible, Security-by-Design should prevent the interaction with personal data. If this is not possible, a full data protection compliance and risk assessment should be carried out prior to implementing technical solutions that potentially violate data protection laws.
4.	**Use Forms**

[6] See: Deliverable D1.2.

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the EU, L 119, 4 May 2016, p. 1.

		If you are processing personal data of researchers, experts or other humans, please use forms (especially for consent) whenever possible. If a form that would support you is missing, please contact the project's DPO.

2.2 Illegal Content

Without doubt the FORESIGHT platform is neither designed to identify illegal content nor does it intend to utilize it. However, especially during the operation of the web-crawling component as part of the "Information Gathering Tool" developed within T9.4 it is possible that the operation of the crawler leads to the collection of illegal material. Just like with regard to data protection, it is important to keep this in mind while developing the tool. It is likely that through the design of the web-crawler a collection of images, videos and other file-types that could contain illegal content can either be completely prevented or at least the risk of unintentional (collateral) collection can be limited.

D3.1 highlights that there are different categories of illegal content that need to be taken into consideration – especially child pornography and terrorist content. Child pornography is in this regard a particularly challenging topic as the degree of criminalization and the consequences of legal compliance are intense.

Actionable Recommendations	
1.	**Be Mindful about Illegal Content**
	The automated collection of threat intelligence is a key feature of the FORESIGHT platform. But it is important to keep in mind that in addition to valuable information about security threats the "Information Gathering Tool" might collect illegal/criminally-relevant information. This needs to be avoided at all cost given that the sole collection of such information may commence a criminal investigation (e.g. in case of child pornography).
2.	**Be Mindful about Differing National Standards**
	While legal standards with regard to illegal content are among the areas where the EU started harmonization, it is important to point out that the extent of criminalization differs from Member State to Member State. What could be legal for researchers to do in one country may already constitute a crime in others. Therefore, seek advice (see 4 below) when in doubt.
3.	**Collecting and Processing Illegal Content can lead to Individual Criminal Liability**
	Researchers involved in the development of the FORESIGHT platform might be the subject of investigations if illegal content is collected by the tool. Investigations could potentially lead to the seizure of computer systems and hardware used to run the platform and interrupt the project.
4.	**Seek Advise**
	If there are any doubts whether potentially illegal content could be collected, contact the project manager prior to implementing solutions to ensure that you receive legal support.

5.	**Security-by-Design**
	If possible, implement security-by-design features that prevent the collection of illegal content in the first place.
6.	**Consult the Ethics Board**
	The interaction with illegal content has not only a legal but also an ethical component. Make sure that prior to implementing solutions you consult with FORESIGHT's Ethics Board to get clearance.

2.3 Misuse of Devices

The "Information Gathering Module" of Task T9.4 will be the use of an automated crawler systematically browsing the Internet. The focus will be on cybersecurity related issues and trends. Unlike traditional web crawlers[8] that create an index of available content the tool utilized within the FORESIGHT platform will focus on the identification of (unknown) cyber threats in order to create scenarios that include latest trends. The crawler will search for relevant data both in the regular part of the Internet as well as in the Darknet[9]. Some underground websites offering a space for discussing vulnerabilities also make available illegal devices such as software tools for circumventing protective measures. In addition, some underground websites also (illegally) offer access codes and passwords (usually for sale). Interacting with such illegal data can lead to criminal liability.

D3.1 highlights that it is important to be mindful about illegally available data (such as access codes or passwords) and illegal devices. Based on the more extensive analysis of legal aspects in D3.1 the following actionable recommendations can be extracted:

Actionable Recommendations	
1.	**Be Mindful that some Underground Websites that contain Relevant Information regarding Cyber Threats might also contain Illegal Data (such as Access Codes and Passwords).**
	The automated collection of threat intelligence is a key feature of the FORESIGHT platform. However, when crawling into underground websites it is important to be mindful that interacting with some of the data offered and provided on such websites may involve to criminal liability.
2.	**Be Mindful about Differing National Standards**
	While legal standards with regard to illegal content are among the areas where the EU started harmonization, it is important to point out that the extent of criminalization differs from Member State to Member State. What could be legal for researchers to do in one country may already constitute a crime in others. Therefore, seek advice (see 4 below) when in doubt.

[8] Regarding the fundamental concepts and functions of web crawling see: *Olston/Najork*, Web Crawling, 2010.
[9] A Darknet is an overlay network within the traditional Internet that can only be accessed through special software. For more details see: *Bancroft*, The Darnet and Smarter Crime, 2019.

3.	**Collecting and Processing Access Codes and Passwords can lead to Individual Criminal Liability**
	Researchers involved in the development of the FORESIGHT platform might be the subject of investigations if the content collected by the tool could lead to criminal liability. Investigations could potentially lead to the seizure of computer systems and hardware used to run the platform and interrupt the project.
4.	**Seek Advice**
	If there are any doubts whether certain features violate existing laws, contact the project manager prior to implementing such solutions to ensure that you receive legal support.
5.	**Security-by-Design**
	If possible, implement security-by-design features that prevent the collection of material that could lead to criminal liability.
6.	**Consult the Ethics Board**
	Accessing Underground Websites where security vulnerabilities are discussed could potentially lead to relevant intelligence. However, there are various ethical concerns. Therefore, please consult the Ethics Board prior to implementing solutions.

2.4 Circumventing Access Restrictions

Some of the most relevant discussions about cybersecurity will most likely not take place in the open but in forums and on websites where measures are put in place aiming to keep unwelcome people (such as investigators) out. Taking into account that the exchange of certain types of data (such as access codes and passwords) could itself be a crime, such efforts are not surprising. There are tools available that are aiming to circumvent access restrictions.

If circumventing access restrictions is something that is taken into consideration, D3.1 summarizes legal limitations that need to be reflected. In this case the following actionable recommendations should be taken into consideration:

Actionable Recommendations	
1.	**Circumvention Access Restrictions – Even if Taking Place for "Good Cause" – can itself be a Criminal Act**
	While it might sound surprising that criminal law protects criminals shielding their illegal activities by setting up access restrictions, this is something to be mindful about. Therefore, actively circumventing access restrictions should not be among the features of the FORESIGHT tool.
2.	**Be Mindful about Differing National Standards**
	While legal standards with regard to illegal content are among the areas where the EU started harmonization, it is important to point out that the extent of criminalization differs

	from Member State to Member State. What could be legal for researchers to do in one country may already constitute a crime in others. Therefore, seek advice (see 4 below) when in doubt.
3.	**Circumventing Access Restrictions (such as Passwords) can lead to Individual Criminal Liability**
	Researchers involved in the development of the FORESIGHT platform might be the subject of investigations if they are involved in illegally circumventing access restrictions. Investigations could potentially lead to the seizure of computer systems and hardware used to run the platform and interrupt the project.
4.	**Seek Advice**
	If there are any doubts whether certain features violate existing laws, contact the project manager prior to implementing such solutions to ensure that you receive legal support.
5.	**Consult the Ethics Board**
	With regard to all features that could potentially violate law, please get in touch with the Ethics Board as this might lead to ethics concerns in addition.

2.5 Copyright Issues and Licensing Issues

The "Information Gathering Tool" does not raise issues with regard to potentially criminal content - there are also concerns related to copyright violation and licensing issues. The web-crawler might copy and save content in a database that is protected by copyright laws or licensing agreements.

Actionable Recommendations	
1.	**Be Mindful that Not All Content Available Online is "Free"**
	While it is technically possible to crawl and copy almost any content available online, it is necessary to pay attention to the fact that copying such data might violate copyright laws and license agreements.
2.	**Keep in Mind, that Copyright Laws Differ Largely**
	From a technical perspective, the physical storage location seems of limited relevance. Data targeted by the crawler could be stored on a server located either inside or outside the European Union. However, from a legal perspective, it is significant that copyright laws differ largely from country to country. Therefore, seek advice (see 4 below) when in doubt.
3.	**Exceptions such as "Fair Use" or "Personal Use" May not Apply**
	Be aware that while research projects benefit from various exceptions under law, not everything permitted for private users is necessary also within reach for FORESIGHT. Therefore, seek advice (see 4 below) when in doubt.
4.	**Seek Advise**

	If there are any doubts whether certain features violate existing laws, licencing agreements or the terms and conditions of platforms, contact the project manager prior to implementing solutions to ensure that you receive legal support.
5.	**Consult the Ethics Board**
	With regard to all features that could potentially violate law or licensing agreements, please get in touch with the Ethics Board as this might lead to ethics concerns in addition.

3 The Ethical Framework

For ethical compliance, it is not only necessary to evaluate whether any software solution and tool developed in phase three of the FORESIGHT project and based on autonomous and automating algorithms actually respects human autonomy and serves non-maleficence, beneficence as well as justice. For this evaluation, it is important to realise which decisions are delegated to a software solution and/or tool, what advantages and disadvantages might be involved and who is accountable and/or liable for its use. Only if this evaluation allows to conclude that the design, development and use of the software solution and/or tool fully respects the human rights and values, then the software solution is trustworthy and ethically compliant.

The use of the envisioned Information Gathering Module is intended to automate gathering cyber threat intelligence which is currently carried out by human experts. For that purpose, the Information Gathering Module should provide reliable data concerning cyber-attack actors, methods, techniques and procedures which may be verified and converted into a simulation as potential cyber threat in a cyber-range.

3.1 Human Agency and Oversight

The Information Gathering Module should support human agency and human decision-making. D3.1 highlights that it is important for the software solutions and tools developed for the Information Gathering Module not only support the user's agency for the benefit of society, but also allow for sufficient human oversight in order to uphold fundamental rights. Based on the more extensive analysis of ethical aspects in D3.1 the following actionable recommendations can be extracted:

Actionable Recommendations	
1.	**Make end-users sufficiently aware which decision, content, advice or outcome is the result of an algorithmic decision**
	The evaluation of cyber threat intelligence is a cognitive process which ultimately has to rest with a human operator. Therefore, it is vital to ensure that the human operator is adequately made aware that a decision, content, advice or outcome is the result of an algorithmic decision.
2.	**Avoid that end-users over-rely on the software solution and/or tool**
	Put procedures in place to Software solutions and tools can affect human autonomy by generating over-reliance by end-users.
3.	**Prevent the end-user's decision-making process from being interfered with inadvertently**
	Put procedures in place to avoid unintended and undesirable interference with the end-user's decision-making process.
4.	**Document the governance mechanism ensuring human oversight**
	For end-users and their specific training it is vital to know whether human intervention is possible (a) in every decision cycle of the Information Gathering Module (*human-in-the-*

	loop), or (b) during its design cycle and by monitoring its operation (*human-on-the-loop*), or (c) by overseeing its overall activity and the power to decide whether and how to use it in any particular situation (*human-in-command*).
5.	**Put a procedure in place to safely abort an operation when needed**
	End-users evaluating cyber threat intelligence ideally need detection and response mechanisms for undesirable adverse effects of software solutions and/or tools developed for the Information Gathering Module. As minimum, end-users should have an equivalent to a 'stop button'.
6.	**Seek Advice**
	If there are any doubts whether certain features negatively affect human agency or oversight, contact the project manager and the Ethics Board prior to implementing solutions to ensure that you receive the necessary multidisciplinary support.

3.2 Quality of Cyber Threat Intelligence

The Information Gathering Module should identify accurate and reliable cyber threat intelligence. For that purpose, D3.1 highlights that the software solutions and tools developed for the Information Gathering Module must be dependable and resilient. Based on the more extensive analysis of ethical aspects in D3.1 the following actionable recommendations can be extracted:

Actionable Recommendations	
1.	**Ensure the integrity, robustness and overall security of the software solutions and/or tools against attacks**
	Safeguarding the software solutions and/or tools developed for the Information Gathering Module against vulnerabilities potentially emanating from manipulation of data or classifications, specific measures have to be put in place.
2.	**Define risks, risk metrics and risk levels for each specific use case**
	Put processes in place to continuously measure and assess risks and ensure that end-users will be aware of these risks.
3.	**Put measures in place monitoring and documenting the accuracy of a software solution and/or tool so that the level of accuracy is communicated to end-users**
	The level of accuracy of the collected Cyber Threat Intelligence is crucial. Therefore, it not only has to be monitored and documented, but also communicated to the end-user.
4.	**Put a process in place to monitor whether the software solutions and/or tools are meeting their intended goals**
	Verification and validation methods as well as documentation need to be put in place for the evaluation of a software solution's and/or tool's reliability and reproducibility.

5.	**Seek Advice**
	If there are any doubts whether certain features negatively affect the quality of Cyber Threat Intelligence or oversight, contact the project manager and the Ethics Board prior to implementing solutions to ensure that you receive the necessary multidisciplinary support.

3.3 Transparency

The Information Gathering Module can only achieve ethical compliance when its functioning is sufficiently transparent. For that purpose, D3.1 highlights that the software solutions and tools developed for the Information Gathering Module must be traceable and explainable. Whereas traceability refers to the proper documentation of the development processes, explainability refers to the ability to explain not only the technical processes but also the reasoning behind the decisions or predictions a software solution or tool makes. In addition to their traceability and explainability, their limitations also need to be openly communicated. Based on the more extensive analysis of ethical aspects in D3.1 the following actionable recommendations can be extracted:

Actionable Recommendations	
1.	**Put measures in place ensuring the traceability of all functions of the Information Gathering Module**
	The quality of the input and the output data has to be continuously assessed and it must be possible to trace back which data and which rules were used for specific decisions or recommendations of the Information Gathering Module.
2.	**Explain the decisions and recommendations of the Information Gathering Module to the end-users**
	The decisions and recommendations by the Information Gathering Module must be explained and understood by the end-users, in order to allow for contesting of such decisions. However, an explanation might not always be possible (black box) triggering compensatory measures like traceability, auditability and the open communication of the software solution's and/or tool's capabilities.
3.	**Establish mechanisms informing end-users about the purpose, criteria and limitations of the decisions and recommendations generated by the Information Gathering Module**
	The Information Gathering Module's capabilities and limitations have to be communicated in an appropriate manner to the end-users. This involves communicating the benefits as well as the technical limitations and potential risks of the Information Gathering Module's functions, so that end-users can be adequately trained for its use.
4.	**Seek Advice**
	If there are any doubts whether certain features negatively affect the transparency of the Information Gathering Module's capabilities or limitations, contact the project manager and

	the Ethics Board prior to implementing solutions to ensure that you receive the necessary multidisciplinary support.

3.4 Unfair Discrimination

The Information Gathering Module is envisioned to infer a pattern by means of data mining and thereby construct a profile which inevitably misguides its focus and leads to discrimination if based on a biased intelligence decision-making process. Furthermore, an individual cyber threat actor is profiled based on connections with others identified by the same set of software solutions and/or tools, rather than based on actual behaviour.

For that purpose, D3.1 highlights that the software solutions and tools developed for the Information Gathering Module contain the risk of misguiding its focus and creating unfair discrimination against groups or people because of using threat indicators which are unreasonably based on prejudice about the likely characteristics of cyber threat actors. Based on the more extensive analysis of ethical aspects in D3.1 the following actionable recommendations can be extracted:

Actionable Recommendations	
1.	**Establish a strategy and procedures to avoid creating or reinforcing unfair discrimination concerning the software solution's and/or tool's design as well as its use of input data**
	Identifiable and discriminatory bias needs to be removed in the collection phase where possible. This also necessitates a coherent definition and implementation of fairness.
2.	**Establish the most appropriate indicators for Cyber Threat Intelligence**
	For this purpose, it is necessary to document how likely cyber threat actors and legitimate threat intelligence sources may be to use the terms selected as indicators for Cyber Threat Intelligence. This involves elaborating not only the ratio between potentially cyber threat relevant users of a specific threat indicator and the innocent people using the same term, but also a mechanism for distinguishing between potentially cyber-attack relevant users and innocent users of those terms selected as threat indicator.
3.	**Put mechanisms in place for the flagging of issues related to bias, discrimination and poor performance of the Information Gathering Module**
	For this purpose, clear processes have to be established for how and to whom such issues need to be raised.
4.	**Establish mechanisms to ensure fairness in each software solution and tool as well as in the Information Gathering Tool as a whole**
	In this respect, it is helpful to ensure a qualitative analysis or metrics to measure and test the applied definition of fairness.
5.	**Seek Advice**

	If there are any doubts whether certain features might create unfair discrimination by the Information Gathering Module, contact the project manager and the Ethics Board prior to implementing solutions to ensure that you receive the necessary multidisciplinary support.

3.5 Accountability

The Information Gathering Module is intended to be operated as covert online cyber threat surveillance. In this operational area, the software solutions and/or tools developed for the Information Gathering Module have potential not only to create a risk for social trust and cohesion, but also to endanger each facility the cybersecurity experts of which have been trained with the FORESIGHT platform.

For that reason, D3.1 highlights that mechanisms have to be established ensuring responsibility for the development, deployment and use of the software solutions and tools developed for the Information Gathering Module. Based on the more extensive analysis of ethical aspects in D3.1 the following actionable recommendations can be extracted:

Actionable Recommendations	
1.	**Establish mechanisms facilitating the Information Gathering Module's auditability**
	For this purpose, the development process has to be traceable and the processes, outcomes, positive and negative impacts of each software solution and/or tool has to be logged. Ideally, it should at least be possible for a trusted but independent third party to audit the Information Gathering Module.
2.	**Establish a process to continuously monitor and assess the ethical compliance of each software solution and/or tool and the Information Gathering Module as well as the entire FORESIGHT platform**
	For this purpose, conflicts between different ethical requirements or principles have to be identified, discussed and resulting "trade-off" decisions properly documented. Further, a process should be established for anyone to report potential vulnerabilities, risks and biases in the Information Gathering Module.
3.	**Seek Advice**
	If there are any doubts whether certain features might be relevant for allocating responsibility for the development of a software solution and /or tool for the Information Gathering Module, contact the project manager and the Ethics Board prior to implementing solutions to ensure that you receive the necessary multidisciplinary support.

3.6 Impact on Society at Large

The development of software solutions and/or tools for the Information Gathering Module forms an essential part of the FORESIGHT project which also needs to reflect on how to improve societal engagement with aspects of cybersecurity. In this respect, the FORESIGHT project has the potential to

make cybersecurity of critical infrastructures more inclusive and generally more aligned with societal needs by enhancing public awareness concerning the positive contributions of the federated platform to critical infrastructure security.

Drawing on the framework for Responsible Research and Innovation (RRI),D3.1 emphasises how the FORESIGHT project's impact on society at large can be made more sustainable and aligned with societal needs by taking into account public engagement, gender equality, science education, open access and social justice and inclusion.Based on the more extensive analysis of societal aspects in D3.1 the following actionable recommendations can be extracted:

Actionable Recommendations	
1.	**Ensure that interfaces for end-user access do not create access-barriers for people with disabilities**
	The interface design has to be considered not only from a technical design perspective but also from a social perspective, ensuring that accessibility is well supported.
2.	**Ensure that the promotional material of the FORESIGHT project and platform reflects gender equality and creates interest and information on the science**
	Be aware that the FORESIGHT project's promotional material also contributes to a perception of gender equality and the science behind the project. This perception should ideally include a positive signal for women in general and facilitate interest in cybersecurity education by stimulating interest in learning platforms.
3.	**Seek Advice**
	If there are any doubts whether certain promotional material or design features might be insufficiently aligned with societal needs, contact the project manager and the Ethics Board prior to implementing solutions to ensure that you receive the necessary multidisciplinary support.

4 Conclusion

This Deliverable D3.3 has provided practical and actionable guidelines for all Consortium members developing software solutions and/or tools for the FORESIGHT platform in general and for its Information Gathering Module in particular. These guidelines are aimed at ensuring legal and ethical compliance throughout the FORESIGHT project. They are intended not only to create the necessary legal awareness and sensitisation but also for encouraging thoughtful reflection to provoke appropriate action and nurture an organisational culture within the FORESIGHT consortium. The FORESIGHT project is committed to developing and maintaining federated Cyber Ranges in line with all legal requirements and ethically firmly grounded in the protection of people's fundamental rights.

The key takeaways from this Deliverable is that everybody participating in the FORESIGHT project has to be fully aware of the legal and ethical framework presented in this Deliverable:

- The legal framework requires special attention regarding the areas of data protection (section 2.1 above), illegal content (section 2.2 above), misuse of devices (section 2.3 above), circumventing (section 2.4 above) as well as copyright and licenses (section 2.5 above).
- The ethical framework mirrors the requirements for trustworthy AI and anticipates a need for particular awareness of ensuring human agency and oversight (section 3.1 above), accurate and reliable quality of cyber threat intelligence (section 3.2 above), sufficient transparency via traceability and explainability (section 3.3 above), fairness and non-discrimination (section 3.4 above), operative mechanisms for responsibility and accountability (section 3.5 above) and an awareness of the project's impact on society at large (section 3.6 above).

