D2.1.1 Mission Definition Review Report

Document Summary Information

Project Identifier	EDIDP-SME-2020-099-HERMES		
Acronym	HERMES		
Start Date	01/12/2021	**Duration**	33 months
Project URL	http://www.hermes-dxp.eu		
Deliverable	D2.1.1 Mission Definition Review Report		
Work Package	WP2: Studies		
Contractual due date	June 30, 2022	**Actual submission date**	June 30, 2022
Type	R	**Dissemination Level**	PU
Lead Beneficiary	ITL	**Classification Level**	UNCL
Responsible Author	Frédéric Pierret (ITL)		
Contributors	Michal Chilinski (ITL), Christos Skoufis (EBOS), Marcin Przybyszewski (ITTI), Luc Dandurand (TALGEN Cybersecurity OÜ)		
Peer reviewer(s)	Frini Lazarou (EBOS), Piotr Tyczka (ITTI)		

This project has received funding from the European Defence Industrial Development Programme (EDIDP), under grant agreement "EDIDP-SME-2020-099-HERMES"

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete	Changes	Contributor(s)
v0.1	02/05/2022	20	Initial Deliverable Structure	Frédéric Pierret (ITL)
v0.2	16/05/2022	40	Initial content	Frédéric Pierret (ITL)
v0.3	23/05/2022	50	Support on MDR questionnaire	Luc Dandurand (TALGEN)
v0.4	02/06/2022	70	Improvements and additional content from ITTI and EBOS, validate current content complies with EUAB feedback and write introduction and conclusions.	Marcin Przybyszewski (ITTI) Christos Skoufis (EBOS) Frédéric Pierret (ITL)
v0.5	10/06/2022	100	Setup requirements, add Annexes with EUAB MDR questionnaire and result.	Frédéric Pierret (ITL)
v0.6	17/06/2022	100	Peer review	Frini Lazarou (EBOS)
v0.7	22/06/2022	100	Peer review	Piotr Tyczka (ITTI)
v0.8	27/06/2022	100	Additional content and clarification on MDR questionnaire feedback from EUAB.	Frédéric Pierret (ITL)
v0.9	30/06/2022	100	Final quality check, adjustments, and submission	Christos Skoufis (EBOS)

Disclaimer

The content of this document reflects only the author's view. Neither the European Commission nor the INEA are responsible for any use that may be made of the information it contains.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the HERMES consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the HERMES Consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the HERMES Consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

© HERMES Consortium. This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

Table of Contents

List of Figures

List of Tables

Glossary of terms and abbreviations used

Abbreviation / Term	Description
API	Application Programming Interface
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CIA	Confidentiality, Integrity, and Availability
COI	Independent Communities of Interest
CS	Cybersecurity Application
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
DXP	HERMERS Data Exchange Platform
EUAB	End User Advisory Board
FIRST	Forum for Incident Response and Security Teams
GA	Grant Agreement
GUI	Graphical User Interface
HAPI	HERMES Application Programming Interface
HDM	HERMES Data Management
HDS	HERMES Data Store
HDX	HERMES Data Exchange
HUI	HERMES User Interface
ICT	Information and Communications Technology
IEP	Information Exchange Policies
ITO	Independent Topic Ontologies
MDR	Mission Definition Review
MoD	Ministry of Defence
NDA	Non-Disclosure Agreement
QA	Quality Assurance
QCP	Quality-Control Processes
UGS	Unmanned Ground System
UGV	Unmanned Ground Vehicle

Executive Summary

This document describes the work that has been performed during the first seven months of the project, in Task 2.1 – "Pre-Feasibility Study".

The objective of this document is to present the feedback from the End-User Advisory Board (EUAB) on the overall concept, the use cases and provide the recommended Common Requirements for the Member States to consider for the HERMES system.

The EUAB plays a key role in HERMES as the body responsible to provide the measure of success of the project through the five different milestone reviews scheduled during project execution. The first milestone related to Task 2.1 (Mission Definition Review - MDR) has been captured on M7 and the results are provided in this document, but also presented on a live Consortium meeting performed on June 15th. During this meeting, the EUAB discussed with the Consortium and the representatives from the EU, the feedback from the MDR questionnaire.

To define the capability needed to meet the objectives (section 2.4), the problems associated with information sharing and automation in the cybersecurity domain were examined. As a result, the challenges (listed in section 2.1), as well as several key considerations applicable to that domain were identified. This led to the identification of eleven high-level requirements (section 3.2) that the HERMES capability must meet to achieve its objectives.

This report is also based on prior work for which the relevant parts have been published by the NATO Communications and Information Agency [DS13] and [SDB14].

The results of the "Pre-Feasibility Study" will be used during the project's lifecycle and more specifically in Task 2.2 – "Feasibility Study" and Task 3.2 – "Architecture".

1 Introduction

The goal of this section is to provide a brief outline of the objectives of the specific HERMES Deliverable, how are those aligned and relevant with the overall project, and what was the approach followed in order to achieve them.

1.1 Mapping HERMES Outputs

The purpose of this section is to map HERMES Grant Agreement commitments, both within the formal Deliverable and Task description, against the project's respective outputs and work performed.

Table 1: Adherence to HERMES GA Deliverable & Tasks Descriptions

HERMES GA Component Title	HERMES GA Component Outline	Respective Document Chapter(s)	Justification
DELIVERABLE			
D.2.1.1 - Mission Definition Review Report *The Mission Definition Review will gather the feedback from the End-User Advisory Board on the overall concept and use cases and provide the recommended Common Requirements for the Member States to consider for the HERMES system.*			
TASKS			
Task 2.1 - Pre-Feasibility Study	*The first objective of this task is to elaborate the operational requirements in terms characterizing needs and required performance, identifying security, dependability, and safety goals, and specifying the operating constraints for the foreseen physical and operational environment. This task will update the concept established in prior work, elaborate the main uses cases, identify the preliminary technical requirements, and assess the longer-term economic viability of the HERMES system. It will produce recommended Common Requirements for the Member States to consider during the Mission Definition Review, allowing the release of the capability statement with associated operational requirements and the Member States' assessment of the plans for the following steps.*	*Section 2.4* *Chapter 3* *Annexes 1, 2*	*Section 2.4 presents HERMES use-cases and Chapter 3 produces the list of recommended Common Requirements that HERMES platform should comply with. A summary of End User Advisory Board answers to questions (based on Questionnaire in Annex 1) is provided in Annex 2.*

1.2 Deliverable Overview and Report Structure

In Chapter 2, an overview of the current cybersecurity challenges is provided. It is described how the HERMES Data Exchange Platform and use-cases can contribute at solving these challenges from the standard use-case to the autonomous military systems.

In Chapter 3, the list of recommended Common Requirements that a HERMES Data Exchange Platform should comply with is given, along with the setup and view on End User Advisory Board.

Annex 1 provides the MDR Questionnaire which has been utilised to collect the feedback from the EUAB, and Annex 2 shows the consolidated feedback from the EUAB.

2 HERMES Data Exchange Platform

The following parts are based on EDIDP-SME-2020 call, Section 6.

2.1 Overview of the general situation

Taking the broadest of views, cybersecurity remains a major challenge because:

- Security requirements are often underestimated or ignored;
- The design and implementation of security in systems is generally underfunded;
- Components used in building systems have inherent vulnerabilities and weaknesses that supply chain hasn't addressed;
- Modern cyberthreats are complex and sophisticated;
- Some of them can bypass traditional security solutions.

The result is inadequate security in cyberspace, affecting every entity from individual persons to Nation States. In the defense domain, as components from Information and Communications Technology (ICT) are increasingly used in military units and command structures, the impact of cyber threats and potential incidents on the Member States' defense capabilities, both at tactical and strategic level, is constantly growing. In the military domain, a major cyber incident potentially jeopardizes the nation's security, defense and poses a direct threat.

Modern digital solutions that are being implanted in the military domain bring complex new threat vectors, hindering the efficient utilization of a technology or solution. Such new technologies are Unmanned Autonomous Vehicles, Artificial Intelligence/Machine Learning or Digital Soldier concepts. As increasing ICT components apply, variety of challenges emerge from securing the access and availability of data along with its integrity and confidentiality (Confidentiality, Integrity, and Availability model). To address these challenges, mitigation measures in the form of operational cybersecurity solutions are added to inherently insecure systems to bolt-on security. While they provide benefit, they rarely fully address the problems and fail at times.

Nevertheless, improving cybersecurity solutions and operations leads to palliative benefits worth pursuing while the root causes get addressed. One of the main problems in cybersecurity operations is the overload of poor quality and irrelevant information. This happens at two levels: cognitive for humans and data for systems. At the cognitive level, cybersecurity experts are overwhelmed with information of varying accuracy that needs to be analyzed to determine applicability and usefulness to their specific situation. At the data level, while cybersecurity systems can usually scale to meet higher volumes of data, they suffer from the use of proprietary or difficulty to update data formats which limits their rapid evolution. They are also often operated in silo, leading to massive redundancy in data and poor exploitation of extremely useful correlations. Highly integrated sets of cybersecurity solutions are available from vendors using proprietary interoperability, but these are typically avoided preventing vendor lock-in and single points of failure. As in the case for cognitive activities by humans, cybersecurity solutions are equally plagued by data quality issues.

Finally, many cybersecurity solutions generate an unmanageable number of false positives, requiring a level of human analysis unavailable to most organizations. Collaboration on cybersecurity information and data is improving, but organizations still struggle to fully exploit burden-sharing opportunities due to lack of control over exchanged information and data, mismatch, unclear and fast-changing semantics versus the perceived low return-on-investment. "Actionable" Cyber Threat Intelligence (CTI) is a recent trend promoted by cybersecurity data vendors that does not fully deliver the promised benefits. To be actionable, data needs to be curated for the consumer's specific system configuration and risk profile. Consumers of CTI are generally unwilling to share their specific situation, fearing the details could be exploited. Data feeds can then only be grossly curated, and systems operators still need to follow up with human analysis to truly deliver "actionable" intelligence.

2.2 Military domain

Looking more specifically at the military domain, successful and economical military operations can be increasingly attributed to information superiority, derived from what some call net-centric warfare, and a line of action in the 2018 European Union Capability Development Priorities.

As a result, Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems are targeted for information superiority. These highly complex systems must be secured in the face of high risks, despite constrained budgets and limited resources. In parallel, modern weapon systems rely significantly on electronics of various forms, some of which continue to be built on insufficiently secured hardware and software components to meet implementation constraints. The rapidly increasing degree of interconnectivity in the pursuit of information superiority renders them more and more vulnerable.

Given the legal obligations related to the use of minimum force, kinetic munitions will therefore increasingly become less attractive to defeat modern weapon systems compared to cyberattacks. Logistical supply chains are also heavily dependent on automation and information management, and the cyberattack risk they face increases steadily.

Offensive cyber operations targeting C4ISR, weapon systems, and logistical supply chains are, therefore, the asymmetric threats of the greatest concern today. This concern will continue to proliferate for the foreseeable future as the creation of a capable cyber force is undetectable and trivial for most Nations. Force, used or convincingly threatened, will have an increasingly significant cyber component, as confirmed in various political declarations, notably NATO's 2016 recognition of cyberspace as a domain of operations. But while most military forces are addressing cybersecurity, some with significant efforts, the nature of warfare is also changing with the advent of robotics and artificial intelligence. Force will be increasingly delivered through autonomous systems, with humans playing an ever-decreasing role. Even if not used in the delivery of munitions, autonomous systems will likely play pivotal roles in the logistic supply chain and combat support roles. This massive reliance on computer and electronic systems in the battlefield will introduce pressure points of no equivalent significance in the history of warfare. Cyber will make future wars very unpredictable, with extremely fast changing situations spanning immense geography, and merging concerns regarding military, civilian and social infrastructures. The notion of war itself is becoming increasingly vague as critical infrastructures, supply chains and military systems are compromised in advance of conflict, requiring a level of peacetime cyber readiness and resilience, unusual for military forces, governments, and industry. Among all this, the role of timely and accurate information and data remains central to information superiority, the minimal and effective use of force, and the cyber defense of systems used or relied upon by military forces. More specifically in the cyber domain, "enabling capabilities for cyber responsive operations" has also been identified as one of the EU Capability Development Priorities. One of the areas where the development of new capabilities can be done is "cyber defense research and technology activities". More specifically in crucial domains such as cyber situational awareness technologies, defensive cyber technologies, autonomous cyber response systems, cyber threat intelligence capabilities, predictive analysis and modeling and simulation.

2.3 The contribution of HERMES

HERMES is a military-grade, enterprise system composed of different software components that are deployed in various parts of an organization, including across security domains. It is various experts that gather, curate, and distribute cybersecurity information to various other systems, including integrated Unmanned Ground System (UGS).

As a system, HERMES provides a foundation that addresses the challenges of overloading a cybersecurity system with poor quality, untimely, and irrelevant cybersecurity information:

- For experts, HERMES will help manage the breadth and depth of cybersecurity knowledge necessary for cyber information superiority;
- For systems, HERMES will help feed data to cybersecurity applications, increasing their ability to interoperate and function autonomously.

HERMES achieves this in ways that recognize and address many of the issues currently plaguing cybersecurity data, information sharing and exploitation. HERMES, as proposed under the EDIDP-SME-2020 call, focuses on the specific domain of autonomous military systems. According to this, it will help cybersecurity solution vendors as well as manufacturers and operators of autonomous military systems to work together more efficiently and to better support autonomous cyber-defence, even in highly constrained and risky environments.

2.4 Objectives

The overall objectives of HERMES are to:

- Enable automation and autonomy in cybersecurity operations;
- Improve controlled information sharing of high-quality cybersecurity data;
- Facilitate burden-sharing collaboration and outsourcing of cybersecurity data management.

The approach taken with HERMES to achieve these objectives is a disruptive paradigm shift. Indeed, the current approach for enabling information sharing, data exchange and collaboration is to develop standards for interoperability, individually develop and operate solutions that leverage these standards. Developing standards is long and costly. It is a significant drawback for the field of cybersecurity which is fast-moving and financed with parsimony and therefore, more focused on immediate needs than innovative approaches. Data modeling in cybersecurity is also more difficult than in the conventional military domain because the realities to be modeled are not well understood. To make matters worse, sensitivity of data, reputation and liability concerns, and privacy regulations further complicate information sharing efforts and collaboration. The result is that collaboration and information sharing are by far suboptimal. Indeed, existing trust relationships and mutual benefit situations are not exploited. In consequence, outsourcing of data management activities to leverage specialization is very limited.

Addressing these domain-specific constraints is a common problem for all seeking to exchange data and collaborate. Most communities continue to follow the traditional approach based on interoperability standards, with each then expending time and resources individually to build their own systems to address the exact same problems they face. These systems become far less effective because they are constrained by the need to meet the agreed standards which become difficult to evolve, and collectively far more expensive as everyone tackles the same challenges separately instead of working together towards a common solution.

With HERMES, a line is drawn between the concerns of data representation, storage and exchange, and the concerns related to the uses made of exchanged data. HERMES looks at all data just as data, regardless of the use made of it. It recognizes that data format (syntax and semantics) needs to change at different places for different participants to an exchange. It recognizes that exchange of cybersecurity data is far more complex than most people realize and tackles this complexity head-on. HERMES is a foundational system intended to be available to all, a joint effort to address the full set of common problems faced by all. By disassociating management and use of data, HERMES offers the opportunity for applications to obtain their data from a common system that takes care of the common data representation, storage, and exchange issues. This is a significant effort saved by all, and the savings can be applied to developing better applications for individual and specific needs.

2.4.1 HERMES components and General Use Case

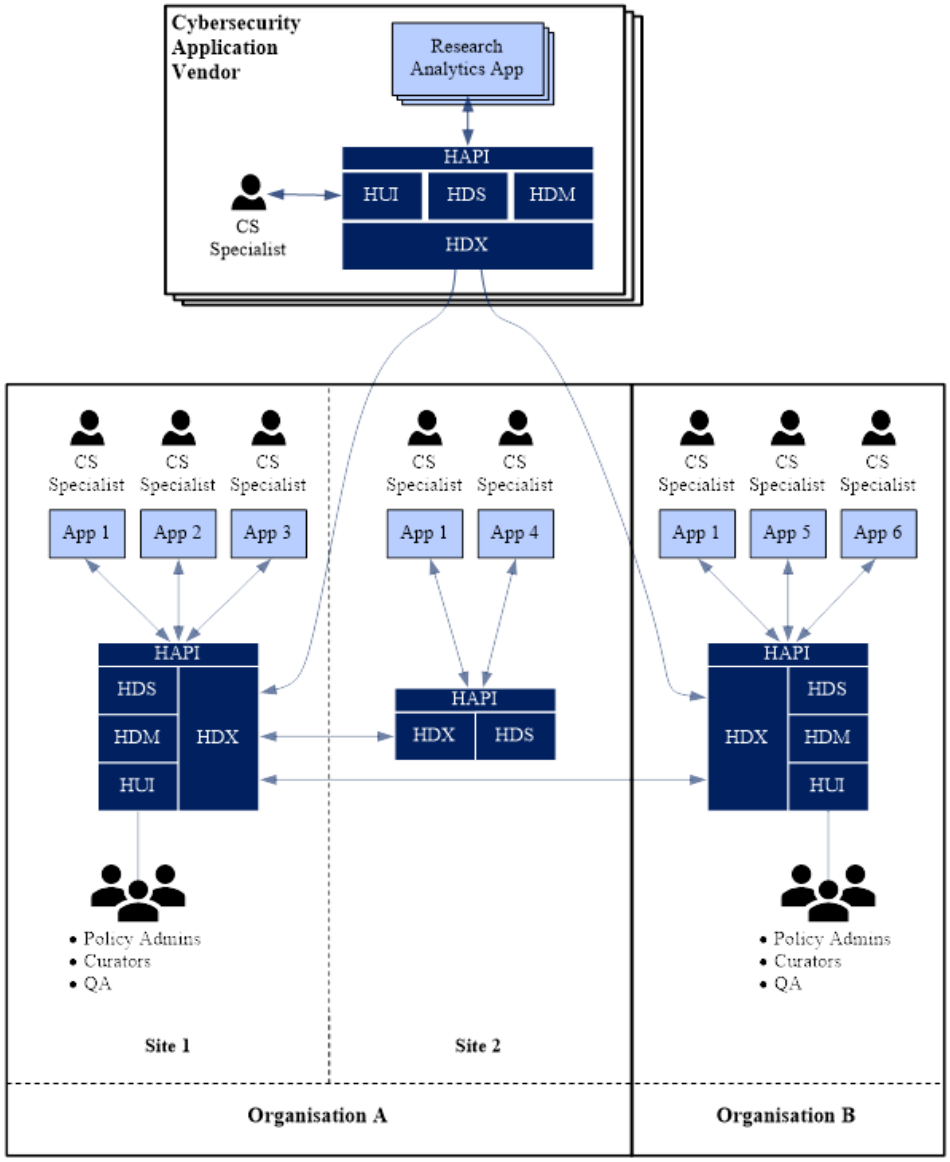


Figure 1: General Use Case

In terms of nomenclature, HERMES and the HERMES Data Exchange Platform are used interchangeably. The term "Data Exchange Platform" is abbreviated "DXP" and has been chosen for the following reasons:

- "Data" because the primary usage of the information held in HERMES is automated and autonomous cybersecurity which require relevant and timely data;
- "Exchange" because one of the key strengths of HERMES is to facilitate the exchange of data across cybersecurity solutions, organizational boundaries, and security domains;
- "Platform" to stress the fact that HERMES is not a cybersecurity tool per se, but rather a foundational system that provides data to cybersecurity applications.

The general use case supported by HERMES is illustrated in Figure 1. It shows two organizations, A and B, and some cybersecurity application vendors. To illustrate the distributed nature of HERMES, Organization A is shown

to be in two Sites, 1 and 2. In Figure 1, HERMES is illustrated at the conceptual level by the following components in dark blue:

- The HERMES Data Store (HDS) component, which stores all data within HERMES;
- The HERMES Data Management (HDM) component, which provides automated data management functions defined in policies;
- The HERMES User Interface (HUI) component, which provides the functionality for Policy Administrators, Data Curators and Quality Assurance Experts to manage the data throughout its lifecycle;
- The HERMES Data Exchange (HDX) component, which is responsible for exchanging data with other instances of HERMES according to the defined policies;
- The HERMES Application Programming Interface (HAPI) component, which provides access to data to cybersecurity applications (for a given cybersecurity application X, it is abbreviated "CS App X" or simply "App X").

2.4.2 HERMES for Autonomous Military Systems

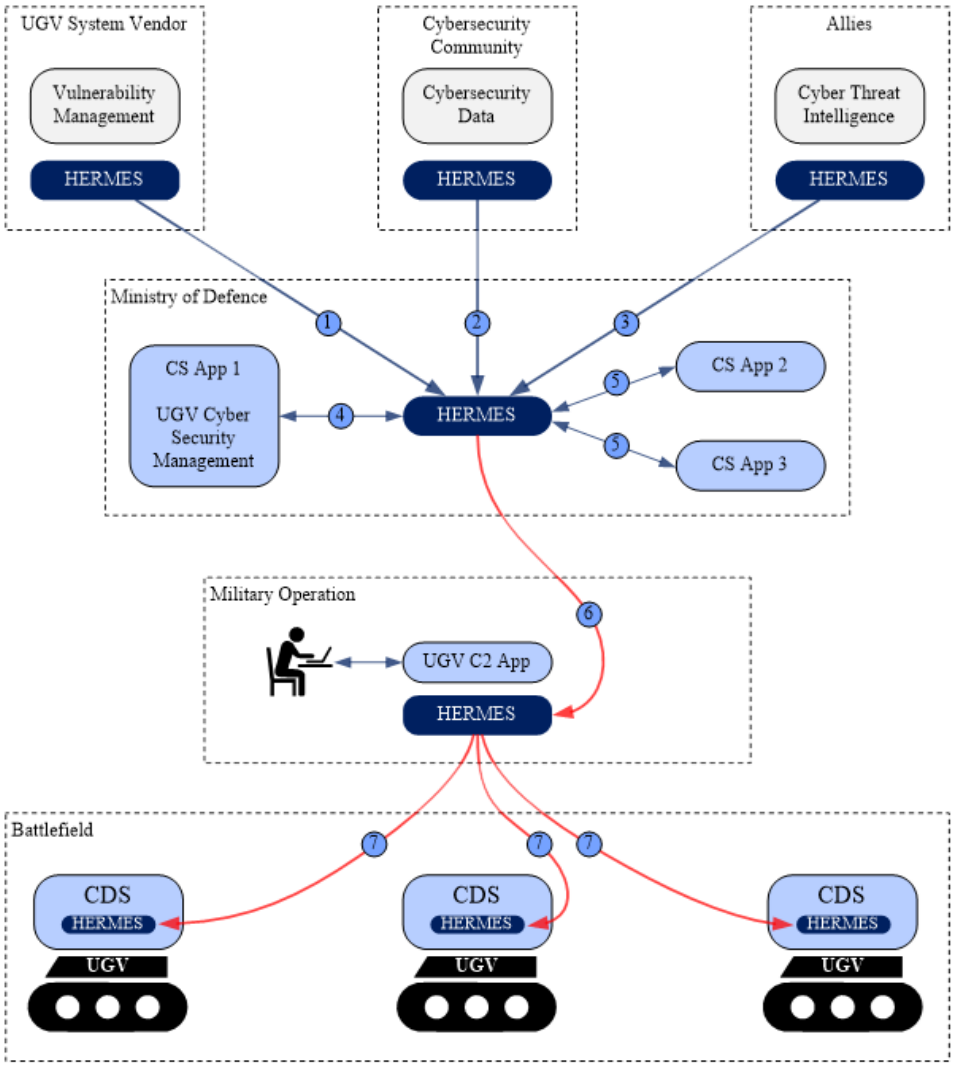


Figure 2: Autonomous Military Systems Use Case

In the use case illustrated in Figure 2, HERMES provides the ability to channel data from various sources and communities to Unmanned Ground Vehicles (UGVs).

On Figure 2, data flow #1 shows that the UGV System Vendor has information about potential vulnerabilities in its systems, which it will share with its customers through HERMES data exchange functionality. This functionality provides confidentiality and data exchanges according to policies that cover licensing, copyrights, and authorized uses, among other things. This gives to vendors the ability to prevent customers from further sharing this information, at least from a contractual and system point-of-view.

Data flow #2 shows a generic cybersecurity data exchanged within the global cybersecurity community. This could be through organizations such as the Forum for Incident Response and Security Teams (FIRST) or a national Computer Security Incident Response Team (CSIRT). This type of data is generic and may contain for example, vulnerabilities or security patches for operating systems and common software libraries.

In terms of illustrating the various sources of cybersecurity data, Figure 2 also shows generic cyber threat intelligence being shared by Allies via HERMES. This is data flow #3 in the diagram.

All this data and information is received at an office within the Ministry of Defense of the country operating the UGVs, for example, responsible for managing the UGV program. This could be done via a dedicated cybersecurity application ("CS App 1" in Figure 2) connected to HERMES, shown as data flow #4.

Other cybersecurity applications ("CS App 2" and "CS App 3") could also use HERMES as their source of data for other purposes, shown as data flows #5 in the diagram. The application used to manage the cybersecurity of the UGVs could be provided by the UGV vendor, giving the overall functionality to maintain the fleet of UGVs during its lifecycle, including the functionality required to manage cybersecurity of the fleet.

Once the staff managing the UGV fleet have considered the available information and decided how to address cybersecurity issues, the data would be passed to the operators of the UGV on deployed operations. This is data flow #6. It is expected that this would happen at a higher security classification, which would be facilitated by HERMES within the DXP installed at the Ministry of Defense. Data flow #6 is therefore shown as a red line.

The operators of the UGVs employed in military operations can then use a Command-and-Control application ("UGV C2 App" in Figure 2) to consider the information send by the managers of the UGV fleet. Then, merge this information with the current mission parameters and local threat information available in the theater of operations. Based on the assessed risks, which incorporates data from the UGV manufacturer, the cybersecurity community, Allies, UGV program managers, and operational considerations, the operators can decide which available measure to take. Then, use HERMES to transfer the data directly to the deployed UGVs. This is data flow #7, also in red as it is expected that it would be done at a higher level of classification.

Finally, Figure 2 shows a smaller HERMES application being part of a Cyber Defense System ("CDS" on the diagram). This part is most likely provided by the UGV vendor, showing how the components of HERMES can be designed to be minimalistic for constrained environments and embedded into other applications.

3 Common Requirements Collection

To define the capability needed to meet the objectives stated in section 2.4, the problems associated with information sharing and automation in the cybersecurity domain were examined. As a result, the challenges listed in section 2.1, as well as several key considerations applicable to that domain were identified. This led to the identification of eleven high-level requirements that the HERMES capability must meet to achieve its objectives. Those objectives are listed below and further analysed in the following section 3.2.

- **Requirement A**: Provide an adaptable, scalable, secure, and decentralized infrastructure based on a freely available core
- **Requirement B**: Provide for the controlled evolution of the syntax and semantics of multiple independent data models and their correlation
- **Requirement C**: Securely store both shared and private data
- **Requirement D**: Provide for customizable and controlled multilateral sharing
- **Requirement E**: Enable the exchange of data across non-connected domains
- **Requirement F**: Provide human and machine-readable interfaces
- **Requirement G**: Provide collaboration tools that enable burden sharing for the generation, refinement, and vetting of data
- **Requirement H**: Provide customizable quality-control processes
- **Requirement I**: Expose dissension to reach consensus
- **Requirement J**: Support continuous availability of data
- **Requirement K**: Enable commercial activities

3.1 End User Advisory Board (EUAB) and their Contribution

The above-mentioned high-level requirements are both necessary and sufficient. The following requirements are based on previous work from [DS13] and have been subject to feedback from the End User Advisory Board (EUAB) which can be found in Annex 2 together with a mapping to the following requirements. Each requirement will be further examined below. To receive the feedback from the EUAB a structured MDR questionnaire has been prepared. This is presented in Annex 1 of this document.

In alignment with the Grant Agreement and to ensure the project delivers a design that meets the functional requirements and produces deliverables that are satisfactory to the intended user community, an EUAB was set up. The EUAB includes representatives from the partners' involved Ministries of Defence (MoD) as well as domain experts (on cybersecurity information sharing and product development as well as other relevant areas).

The table below lists the existing members of the EUAB. As it can be identified, three out of the five representatives of EUAB come from Cyprus MoD (they provide 1 consolidated feedback to the project, where this is needed), and 2 of them are external domain experts. All the EUAB members have signed a non-disclosure agreement (NDA), to be able to participate to the project activities.

The Consortium will try to further increase the number of the EUAB members engaging the Estonian, French and German MoDs as well.

Table 2: HERMES EUAB Members

Contact Person	Organisation	Current Role/Position
Pafitis Aristodemos	Cyprus Ministry of Defense / National Security Authority	Communications and Cyber Defense
Polidoros Chatzidemetriou	Cyprus Ministry of Defense	Research and Innovation
Evangelos Englezakis	Cyprus Ministry of Defense / National Security Authority	Cyber Defense
Julien-Christophe Regragui	JIT SEC	Technical leader at a security operations center, but also a security specialist in code auditing, infrastructure auditing, intrusion auditing, and conformity auditing (PDIS - security incident detection contractor conformity auditing)
Joanna Śliwa	Employed at Military Communication Institute – National Research Institute (MCI-NRI)	Head of C4I Systems' Department

The EUAB is specifically setup to ensure the intended end-users of HERMES can exert influence over its design. It is also the key body that will provide the measure of success of the project through the five different milestone reviews scheduled during project execution. The first milestone related to Task 2.1 (Mission Definition Review - MDR) has been captured on M7 and the results are provided in this document, but also presented on a live Consortium meeting performed on June 15th. During this meeting, the EUAB discussed with the Consortium and representatives from the EU, the feedback from the MDR questionnaire.

3.2 List of Common Requirements

- **Requirement A: Provide an adaptable, scalable, secure, and decentralized infrastructure based on a freely available core**

Collecting data from a heterogeneous set of data sources, sharing part of it with partners and supporting automated cybersecurity operations while exploiting collaboration and outsourcing opportunities is a daunting challenge. While many organizations have established trust relationships within and outside their network of partners, few are able to agree on one single system that fits their specific set of requirements. Organizations are not only different in terms of size and type. Each organization is a unique ecosystem, facing different constraints and challenges while aiming to achieve its objectives. Adaptability is therefore necessary so that different organizations can deploy HERMES in a way that adapts to their specific situation. The organizations that HERMES must support range from a very small, single-site company to a large multinational federated organization. In many cases, the need to exchange information will be the only common point and mandating a fixed configuration will lead to an ineffective and inefficient solution, if not outright failure. HERMES must be scalable, not in terms of data quantity (which remains quite modest in cybersecurity) but rather because of an "evolutive data model" where correlation capabilities are necessary (see requirement B) to support dissension (see requirement I). These two requirements are expected to increase the need for storage capacity. As well, HERMES components must be scalable to meet a wide range of hosting constraints and performance requirements in different deployment scenarios. As the increasing need to share does not diminish the level of

confidentiality, availability, and integrity requirement of the exchanged data, HERMES must also be secure. Therefore, HERMES should provide flexible access controls to allow protection of the data as well as the possibility for custom workflows that will enable multi-step approval for actions affecting sensitive data. To allow greater exploitation of shared data while maintaining privacy requirements, HERMES must allow organizations to identify data elements that must be consistently replaced by privacy-protecting labels before being shared, as well as provide privacy-preserving query functionality. HERMES must allow organizations to contribute data anonymously. The HERMES architecture must also allow an organization to replace individual components to achieve a higher degree of assurance where it thinks it is necessary. Finally, organizations relying on HERMES must be able to review data exchanges to allow detection of security issues. Organizations that need to exchange information with each other do not always recognize a single common centralized authority for establishing trusted channels for the exchange. Organizations must therefore be able to deploy and interconnect their own HERMES "instance" as they see fit. HERMES must provide for "knowledge exchanges" that allow organizations to offer their data to others as well as discover other data offerings. As establishment of such knowledge exchanges is open to any organization, they will provide a way to mimic the current practice whereby organizations meet with each other in different, independent communities of interest (COI) that they control. In the service offerings published through the knowledge exchanges, data providers must be able to set the terms and conditions under which others can gain access to the offered data. A decentralized model allows COIs to emerge and subside without a central authority being aware of or needing to approve this. By making the HERMES software freely available, users will have access to data of improved quality that is contributed by the global security community. If there is convergence towards HERMES then a "critical mass" will be reached, at which point the monetary value of the data will far exceed the cost of implementing HERMES.

- **Requirement B: Provide for the controlled evolution of the syntax and semantics of multiple independent data models and their correlation**

In early work related to cybersecurity information exchange, one of the key difficulties encountered was obtaining agreement within a community to a standard data model. Over time, the situation has improved and there are now several standards that define data models and protocols that support information sharing and automated cybersecurity. However, there is no consistent use of these standards, models, and protocols, which makes information sharing, collaboration, and automation difficult, particularly in the absence of mappings between existing data models. Furthermore, organizations are often compelled to use the data models (standardized or not) implemented in the commercial products they have acquired. These are sometimes not interoperable, which means additional effort is required to correlate the data across products. In some cases, they are also inadequate, which means an organization must complement them to meet its specific needs. Despite the existence of standardized data models, organizations must still perform a substantial amount of effort to manage data models. Therefore, to achieve the stated objectives, HERMES must allow organizations to implement standardized data models of their choice via an evolutive data model that allows easy definition of new or existing data models without requiring a software development cycle. The proposed HERMES approach is to use "independent topic ontologies" (ITO) that capture each data model independently. This approach allows correlation of data elements across ITOs. In this context, the term ontology is used as defined in [GT93]: "a formal explicit specification of a shared conceptualization" and does not necessarily imply the use of ontological languages. From a software development point of view, an ITO can be seen as a logical container for a set of classes and relationships with associated attributes. An ITO is therefore a data model covering a defined domain of interest and HERMES does not limit the size, scope, or depth of ITOs in any way. Each instance of a class or relationship must have a globally unique identifier that can be used to correlate data across available ITOs, subject to access controls. The use of an evolutive data model implies that HERMES can support any data model and does not try to force a particular one on an organization or community of interest. The latter condition is necessary because defining a single, standardized ontology that covers the entire cybersecurity domain is not practical. Moreover, the evolutive data model allows HERMES users to easily implement new data models for which no current standards exist, as is the case for enterprise security models [ACG05] and network security

policies [CCSM05]. Sharing ITOs while they are in the process of being defined, and collaborative refinement of them, may also facilitate standardization efforts [SST04]. The evolutive data model allows existing data sources to be brought into HERMES relatively easily, thus taking advantage of prior investments. HERMES's support for correlation across ITOs will facilitate interoperability by allowing organizations to compose data queries that exploit ITOs covering the same topics at the same granularity. In a large organization, this work would be done by ontologists for the benefit of end-users. Finally, controlled evolution of ITOs must be possible. The HERMES objective of enabling automation will be achieved when organizations use data obtained through HERMES in cybersecurity applications. However, the evolutive data model allows users to modify existing ITOs as domain knowledge evolves by adding, modifying, or deleting classes, relationships, or attributes and by modifying the ITO syntax or semantics. Allowing ITOs to be freely changed would give rise to problems because organizations would have to revise their cybersecurity applications after every ITO change to accommodate the new syntax and semantics. By enforcing comprehensive version control of ITO definitions, HERMES will allow data providers to modify their data models and data consumers to adjust their automated applications independently and at their own pace.

- **Requirement C: Securely store both shared and private data**

HERMES should provide the possibility to an organization to store cybersecurity data that can be either kept private or shared with other organizations. When user data is identified as being private, HERMES must ensure that those data will never be available outside the organization. This allows organizations to exploit the evolutive data model and correlation capabilities in HERMES to store organization-specific data that is never intended to be shared. They will link it to data obtained from external sources and use the correlated information to support automated applications.

- **Requirement D: Provide for customizable and controlled multilateral sharing**

Since most cybersecurity organizations need to interact with a range of partners for different information exchanges, HERMES must provide mechanisms that allow customizable and controlled multilateral sharing. Organizations must be able to create and manage information-sharing relationships with their partners using the security protocols most appropriate for each individual case. All exchange of data must be through "Information Exchange Policies" (IEP) set up by the organizations themselves. It must be possible to define any number of IEPs to meet the various exchange requirements. HERMES must allow for the definition of any number of "communication channels" that implement encryption, authentication, and authorization mechanisms. HERMES must allow organizations to freely associate IEPs with communication channels to select the most appropriate means over which a particular exchange can take place. The decision to share can be applied to entire ITOs or sub-elements of ITOs, and to all the data or to individual data records. It must be possible to define a custom workflow for activating an IEP, as well as for authorizing the sharing of individual records in an IEP when needed. Therefore, when two or more organizations agree to exchange information with each other, they must select the applicable ITOs (thus choosing a particular ontology that describes the syntax and semantics of the data to be exchanged). Then, identify the parties to the exchange, capture the terms and conditions under which the exchange will take place, and select the communication channels that HERMES will use to execute the exchange. This approach decouples the technical details of how to create a secure tunnel for the information over possibly insecure networks. This is based on the details related to fine-grained access controls and the terms and conditions of the exchange, such as the intellectual property rights, rights to further distribute the data and uses that can be made of it. IEPs must also allow organizations to choose a suitable accounting mechanism to support commercial activities (see requirement K). Finally, IEPs must also indicate whether recipients can edit the exchanged data. Such authorization would be given to support collaboration or outsourcing. All exchanges must be logged and made available for audit review. Furthermore, exchanged data must always remain associated with the IEP under which it was received. HERMES must enforce the terms and conditions set forth in IEPs, and specifically the condition for redistribution of the data.

- **Requirement E: Enable the exchange of data across non-connected domains**

HERMES is expected to be deployed in various CISs that may not be directly interconnected (e.g., highly secure networks). Therefore, HERMES should provide mechanisms to facilitate exchange across these "air gaps". Such mechanisms must provide for the auditing of the transfers in a manner that would allow for the detection of sensitive information leakage or the introduction of malicious code. The exchange of data across non-connected domains must facilitate the efficient reconciliation of conflicting changes concurrently made in all HERMES deployments participating in an exchange of data.

- **Requirement F: Provide human and machine-readable interfaces**

A key requirement of HERMES is that it provides both human-specific and machine-specific interfaces. HERMES must provide a set of graphical user interfaces (GUI) that facilitate human interaction with the data, and a set of application programming interfaces (API) that facilitate machine interaction with the data. These interfaces must be well adapted to the needs of these very different types of users.

- **Requirement G: Provide collaboration tools that enable burden sharing for the generation, refinement, and vetting of data**

One of the key objectives of HERMES is to facilitate burden-sharing collaboration and/or outsourcing for the generation, refinement and vetting of cybersecurity data. While several organizations have established a sufficient degree of trust between each other allowing collaboration, current information systems do not provide sufficient support to make collaboration an effective and efficient approach for generating, refining, and vetting of data. In many cases the associated level of effort for collaboration is simply too high. Where collaboration does take place, it is often inefficient due to the absence of a facilitating system. HERMES must therefore provide tools that will address this issue. As a minimum, HERMES must provide a timely threaded discussion mechanism that can be used to annotate different data elements. As well, it must provide a chat facility that is subject to access controls and IEPs and that provides a capability to quickly establish a shared context to support discussing a particular data element.

- **Requirement H: Provide customizable quality-control processes**

HERMES will be used to aggregate and transform information from many sources to feed decision-making and automated processes. Inaccurate information could cause a business process to fail, resulting in undesired effects that can vary greatly in terms of significance. To successfully enable automation in cybersecurity, HERMES must provide the means to assure the quality of the data it provides. Quality assurance (QA) within HERMES refers to the planned and systematic activities that ensure that the data in the HERMES system meets the quality requirements specific to its intended use. QA is achieved through the application of custom quality-control processes (QCP) that are defined by users and partly managed within HERMES. Because HERMES data can be re-used for many purposes, ITOs, QCPs and quality requirements are associated to the use that will be made of the data, based on the concept of "curation". The curation identifies the ITOs that are needed to support an automated application as well as the QCPs that will be used to filter the data to provide only that data that meets the required quality. This allows QCPs to be re-used for different ITOs where applicable, and for ITOs to be re-used for different purposes (i.e., for different curations) even if those purposes have different quality requirements. QCPs can also be included in IEPs to ensure that data exchanged with external parties meets the desired quality requirement. In addition, HERMES must allow organizations to exchange QCPs and associated information so that QCPs can be re-used, outsourced, or performed in a collaborative fashion.

- **Requirement I: Expose dissension to reach consensus**

The fact that most databases are designed to hold a single value for each attribute of a data element, means that users cannot express disagreement about a value except by changing the value in the database (assuming they have the necessary privileges to do so). In consequence, it would change the value for all users. Since most common data repositories have no means to expose dissension about attribute values, errors and inaccuracies recognized by users remain hidden, which limits an organization's ability to improve the data upon which it relies for operations. HERMES must therefore expose dissension by allowing multiple possible values to be shown for each field. That would allow users to see that there is disagreement and eventually either reach consensus on which value is correct or agree to disagree. Data managers in the organizations participating in an exchange of data would have the ability to see all proposed values for an attribute and to select the one they consider to be correct for their organization. They can also choose to have HERMES always use the most recently entered value if they do not have the expertise to decide themselves for a particular type of data. Finally, HERMES must also let users to easily correct detected errors and inaccuracies by allowing "divergent values" to be used locally within an organization so that automated processing can proceed with the corrected data. This functionality can also help detect and address mischievous activities directed at data sources by malicious users.

- **Requirement J: Support continuous availability of data**

HERMES aim is to also meet availability requirements, even in the presence of cyberattacks. It cannot be assumed that an organization will always have external connectivity tool to obtain cybersecurity data. HERMES should therefore allow an organization to choose to hold a local copy of selected data previously exchanged. In such a case, the organization can continue to use that data even after disconnecting all external communication links (subject to the terms and conditions set forth in IEPs).

- **Requirement K: Enable commercial activities**

The private sector will be more motivated to use HERMES if it provides accounting models and functionality for selling data or data-related services. This in turn will lead to better-quality data for HERMES users. HERMES should therefore provide various accounting models for the usage of data, and the mechanisms must allow vendors of data and data services to control the dissemination of data exchanged under the terms of a commercial contract. Organizations need to be able to sell any data element, such as content (ITO data), the application of quality control processes, as well as professional services related to the management and refinement of HERMES data (such as assistance in defining ITOs, correlation and translation). If commercial activities are supported, organizations using HERMES will be able to make use of industry's extensive resources and expertise to obtain the data they require at a cost determined by market forces. As a result, end-users will have access to the best available data.

4 Conclusions

This document describes the work that has been performed during the first seven months of the project, in Task 2.1 – "Pre-Feasibility Study" and the outcomes which will be used during the project's lifecycle and more specifically in Task 2.2 – "Feasibility Study" and Task 3.2 – "Architecture".

This work, and report is also related to the first project Milestone "Mission Definition Review", captured at M7 (June 2022) of the project, with the involvement of the EUAB.

In addition, both HERMES use-cases have been presented as well as the components of the platform. The focus of the document was the identification and presentation of the common requirements that the platform should comply with. The identification of those common requirements has been performed via the feedback received from the EUAB with the completion of the MDR questionnaire.

The feedback from the EUAB is provided in this document along with the common requirements in align with the overall project concept and use cases.

5 References

[ACG05] Anderson, E., Choobineh, J., & Grimaila, M. (2005). An Enterprise Level Security Requirements Specification Model. 38th Hawaii International Conference on System Sciences. IEEE Computer Society.

[CCSM05] Cuppens, F., Cuppens-Boulahia, N., Sans, T., & Miège, A. (2005). A Formal Approach to Specify and Deploy a Network Security Policy. International Federation for Information Processing, 173, 203-218.

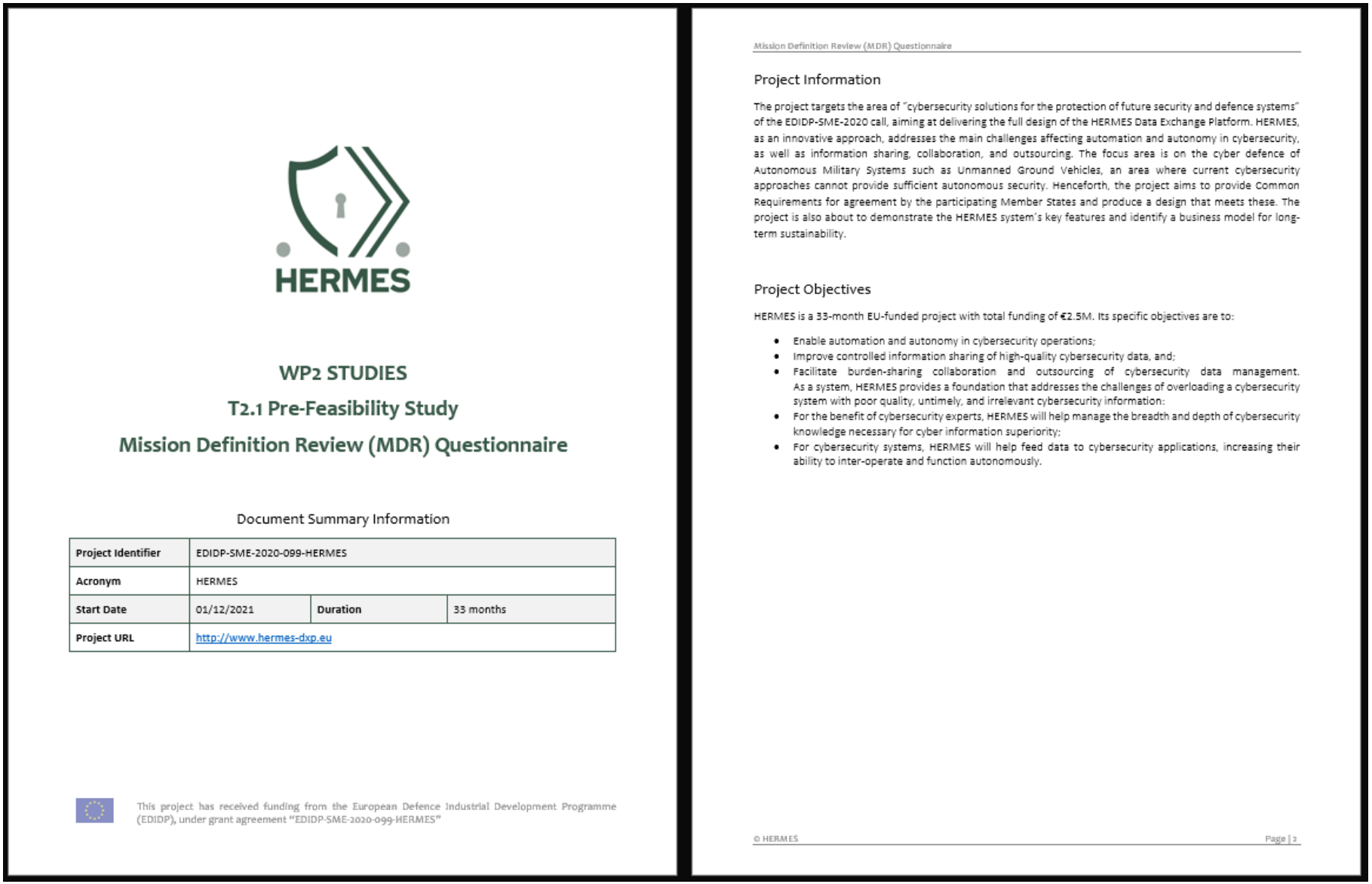
[DS13] Dandurand, L. and Serrano, O. S. (2013). Towards Improved Cyber Security Information Sharing. In Proceedings of the 5th International Conference on Cyber Conflict.

[GT93] Gruber, T. (1993). A translation approach to portable ontologies. Knowledge Acquisition, 5(2), 199-220.

[SDB14] Serrano, O. S., Dandurand, L. and Brown, S. (2014). On the Design of a Cyber Security Data Sharing System. In the Proceedings of WISCS'14.

[SST04] Sofia Pinto, H., Staab, S., & Tempich, C. (2004). DILIGENT: Towards a fine-grained methodology for DIstributed, Loosely controlled and evolvInG Engineering of oNTologies. Proceedings of the 16th European Conference on Artificial Intelligence (ECAI 2004), 393397. Valencia, Springer.

Annex 1: MDR Questionnaire for the EUAB



HERMES

WP2 STUDIES

T2.1 Pre-Feasibility Study

Mission Definition Review (MDR) Questionnaire

Document Summary Information

Project Identifier	EDIDP-SME-2020-099-HERMES		
Acronym	HERMES		
Start Date	01/12/2021	**Duration**	33 months
Project URL	http://www.hermes-dxp.eu		

This project has received funding from the European Defence Industrial Development Programme (EDIDP), under grant agreement "EDIDP-SME-2020-099-HERMES"

Project Information

The project targets the area of "cybersecurity solutions for the protection of future security and defence systems" of the EDIDP-SME-2020 call, aiming at delivering the full design of the HERMES Data Exchange Platform. HERMES, as an innovative approach, addresses the main challenges affecting automation and autonomy in cybersecurity, as well as information sharing, collaboration, and outsourcing. The focus area is on the cyber defence of Autonomous Military Systems such as Unmanned Ground Vehicles, an area where current cybersecurity approaches cannot provide sufficient autonomous security. Henceforth, the project aims to provide Common Requirements for agreement by the participating Member States and produce a design that meets these. The project is also about to demonstrate the HERMES system's key features and identify a business model for long-term sustainability.

Project Objectives

HERMES is a 33-month EU-funded project with total funding of €2.5M. Its specific objectives are to:

- Enable automation and autonomy in cybersecurity operations;
- Improve controlled information sharing of high-quality cybersecurity data, and;
- Facilitate burden-sharing collaboration and outsourcing of cybersecurity data management. As a system, HERMES provides a foundation that addresses the challenges of overloading a cybersecurity system with poor quality, untimely, and irrelevant cybersecurity information:
- For the benefit of cybersecurity experts, HERMES will help manage the breadth and depth of cybersecurity knowledge necessary for cyber information superiority;
- For cybersecurity systems, HERMES will help feed data to cybersecurity applications, increasing their ability to inter-operate and function autonomously.

© HERMES

This project has received funding from the European Defence Industrial Development Programme (EDIDP), under grant agreement "EDIDP-SME-2020-099-HERMES"

Mission Definition Review (MDR) Questionnaire

This questionnaire is about orienting discussions and feedback from experts in the domain of, or close to, data manipulation and exchange either in a high-level view or in the context of using technical solutions available on the market to handle exponential increase of data. In what follows, data may refer either to Threat Intelligence or vulnerabilities and sensitive information that affect an information system. The key points to have in mind are confidentiality, integrity, and availability of data - which are the three main principles in cybersecurity.

Particular attention to have to the "need-to-know" principle and how it scales among cybersecurity infrastructures. For each question, you may answer in shortly detailed points. When asking for a scale of importance from one to five, **one (1) refers to the least important and (5) five to the most important**. Please circle the selected answer, or put it marked area where applicable.

Based on your knowledge and expertise in the field, please feel in the questions below:

1. What do you think are the main challenges to manage and share the data?

   ☐ security of infrastructures
   ☐ trust in the supply chain (software and hardware integrity at all stages of the delivery)
   ☐ quality of data
   ☐ formats (in)compatibility
   ☐ insufficient tools to handle data processing and sharing (process is manual and too slow)
   ☐ organizational (e.g., complex approval process for data sharing)
   ☐ other:

2. In the context of multiple organizations, how would you explain the current limitations in sharing data even if agreements exist among these organizations?

   ☐ general lack of trust
   ☐ lack of controls over recipients
   ☐ rapidly increasing amount of information
   ☐ existing solutions limitations (e.g., specific type and format of data)
   ☐ other:

© HERMES

3. When more and more actors are involved, with possibly several different data formats to be shared, on a scale of one to five, how important is the format standardization for data?
   1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

4. On a scale of one to five, how important the data sharing infrastructure should be scalable?
   1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

5. On a scale of one to five, how important the data sharing infrastructure should be decentralized?
   1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

6. On a scale of one to five, how important is the possibility to exchange data with air-gaped systems?
   1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

7. On a scale of one to five, how important is the ability to automatically share important data according to the policy, and optionally handle automatic remediation based on transmitted data in the case of autonomous system systems (e.g., firmware update or adaptative strategy against a threat)?
   1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

8. On a scale of one to five, how important control on both sides of the data sharing process is important (e.g., allowing policies definitions or refinements)?
   1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

9. On a scale of one to five, how important is it to provide built-in tools to manage the data in addition to built-in human and machine-readable interfaces?
   1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

10. Knowing that automatically processing an enormous amount of data may reduce the value and interest of the shared data, how important - on a scale of one to five - is introducing quality-control processes?
    1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

11. Does improper data formatting and categorization limit or prevent data sharing with other organizations? In what cases raw data could be shared if there is no time for manual processing?

12. In an effort of solving possible issues raised in previous questions, what would be the requirements that existing solutions or an alternative one, should prioritize?

© HERMES

Annex 2: EUAB Feedback on MDR Questionnaire

Below are the combined answers, received from all members of EUAB, for Question 1 and 2.

1. What do you think are the main challenges to manage and share the data?

- ☒ security of infrastructures (this answer appeared 3 times)
- ☒ trust in the supply chain (this answer appeared 2 times)
- ☒ quality of data (this answer appeared 2 times)
- ☐ formats (in)compatibility
- ☒ insufficient tools to handle data processing and sharing (process is manual and too slow)
- ☒ organizational (e.g., complex approval process for data sharing)
- ☒ other:

  Mentality and engagement are also key aspects of this challenge. Only an enforced authority regulation or a regulatory system to embed in states security platform could ensure (possibly) the broad sharing of information.

2. In the context of multiple organizations, how would you explain the current limitations in sharing data even if agreements exist among these organizations?

- ☒ general lack of trust (this answer appeared 2 times)
- ☒ lack of controls over recipients (this answer appeared 2 times)
- ☒ rapidly increasing amount of information (this answer appeared 2 times)
- ☒ existing solutions limitations (e.g., specific type and format of data)
- ☒ other:

  The lack of trust is for sure the first aspect, because once send to the wild, you never know between which hands the information will fall. Moreover, organization will not want to share some kind of information because of “internal matters of security”. Many standards exist today, that does not prevent such behavior. Let only the air-gapped system, which are massive “black hole” of information.

This project has received funding from the European Defence Industrial Development Programme (EDIDP), under grant agreement “EDIDP-SME-2020-099-HERMES”

The Table below lists the scorings received from all members of EUAB, for the Questions 3 to 10. The mean (average) score for each question is also presented.

Table 3: EUAB Feedback on MDR Questionnaire

Question	Related requirements	Member A	Member B	Member C	Mean Score
3. *How important is the format standardization for data?*	B, I	2	5	5	**4,00**
4. *How important the data sharing infrastructure should be scalable?*	A	3	3	3,5	**3,17**
5. *How important the data sharing infrastructure should be decentralized?*	A	5	4	2	**3,67**
6. *How important is the possibility to exchange data with air-gaped systems?*	E	5	3	2	**3,33**
7. *How important is the ability to automatically share important data according to the policy, and optionally handle automatic remediation based on transmitted data in the case of autonomous system systems?*	C, D, G	4	5	4	**4,33**
8. *How important control on both sides of the data sharing process is important (e.g., allowing policies definitions or refinements)?*	C, D	3,5	5	3	**3,83**
9. *How important is it to provide built-in tools to manage the data in addition to built-in human and machine-readable interfaces?*	F	4	5	2,5	**3,83**
10. *How important is introducing quality-control processes?*	H	5	5	4	**4,67**

Below are the answers received from member A of EUAB, in Question 11 and 12.

11. Does improper data formatting and categorization limit or prevent data sharing with other organizations? In what cases raw data could be shared if there is no time for manual processing?

At the moment of writing, a standard exists in data exchange authorization: TLP (Traffic Light Protocol), that authorizes diffusion and sharing of intels (most of the times Threat Intels, containing markers and such important information). There are 4 levels, getting from public information (TLP: White), to Government and Industries secret (TLP: Red). In between there is Level Green and Amber. From Green Level and above, explicit authorization shall be given in order to authorize diffusion of information.

This can possibly be implemented in Autonomous system, although it would require maximum trust in such system, and chain of custody at all levels (leveraging the tripe-A scheme: Accountability, Authorization and Authentication Scheme, maybe usage of a private blockchain of some sort). Going in full AI is then a little bit trickier. Indeed, the level definition (White, Green, Amber, Red) not only lies in the end in the sole objective of the threat, but also giving the current geopolitical aspect. It is no more a matter of "security" but rather contextualization of the threat in the current world political state. Training AI in such broad area will require months or rather years, but should be possible. However, the trust in such technology might take longer, because of the highly sensitive nature of the date impacted by the decision of the AI.

12. In an effort of solving possible issues raised in previous questions, what would be the requirements that existing solutions or an alternative one, should prioritize?

As stated previously, letting AI the power to decide what to share could be problematic and could even be refused or deactivated in some industries. In such scenario, sharing of the information will stay as well done as per today: that means poor information sharing.

There are ways we could leverage such restrictions:

- Implanting (imposing legally?) systems (sensors) that will "catch" the information and send the raw information securely to the central system that will anonymize the source (could be done directly at the source), and according to filters will share the information to other system. AI will have the work of detecting threats also in such scenario and could possibly understand current political state from a "deeper" level. However, this would have to be enforced at each state level.
- As sharing is knowing, it is a fact that most of the times industries would like to receive data but not so much about sharing. Ideas would be to implement a ratio, allowing to get data if a defined ratio of inside sharing of own data is reached. If not, getting data will not be allowed. Such system is great to enforce sharing but could also be easily abandoned. Air gapped system are the target here as sharing from such systems will be more problematic.

The main questions about sharing the data remain the same as before:

- Where do we get data from inside the whole platform?
- How do we know we got sufficient data?
- Can we understand what kind of information we didn't get and why?
- What kind of information we need?

Today, there exist exchange standard like DXL (Data Exchange Layer) that is implemented by many security companies: McAfee (inventor), MISP, VirusTotal, Cortex. However, once again, we rely only on the quality of the data ingested. How and with what kind of power Hermes can do better from a technical / objective point of view?

Below are the answers received from member B of EUAB, in Question 11 and 12.

11. Does improper data formatting and categorization limit or prevent data sharing with other organizations? In what cases raw data could be shared if there is no time for manual processing?

Improper data formatting and categorization may totally hinder the usefulness of this data and even cause system faults when automatic data processing is applied, and the information is understood wrongly at the receiving side.

Both – semantics and syntax of messages must be understood in the same way by all sides of communication. Raw data can be shared only if it originally conforms to an agreed information sharing format.

12. In an effort of solving possible issues raised in previous questions, what would be the requirements that existing solutions or an alternative one, should prioritize?

The exchange of sensitive data about observed breaches and e.g., signatures created on this basis should be done with security mechanisms in place, especially privacy of this information, anonymization of the source of the breach, and control over further propagation of this information. Creating threat intelligence over such information sharing platform is important and valuable.

The information scope should enable advanced reasoning and machine learning, so it should include metadata related to the environment, symptoms, impact, etc.

It is also worth to share AI trained models, however their applicability may differ depending on specificity of the environment it has been learnt on. It would be also interesting to research on distributed learning techniques based on shared data.

Below are the answers received from member C of EUAB, in Question 11 and 12.

11. Does improper data formatting and categorization limit or prevent data sharing with other organizations? In what cases raw data could be shared if there is no time for manual processing?

I don't believe that differences in data formatting can prevent data sharing. Having a common standard would definitely be helpful. Raw data should not be shared unless lives are at risk and all other means sharing are not available. In any way this should be agreed beforehand by all participants in the information sharing system.

12. In an effort of solving possible issues raised in previous questions, what would be the requirements that existing solutions or an alternative one, should prioritize?

In my opinion the most important part of an information sharing system is to have a clear process of information flow/data dissemination. Careful design of the process and protocols that would facilitate data sharing would also solve any data format issues.

Any data management policies should be part of the agreement among the participants, taking into consideration integrity, availability, and confidentiality. In case of no strict requirements, participants should make effort to follow a common guide-line. Regarding system scalability, this should be considered in the design phase. A distributed system can be scalable if designed correctly.

I don't have strong opinion in favor of decentralization. In fact, the latest rise of decentralization hype (in the advent of cryptocurrencies and the so-called "web3") makes me skeptical.