



FP7 Grant Agreement N° 312450

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Project type: Network of Excellence (NoE)

Thematic Priority: FP7 Cooperation, Theme 10: Security

Start date of project: March 1, 2013

Duration: 48 months

D8.4 Publicly Announced CIPedia

Due date of deliverable: 30/04/2014

Actual submission date: 2/06/2014

Revision: Version 1

European Commission – Joint Research Center

Project co-funded by the European Commission within the Seventh Framework Programme (2007–2013)		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Author(s)	Marianthi Theocharidou, Christer Pursiainen (JRC)
Contributor(s)	Erich Rome, Jingquan Xie (Fraunhofer) Vittorio Rosato (ENEA) Eric Luijf (TNO)

Security Assessment	Dominique Serafin (CEA)
Approval Date	12/05/2014
Remarks	No security issue.

The project CIPRNet has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312450.

The contents of this publication do not reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the authors.

TABLE OF CONTENTS

1	INTRODUCTION – RATIONALE OF THIS DOCUMENT	4
1.1	Goal of CIPedia	4
1.2	Structure	5
2	CIPEDIA MODEL	6
2.1	List of terms	6
2.2	Glossary	6
2.3	Thesaurus	7
2.4	Taxonomy	9
2.5	Ontology	9
2.6	Proposed model: Wiki	9
3	CONTENTS	11
3.1	Proposed wiki page structure	11
3.2	Sources	12
3.3	Prototype Design	13
3.4	Users	14
4	SOFTWARE AND INTERFACE: PROPOSED SOLUTION	15
5	RISK AND COPYRIGHT	17
5.1	Risk factors	17
5.2	Liability and Terms of Use	17
5.3	Moderation	17
5.4	Copyright	18
6	PLANNING	19
7	MAINTENANCE	20
7.1	Server	20
7.2	Security and backups	20
7.3	Ethics and moderation	20
7.4	Statistics	20
8	USER INSTRUCTIONS	21
8.1	Page creation	21
8.2	Basic editing	22
8.2.1	Formatting	22
8.2.2	Links	22
8.2.3	Headings	23
8.2.4	List items	23
8.2.5	Files	23
8.2.6	References	23
9	REFERENCES	24
	ANNEX A: PREPARATORY WORK ON TERMINOLOGY	26
A.1	Existing definitions of basic terms	26
A.2	Discussion	29
A.3	Additional terms and definitions needed	31
	ANNEX B: AUTOMATED EXTRACTION OF GLOSSARY TERMS	32

1 Introduction – Rationale of this document

This deliverable¹ deals with CIPedia[®], which, as described in the project’s Work Programme, is a Wikipedia-like online community service focusing on Critical Infrastructure Protection and Resilience-related issues, to be hosted on the web server of the CIPRNet project. It is a multinational, multidisciplinary and cross-sectoral web collaboration tool for information resources on CI-related matters. It will promote communication between CIP-related stakeholders, including (multi)national emergency management, critical infrastructure operators and owners, manufacturers, CIP-related facilities and laboratories, academic researchers, policy makers, and the public at large. The CIPedia[®] service aims to establish itself as a common reference point for CIP concepts and definitions. It will gather information from various CIP-related sources and combine them in order to collect and present knowledge on the CIP knowledge domain. It will be dynamic, as it will allow stakeholders to update information as the domain evolves and new concepts emerge or receive different meaning.

This is a living document and it will reflect the current status of the CIPedia[®] service. This deliverable will require an update when CIPedia[®] is published to include examples of the final form of CIPedia[®] and reflect changes that occurred and could not have been foreseen when this deliverable was created.

1.1 Goal of CIPedia

CIP terminology varies significantly due to contextual or sectoral differences, which combined with the lack of standardization, create an unclear landscape of concepts and terms. In various cases similar terms are often used synonymously, e.g., Effect / impact / consequence / outcome, Hazard / threat / damage / harm, Event / incident or Emergency / crisis / disaster / catastrophe [TDTerm]. Moreover, some of the definitions provided by guidelines and standards are vague, misleading or require explanation by their authors (which is not available) [TDTerm]. Another problem is conflicting definitions. For example the established term of “consequence analysis” as used in the ECI directive, would need to be renamed to “impact analysis” when adopting ISO definitions [TDTerm]. As it is not likely that a new name for this term would be adopted by the communities, a definition of consequence analysis would be required.

CIPedia[®] will not aim at solving such conflicts. On the contrary, CIPedia[®] should try to serve as a point of disambiguation where various meanings and definitions are listed and discussed, guiding the reader to seek additional information to the relevant sources. CIPedia[®] should not attempt to decide upon a common definition, as this should be a process achieved collectively by the CIP community. CIPedia[®] will be a collaboration platform that may facilitate towards such a direction, but it will not act as a moderator on terminology discussion.

Communicated through the EC DG JRC, CIPedia[®] will have a trusted authority, which will provide the design and the initial content of CIPedia[®]. All the CIPRNet partners will contribute in enriching the information shared by CIPedia[®] in its initial stages of development. Fraunhofer, the CIPRNet lead partner, will be responsible for the hosting and maintenance of CIPedia[®] in the CIPRNet Portal. Following the completion of its initial stage, all partners will communicate CIPedia[®] to CIP stakeholders and the public in order to ensure the community gets acquainted and participates. The announcement will also be included in the European CIIP Newsletter (ECN), which is the official dissemination outlet of CIPRNet. JRC will

¹ The authors would like to thank Simona Canterella (JRC), Athina Mitsiara (JRC), Gerald Vollmer (JRC) and Erich Rome (Fraunhofer IAIS) for their collaboration and useful comments.

communicate the existence of CIPedia[®] through the European Reference Network for Critical Infrastructure Protection (ERNICIP) [ERNICIP].

1.2 Structure

This deliverable aims to clarify and define the main parameters and components of the CIPedia[®] service, as well as to identify the main related challenges and risk factors. It is thus aimed to be an orientative plan, whose proposals should be agreed upon with the main stakeholders before one goes forward to build the service itself. It is hoped it helps to find the right focus and scope of CIPedia[®], avoiding harmful overlaps and instead creating synergies between related activities, and taking into account the user requirements and needs of the target groups.

Section 2 discusses available knowledge models that could be used for CIPedia[®], as well as CIP-related approaches that currently exist (glossaries, taxonomies, thesauri, etc.). Then the proposed wiki model is described and the rationale for selecting a wiki service is discussed. Section 3 describes the procedure for creating the contents of CIPedia[®], while Section 4 describes the software and interface that was selected. Risk and copyright issues are discussed in Section 5. The plan for publishing CIPedia[®] is presented in Section 6 and Maintenance procedures in Section 7. A short manual is included in Section 8. The references used for this document can be found in Section 9. Annex A presents preparatory work performed by consortium members regarding terminology. Finally, Annex B depicts examples of the use of automated extraction tools.

2 CIPedia Model

CIPedia[©] aims at providing knowledge on CIP to a wide international audience. There are multiple models to represent such knowledge, ranging from simple glossaries to complex ontologies. In this subsection, we will examine various models and identify existing, relevant approaches already designed for CIP.

On the Semantic Web, vocabularies define concepts and relationships (also referred to as “terms”) used to describe and represent an area of concern, such as the domain of Critical Infrastructure Protection. A concept is “a unit of thought, formed by mentally combining some or all of the characteristics of a concrete or abstract, real or imaginary object. Concepts exist in the mind as abstract entities independent of terms used to express them” [ANSI/NISO].

Figure 1 depicts various types of knowledge representation suitable for CIP, as we progress from simpler towards more formal data structures. Let us describe the different alternatives listed in this figure in some detail before proposing a suitable format for CIPedia[©].

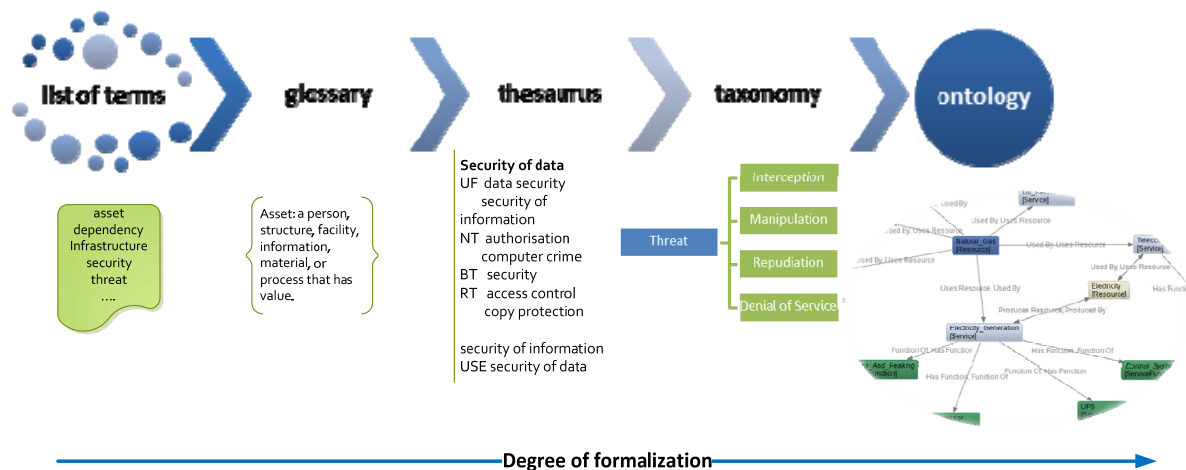


Figure 1: Models for knowledge representation²

2.1 List of terms

A list of terms, or dictionary, is “a reference book that contains words listed in alphabetical order and that gives information about the words' meanings, forms, pronunciations, etc. or shows their meanings or translations in a different language or a reference book that lists in alphabetical order words that relate to a particular subject along with their definitions and uses” [MWD].

2.2 Glossary

Glossary is “a list that gives definitions of the hard or unusual words found in a book or a dictionary of the special terms in a particular field or job” [MWD]. It is usually bound to a

² The figure has been adapted from [Navigli08]; it also contains information from [Ferigato12; Vlacheas11; SERSCIS].

particular scientific domain and the terms may be accompanied by descriptive comments and explanatory notes, such as definitions, synonyms, references, etc.

In the literature there are various CIP-related glossaries provided by international organizations. Examples include the multilingual glossary “2009 UNISDR Terminology on Disaster Risk Reduction” by the United Nations International Disaster Reduction Strategy (UN IDRS) [UNISDR]. The glossary provides basic one-sentence definitions on disaster risk reduction, based on a broad consideration of different international sources. Each definition is followed by a comments paragraph in order to give additional context, qualification and explanation.

One of the activities of the EU CBRN Action Plan, performed by the EC Joint Research Centre is the development of an “Information Tool on chemical, biological, radioactive and nuclear hazards for Practitioners in Protection and Response” (CBRN Glossary) in all EU languages (H.53) [CBRNG]. The project is developed in cooperation with EUROPOL and is cofunded by DG HOME. It has now evolved to include the explosives aspect (CBRNE glossary). The glossary has been developed with the participation of experts in Chemical Biological, Radioactive, Nuclear and Legal Issues from Member States Authorities, Europol, Eurojust, JRC Ispra and JRC Karlsruhe. At the moment, the glossary contains 330 short and concise entries of terms and their definitions, available in 23 languages. The content is aimed for professional use to practitioners, not to scientists or the general public, as opposed to CIPedia which aims to have a wider coverage both in terms of content and in terms of audience.

The glossary of the US National Infrastructure Protection Plan 2013 [NIPP13, p.29] collects the basic terminology from US legislation and guidelines. Similar definitions can be found in the glossary by the Federal Emergency Management Agency [FEMA] of the U.S. Department of Homeland Security, as part of the Critical Infrastructure Protection and Resilience Toolkit. A brief glossary of CIP-related terms can also be found on “The Preliminary Cybersecurity Framework” [NIST, p.42] which is developed by the National Institute of Standards and Technology (NIST), in collaboration with industry, and aims in providing guidance for managing cybersecurity risk, in response to the US Executive Order 13636, “Improving Critical Infrastructure Cybersecurity”.

There are also glossaries which are sector-specific. For example, there is the IAEA Safety Glossary (edition 2007) [IAEA07] by the International Atomic Energy Agency, which contains terminology used in nuclear safety and radiation protection. The North American Electric Reliability Corporation (NERC) glossary [NERC] clarifies the terms used in the NERC Reliability Standards, which focus on electric energy. Similarly, the Department of Energy has published a relevant glossary [DoE].

2.3 Thesaurus

According to ISO 25964-1:2011, a thesaurus is defined as a “controlled and structured vocabulary in which concepts are represented by terms, organized so that relationships between concepts are made explicit, and preferred terms are accompanied by lead-in entries for synonyms or quasi-synonyms” [ISO 25964-1:2011]. A thesaurus is thus a controlled closed set of terms, which means that it contains the language of a specific domain and the relationships between its words. ISO 25964-1 explains how to build a monolingual or a multilingual thesaurus, how to display it, and how to manage its development. There is a data model to use for handling thesaurus data [ISO 25964-1:2011] (especially when exchanging data between systems) and an XML schema for encoding the data. The data model sets out five basic classes: Thesaurus, ThesaurusArray, ThesaurusConcept, ThesaurusTerm, and Note [Dextre12]. The main types of relationship include: (a) equivalence (between synonyms and near-synonyms), (b) hierarchical (between broader and narrower concepts) and (c) associative (be-

tween concepts that are closely related in some non-hierarchical way) [Will12]. In multilingual thesauri equivalence also applies between corresponding terms in different natural languages.

For instance, the EUROVOC Thesaurus [EUROVOC] is a multilingual, multidisciplinary thesaurus covering the activities of the EU, the European Parliament in particular. It contains terms in 23 EU languages (Bulgarian, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish), plus Serbian. It covers CIP-related sectors, such as the energy or transport sector.

In an attempt to define the CIP domain, a CIP Thesaurus [Cantarella12] is been prepared by JRC. Through it, European stakeholders can organize their documents in a shared, common language, avoid misinterpretation of concepts and standardize information exchange. The thesaurus is been created based on a corpus of documents in the CIP domain, with an emphasis on critical information infrastructures. Index terms were chosen using two main thesauri, INSPEC³ and Eurovoc. It is a multilingual thesaurus; it was created in English and translated in Italian and French. An example of the term “advanced persistent threats” is presented in Table 1.

Table 1: CIP Thesaurus example

advanced persistent threats	
	<i>menaces persistantes avancées</i> (fr)
	<i>minacce persistenti avanzate</i> (ita)
Class/Facet:	Actions: Activities
UF	APT
TT	Activities
BT	cyber-threats
RT	Attacks
	cyber espionage
	Hackers
	data transmission
	Internet
	political espionage
	security of data

³ The INSPEC thesaurus has been developed by the Institute of Engineering and Technology (IET), in order to support search functions of the INSPEC database, which contains bibliographic and indexed records to physics and engineering global research literature. The 2012 edition contains 18,755 terms and is commercially available.

2.4 Taxonomy

Taxonomy is a “collection of controlled vocabulary terms organized into a hierarchical structure. Each term in the taxonomy is in one or more parent/child (broader/narrower) relationships to other terms in the taxonomy” [ANSI/NISO]. Taxonomy does not necessarily have the related-term relationships and other features of a standard thesaurus and it could be a subset of a thesaurus.

The US Department of Homeland Security has created an Infrastructure Data Taxonomy [DHS] to facilitate a common understanding of terminology within the critical infrastructure protection community. This taxonomy categorizes infrastructure assets into their respective sectors and further categorised into more detailed levels, such as sector, subsectors, segment, sub segment, and asset type. It is intended for use within the USA and it is not publically available.

2.5 Ontology

Gruber defines ontology in the context of computer and information sciences [Gruber08], as a set of representational primitives -typically classes (or sets), attributes (or properties), and relationships (or relations among class members) - with which to model a domain of knowledge or discourse. The definitions of the representational primitives include information about their meaning and constraints on their logically consistent application.

Ontology differs from a thesaurus in the sense that it is “a model of the domain of interest and is used for proving the validity of logical inferences on that domain, [while]... a thesaurus is a purely grammatical construction whose model is in the indexed sets of documents” [Ferigato12].

In the literature, there are a few attempts to form CIP-related ontologies. For example, European Union Agency for Network and Information Security (ENISA) proposed the combination of several taxonomies and ontology for understanding resilience as a network design target [Vlacheas11]. The DIESIS project designed a Knowledge-Based System (KBS) [Masucci09; Tofani10] that incorporates a meta knowledge infrastructure ontology, which is a general template to describe infrastructures and their dependencies, infrastructure ontologies for specific critical infrastructures and federation ontology to express dependencies between infrastructures.

2.6 Proposed model: Wiki

All the above models present potential formal ways to represent CIP-related knowledge. CIPedia aims at reflecting the collective knowledge of its domain. Thus, it will invite users (CIP-related stakeholders) to engage in the process of content creation, evaluation and maintenance. This means that users will be able to not only view CIP-related content but also suggest additional topics or edit existing ones. Thus, it is important that CIPedia provides simple tools, usable by the majority of users, such a web browser and simple text editing. Therefore, the wiki model is proposed, as opposed to more complex data structures, such as thesaurus or ontology. The latter would require expert assistance and heavy moderation in order to maintain the structure and especially the relationships between the terms. While the moderators should ensure that the topics in CIPedia are related in a meaningful way, the adopted structure should be ad hoc, only performed via page links. Such a scheme is easier to maintain and will allow more timely update of the content, which is crucial for the success of

CIPedia. Currently standard wikis offer limited support for collecting structured data, but the Wikidata project is working towards such a direction⁴.

In its initial stages of development, CIPedia may resemble to a glossary, which means it will be a collection of pages – one page for each concept with key definitions – but it aims to expand more and include discussion on each concept, links to useful information, important references, disambiguation notes, etc. Just like Wikipedia, articles should begin with an appropriate definition or possible two or more rival definitions, but they should provide other types of information about that topic as well. The full articles will eventually grow into a form very different from dictionary entries. Moreover, if two concepts are used in a similar way, they can be merged into one page and a discussion on their use can follow. CIPedia will not try to reach consensus about which term or which definition is optimum, but it will record any differences in opinion or approach.

One of the advantages of a wiki is the ability to perform edits in real-time, meaning that content updates can appear almost instantly online. In most public wikis, moderation is light, meaning that there is no review before modifications are accepted.

Usually though, wikis are open to alteration by the general public with some form of user registration. To avoid potential abuse of CIPedia, user registration will be required and content changes (comments, changes, corrections, new pages) will be accepted by a team of experts, responsible for moderating CIPedia.

Despite this limitation, the key principles will be the following:

- CIPedia will be easy to use and learn
- Any user will be able to view content (including history, comments and previous versions)
- Any (logged in) user can comment and suggest changes (similarly to the talk section of Wikipedia)
- The moderator(s) will be able to edit content in real-time

Currently, there are few wikis that have CIP-related content. Examples include the wiki-glossary of the FOCUS project regarding European security research [FOCUS], which contains the definition of various security related terms, including a limited collection of CIP-related terms. The Wikipedia page of Critical Infrastructure Protection [WIKI] offers some CIP-related information, mainly regarding US policy on the issue. Similarly there are pages related to CIP in public wikis, such the ITLaw Wiki [ITLW]. The Cybersecurity wiki of the Berkman Center for Internet and Society at Harvard University [BCIS] also offers a list of documents categorised according to types of Critical Infrastructures.

However, none of these approaches covers in depth CIP-related information, nor reflects sufficiently the European perspective in CIP.

⁴ Unlike Wikimedia Commons, which collects media files, and Wikipedia, which produces encyclopedic articles, Wikidata collects data, in a structured form. The goal is to enable easy reuse of that data by Wikimedia projects and third parties, and will enable computers to easily process and “understand” it. More information is available here: <http://www.wikidata.org>.

3 Contents

CIPedia will include non-restricted information on CIP-related matters, including such elements as CIP glossary, information on European and international CIP policies, links to main policy and regulatory documents, CIP-related inventories and databases, and so forth. It will include but extend beyond CBRNE, as the field is too specialised for the general public. The prototype will be created in English, with the possibility to translate it to other languages as well.

3.1 Proposed wiki page structure

Each term will have a dedicated wiki page, where the text contains links to other related terms (if any). A possible structure of a typical page may include the following:

- **“Page” tab:** This is the information section of the page.
 - **Read mode:** This mode presents the wiki page which is available to be read by the users of the wiki. An indicative structure is the following one:
 - Introduction
 - Key definitions
 - Official European definition
 - Definitions from international organizations
 - National definitions
 - Standards’ definitions
 - Discussion topics
 - Relevant terms (disambiguation pages)
 - Notes (containing the links of the document)
 - References (containing additional references or reading material).
 - **Edit mode:** This mode allows a page to be edited and contains three tabs:
 - Wikitext: Displays the current source code of the page and toolbars for editing.
 - Preview: Shows how the page will appear after the current changes.
 - Changes: Lists the current changes performed on the page.
 This mode also offers a textbox for a summary to be inserted, as well as three buttons, namely Save page, Show preview and Show changes.
 - **History mode:** This mode lists the versions of the page coupled with a timestamp, information on the user who performed the change, and information on the changes performed. It offers an option to compare various selected versions of the page.
- **“Discussion” tab:** This is an area where users can post changes or comment on the quality of information, so that moderators can update content. An equivalent in Wikipedia is the “Talk” tab which accompanies each wiki page.

In the figure an example wiki page is presented, i.e. the wiki page of the term “critical infrastructure”⁵. The page follows the structure described above.

⁵ https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Critical_Infrastructure

The screenshot shows a CIPedia page for "Critical Infrastructure". The page is in "Read" mode. The main content area includes a "Contents" table of contents, a "Definitions" section with an "Official European Definition" and "National Definitions", a "US Definition", a "See also" section with links to "European Critical Infrastructure (ECI)" and "Critical Infrastructure Protection (CIP)", and a "Notes" section with two references. The page footer indicates it was last modified on 30 April 2014 and has been accessed 23 times. The sidebar contains navigation links like "Main page", "Community portal", and "Aktionen".

Figure 2: Example of a CIPedia page (on Read mode)

3.2 Sources

CIPedia will try to utilise the knowledge acquired by the existing approaches reviewed earlier, while respecting copyright restrictions. In its initial phase, CIPedia's prototype will resemble more to a glossary in the sense that the initial wiki pages will be a core set of index terms coupled with key definitions and references. The information already collected in the CIPR-Net report TechDoc2: Terminology [TDTerm] will be used and updated. As indicated in this report, CIPRNet uses terms from various scientific and technical domains. CIPRNet makes use of and extends a glossary of terms and definitions started in an earlier related project (IR-RIIS) and continued in the related project DIESIS. This glossary of terms and definitions will be a basis for a common understanding inside CIPRNet and will be updated in CIPedia. It covers topics in the domains of critical infrastructures (CI) and their protection (CIP), security, safety, some fields within computer science, some CI sectors and more. The report extends this set of terms including definitions from several relevant sources, including ISO standards, United Nations reference documents and definitions gathered from related EU projects. Exempts from the report are included in Annex A. Reporting on the pros and cons of certain definitions will be added later in CIPedia, with references to literature.

In order to select these index terms, two thesauri will be used as a starting point, JRC's CIP Thesaurus and the CBRNE Glossary. From these, terms will be selected in order to form the initial pool of wiki pages. The main criteria for such a selection would be their existence in both sources, their strong relevance to CIP, their importance for the general public, as well as their non-confidential nature. To supplement the initial set of index terms/pages, the CIPRNet consortium will also collect a pool of key CIP documents (policy, research, deliverables), which will be parsed with available automated tools for retrieving additional index terms.

Term extraction solutions can be found freely available on the web [TES] and some of them are available as a web service, for example the Termine service [TERM] or the Fivefilters [FF] tool. Annex B demonstrates the outcome of such a tool on legislative or policy docu-

ments. Similarly, named entity extraction systems like TextRazor [TRZ], can provide a deeper analysis of the content and extract relations, dependencies between words and synonyms, enabling powerful context aware semantic applications.

For this initial set of terms, definitions will be retrieved by key legislative documents of the European Commission, as well as from the available CIP-related glossaries presented earlier, such as the CBRNE glossary, the 2010 DHS Risk Lexicon, and others. The collected pool of CIP documents will be also used as reference in order to (a) expand the content of the wiki pages, (b) initiate discussion topics, (c) analyse sub-terms and related concepts and (d) create new related pages.

Where official standard definitions (e.g. ISO, IEC, CEN/CENELEC, ETSI etc.) exist, these will be referred to. Similarly, official national or international definitions will be added.

3.3 Prototype Design

Verardi et al. propose a semi-automated method in order to create a taxonomy that characterizes a scientific domain for a particular Network of Excellence (NoE) [Veraldi07]. Their method allows for progressively creating more formal data structures (lexicon, glossary, taxonomy, ontology). Each of these structures are created by automatic extraction and enhanced manually by the community members, using suitable Web collaborative work tools, like the CIPedia wiki software. We draw upon this proposed method and recommend the following process in order to create the CIPedia prototype.

1. Select domain sources: Create manually an archive of key documents for CIP (e.g., CIP Plans, Standards, Directives, Project Deliverables etc.)
2. Define a list of terms
 - a. Use (free) term extraction tools to automatically create an initial glossary of “popular” terms (examples)
 - b. Manually collect additional terms by existing glossaries
 - c. Manually process the list to create an initial set of terms
3. Identify definitions (manually)
4. Manually validate the obtained glossary
5. Identify relationships between terms (to create taxonomy)
6. Enrich the glossary with related terms
7. Add terms to the selected wiki tool
8. Communicate prototype and receive feedback to the CIPRNet partners⁶
 - a. Remove irrelevant entries
 - b. Add missing entries
 - c. Add or modify definitions and descriptions
9. Add terms to the selected wiki tool

⁶ Glossary evaluation-extension [Veraldi07]: In this phase, partners were solicited to express a graded vote for each definition, ranging from -3 to +1. A -1 vote is given to “not fully convincing” definitions; -3 are unacceptable definitions. Partners were also encouraged to add a new definition if they felt that none of the available definitions were adequate or if no definition was available for a term.

3.4 Users

Initial contents will be provided by the EU DG JRC team and will be reviewed, updated and expanded by all CIPRNet partners. It would be useful to have a committee which will review the initial contents of CIPedia before its publication.

Since the information published in CIPedia will be publically available, it was assessed that CIPedia does not require a complex access control scheme, such as the one of CIWIN (Critical Infrastructure Warning Information Network)⁷.

Therefore, the suggested user roles for CIPedia are the following:

- Readers: all unregistered user who can access the content⁸.
- Editors: a registered user who can recommend content.
- Moderators: Responsible for updating the content and managing editor register.
- Administrators: Responsible for software and hardware maintenance, backup and security.

Users will be supported with a brief online help manual (see chapter 8). The option of a ‘video’ help will also be considered in future releases of CIPedia.

⁷ CIWIN defines three user types with various levels of content access and private areas for the member states, where they can exchange information on a national level.

⁸ The option to only have registered users accessing content will be examined, as a way to monitor the demographics of the users (audience of CIPedia) accessing the wiki.

4 Software and interface: proposed solution

The CIPedia software should have or support the following features:

- Support of multiple languages
- Search capabilities
- Moderation capabilities / Access control/ Process for approval of user registration
- Simple interface (to appeal to more users)
- Versioning and error controls
- Open source/ Free
- Capability to recommend links on a page before posting (to make sure the content is interconnected)

The preferred solution in order to integrate a Wiki type system⁹, fulfilling the above criteria, will be based on the solution already existing at Fraunhofer IAIS. Thus CIPedia will be hosted on Fraunhofer's WiKi farm, and it can be available immediately. The provided software is MediaWiKi (known from Wikipedia) and some MediaWiKi extensions¹⁰ can be provided by Fraunhofer's WikiFarm support team. Maintenance (software, hardware, backup, security) will be provided by Fraunhofer. Moreover, external persons can function as administrators/moderators. The CIPRNet logo can be integrated and the interface can be altered if needed. The access control is flexible and it can be access with a password at the early stages of development and later on, read-only access for everyone and write access to registered users.

CIPedia is currently hosted on the Fraunhofer wiki farm¹¹. The main page is depicted on the figure below, but access to the wiki is restricted, as it is currently under development.

⁹ Web collaboration solutions (emphasis on wiki software) are discussed in: http://collaboration.wikia.com/wiki/List_of_wiki_software; <http://www.wikimatrix.org/> (tool to compare various wiki options); http://en.wikipedia.org/wiki/Comparison_of_wiki_software

¹⁰ Mediawiki (<http://www.mediawiki.org>) is the most widely used free wiki type software. It also includes an extension 'LinkTitles' (<http://www.mediawiki.org/wiki/Extension:LinkTitles>) which links the words within the page to pages which have the same name. Article/Page workflow approval process is available through extension: <https://www.mediawiki.org/wiki/Extension%3aFlaggedRevs>.

¹¹ <https://publicwiki-1.fraunhofer.de/CIPedia/index.php>

Talk Preferences Watchlist Semantic watchlist My new messages (none) Contributions Log out

Page Discussion Read Edit View history

CIPedia© Main Page

CIPedia©, as described in the CIPRNet's Work Programme, is a Wikipedia-like online community service focusing on **Critical Infrastructure Protection and Resilience**-related issues, to be hosted on the [web server of the CIPRNet project](#).

Starting from the CIPRNet Work Programme, CIPedia© is planned to be a **Wikipedia-like online community service** that will be one component of the CIPRNet's **VCCC (Virtual Centre of Competence and expertise in CIP)** web portal, to be hosted on the web server of the CIPRNet project. It is a multinational, multidisciplinary and cross-sectoral web collaboration tool for information sharing on CI-related matters. It will promote communication between CIP-related stakeholders, including policy-makers, competent authorities, CIP operators and owners, manufacturers, CIP-related facilities and laboratories, and the public at large. The CIPedia© service aims to establish itself as a common reference point for CIP concepts and definitions. It will gather information from various CIP-related sources and combine them in order to collect and present knowledge on the CIP knowledge domain. It will be dynamic, as it will allow stakeholders to update information as the domain evolves and new concepts emerge or receive different meaning.

CIP terminology varies significantly due to contextual or sectoral differences, which combined with the lack of standardization, create an unclear landscape of concepts and terms. CIPedia© will not aim at solving such conflicts. On the contrary, CIPedia© should try to serve as a point of disambiguation where various meanings and definitions are listed, guiding the reader to seek additional information to the relevant sources. CIPedia© should not attempt to decide upon a common definition, as this should be a process achieved collectively by the CIP community. CIPedia© will be a collaboration platform that may facilitate towards such a direction, but it will not act as a moderator on terminology discussion.

CIPedia© aims at providing knowledge on CIP to a wide audience, including professionals, scientists and the public at large. There are multiple models to represent such knowledge, ranging for simple glossaries to complex ontologies. In this subsection, we will examine various models and identify existing, relevant approaches already designed for CIP.

In its initial stages of development, CIPedia© may resemble to a glossary, which means it will be a collection of pages – one page for each concept with key definitions – but it aims to expand more and include discussion on each concept, links to useful information, important references, disambiguation notes, etc. Just like Wikipedia, articles should begin with an appropriate definition or possible two or more rival definitions, but they should provide other types of information about that topic as well. The full articles will eventually grow into a form very different from dictionary entries. Moreover, if two concepts are used in a similar way, they can be merged into one page and a discussion on their use can follow. CIPedia© will not try to reach consensus about which term or which definition is optimum, but it will record any differences in opinion or approach.

This page was last modified on 4 April 2014, at 14:14.

This page has been accessed 24 times.

[Privacy policy](#) [About CIPedia](#) [Disclaimers](#)

Powered By

Figure 3: CIPedia main page

5 Risk and Copyright

5.1 Risk factors

The CIPedia process may face risk, both during the development phase and after its publication.

Table 2: CIPedia Risk

Risk Scenarios	Scale	Contingency Plan
Use of copyrighted or confidential information	Low	Clear list of rules Moderation
Open to SPAM or Vandalism	Medium	Required login to edit page Mechanism to ensure reverting to older version easily
Wrong or outdated content	Low	Moderation by scientific staff
Failure to update – Low visibility	Medium	Communicated via various communication channels of the consortium
Moderating challenges (too many updaters, too few moderators)	Medium	Responsibilities should be defined for the partners of the consortium
Double entries – Conflicting entries	Medium	Moderation The use of appropriate tools will be explored
Disagreement in terminology	Low	CIPedia's structure will allow the listing of various definitions of a term
Corrupted structure	Low	Moderation The selection of the wiki model does not require a strict structure

5.2 Liability and Terms of Use

In order to avoid most of the risks, CIPRNet –type of service needs to establish Terms of use to define liability (check https://wikimediafoundation.org/wiki/Terms_of_Use).

5.3 Moderation

The moderating options suggested in order to avoid problems are: (a) accept, (b) reject (totally), (c) reject with comments. The moderators should not edit existing text posted by users. Owner of CIPedia[®] is the CIPRNet consortium.

5.4 Copyright

In terms of copyright, the term of use should mention that the wiki should not be used for commercial purposes; there should be appropriate citations and care to not cite confidential information.

Moreover, CIPedia[®] needs creative commons license (<http://creativecommons.org/>)

6 Planning

The construction of CIPedia will have following phases:

Table 3 CIPedia Plan

Date	Phases
March – April 2014	Fraunhofer IAIS provides the WIKI software (see section 5) JRC collects contents for a pilot version of CIPedia (see section 3.3)
15 May 2014	First version of CIPedia is created by JRC
20 May 2014	Internal review and update is completed by JRC (ERNCIP office) Stakeholders are informed (DG-HOME)
07 June 2014	Fraunhofer and TNO contribute changes and updates to the pilot CIPedia
June-August 2014	All CIPRNet partners comment and contribute to the pilot CIPedia
September 2014	Announcement of CIPedia (ECN Newsletter)
October 2014 onward	Marketing A demo is scheduled to be presented on the 9th International Conference on Critical Information Infrastructures Security (CRITIS 2014), October 13-15, 2014, Limassol, Cyprus.

7 Maintenance

7.1 Server

Fraunhofer IAIS will host the service in its server. CIPedia can be currently be found here:

<https://publicwiki-01.fraunhofer.de/CIPedia/index.php>. Please note that currently it is under development and the access to the wiki is restricted.

7.2 Security and backups

CIPedia follows Fraunhofer IAIS practices as to security and backup issues.

A periodic security review of CIPedia articles will be needed, as to assess whether they contain sensitive information above CIPedia's security classification level (above PU). The first review should take place before CIPedia is released and then it should be performed at least bi-annually. In the case of significant update to the contents of CIPedia, a security review should also be performed. The most suitable body to perform a security review is CIPRNet's Security Advisory Group (SAG). The assessment should follow the rules described in the D1.20 Project Handbook [D1.20].

7.3 Ethics and moderation

CIPedia should undergo ethical review on a periodic basis or when significant content changes are performed. The ethical review should comply with the guidelines of the deliverables D1.20 Project Handbook [D1.20] and D2.51 Initial Ethics Report [D2.51]. The review should examine the following issues:

- (1) data privacy and data protection, i.e. the right of any individual to expect that his/her personal information are processed securely and not disseminated without their written consent as well as the technical mechanisms to ensure the protection of data,
- (2) dual use or misuse of research, i.e. research involving or generating methods or knowledge that could be misused for unethical purposes,
- (3) mission or function creep, i.e. information or data is used beyond the approved initial plan and thereby could harm fundamental ethical values or civil rights, and
- (4) misuse or malevolent use, i.e. research generating materials or knowledge that can be used for unethical purposes. [D2.51]

It is recommended to perform the review at least **twice a year**. This period can be shorter when a significant update or release of CIPedia is performed. The most suitable body to perform the review is CIPRNet's **Independent Ethics Board** (EB).

The suggestions of the review will mean a revision of CIPedia by a **moderator**. The moderator will also need to overview all the changes performed (by internal users and recommended by external users). Therefore, CIPRNet will discuss the issue of moderator in its next governing body meetings. As the software allows for non-Fraunhofer moderator, this option or some kind of a rotation could be discussed. For the project time (up till March 2017) the issue is easier to solve, but one has to come up also with a more long-term solution.

7.4 Statistics

User and other statistics will be kept and surveyed regularly in order to further develop and market CIPedia.

8 User instructions

Detailed instructions on creating a new page can be found in MediaWiki's help pages [MWHelp].

8.1 Page creation

There are three ways to create a new page:

- By linking a wiki page using a standard syntax¹². If you (or anyone else) create a link to an article that doesn't exist yet, the link will be colored red. Clicking a red link will take you to the edit page for the new page. Simply type your text, click save and the new page will be created. Once the page has been created, the link will change from red to blue (purple for pages you've visited) indicating that the page now exists.
- If you search for a page that doesn't exist (using the search box and “Go” button on the left of the page) then you will be provided with a link to create the new page.
- You can use the wiki's URL for creating a new page. The URL to an article of the wiki is usually something like this:

```
https://publicwiki-01.fraunhofer.de/CIPedia/index.php/ARTICLE
```

The template that should be used for creating the content of a new page can be found below and is also available on the CIPedia wiki¹³.

```
<!--Insert here introductory text regarding the term.-->

==Definitions==
<!-- This section presents all available definitions of the above term.-->

=== Official European Definition ===
<!--Insert here the text of the definition, if available. -->

=== Other International Definitions ===
<!-- Insert here definitions from international organizations, if available. Each new definition should be formatted as a heading level 4, followed by the unformatted text of the definition. An example follows below: -->
==== United Nations' Definition ====
<!-- Insert the definition found in the document "2009 UNISDR Terminology on Disaster Risk Reduction" (this is an example). -->

=== National Definitions ===
<!-- Insert official national definitions, if available. Each definition should be formatted as a heading level 4, followed by the text of the definition. An example follows below: -->
```

¹² See <http://www.mediawiki.org/wiki/Special:MyLanguage/Help:Links> on how to link a page.

¹³ This template is available on the CIPedia wiki: <https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Template>. When on Edit mode, users can copy the template text and use it to create new pages. The text within <!-- --> is considered a comment and does not appear on the wiki page (Read mode).

```

==== US Definition ====
<!-- Insert the definition found on the DHS Lexicon (this is an example). -
->

===Standard Definition===
<!--Insert the text of the definition. Each definition should be formatted
as a heading level 4, followed by the text of the definition. -->

== Discussion Topic ==
<!-- Discuss topics related to the term, such as closely-related terms,
differences among definitions, how to use the definitions provided, open
issues, etc. -->

==See also==
<!-- Add links to related terms -->
* [[Related term 1]]
* [[Related term 2]]

==Notes==
<!-- The references will be automatically be listed below. In order to ref-
erence -->
<references />

==References==
<!-- Additional references can also be added below.-->
* Reference 1.

```

8.2 Basic editing

Editing a page is fairly simple. The steps are:

- Click the "Edit" page tab at the top of the page (you are now on Edit mode).
- Make changes to the text.
- Click the "Save page" button.

The following tables present basic guidelines in order to create a simple wiki page. They can also be found when pressing the help button (on Edit mode) of the CIPedia Wiki (based on MediaWiki).

8.2.1 Formatting

Description	What you type	What you get
Italic	"Italic text"	<i>Italic text</i>
Bold	""Bold text""	Bold text
Bold & italic	"""Bold & italic text"""	<i>Bold & italic text</i>

8.2.2 Links

Description	What you type	What you get
Internal link	[[Page title Link label]]	Link label
	[[Page title]]	Page title

External link	[http://www.example.org Link label]	Link label
	[http://www.example.org]	[1]
	http://www.example.org	http://www.example.org


8.2.3 Headings

Description	What you type	What you get
2nd level heading	== Heading text ==	Heading text
3rd level heading	=== Heading text ===	Heading text
4th level heading	==== Heading text ====	Heading text
5th level heading	===== Heading text =====	Heading text

8.2.4 List items

Description	What you type	What you get
Bulleted list	* List item * List item	• List item • List item
Numbered list	# List item # List item	1. List item 2. List item

8.2.5 Files

Description	What you type	What you get
Embedded file	[[File:Example.png thumb Caption text]]	 Caption text

8.2.6 References

Description	What you type	What you get
Reference	Page text.<ref name="test"> [http://www.example.org Link text], additional text.</ref>	Page text. ^[1]
Additional use of same reference	<ref name="test" />	Page text. ^[1]
Display references	<references />	1. [^] Link text , additional text.

9 References

- [ANSI/NISO] ANSI/NISO Z39.19, Guidelines for the Construction, Format, and Management of Monolingual Controlled Vocabularies, 2005 (Revised in 2010).
- [Cantarella12] Cantarella S. Initial report on CIP thesaurus - Description of a method and preliminary stages of its completion. Ispra (Italy): European Commission, Joint Research Centre; 2012. JRC78143
- [D1.20] Deliverable D1.20, CIPRNet Project Handbook.
- [D2.51] Deliverable D2.51, CIPRNet Initial Ethics Report.
- [D8.211] Deliverable D8.211, CIPRNet cooperation meeting - ERNCIP.
- [Dextre12] Dextre Clarke, S. G., Zeng, M.L., From ISO 2788 to ISO 25964: The evolution of thesaurus standards towards interoperability and data modeling. *Information standards quarterly*, 24(1), pp. 20-26, 2012. Also available at: <http://www.niso.org/publications/isq/2012/v24no1/clarke/>
- [EC08] European Commission, COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Brussels, December 8, 2008.
- [EC06] European Commission, Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment to improve their protection, COM(2006) 787 final, Communication from the Commission to the Council and the European Parliament, Brussels, 12 December 2006.
- [Ferigato12] Ferigato C, Cantarella S, Owusu E. First report on ontologies, taxonomies and thesauri for critical infrastructures protection. European Commission; 2012. JRC70128.
- [Frantzi00] Frantzi, K., Ananiadou, S. and Mima, H. Automatic recognition of multi-word terms. *International Journal of Digital Libraries* 3(2), pp.117-132, 2000.
- [Gruber08] Gruber T., Ontology. Entry in the Encyclopedia of Database Systems, Ling Liu and M. Tamer Özsu (Eds.), Springer-Verlag, 2008
- [ISOG73] ISO Guide 73: Risk management — Vocabulary, ISO, Geneva, Switzerland, 2009.
- [ISO25964] ISO 25964-1:2011, Thesauri and interoperability with other vocabularies. Part 1: Thesauri for information retrieval. Geneva: International Organization for Standards, August 8, 2011.
- [ISO22399] ISO/PAS 22399:2007, Societal security - Guideline for incident preparedness and operational continuity management, ISO, 2007.
- [ISO12100] ISO 12100:2010, Safety of machinery -- General principles for design -- Risk assessment and risk reduction, ISO, 2010.
- [Masucci09] Masucci V, Adinolfi F, Srivillo P, Dipoppa G, Tofani A. Ontology-based Critical Infrastructure Modelling and Simulation, P. C. Palmer and S. Shenoj (Eds.): Critical Infrastructure Protection III, IFIP AICT 311, pp. 229–242, 2009
- [Navigli08] Navigli, R., Velardi, P., Ontology Learning and Population: Bridging the Gap between Text and Knowledge (P. Buitelaar and P. Cimiano, Eds.), Series information for Frontiers in Artificial Intelligence and Applications, IOS Press, 2008, pp. 71-87.
- [OG] The Open Group: Technical standard – Risk Taxonomy, Doc. No. C068, ISBN 1-931624-77-1, Reading, Berkshire, UK, January 2009.
- [Tofani10] Tofani A., Castorini E., Palazzari P., UsovA., Beyel C., Rome E., Servillo P., An ontological approach to simulate critical infrastructures. *J. Comput. Science* 1(4): 221-228 (2010)
- [Veraldi07] Velardi P., Cucchiarelli A., Petit M., A Taxonomy Learning Method and Its Application to Characterize a Scientific Web Community, Knowledge and Data Engineering, IEEE Transactions on, vol.19, no.2, pp.180-191, Feb. 2007

- [Vlacheas11] Vlacheas P.T., Stavroulaki V., Demestichas P., Cadzow S., Gorniak S., Ikonou D., Ontology and taxonomies of resilience, v.1.0, ENISA Report, Dec 21, 2011.
- [Will12] Will, L. The ISO 25964 data model for the structure of an information retrieval thesaurus. Bulletin of the American Society for Information Science and Technology, volume 38, issue 4, April/May 2012, p.48-51. Available at: http://www.asis.org/Bulletin/Apr-12/AprMay12_Will.pdf

URLs

- [BCIS] Berkman Center for Internet and Society, Harvard University, Cyber Security Wiki, http://cyber.law.harvard.edu/cybersecurity/Table_of_Contents
- [CBRNG] CBRN Glossary, <http://cbrn.jrc.ec.europa.eu/>
- [DHS] Department of Homeland Security (U.S.), Infrastructure Taxonomy, <https://www.dhs.gov/infrastructure-taxonomy>
- [DoE] Department of Energy (U.S.), SmartGrid Glossary, http://www.smartgrid.gov/lexicon/6/letter_a
- [ERNICIP] European Reference Network for Critical Infrastructure Protection, <http://ipsc.jrc.ec.europa.eu/?id=688>
- [EUROVOC] EUROVOC Thesaurus, <http://eurovoc.europa.eu/>
- [FEMA] FEMA Glossary, http://emilms.fema.gov/IS921/921_Toolkit/glossary.htm
- [FF] Five Filters, <http://fivefilters.org/term-extraction/>
- [FOCUS] FOCUS Project, European Security (Research) Glossary, www.focusproject.eu/web/focus/wiki/-/wiki/ESG
- [IAEA07] IAEA Safety Glossary (edition 2007), <http://www-ns.iaea.org/standards/safety-glossary.asp>
- [ITLW] IT Law Wiki, Critical Infrastructure Protection (CIP) entry, http://itlaw.wikia.com/wiki/Critical_information_infrastructure
- [MWD] Merriam-Webster Dictionary online: <http://www.merriam-webster.com/dictionary>
- [MWHelp] MediaWiki User Help pages: <http://www.mediawiki.org/wiki/Help:Contents>
- [NERC] NERC Glossary, http://www.nerc.com/files/glossary_of_terms.pdf (updated 02/01/14)
- [NIPP13] National Infrastructure Protection Plan 2013, <http://www.dhs.gov/national-infrastructure-protection-plan>
- [NIST] NIST, The Preliminary Cybersecurity Framework, <http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf>
- [SERSCIS] SERSCIS project (ontology example): <http://www.serscis.eu/wp-content/uploads/sites/5/2009/10/attcd639.gif>
- [TDTerm] CIPRNet report TechDoc2: Terminology, v.5, <https://bscw.iais.fraunhofer.de/bscw/bscw.cgi/d325849/CIPRNet-TechDoc-Terminology-v5.docx>
- [TERM] Termine, <http://www.nactem.ac.uk/software/termine/>
- [TES] Term Extraction Software, <http://termcoord.wordpress.com/about/testing-of-term-extraction-tools/free-term-extractors/>
- [TRZ] TextRazor, <http://www.textrazor.com/>
- [UNISDR] 2009 UNISDR Terminology on Disaster Risk Reduction, <http://www.unisdr.org/we/inform/terminology>
- [WIKI] Wikipedia, Critical Infrastructure Protection (CIP) entry, http://en.wikipedia.org/wiki/Critical_infrastructure_protection

Annex A: Preparatory work on terminology

Sections 2 and 3.2 of this deliverable presented examples of existing attempts on CIP terminology. The following sections have been largely derived by the CIPRNet report TechDoc2: Terminology [TDTerm] and are included in this document to depict the preparatory work performed by members of the consortium on Terminology for CIP.

A.1 Existing definitions of basic terms

The table that follows presents existing definitions on basic risk and disaster management terms, which are relevant for CIP.

risk	effect of uncertainty on objectives	The combination of the probability of an event and its negative consequences.	Risk is the probable frequency and probable magnitude of future loss.	
threat	potential cause of an unwanted incident , which may result in harm to individuals, a system or organization, the environment or the community [ISO22399]			Any indication, circumstance, or event with the potential to disrupt or destroy critical infrastructure, or any element thereof
hazard	source of potential harm [ISOG73] possible source of danger, or conditions physical or operational, that have a capacity to produce a particular type of adverse effects [ISO22399]	A dangerous phenomenon, substance, human activity or condition that may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage.		
harm effect	physical injury or damage to health [ISO 12100] (NOTE 1 (risk): An effect is a deviation from the expected — positive and/or negative)			
impact	evaluated consequence of a particular outcome [ISO22399]			
event	occurrence or change of a particular set of circumstances			
incident	event that might be, or could lead to, an operational interruption, disruption , loss, emergency or crisis [ISO22399]			
disruption	incident , whether anticipated (e.g. hurricane) or unanticipated (e.g. a blackout or earthquake) which disrupts the normal course of operations at an organization location [ISO22399]			
consequence	outcome of an event (3.5.1.3) affecting objectives			
risk management	coordinated activities to direct and control an organization with regard to risk (1.1)	The systematic approach and practice of managing uncertainty to minimize potential harm and loss.		
risk assessment	overall process of risk identification (3.5.1), risk analysis (3.6.1) and risk evaluation (3.7.1)	A methodology to determine the nature and extent of risk by analysing potential hazards and evaluating existing conditions of vulnerability that together could potentially harm exposed people, property, services, livelihoods and the environment on which they depend.		
risk identification	process of finding, recognizing and describing risks (1.1)			
risk analysis	process to comprehend the nature of risk (1.1) and to determine the level of risk (3.6.1.8)		Any analysis that accounts for the risk from a single threat community against a layered set of assets (e.g., defense in depth).	consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure
risk evaluation	process of comparing the results of risk analysis (3.6.1) with risk criteria (3.3.1.3) to determine whether the risk (1.1) and/or its magnitude is acceptable or tolerable			
risk source	element which alone or in combination has the intrinsic potential to give rise to risk			

level of risk	magnitude of a risk (1.1) or combination of risks, expressed in terms of the combination of consequences (3.6.1.3) and their likelihood (3.6.1.1)		
vulnerability	intrinsic properties of something resulting in susceptibility to a risk source (3.5.1.2) that can lead to an event with a consequence (3.6.1.3)	The characteristics and circumstances of a community, system or asset that make it susceptible to the damaging effects of a hazard.	Vulnerability is the probability that an asset will be unable to resist the actions of a threat agent.
disaster	event that causes great damage or loss [ISO22399]	A serious disruption of the functioning of a community or a society involving widespread human, material, economic or environmental losses and impacts, which exceeds the ability of the affected community or society to cope using its own resources.	
crisis	any incident(s) , human-caused or natural, that require(s) urgent attention and action to protect life, property, or environment [ISO22399]		
emergency	sudden, urgent, usually unexpected occurrence or event requiring immediate action [ISO22399]		
disaster risk		The potential disaster losses, in lives, health status, livelihoods, assets and services, which could occur to a particular community or a society over some specified future time period.	
mitigation	limitation of any negative consequence of a particular incident [ISO22399]	The lessening or limitation of the adverse impacts of hazards and related disasters.	
prevention	measures that enable an organization to avoid, preclude, or limit the impact of a disruption [ISO22399]	The outright avoidance of adverse impacts of hazards and related disasters.	
crosscutting criteria			(a) casualties criterion (assessed in terms of the potential number of fatalities or injuries); (b) economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects); (c) public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services).

Table 4: Basic risk and disaster management terms relevant for CIPRNet. All definitions are quotations from the sources listed in the column heads, thus quotation marks have been omitted for reasons of readability.

A.2 Discussion

While the table above contains several definitions, there are terms that remain vague [TDTerm]. For example, it is difficult to distinguish between a potential source of harm and the realisation of the source of harm, that is, the events or incidents that are really happening and causing real harm or damage. One would often need to be able to talk about, for instance, a possible future earthquake that might hit an earthquake prone area and an earthquake that really happened. In the first case, the earthquake would qualify as one threat (out of a multitude of other threats), and in the latter case it would qualify as a disaster that actually took place. The available definitions suggest the following wording: “earthquake threat” and “earthquake incident”.

In the CIP field, one may need to be able to talk about a “chain” from threat (to CI) to consequences (of a CI disturbance or failure). It would look like this:

1. Threats to CI: Already defined (see VITA threat taxonomy) sources of *potential* harm. Example: Flooding events *may* cause disturbances to some CI. The ISO definition of threat can be used.
2. Threats may become real events or incidents (single general term: incident?). A particular threat may be called a “flooding incident”, for example.
3. Incidents (realised threats) may cause first order effects (in a CI). Example: A flooding causes a power outage in a city quarter
4. First order effects may cause second and higher order effects (“cascading effects”). Example: The power outage leads to a loss of pressure in the drinking water system.
5. The effects will have consequences (along the cross-cutting criteria of the ECI directive) or impacts (along the ISO guide 73). Example: Several people drink contaminated water and get ill or die; the enduring loss of power and drinking water cause a direct economical damage of 10 million Euro; the flooding makes 200 hectare of agricultural area unusable for the next 5 years, resulting in an additional economic damage

Therefore, it is clear that the terms “consequence analysis”, “first order effect”, “higher order effect” need to be defined or an appropriate existing definition be identified.

If we place emphasis on natural events, the following definition of Risk can be adopted¹⁴:

Risk indicates the possibility of suffering harm or losses (due to some event) and its extent (in probabilistic terms).

The term “Risk” can be used for Critical Infrastructures in relation to two variables: the CI **element** that can be lost or damaged and the cause, produced by some natural **event**, whose occurrence transforms a threat into a harm. Therefore, the value of Risk is the product of three terms:

- (1) the probability that the event occurs with given characteristics (i.e. having manifestation(s) of given strength)
- (2) the vulnerability of a given CI element to that event (i.e. the conditional probability that if the event would occur with given characteristics, the resulting harm will be of a given extent)
- (3) the impacts and the consequences that the resulting harms(s) can produce at the different levels.

¹⁴ This definition was proposed by ENEA. The detailed definitions proposed by ENEA for the main terms used in order to define Risk can be found in [TDTerm].

The following table provides a simplified version of the larger table in the previous section. It does not replace those definitions, but merely relates the main definitions in a different way for preparing usage examples. Also, some new sub definitions are introduced.

Term	Definition	Related definitions				
Hazard	Potential source of harm	Natural hazard	t.b.d.	Anthropic hazard	t.b.d.	
Harm	Physical injury or damage to health	Direct harm	Damage caused directly by a realised hazard	Indirect harm	Damage caused indirectly by a realised hazard (e.g. as a impact of direct or indirect harm)	
Threat	potential cause of an unwanted incident, which may result in harm to individuals, a system or organisation, the environment or the community	Natural threat		Anthropic threat	t.b.d.	
Event	occurrence or change of a particular set of circumstances	Incident	event that might be, or could lead to, an operational interruption, disruption, loss, emergency or crisis	Natural incidents, anthropic incidents	t.b.d., t.b.d.	
Incident	event that might be, or could lead to, an operational interruption, disruption, loss, emergency or crisis					
Impact	outcome of an event			risk	The combination of the probability of an event and its negative impacts.	
Consequence	evaluated particular impact					

From the table above, it is apparent that the definitions of “hazard” and “threat” are very similar, so maybe the terms do not need to be distinguished. An usage example for the above terms is presented below:

“The weather report indicated that a flood **threat/hazard** would be emerging. Shortly thereafter, an extreme weather **event** occurred, bringing heavy rainfall. This led to a flooding **incident** along the Elbe. As **impacts** of the flood, a bridge collapsed because it was **damaged** by the flood, a dike broke and a flooded purification plant ceased operation. **Indirect impacts** were the interruption of road and rail traffic across the bridge, water transport blocked by the collapsed bridge and production of drinking water along the banks of the Elbe had to be stopped. The **consequences** of the flooding incidents were: Seven casualties, an economical damage of 67 Million Euros, and 50 square kilometres of polluted agricultural area. The flooding incident at the Elbe led to several **cascading effects** of CI. The collapsed bridge affected the road, rail, and water transport in the area. The pollution due to the purification plant led to an interruption of drinking water production.”

The last sentence shows that a cascading effect needs not result from damage, but can be a shutdown as a mitigation action to prevent further harm (to people, to a CI, to economy).

A.3 Additional terms and definitions needed

The terms and definitions provided in the reviewed sources do not allow the distinction between first order incidents / effects / consequences / impacts and second, third, and higher order incidents / effects / consequences / impacts. However, when talking about “cascading effects”, an established term frequently used in publications on failing dependent infrastructures, such a distinction is required. Using the ISO vocabulary, the corresponding wording would be “cascading incident”. However, it is not credible that the CIP community would adopt that definition.

The ISO definition of “consequence” is very general and does not distinguish between consequences for CI, for people, for the environment, and for the economy. Such distinctions are required for two reasons:

- 1) For the CIP domain, consequences for CI are of supreme importance, and other consequences may be ignored for certain applications (for example, when assessing the consequences of cascading effects).
- 2) For consequence analysis in the meaning of the ECI directive (the meaning which we adopted for the CIPRNet proposal), assessment of consequences for people, the environment and the economy is needed according to the crosscutting criteria mentioned there.

So far, we do not have a suggestion of specific terms for both cases. **Thus the recommendation for the time being is to always clearly state if “consequence” or “consequence analysis” is being performed for CI alone or for use with the crosscutting criteria.**

Another problem is the difficulty to distinguish the safety and security aspects of CI. CIP is mostly considered as a security related domain. However, when CI emergencies or their consequences affect people, the environment and the economy in a negative way, one enters quickly the domain of safety. Therefore, CIP has also safety aspects. The differences and relations of security and safety aspects of CI and CIP seem to the author of this paper not sufficiently well defined nor understood. This would require further clarification.

Also, the term “**resilience**” (of CI) is currently under discussion. There is a white paper by JRC, contained in the CIPRNet deliverable [D8.211], that elaborates on the resilience topic. An agreed definition will later replace any provisional definitions adopted from other sources.

Annex B: Automated Extraction of Glossary Terms

Examples of the use of the tool Termine [TERM; Frantzi00] on two-CIP related documents are presented below. Such tools will be used in order to identify terms for CIPedia, for which wiki pages will be created.

Example 1: Results of the EU Directive 2008/114/EC

1	member state	75	
2	security liaison officer		12.6797
3	official journal	10	
4	infrastructure protection		9.75
5	european union	7	
5	cross-cutting criterion		7
7	security liaison	6.5	
8	ecip contact point	6.33985	
8	european union 1	6.33985	
10	relevant member state authority		6
10	member states	6	
12	structure protection	5	
12	contact point	5	
14	operator security plan	4.754888	
15	infrastructure asset	4	
15	eci sector	4	
17	member state authority	3.33985	
18	eci osp procedure	3.169925	
18	member state legislation	3.169925	
18	infrastructure protection issue		3.169925
21	european parliament	3	
21	liaison officer	3	
21	sectoral criterion	3	
24	state authority	2.5	
25	relevant cross-border mutual aid agreement		2.321928
26	cross-sector dependency	2	
26	relevant member	2	
26	risk analysis	2	
26	infrastructure protection contact point		2
26	community approach	2	
26	common approach	2	
26	implementation action	2	
26	annual basis	2	
26	infrastructure warning information network		2

26	indicative list	2
26	equivalent exist	2
26	equivalent measure	2
26	transport sector	2
26	multilateral discussion	2
26	european programme	2
26	relevant information	2
26	green paper	2
26	electricity generation	2
26	structure protection contact point	2

Example 2: Results on SWD(2013)318 final: Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection.

1	member state	26
2	critical infrastructure	11
3	council directive 2008/114/ec	9.509775
3	critical infrastructure protection	9.509775
5	risk assessment	9.4
6	dg home	9
7	infrastructure protection	8.333333
8	european critical infrastructure	7.924812
9	eu approach	7
10	commission staff working document	6
11	air traffic	5.857143
12	risk assessment methodology	5.33985
13	gas transmission network	4.33985
14	eu internal security strategy	4
14	ci protection	4
14	european gas transmission network	4
14	stress test	4
14	european programme	4
14	eea joint committee decision	4
14	european union	4
14	network manager	4
14	member states	4
14	union civil protection mechanism	4
14	external dimension	4
14	cip community	4
26	electricity transmission grid	3.754888
27	smart metering system	3.169925

27 eu member state 3.169925
 29 space infrastructure 3
 29 risk management 3
 29 council decision 3
 29 pilot phase 3
 29 official journal 3
 29 european dimension 3
 29 system approach 3
 29 network crisis 3
 37 civil protection mechanism 2.754888
 37 eea joint committee 2.754888
 39 electricity transmission 2.333333
 40 european aviation crisis coordination cell 2.321928
 40 critical infrastructure warning information network 2.321928
 42 critical infrastructure warning 2.169925
 42 air traffic management 2.169925
 44 gas supply 2
 44 epcip communication 2
 44 electric power infrastructure dependency 2
 44 cip policy 2
 44 hazard risk assessment methodology 2
 44 smart grids task force 2
 44 diverse project 2
 44 global navigation satellite system 2
 44 civil protection training network 2
 44 consequence management 2
 44 critical ict infrastructure simulation 2
 44 main energy transmission network 2
 44 air traffic flow management 2
 44 second half 2
 44 gnss signal 2
 44 private sector 2
 44 practical implementation 2
 44 eu air traffic management 2
 44 review process 2
 44 north german transmission grid 2
 44 ieee control systems magazine 2
 44 current directive 2
 44 cip measure 2
 44 commission regulation 2
 44 staff exchange 2

44	eea agreement	2
44	selected pan-european critical infrastructures	2
44	directive 2008/114/ec	2
44	global satellite navigation system	2
44	first half	2
44	european electricity transmission grid	2
44	ict sector	2
44	focal point	2
44	long-term recovery	2
44	energy sector	2
44	resilience measure	2
44	efta country	2
44	current programme	2
44	support tool	2
44	current union civil protection	2
44	volcanic ash cloud crisis	2
44	contingency plan	2
44	transport sector	2
44	actor timeframe	2
44	atm network	2
44	close cooperation	2
44	cyber security	2
44	crisis management	2
44	global infrastructure security toolkit	2
44	cyber threat	2