D4.1 - Tools for methodological support: templates, criteria, and IT requirements

Due date of deliverable: M6/November 2014

Actual submission date: 09/12/2014

Lead Beneficiary: Tecnalia Research and Innovation

Contributing Beneficiary: HCSS and SSSUP

Keywords: Templates, methodology

Dissemination level: PU

Release Number	Release date	Released by
0.1	09/12/2014	Tecnalia
0.2	25/02/2015	Tecnalia
1.0	27/02/2015	Fraunhofer INT

1 Introduction

The mission of WP4 is to provide a consistent evaluation of the development of the work in the case studies conducted in four different EU regions. It furthermore aims to provide the consortium with *“templates permitting maximum flexibility to add, modify, contemplate, and rearrange the different factors of each thread according to their appearance in the case studies”.*

The scope of the methodological support is limited to the first stage of the project, where findings on threat, hazard and risk perceptions, key actors, and ethical considerations are yielded. At this stage insight is provided on how national concepts aggregate at the level of European regions, as quantitative assessment of concepts of security, is carried out.

The WP4 will be implemented based on the methodological framework proposed in WP3 considering the following key documents:

- **Coding Handbook:** Assessing Evolving Concepts of Security. The Document sets out the analytical framework that guides the assessment of the security concepts across Europe in the EvoCS project in four different regional case studies. The methodology of the Coding Handbook laids out the overall approach for the project and the general methodological principles guiding the gathering of the data. On the first place it deals with the definition whether securitisation has taken place, second with how to determine whether particular dimensions are present, and third with how to evaluate their salience. Thus, main goal of the methodology is to bring together the vision of securitisation, dimensions, and salience with the process of gathering and coding evidence. In order to provide uniform and systematic format all of the data will be manually coded and centrally located in a single database which all research teams will get access to.

- **Coding Changes:** The document discusses amendments to the coding procedure in light of WP4 and experiences gained during initial coding. The main points of the document are presented in this deliverable.

- **Coding Better:** The document summarizes lessons learned from the pilot and intercoder exercises, and clarifications of the codebook. It provides furthermore solutions to problems and uncertainties that EvoCS coders have encountered, and reiterates the four golden rules in the EvoCS coding handbook. It offers concise, practical advice based on the principles of the EvoCS project. The main points of the document are presented in this deliverable.

2 Amendments to the Sourcing Evidences

This section addresses issues with insufficient numbers of sources. “Plan B” has been developed for alternative sourcing strategies. For all of these sources, coders should continue using the instructions in the codebook first to source pieces of evidence. They should find these instructions in chapter 4. Only if there is insufficient number of sources as defined in the codebook, coders should follow the instructions below.

2.1 Government Policy Documents

There will inevitably be fewer government policy documents than other sources of evidence. That’s not a problem because one well coded national security strategy is very valuable to the EvoCS project. At least one per country should be coded.

Changes: If obtaining the national security strategy means that coders need to break the rule in section 4.1 of the codebook which says no earlier than 2010, then they can break the rule. The most recent document should be coded. This change only applies to national security strategies. For other government policy documents, coders should continue to use the guidelines in the codebook.

2.2 Parliamentary Publications

There should be plenty of evidence from the parliamentary documents that is specified in the codebook.

Changes: If not, then the following types of document can be added to coders´ list of pieces of evidence as a supplement:

- Committee proceedings and reports
- Working documents such as early day motions
- Bills and laws

2.3 Academic Publications

In the codebook it is stated that coding academic articles takes longer than many of the other sources. Coders therefore recommend a lower number of articles per country: 25.

2.4 Newspaper Articles

There are no sourcing issues relating to newspapers, so coders should continue following the instructions in the codebook. 100 articles per newspaper should be coded, so 200 in total.

2.5 The Corporate Perspective

These instructions supplement those in section 4.5 of the codebook. The coders use Wikipedia’s notability criteria to judge companies worth including in the research.

Changes: If coders are unable to find 100 articles, then they should scroll to the bottom of this Wikipedia page and choose their country. Then they should use the most recent annual reports of all the companies listed to top up the list to 100. If there are more than 100 companies with relevant reports, the companies whose names return the highest number of Google hits in private browsing mode should be coded.

2.6 Non-Governmental Organisations

Due to difficulties accessing and using the budget information in the WANGO database, the methodology team has replaced the procedure in section 4.6 of the codebook. Instead coders should use Wikipedia's notability criteria to judge NGOs worth including in their research. Changes: Instead follow the steps below:

- In private browsing, google the search term [country name] [word for NGO] site:wikipedia.org. For example the researchers for Italy would search Italia ONG site:wikipedia.org.

- Select the first 25 NGOs for which individual dedicated Wikipedia articles are listed in the search results.

- If you are unable to reach 25 in this matter, use the Wikipedia category page (either in English or in the country's national language) to list NGOs. Then follow step 3 in section 4.6 of the codebook to rank them in order of Google hits.

- Search for each NGO's last annual report or their most recent report on a relevant topic regarding security or securitization published in the period 01-11-2013—31-10-2014. Code it.

If not all of these 25 NGOs publish relevant reports, complement with NGOs of the list of 50 that do address security.

3 Amendments to the Coding Method and Form

Cyber and data security are introduced as a core value. Full details on how to code have been added to the Coding Better document, point 2.1. Further changes are:

- Subject and object: Terms used in codebook are now on the forms
- Larger box for subject actors to encourage coders to list all subject actors they can find (see Coding Better document, point 2.2)
- Added information and cyber security as a core value (see Coding Better document, point 2.1)
- Added think tanks and policy institutes as an actor
- Added a box for coders to describe ethical issues identified
- Added Serbia to list of countries

4 Clarifications to Core Values

This section provides solutions to problems and uncertainties that EvoCS coders have encountered regarding the core values. In regard to this the following should be stated:

- **Environmental security can include the interaction between environment and people**, provided that the environment is threatened as a value of primary concern in the securitisation of the issue. Examples: (1) A chemical accident which contaminates a large source of drinking water may be a breach of environmental security, because it is something in the environment which is threatened. (2) Flooding, extreme weather, or famine are matters of physical security only, because they do not necessarily concern the environment as a primary security core value in itself. However if a threat is identified concerning people's ability to withstand such environmental disasters, then environmental security is present.

- **Information and cyber security are now a possible core value to look for.** This is the part of security concerned with measures to protect the confidentiality, integrity, and availability of information.
    - The main features of information and cyber security are confidentiality, integrity, and availability. Other properties such as authenticity, accountability, non-repudiation, and reliability may also be involved.
    - Breaches of information and cyber security involve events which compromise confidentiality (for example leaks or hacks in which unauthorised parties acquire information); integrity (for example failures or attacks which alter or distort information); and availability (for example failures or attacks which disable or destroy systems or block access to files or erase data).

- **Energy security is almost always a matter of economic security,** but coders should use their judgement as it could also fall into other core values such as environment.

5 Perceptions, Actors and Political Levels

Coders should stick to the following instructions:

- **List as many subject actors as you can identify.** If there are multiple subject actors, coders should do not simply write ‘multiple’ or ‘diverse’

- **Government agencies such as police, armed forces, fire service are difficult to code.** Try to reflect the position of these services within the country: for example if they are a government agency, code them as government; if they are independent organisations, code them as civil society or private sector as appropriate.

- **Regional can have two meanings**: interstate and intrastate. If when sourcing articles you come across the wrong one, use related search terms to source relevant articles, for example ‘province’, ‘département’ or ‘länder’.

6 Intercoder Reliability

Ensuring intercoder reliability stage is essential to the quality of our research. Doing an intercoder reliability test is all but compulsory. It is very important to check that team members have understood the codebook, to let them practice what they have learned, and to ensure that coders across the consortium code to the same high standards.

What follows is a set of instructions based on the intercoder reliability exercise of the North West group. Other teams should be able to replicate these steps with no additional effort beyond coding a small number of articles, one hour for calculating the results, and a meeting to review the findings.

4.1 Coding

- Each team members should code the same set of articles. The methodology team used 25, selected from the UK.

- The methodology team replaced the Link/Title/DOI field with an ID number for each article to simplify, save time, and ensure that all coders would insert the same information. That way, coders could use a formula to calculate intercoder reliability. This is optional, but can save lot of time.

4.2 Calculating Results

- **For each of the dimensions (core values, actors, level, ethics), the methodology team used the** COUNTIFS function to count how many coders gave each of the possible answers to each of the questions on the coding form. The methodology team used the formula for each of the possible answers to each question. For example, for the core value of physical security, for each article, the number of coders who classified ‘main topic’ was counted, the number who classified ‘mentioned’ was counted, and the number who classified ‘absent’ was counted.

- **The frequency of the most common answer was noted,** and divided it by the number of coders to show the percentage of coders that agreed on the same answer. For example, for the core value of physical security, for article G1, three out of five coders selected ‘main topic’, two selected ‘mentioned’, and none said ‘absent’. The percentage of agreement was therefore 60%.

- **The methodology team adapted and repeated this formula for every question, for every article.** It tested intercoder reliability on a total of 598 individual answers on the coding form.

4.**3 Reviewing Results**

- **The calculated average percentage of agreement per question and per article.** We used conditional formatting to highlight the questions and articles with the highest and lowest levels of agreement.
- **The standard for good intercoder reliability is 80% agreement per article on average.** The methodology team achieved a score of 75%, which leaves room for improvement.

- The methodology team **held a conference call to discuss our points of agreement and disagreement,** and to see whether disagreements were sporadic or systematic. It was discussed where improvements could be made, and found enough changes were identified to reach the target of 80% agreement on every article. The clarified issues were included in the Coding Better document.

7 General rules

Coders should consider that “Date” means date of publication of a piece of evidence. The date and time of coding are automatically recorded.

Coders are advised to work with a fresh mind. Coding is not an automatic exercise. It is not possible to code well in autopilot. Coding requires intellectual engagement with the subject matter. The methodology team recommends a close reading of each text at the same time as filling in the coding form—this keeps the coding specifications at the front of the coder’s mind.

Keyword searches (for example by using ctrl+F) should be avoided until after the coder has read the whole article. These make it easier not to read the whole article through, but there is a risk of missing something.

Other important rules are:

1. **Only what is explicitly mentioned should be coded**. No inferences or interpretations of the coder should be included. Reading and coding at the same time will help in this. Related instructions are:

   - **Do not be afraid not to code articles**. If the article does not explicitly and fully satisfy the criteria of containing securitisation acts AND dealing with the country coded, please do not code it.

   - **Unless the general public is explicitly mentioned, it is absent**. Securitized issues in newspaper articles are read by, not addressed to the public.

   - **Unless they are explicitly mentioned, the media and journalists are absent**. Only if a journalist articulates their own point of view do they then become an addressor. Examples: (1) Newspaper conducts a survey regarding a specific security issue. In this case the newspaper is securitising an issue and therefore an addressor. (2) Newspaper reports about the government deciding on a new security policy towards Russia. In this case the newspaper is not an actor to code.

   - The mere fact that an actor is mentioned in the article is not enough to make it an addressor, addressee, subject, or object. The **connection between security issue and actor needs** to be established in the text.

   - Levels concern the place where a security challenge is claimed to exist. Coders should ignore the level at which the addressor usually operates, even if they know it. Examples: (1) A national organisation may make claims about security challenges on the local level—these would be coded only as local challenges. (2) A local organisation may make claims about security challenges at the international level—these would be coded only as international challenges. The methodology team recommends an extra reading the text just for this indicator.

   - Some issues may be moral or ethical, but not presented as such in the article. Therefore matters like human trafficking should only be coded as human rights or ethical issues if they are explicitly mentioned as such.

2. **The unit of analysis is the creation of concepts**. Pieces of evidence are therefore examples of the securitisation process in their own right. The validity of claims, the implications of statements, and the effects of actions are not of interest to this research and should be ignored.

    - **Political claims require action**. Mentions of laws, policies, and opinions are not necessarily securitising claims, and the actors behind them should not necessarily be coded. What should be coded is the creation of legislation, the announcement of policies, or the articulation of opinions. Examples: (1) The article mentions a past EU directive which affects the discussion today. This is not a claim; the EU is not an addressor; those affected by the directive are not addressees; and the subject and object of the directive are not subject or object actors to code. (2) An actor (such as the EU) creates a law, announces a policy, or articulates an opinion. At this point, anyone explicitly included as an addressor, addressee, subject, or object actor can be coded.

    - **Code actors according to the 'highest form' of contribution** to discourse. This means that if an actor is an addressor AND an object actor, then they should be coded as addressor. The same applies if the actor is an addressee AND and object actor.

3. **Only domestic concepts** of security are of interest. Evidence of securitisation which does not affect the country coded should be ignored.

4. **Prevent biases** introduced by technological tools. When using Google Search at any point in the coding process, coders should always ensure that they are browsing in a private browser window (incognito in Chrome). If possible, use google.com rather than .de or .fr or whatever other domain. Some Google biases are unavoidable.

8 Templates and homogenisation of the methodology

The result of the coding should be in a uniform, systematic format, and centrally located in a single database in a Google Folder. Each Case Study Leader will get his/her access details which it can then share with the partners participating in the research.

The following templates are provided for the submission of deliverables should be used for the (1) Template for the presentation of the Regional Case Study Results and (2) for the deliverables of the project.

Annex 1:

Template for the presentation of the Regional Case Study Results

Due date of deliverable

Actual submission date

Deliverable approved: Y/N

Lead Beneficiary:

Contributing beneficiaries:

Keywords:

Dissemination level:

Release History

This page is used to follow the deliverable production. All release numbers prior to the submission to EC should be numbered 0.x.

Release 1.0 is the first official version submitted to the EC

The rows including release numbers for non-official versions shall be deleted when the document is submitted to EC.

Please give details in the table below about successive releases:

Release Number	Release date	Released by

Regional Case Study X

1. **Description of Country and Regional Selection of Countries**

2. **Country Analyses (by individual country)**

3. **Predominant ‘concepts of security’ (one or two)**

   3.1 Description of security challenges, political actors, levels, and ethics & human rights in relation to the two predominating core values within the regional and national concepts of security

   3.2 Historical trajectory (context analysis)

   3.3 Overview of current trends with a view to the relation with the European level

4. **Regional Analysis**

   4.1 Predominant regional concepts of security (one or two)

   4.2 Offer characterisation (‘name’)

      4.2.1 Description of roles of security challenges, political actors, levels, and ethics & human rights in relation to the two predominating core values

      4.2.2 Historical trajectory: explanation

      4.2.3 Overview of current trends with a view to the relation with the European level

5. **Findings and Conclusions**

   5.1 Recap Country Profiles

   5.2 Recap Regional Profile and key highlights

   5.3 Frame pathways towards thinking about the foundations of security research and policies.

Annex 2

Generic template for the presentation of the deliverables

Dx.y - Deliverable title

Due date of deliverable

Actual submission date

Deliverable approved: Y/N

Lead Beneficiary:

Contributing beneficiaries:

Keywords:

Dissemination level:

Release History

This page is used to follow the deliverable production. All release numbers prior to the submission to EC should be numbered 0.x.

Release 1.0 is the first official version submitted to the EC

The rows including release numbers for non-official versions shall be deleted when the document is submitted to EC.

Please give details in the table below about successive releases:

Release Number	Release date	Released by

Executive Summary

Table of content

List of Acronyms

Abbreviation / acronym	Description

9 Introduction

Text

10 “Title”

Text

10.1 “Title 2”

Text

Table 1: title

Figure 1: title

10.1.1 “Title 3”

Text

10.1.1.1 “Title 4”

Text

11 Conclusion

12 Bibliography

Annexes