BACHELOR THESIS

University of Twente, Enschede & Westfälische Wilhelms-Universität Münster
1st Supervisor: Dr. Guus Dix
2nd Supervisor: Dr. Annika Jaansoo

In the Name of Cybersecurity

A Qualitative Analysis on Scientific Policy Advice on Cybersecurity in the European Union

Majbrit Luisa Hüttenhein
Student Number: s2596008
Public Governance across Borders, B.Sc

11,998 Words

29-06-2022

UNIVERSITY OF TWENTE.

WWU MÜNSTER

Abstract

This bachelor thesis analyzes the Scientific Opinion given by the High Level Group of Chief Scientific Advisors of the EU to the European Commission on cybersecurity to examine whether the scientific advice was "good" scientific policy advice in the sense of the framework provided by Carrier (2022). Four criteria developed by Carrier are analyzed, which deal mainly with the role of non-epistemic values in scientific advice (i.e. presence of non-epistemic values, fact-value distinction, creation of policy packages, presentation of adequate alternatives). These lead in short to three possible hypotheses: H1: The advice is good – it met all four criteria; H2: The advice was reasonably adequate – it met three out of four criteria; H3: The advice was bad – it met only two or less criteria. The methodological approach of this thesis is a qualitative content analysis that relies on coding. The documents in focus are the Scientific Opinion itself, added on by whitepapers that were taken into account, and critical literature concerning cybersecurity as the third source of evidence. The analysis showed that the Scientific Opinion meets three out of four criteria, therefore H1 and H3 can be rejected. The Opinion shows deficits in the fact-value distinction especially regarding economic values, which tend to be implicitly incorporate in scientific evidence.

Contents

Abbreviations

CEPS	Centre for European Policy Studies
ENISA	European Union Agency for Network and Information Security
EBP	Evidence-based policy
EU	European Union
HLG	High Level Group of Chief Scientific Advisors
NIST	US National Institute of Standards and Technology
SAM	Scientific Advisory Mechanism of the European Union
SAPEA	Scientific Advice for Policy by European Academies

1 Introduction

Due to the steadily increasing global networking, the associated threats, and acute dangers, the discussions about the protection of information and communication infrastructures are becoming more and more explosive. In a global context, critical infrastructures such as the energy network, water supply, and health care form the basis for the ability of state unions and sovereign states to act. The European Union and its economic strength are not only a result of innovations in research and development but also depend on them in the future. In the digital age, the loss of sensitive information in these areas through industrial espionage can wipe out a global player's knowledge advantage within seconds. However, it is not only the economy that repeatedly falls victim to cybercrime, the availability of government and corporate networks is nowadays an attractive target for hackers and organized crime, too. Being the centers of societal wellbeing, it seems feasible to protect these structures and to further promote and demand (inter)national cybersecurity considerations.

For European policymaking, this means that it is of high importance to adopt reasonable and effective strategies to ensure cybersecurity throughout the whole Union. The key regulation for cybersecurity in the European Union is the Cybersecurity Act. First adopted in 2013, the Act was revised and adopted in an updated version on 17 April 2019[1]. The 2013 version focused on the protection of the civilian and military cyber domain from threats that can interfere with or damage the information infrastructure and the networks. As the cyber world develops quickly, a constant revision of the EU's strategy is needed. Therefore, the European Commission requested a Scientific Opinion from the High Level Group of Scientific Advisors which they accepted on 29 January 2016. On 24 March 2017 the High Level Group delivered the Scientific Opinion titled "Cybersecurity in the European Digital Single Market" that provides recommendations regarding the handling of cybersecurity issues (European Commission, Directorate General for Research and Innovation [RTD], 2017). The recommendations ultimately informed the renewed EU Cybersecurity Act. The 2019 version added to this framework, especially by giving ENISA, the European Union Agency for Network and Information Security, a stronger mandate, and anchoring the development of an EU-wide cybersecurity certification framework for ICT products, services, and processes (ENISA, n.d.; European Commission, 2022).

Scientific Evidence plays an important role in cybersecurity policymaking and other policy fields. If policies relied on more rigorous evidence use, proponents say, a lot of unnecessary harm could be avoided, and meaningful social goals could be attained (Parkhurst, 2017, p. 4). Especially in highly specialized fields like cybersecurity, it is crucial to rely on expert advice since most policymakers lack important knowledge. This kind of policymaking, when policy decisions are intended to be led by scientific evidence – meaning the outcomes of scientific research with recognized methods – is called "Evidence-based policy" (EBP). However, evidence-based policymaking also harbors a few risks. Evidence might be cherry-picked or misused for political motives. Public policymaking relies on a different mechanism than technical decision-making. Decision-making in politics "[…] involves trade-offs between multiple competing social values, with only a very small proportion of policy decisions simply concerned with technical evidence of the effects of interventions." (Parkhurst, 2017, p. 5).

European policymakers consider it, too, very important to take scientific findings into account in addition to political or social preferences. To ensure the incorporation of scientific evidence in the European Union, the EU established a Scientific Advisory Mechanism (SAM) which's purpose is to provide the EU with findings from the scientific community. Its functioning is depicted in *Figure 1*. SAM consists of two main bodies. One is the High Level Group of Chief Scientific Advisors (hereafter called High Level Group (HLG)). The group consists of seven Chief Scientific Advisors that come from different disciplines and universities across Europe. They are appointed in their personal capacity and

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 2019

are mandated to act independently of political or institutional interests but in the public interest. They are in place for a maximum of five years (European Commission, n.d.). The other body is SAPEA, the Scientific Advice for Policy by European Academies (SAPEA), which is a consortium, that bundles expertise in all scientific disciplines from natural sciences to engineering and social sciences from over 100 academies across Europe (European Commission, n.d.). The Scientific Advisory Mechanism "aims to match the Commission's short, medium and long term demands for independent scientific evidence and advice by drawing upon the best available expertise across Europe and across disciplines" (European Commission, Directorate General for Research and Innovation, 2016). It oftentimes acts on demand by the Commission and then jointly develops a Scientific Opinion on a requested topic that gathers the scientific state-of-the-art and formulates policy recommendations.

Such a request was made by the Commission regarding cybersecurity at the beginning of 2016 which resulted in the Scientific Opinion on cybersecurity (RTD, 2017). These recommendations informed the updated version of the EU Cybersecurity Act of 2019 as mentioned above. This thesis asks what the Scientific Opinion on cybersecurity looks like against the background of the EU's commitment to the Scientific Advisory Mechanism and the academic literature on EBP. Therefore, a qualitative content analysis of the Opinion, whitepapers used in it, and broader scientific literature is carried out. To determine what good scientific policy advice can look like, it draws in particular on a framework developed by Martin Carrier (2022) that explores the relationship between science and politics and suggests different criteria that are to be attained to make scientific policy advice "good". This thesis draws on this particular framework for reasons mentioned below (see Theory section) but seeks to integrate relevant insights from others to include the broader literature (Jasanoff, 1990; Parkhurst, 2017; Pielke, 2007).

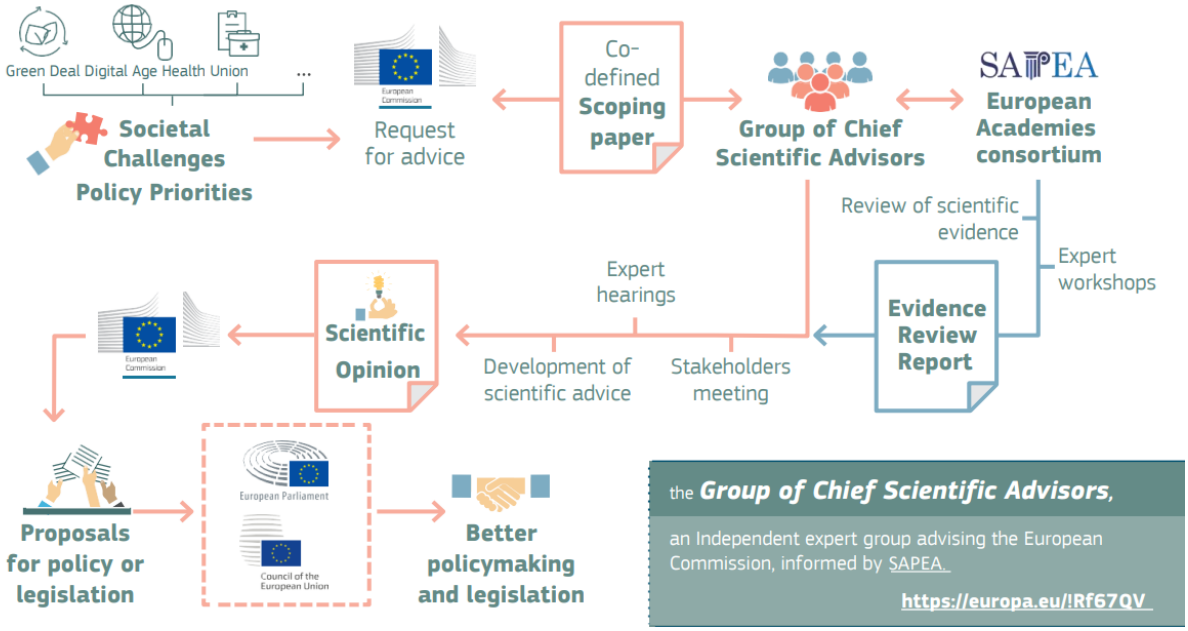

Figure 1: The Science Advisory Mechanism of the EU. Infographic of European Commission, Directorate-General for Research and Innovation (2021)

The scientific relevance of this thesis is the contribution to the understanding of good scientific policy advice in practice. It may account for better comprehension of how scientific policy advice can be designed in a good and beneficial way so that policymakers can adopt decisions and measures based on scientific facts. Since the scientific advice given on cybersecurity is evaluated, the societal relevance of this thesis is that it poses a point of learning for scientific advisors, policymakers, and interested citizens. With the help of my findings and the discovery of potential points of improvement, it will become

possible to assess if the Commission was well-informed for the adoption of the Cybersecurity Act in 2019 and thus also if important suggestions from the scientific community might have been overheard or if responsibilities and areas of competence between the Commission and the High Level Group have been mixed up. It is therefore adding to research on evidence-based policy in a concrete policy field.

2 Research question and aim

In this bachelor thesis, the main focus is going to be the analysis of the Scientific Opinion regarding cybersecurity published by the High Level Group through the lens of Carrier's article, to ultimately answer the question:

> **Was the scientific advice provided "good" scientific advice for the European policymakers in the sense of Carrier's framework?**

To answer this research question several sub-questions are relevant. The sub-questions relate to the three kinds of documents that are to be analyzed. In Section 4.2 these documents are elaborated on further. In order to find out whether the Scientific Opinion was "good" scientific advice, firstly, it needs to be discovered

> **What does good scientific policy advice look like?**

For the answering of this question, several frameworks on the use of scientific evidence in policymaking are taken into account. However, it is not enough to analyze the Scientific Opinion only, to determine whether the advice was good. A second step is to look at the whitepapers that the High Level Group included in its advice.

> **How do the policy suggestions concerning Cybersecurity mentioned in white papers compare to the ones discussed in the Scientific Opinion?**

The third criterion for the assessment is going to be critical literature regarding European cybersecurity policy.

> **How does scientific evidence regarding Cybersecurity discussed in broader critical literature compare to the evidence brought forward in the Scientific Opinion?**

3 Theory

3.1 Framework for good scientific policy advice

In this section, the theoretical basis for answering the research question is laid out. The literature on EBP is extensive and contains many frameworks to address the role of evidence in policymaking processes. This thesis draws on one particular framework for reasons mentioned below but seeks to integrate relevant insights from others to include the broader literature (Jasanoff, 1990; Parkhurst, 2017; Pielke, 2007).

The main framework for the analysis is going to be the one provided by Martin Carrier in his article "What Does Good Science-Based Advice to Politics Look Like?" (2022). This framework serves as the main scope for this analysis as Carrier complements existing theories for evaluating scientific policy advice by devoting a special role to non-epistemic values and by the development of clear guidelines on how to include these values into scientific policy advice. Non-epistemic values are considered in the other frameworks as well, but Carrier offers a more holistic and sophisticated approach toward their role and inclusion which is going to be shown in this section. The application of his framework is therefore specifically interesting for qualitative content analysis in a sensitive field like cybersecurity policies.

Carrier seeks to "address options for providing scientific policy advice and explore the relationship between scientific knowledge and political, economic and moral values" (2022, p. 5). Thereby, he focuses on the role of epistemic and non-epistemic values:

A) As epistemic values Carrier describes values that "delineate what kind of knowledge science is supposed to strive for or what sort of knowledge is worth knowing", whereas
B) non-epistemic values "aim at social utility" and include political, economic, and social values (2022, p. 7).

Science usually follows the value-free ideal meaning that science is an epistemic authority only, while value judgments fall in the area of competence of society and politics. When science becomes engaged in the non-epistemic value arena, these influences might compromise the epistemic integrity of scientific knowledge. One-sided interests might skew studies and research and thus lead to less trustworthiness (2022, pp. 6–7). Carrier proceeds to extract two major objections from the literature to whether it is a reasonable maxim to take value-free science as the only basis of policy advice.

Firstly, the way that science ought to deal with uncertainty and inductive risks is considered (Carrier, 2022, pp. 9–10; Douglas, 2000; Rudner, 1953). Inductive risks are the possibilities that epistemic assumptions might be either falsely assumed to hold true or falsely rejected (false positive/negative), ergo that scientific (epistemic) findings turn out to be wrong in the aftermath. Considering these risks in the light of the non-epistemic dimension of policymaking, assumptions should only be accepted while "comparing and weighing the negative practical impact of the two kinds of potential errors involved" to make them politically relevant (Carrier, 2022, p. 10). Subsequently, here a legitimate role for non-epistemic values in science is found in the context of justification and therefore also in scientific advice. Carrier states that "scientific knowledge in itself fails to bring forth any unambiguous conclusion regarding policy-making" and refusing to take social factors into account makes the advice politically meaningless (2022, p. 10).

Secondly, he considers the so-called gap argument saying that connecting evidence with theoretical states is grounded in value-laden background knowledge. "Questions of social concern are inherently laden with nonepistemic values" (2022, p. 10). Non-epistemic values play an essential and constructive role in this context: they "determine relations of significance" and shape the approach that is made toward a research field (2022, p. 11). However, there are two sides to the coin: non-epistemic values can also lead to "partisan judgement and bias" (2022, p. 11). For Carrier, the key problem lies in "the lack of distinctness between the legitimate domains of epistemic and nonepistemic values" (2022, p. 11). This precludes that "excluding nonepistemic values from the context of justification altogether" would be the better approach (2022, p. 11).

What Carrier seeks to do is to uphold the value-free ideal of science while still making sure that science leads to meaningful suggestions. Originating from this nuanced argument about the relationship between epistemic and non-epistemic values, a five-step approach to good policy advice can be derived (see *Figure 2*). Below, each of these steps is described in more detail while integrating it with relevant insights from the broader literature on EBP. For, as demonstrated in this theory section, Carrier combines elements also considered by other EBP scholars (Jasanoff, 1990; Parkhurst, 2017; Pielke, 2007) and presents them in a new way with a special focus on the role of non-epistemic values. The latter makes it the most relevant framework for an analysis of a specific policy advice and is the reason for its application in this bachelor thesis.

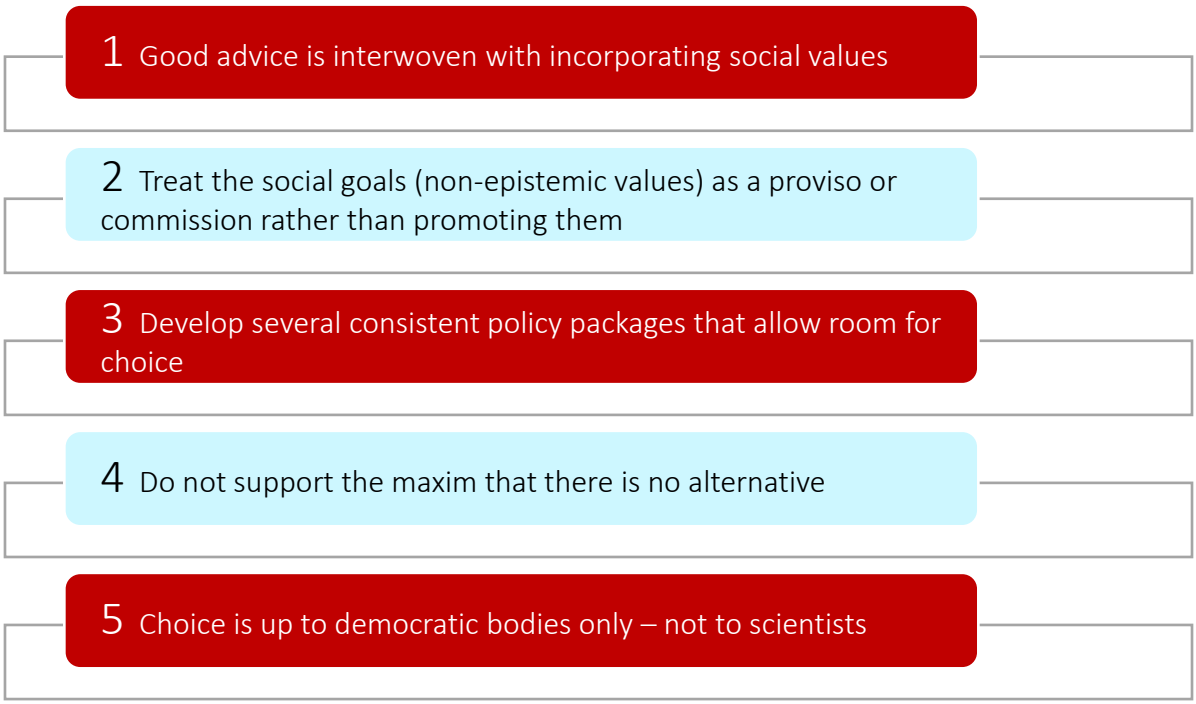

Figure 2: Criteria for good scientific policy advice, own illustration based on Carrier (2022)

1. *Good advice is interwoven with incorporating social values*

The necessity for the inclusion of social values in EBP is shared by many scholars. Parkhurst (2017) and Hawkins and Parkhurst (2016) describe several concepts in their framework on "Good governance of evidence" that are relevant to combining evidence use with the idea of good governance. Good governance connects normative factors with the concept of governing structures and is often used by e.g. the United Nations as a desirable form of governance of countries (Parkhurst, 2017, p. 159). I am going to focus on the extended version of this framework as described by Parkhurst (2017). One of the relevant concepts brought forward by Parkhurst is *Deliberation*. *Deliberation* demands public engagement so that competing social values are included in the policy process and different points of view are reflected in the decision-making (2017, p. 162). To grasp the relevant values, Parkhurst suggests more citizen engagement for example via citizen panels or planning cells. The relevance of non-epistemic values can also be seen in Jasanoff describing that the idea of scientific advisors purely focusing on scientific issues "seems fundamentally misconceived . . . the advisory process seems increasingly important as a locus for negotiating scientific differences that have political weight" (Jasanoff, 1990, p. 249). In line with these works, Carrier (2022, pp. 9–11, 18) argues that social values allow science advisors to justify why their findings are meaningful to policymakers. As they influence research approaches anyway, it is not feasible to neglect their role.

2. *Treat the social goals (non-epistemic values) as a proviso or commission rather than promoting them*

Probably most important for good scientific advice, Carrier argues, is to carefully distinguish between scientific facts and non-epistemic values. Scientists seem to tend to mistake a feature that is actually a value judgment for a fact. This hidden influence can make recommendations misleading to policymakers. It is of crucial importance to explicitly state the value-choice made and lay them open for the policymakers and the public. This is also a matter of transparency. It is an "important virtue of scientific policy advice to make values visible and subject to explicit judgment" (Carrier, 2022, p. 13). The key to good policy advice is "presupposing" non-epistemic values and not "promoting" them (2022,

p. 15). Promoting a value means actively committing to a value and trying to pursue it with one's research and advice. Presupposing however means to state values as separate premises elaborate policy advice "as if" a certain value would be aimed for, explicitly flagging the value presupposed. Thus, the advice does not conflict with the value-free ideal (2022, pp. 15–16, 18). In arguing for proviso over promotion, Carrier extends upon a warning for 'issue advocacy' in Pielke's (2007) classic in the field of EBP. Pielke (2007) discusses the distinction between scientific and non-epistemic values in a similar way. He recognizes that even those scientists that claim to focus only on scientific facts oftentimes slip into "stealth issue advocacy" meaning that they actually do express political or social preferences hidden in the guise of science (2007, p. 4). Pielke observes that "[t]his is why battles over science take on such importance across a wide range of areas. People can debate policy options through science without ever making their value commitments explicit. They can hide them behind science." (2007, p. 4). The scholar describes that this mixing up of science and value choices is generally seen as unfavorable since science thus can easily be misused by politicians for political purposes but recognizes that keeping the two apart is difficult.

3. Develop several consistent policy packages that allow room for choice

Science advisors should develop a plurality of policy packages that "combine facts, scientific accounts and nonepistemic premises" and tag these policy packages with "provisos that express a non-committal attitude to their nonepistemic objectives" (Carrier, 2022, p. 16). This also accounts for the independence of scientific policy advice. By highlighting different options and risks that may also be contrary to current social endeavors, advisors showcase that they are nonpartisan and "avoid the biased adherence to powerful social forces" (Carrier, 2022, p. 17).

Again, Carrier's framework embraces an aspect Pielke argues for, too. Pielke's (2007) work consists of bringing forward four possible roles that science advisors can take. One of them is the *Honest Broker of Policy Alternatives*. The Honest Broker comes close to what Carrier suggests in his article, especially regarding the development of policy packages. Scientific advisors that pursue this role would inform about and explain to policymakers all possible options and their consequences but leave the final choice up to the political decision-makers. The Honest Broker thereby includes social values that are related to the scientific evidence which enables policymakers to decide or narrow the scope of options along the lines of their political preferences. Honest Brokers usually work in interdisciplinary teams to enhance the perspective on the particular issue that they work on (Pielke, 2007, pp. 2–3). To avoid scientists' contribution to a "conflation of scientific and political debates" Pielke argues for the role of the Honest Broker to openly discuss possible consequences and values associated with a policy choice based on scientific evidence which connects also to the second criterion of Carrier's framework (2007, p. 7).

4. Do not support the maxim that there is no alternative

This point goes hand in hand with the development of several different policy packages as suggestions for policymakers. It is more an appeal to the courage of researchers to create alternative scenarios and "resist the urge of politicians to get unambiguous advice" (Carrier, 2022, p. 17). The advice should rather allow for a good fact- and value-based decision.

Parkhurst's concepts in good governance of evidence support this criterion in several ways. He argues for *Appropriateness* of evidence which means that the evidence should be suitable for policy advice i.e. that it addresses social concerns, provides useful options for policymakers, and applies to the specific context in discussion (Parkhurst, 2017, p. 161). This links also to Carrier's first criterion demanding the presence of social values but also stresses the need for different policy alternatives and options discussed in this criterion. Additionally, Carrier brings forward that the advice should enable a good fact- and value-based decision. To achieve this, Parkhurst instances three further concepts. *Quality* aims at a high standard of the evidence meaning that it is in line with scientific methodological

principles. *Rigour* considers the gathering of evidence and the avoidance of cherry-picking. Finally, *Contestability* points toward that the evidence and the research behind it ought to be open to critical questioning and challenging e.g. by peers. (Parkhurst, 2017, pp. 161–162). All three concepts are relevant to ensure a balanced decision that relies on state-of-the-art scientific evidence and is not skewed by presenting only a limited scope of evidence.

5. *Choice is up to democratic bodies only – not to scientists*

Carrier finishes by stressing the importance of this clear separation. Scientists must not interfere with political decision-making and appear to "illegitimately impose values on the public" by either not leaving room for choice or by violating the second step of this framework and actively promoting social values (Carrier, 2022, p. 18). Not infringing the democratic rule ultimately leads to more trustworthy and independent advice.

This was already mentioned before in Pielke's Honest Broker who narrows down and bundles the scope of options but leaves the final choice up to political decision-makers (see criterion 3, Pielke, 2007, pp. 2–3). In Parkhurst's framework, we find an explicit concept about this, too, called *Representation*. It means particularly what is of discussion here, namely that the final policy decision is up to democratic authorities only, not the scientific advisors.

3.2 Hypotheses

In addition to Carrier's (2022) framework the analysis is added on by the insights provided through whitepapers used in the Scientific Opinion of the HLG and critical literature regarding European cybersecurity policy (see Section 4.2) to ultimately determine if the advice given was "good" scientific policy advice. From the five criteria brought forward by Carrier, the first four are going to be considered in the analysis. The fifth criterion is strongly tied to criteria two and four and is excluded from answering the hypotheses and therefore from the analysis. A further justification for this is given in Section 4.3.

The theoretical basis guides toward three possible hypotheses:

H1: The advice given by the High Level Group regarding cybersecurity was good scientific policy advice. It met all four of Carrier's criteria for good scientific advice.

H2: The advice given by the High Level Group regarding cybersecurity was reasonably adequate. It met three out of four of Carrier's criteria for good scientific advice.

H3: The advice given by the High Level Group regarding cybersecurity was overall bad advice. It met only one or two out of four of Carrier's criteria for good scientific advice.

4 Methods

The following sections explain the methodological approach of this thesis which includes the research design, the choice of data, the conceptualization of the criteria of analysis, and, finally, the operationalization through a coding scheme.

4.1 Research design and methodology

In this bachelor thesis, I am going to make use of qualitative content analysis. Qualitative content analysis is a way of analyzing textual data to identify hidden key contents, themes, messages, and statements that are not explicitly visible at first sight but implicitly incorporated into the textual data at hand. Content analysis can manage to derive meaning from that data by grouping it into similar

categories or conceptual sets (Julien, 2008). This interpretative analytic approach recognizes that textual data is subjective and may reflect several meanings that are dependent on its specific context. Oftentimes qualitative content analysis relies on coding typically with the help of a qualitative analysis software like Atlas.ti. A code is "a word or short phrase that symbolically assigns a summative, salient, essence-capturing, and/or evocative attribute for a portion of language-based or visual data" (Saldana, 2016). These interpretative constructs generated by the researcher translate textual data into something meaningful for analysis. Originating from this first step of coding, the coded data can then further be organized into categories that symbolize certain shared characteristics or the beginning of a pattern a researcher might encounter (Saldana, 2016).

4.2 Choice of data and documents

Qualitative content analysis is suitable for identifying the core of and potentially hidden values in the documents analyzed. In terms of data collection, the main document in examination is the Scientific Opinion of the High Level Group of Chef Scientific Advisors of the European Union on "Cybersecurity in the European Digital Single Market" (RTD, 2017). It forms the center of my research since the main goal of this thesis is to find out whether this advice was "good" scientific policy advice according to Carrier's (2022) criteria. This scientific advice ultimately informed the EU Cybersecurity Act that was adopted on 17 April 2019. Therefore, it is a document of high responsibility and impact which makes it very interesting for analysis, plus the question of whether this advice was good and European policymakers were well informed is even more pressing. A second basis for the analysis is whitepapers that were taken into account in the Scientific Opinion namely the one of the European Research Consortium for Informatics and Mathematics (2014) and the one of the Association for Computing Machinery (2016). It is of high interest to find out how the suggestions in the whitepapers are taken into account – or not – in the Opinion. The third kind of document analyzed is critical literature regarding European cybersecurity policy to find out what other experts suggest and criticize in terms of cybersecurity and to see whether these issues are reflected in the Scientific Opinion or not. The contributions of Bendiek et al. (2017), Krumay, Bernroider, and Walser (2018), Gonzáles Fuster and Jasmontaite (2020), Carrapico and Barrinha (2017), and Pupillo (2018) are especially valuable in this regard, same as the CEPS (Centre for European Policy Studies) report "Strengthening the EU's Cyber Defence Capabilities" (Pupillo, Griffith, Blockmans, & Renda, 2018). These articles pose other possible perspectives the HLG could have taken. Since none of the articles was published before 2017 the scientific advisors could not literally consider these particular articles. Still, the publications rely mostly on literature from the period before 2017 which makes them comparable to the Scientific Opinion. The relation between the three data and evidence sources is depicted in *Figure 4*.

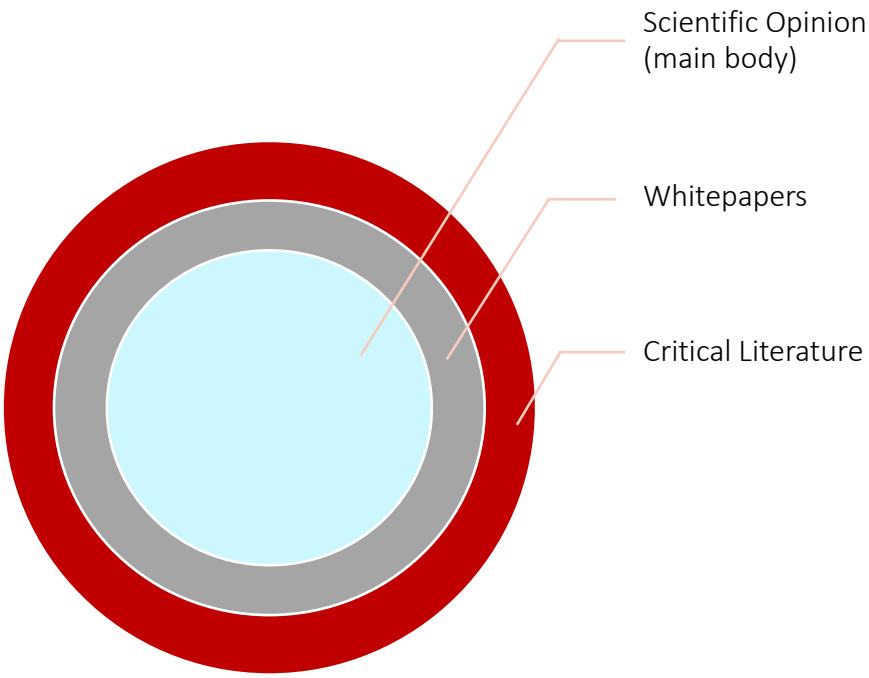

Figure 3: Visual representation of the data

4.3 Conceptualization of Carrier's criteria

To test my hypotheses it is central to investigate whether Carrier's criteria were met in the Scientific Opinion on cybersecurity by the HLG (RTD, 2017). To assess whether the criteria are met I am going to distinguish in line with the hypotheses in a dichotomous way in met and not met.

The *first criterion* can be answered in a relatively simple way by analyzing the Scientific Opinion in terms of the existence of non-epistemic values in the advice. If any non-epistemic values can be identified the criterion is met.

The assessment of the *second criterion* is more complex. Not only the existence of non-epistemic values is relevant but whether they are highlighted clearly when they come into place. The criterion is met when value choices are openly addressed and explicitly distinguished from scientific facts and not met if (a) the value choices either become apparent in the analysis but are not necessarily explicitly addressed or (b) if non-epistemic values are (implicitly) promoted instead of being presupposed.

For the *third criterion*, it is important to look for different policy recommendations that are explicitly connected to non-epistemic premises – so-called policy packages. The criterion is met when the policy advice brings more than one policy package to the fore. The criterion is not met when (a) different alternatives are presented while the connection between values and the policy suggestion (the policy package) is unclear or (b) there are no alternatives presented at all.

The *fourth criterion* seems very similar to the third one but if one takes a closer look, it becomes clear that the existence of different policy recommendations is not enough to fulfill its conditions. In addition to the Scientific Opinion, it is needed to analyze the whitepapers and the critical literature at this point to be able to determine if the alternatives presented by the HLG reflect the points suggested by other actors in whitepapers and raised in relevant literature or if they are not well-covered. If the other evidence sources are (a) incorporated to the full extent or (b) the most important suggestions are taken into account, the criterion is met. If it fails to incorporate the remarks of other evidence sources, it is not met.

The *fifth criterion* depends on the assessment of the second and the fourth criterion as it states that scientists should not interfere with political decision-making which means that the Scientific Opinion left room for choice, reflected the academic state-of-the-art, and did not promote social values. Due to its boundness to other criteria, the fifth criterion is excluded from answering the hypotheses and therefore from the analysis.

4.4 Operationalization of Carrier's criteria

For the analysis a coding scheme was developed to enable to search the documents for the elements necessary to determine the assessment of the criteria and therefore ultimately for the assessment of the hypotheses:

Table 1: Coding scheme

Concept	***Category***	***Code***
Carrier's first criterion of good policy advice	Non-epistemic values	Presence of values in the advice e.g.: security, privacy, data protection, awareness spreading, democratization/ inclusivity, fundamental rights, responsibility, trust (of citizens and other actors), autonomy, cooperation
Carrier's second criterion of good policy advice	Fact-value distinction	Presence in the advice of values that are openly discussed (see value list above); values that remain implicit; facts that are treated as distinct from values; authors agreeing with certain values (promotion); authors that list values as options (presupposition)
Carrier's third criterion of good policy advice	Policy package	Only one policy package; alternative policy packages; policy suggestion connected explicitly to value (presupposition); policy suggestion implicitly connected to value (promotion); possible policy suggestions: Cryptographic standards, best-practice systemic approach, limit technical vulnerabilities, digital identity management, education, user choice, development of EU cybersecurity industry, evidence sharing, worldwide cybersecurity governance

Carrier's fourth criterion of good policy advice	Alternative sources of evidence	Suggestions from literature/whitepapers present in advice (see list 3rd criterion); whitepapers and critical literature differ in kinds of evidence; inclusion of alternative sources; exclusion of alternative sources but with justification; alternative sources not discussed

The analysis and coding were carried out with the help of the qualitative analysis software Atlas.ti.

5 Analysis

This section presents the results of the analysis of the four criteria provided by Carrier (2022) and finally includes the assessment of the hypotheses.

5.1 Non-epistemic values: Analysis of Carrier's first criterion

To be able to assess the hypotheses the elaborated criteria derived from Carrier (2022) need to be carefully analyzed one by one. The first criterion is: "*Good advice is interwoven with incorporating social values"*. This is the easiest and clearest criterion to analyze as it only discriminates between the presence or absence of non-epistemic values in the Scientific Opinion. For the analysis of the criterion, only the Scientific Opinion (RTD, 2017) is relevant. As seen in *Table 2*, the coding of this document led to the identification of several non-epistemic values. The values ranged from concerns about fundamental rights to economic values. In a second round of coding, the values could be grouped into five value "families".

First value family: Citizen's rights

The biggest value family is bound up with *citizens' rights*. It includes the values of *data protection, freedom of expression and information, informed choice, privacy*, and *self-determination*. To start with, *data protection* refers to the responsible use and storage of personal data of citizens and assumes that it is desirable to protect personal data from cybercrime and misuse. *Freedom of expression and information*, second, is a fundamental right that enables citizens to express their opinions without fearing prosecution and to share and consume information from several sources without censorship, which is of special relevance in the online world, too. *Informed choice* is a core principle of research ethics but is also applicable to the handling of personal data unrelated to research on- and offline. It is valued that people can decide what happens to their data and that they are informed about the possibilities and consequences of their choices. Informed choice is also listed as a policy suggestion later in this thesis. An example of the encounter of this value can be found in the discussion about giving consent to collect personal data online through "ticking a box" – which is the most common way used to receive this consent. The scientific community considers this type of consent insufficient as it needs to be "[f]reely given, specific, informed and unambiguous" (RTD, 2017, p. 24).

> "An important condition for this to happen, is that there be **acceptable alternatives available to the user for services of the same level of quality**. If the **information for users is too much/too**

> **legalistic, or if they do not trust it,** and if users do not have good alternatives to turn to, **the enabling conditions for real consent are not fully in place.**" (RTD, 2017, p. 24, own emphases)

Informed choice is in close relation to the fourth value of *self-determination*. *Self-determination*, however, puts greater emphasis on the right to know and decide for which purposes one's data is stored and used and to have them at one's disposal. The desirability of this value (among other values) becomes obvious for example in this quote:

> "The lack of transparency about **what happens to personal data provided by users on-line either knowingly or unwittingly, is a key concern**. Service providers allow different identities to be created, but they can **link all these data to build highly sophisticated behavioural and psychological profiles of the person, as well as of one's friends and connections**. Technically, this **intimate knowledge of a person can be used by different actors** in different ways for example to commercially target the person, monitor behaviour, influence political choices including voting, or cyberattack through spear phishing" (RTD, 2017, pp. 23–24, own emphases)

The last value in this group of citizens' rights is *privacy*, which is one of the most natural values related to cybersecurity. The right to *privacy* refers to being able to keep data and actions private and not having to share them on- or offline when one does not want to. It is a central and often applied value when handling personal data. All citizens' rights values accumulated are mentioned 52 times in the Opinion and build on fundamental and human rights that the EU committed itself to. Thus, it is not surprising that these values also mark the Scientific Opinion on cybersecurity since they form a basis of the European self-understanding.

Second value family: Bridging values

The second biggest family mentioned 51 times are the so-called *bridging values.* These non-epistemic values deal with connective elements between politics, society, and businesses shaping the relationship between all actors in cybersecurity. They are called bridging values as they are considered necessary to bridge the possible gap between the actors, their choices, and their intentions. Bridging values are *responsibility*, *security*, *sustainability/comprehensiveness*, *transparency*, *and trustworthiness. Responsibility* refers to all actors in cybersecurity but especially to political actors and businesses. These actors should be equally accountable for their actions and not back up from tasks assigned to them. The meaning of this value becomes clear in the analysis of governance structures in the Opinion:

> "Yet another is the failure of governments and non-state actors, including businesses, to **commit to and act upon shared responsibility for cybersecurity**, where both public and private actors **partially cede or compromise their habitual spheres of autonomy and control in the interests of long-term benefits for all**." (RTD, 2017, p. 34, own emphases)

Security is another obvious value already present in the word "cybersecurity". It includes different dimensions from the security of personal data and security of technical systems to national security in a broader sense and forms together with *privacy* the most central value in cybersecurity politics (*security* mentioned 20 times, *privacy* mentioned 22 times). *Sustainability and comprehensiveness* aim at holistic systems and solutions that – in the case of products – last a whole product lifecycle beginning with the design phase and – in the case of strategies – provide long-lasting and inclusive guidance or care. It is assumed to be desirable that systems and strategies provide comprehensive and far-sighted solutions. *Transparency* refers to the desired openness of institutions handling data about how they process and store these data. In the Opinion this value is defined as follows: "[P]ublic authorities, service providers

and system developers must handle data in a transparent manner" (RTD, 2017, p. 19). The last value in this group is *trustworthiness*. Technical systems and encryption methods should be designed in such a way that citizens can trust service providers with their personal data and do not need to fear misuse. Trust is central in enabling the functioning of information and communication technologies and a digitalized world as these technologies need to be fed with data. If people do not trust a system, they are most likely not going to use it. This is seen as not aspirational.

Third value family: Economic values

A third value family is posed by *economic values* which are mentioned 37 times. Economic values focus on the economic impact of cybersecurity. The single values here are *economic competitiveness, economic "fairness", economic growth, economic incentives,* and *innovation* in an economic sense. *Economic competitiveness* provides mainly a global perspective on the economy. It is wished-for that European businesses perform well in the global economy and are able to compete with e.g. American businesses from Silicon Valley, which are known to lead the technical market. *Economic fairness* on the other hand has a Europe-centered perspective and refers to creating a "level playing field" (RTD, 2017, p. 13) for all businesses within the EU and enabling also smaller companies and start-ups to enter the market and compete with bigger players. *Economic growth* is a value that is easily overseen by unaware readers as it is a value that can almost be considered internalized by capitalistic societies. It means that economic growth is considered as something that should be achieved and supported by political means: "[D]eveloping and applying appropriate standards is an opportunity for EU companies to attain competitive advantage in the global markets, promoting privacy-friendly products for example" (RTD, 2017, p. 27). In this quote *economic growth* can be identified as a value together with *economic competitiveness* and *privacy*. Commonly, several values from the group *economic values* are found together. *Economic incentives* stand for a perceived possibility and necessity to guide cybersecurity actors and especially businesses toward certain actions by linking it to financial benefits. In the Opinion this value can be found for example in this way: "Provide at EU level appropriate incentives (including economic and legal) to encourage responsible disclosure and repair of vulnerabilities" (RTD, 2017, p. 42). The final value in this group is *innovation* which refers to aiming to stimulate and achieve new developments in technology or other areas. For example, in the section discussing trust and security in the Scientific Opinion this value can be identified:

> "There is a need to maintain and increase participation in the digital market, so that people do not limit or reduce their digital transactions because of a lack of trust and, in the process, **deprive current and future generations of innovative economic and social opportunities.**" (RTD, 2017, p. 29, own emphases)

The presence of economic values in the Scientific Opinion is a surprising outcome of the analysis as it diverges from the expected values described in the coding scheme (see Table 1). I as a qualitative researcher did not expect to find economic values in a high quantity in the Opinion as I did not associate cybersecurity with e.g. the value of economic growth. Which impact these unexpected values have on the fact-value distinction and the value-free ideal of science is going to be discussed in the evaluation of the second criterion below.

Fourth value family: Political values

Political values can be found 38 times. This family deals with the political side of cybersecurity and values concerning mainly the political actors (e.g., the Commission and Parliament, but also the Member States and foreign political partners). The group consists of the non-epistemic values of *criminality and*

law enforcement, enhance international cooperation, European values, and *democratic governance. Criminality and law enforcement* means that it is generally wanted to prosecute cybercrime and increase the application and enforcement of legal rules in cyberspace. *Enhance international cooperation* is a value that strives for more intensive cooperation between cybersecurity actors worldwide. Governments and political actors as well as businesses and societal actors should connect across national borders. A call for *enhanced international cooperation* can look like this in the Scientific Opinion:

> "Given the global and rapidly-evolving nature of cybersecurity challenges, **Europe should be at the forefront of establishing worldwide and coherent cybersecurity governance** for the digital economy. This should be consistent with and build upon a strong European cybersecurity governance framework, fully aligned with **European values and the fundamental rights of EU citizens**." (RTD, 2017, p. 46, own emphases)

Other values identified in this quote are *European values, privacy* as a fundamental right, and *economic incentives*. Another value included here appears a bit blurry and unclear: I name it "*European values*". This value when found in text often refers to the uniqueness of the EU and the boundness to fundamental rights. It also includes the idea that Europe should engage at the forefront of international cooperation. If one reads carefully, one might also find a slight conveyance of assumed European superiority: "However, given the strategic importance of cybersecurity to ensure European sovereignty, to protect European values and promote them worldwide, SAM HLG strongly recommends that the EU play a more prominent leading role in establishing effective cybersecurity governance globally." (RTD, 2017, p. 37). Finally, *democratic governance* is a value that aims for democratic governance structures including citizens and elected institutions in the policy process. Democratic principles ought to be respected in cybersecurity policy.

Fifth value family: Societal values

The last and least mentioned family are *societal values* with a total of 18 times. These non-epistemic values concern the European society and its members via *citizen participation,* the *contribution to public good,* or broader *non-epistemic challenges*. *Citizen participation* stands for the inclusion of citizens and fostering the active participation of citizens in the cybersphere and political, and social topics surrounding this area. *Contribution to public good* is a value that describes a desire for actions related to cybersecurity to be a benefit to the overall society and make a positive contribution. The values of *citizen participation* and *contribution to public good* can occur like this in the Scientific Opinion:

> "The EU can play a role in enabling citizens' trust in the digital ecosystem. When people trust that a system will protect their personal data, they may be **more willing for example to share** their **medical records in order to promote innovations in health**, rather than when they suspect strongly that their openness will be used against them." (RTD, 2017, p. 29, own emphases)

The *non-epistemic challenges* code serves as a catch-up for all articulation of broader, social, or political challenges that are left without a clear direction in the Scientific Opinion but clearly express a non-epistemic struggle or challenge related to cybersecurity issues. Cybersecurity is assigned a (general) social dimension in quotes marked with this value code: "The Opinion had to draw on these different domains and could not address science and technology separately from the rest [of the non-epistemic values]. The scope of the Opinion was thus refined in consultation with experts" (RTD, 2017, p. 16).

Table 2: Quantity of all non-epistemic value codes in the Scientific Opinion

Non-epistemic value codes	Quantity
Citizens' rights:	***52 (sum)***
data protection*	8
freedom (expression + information)*	3
informed choice*	10
privacy (fundamental rights)*	22
self-determination (right)	9
Bridging values:	***51 (sum)***
responsibility*	11
security*	20
sustainability/comprehensiveness*	3
transparency*	6
trustworthiness	11
Economic values:	***37 (sum)***
economic competitiveness	10
economic "fairness"	4
economic growth	15
economic incentives	4
innovation (economic)	4
Political values:	***25 (sum)***
criminality and law enforcement	3
enhance international cooperation*	9
European values*	8
democratic governance	5
Societal values:	***18 (sum)***
citizen participation*	7
contribution to public good	8
non-epistemic challenges	3
Total: 22 (in 5 value families)	**183**

**Values laid down as principles in the Scientific Opinion (presupposed/proviso)*

5.2 Fact-value distinction: Analysis of Carrier's second criterion

The second criterion "*Treat the social goals (non-epistemic values) as a proviso or commission rather than promoting them"* is a lot more complex to answer in comparison to the first one. Now that the existence of non-epistemic values could be demonstrated this criterion looks for whether these values are clearly highlighted when they come into place –to count as a 'proviso' – or whether they are implicitly promoted by the High Level Group. The Scientific Opinion includes a "Principles" section that lists the principles – which are non-epistemic values – underlying the Opinion. The HLG considers these values important for the Commission and its policymaking and thus treats them as if they were aimed for. These include values taken from the EU Charter of Fundamental Rights like *citizen participation, data protection, privacy,* and *freedom of expression and information*. In addition to the values stemming from the Charter of Fundamental Rights, the HLG identified a handful more values in three bullet points: the first value is "*transparency*". The Opinion presupposes that it is desirable that data is handled transparently by service providers, public authorities, and system developers (RTD, 2017, p. 37). The second point of additional principles is called "duty of care towards customers" and entails the values *responsibility* and *sustainability*/*comprehensibility*. The idea of a duty of care towards

customers is that soft- and hardware producers "must follow due diligence with respect to cybersecurity for the whole product lifecycle, starting from the design phase" (RTD, 2017, p. 37). The last one is "shared responsibility for cybersecurity" with the values *responsibility* and *enhance international cooperation*. The HLG assumes that not only one but all actors, public and private, European and global are jointly responsible for tackling cybersecurity issues.

Whenever one of the values stated in the principles section occurs, it can be assessed as a proviso since it was explicitly stated in the principles section. Non-epistemic values for which this holds are marked with an asterisk in *Table 2.*

First value family: Citizens' rights

Taking a closer look at the groups in *Table 2* it becomes obvious that in the group of *citizens' rights* all values except *self-determination* are marked as presupposed. *Self-determination*, however, is closely connected to *informed choice* which is a presupposed value. It is not surprising that the citizens' rights values, which are the ones found most often, are presupposed since these rights are part of the Charter of Fundamental Rights which not only served as a basis for the principles of the Opinion but is fundamental to the European Union itself.

Second value family: Bridging values

What is more interesting, is that four out of five bridging values count to the presupposed principles: *Responsibility, security, sustainability/comprehensiveness*, and *transparency.* Subsequently, it appears that the HLG assumes that the Commission has an interest in connecting politics, society, and businesses and performing an integrative power in cybersecurity politics. This would be in line with the Commission's tasks and role as the supranational part of the executive (Hix & Høyland, 2011, p. 47). As an interim summary, it can be noted that the two value groups that are mentioned most often, are almost entirely presupposed.

Third value family: Economic values

To continue with the analysis of the second criterion now the group of *economic values* is in focus. None of the economic values were laid out as principles of the Scientific Opinion, and nor were they expected to occur in the coding scheme developed prior to the analysis. However, they were articulated 38 times in it. Can it subsequently be said that the HLG promotes economic values in the disguise of science? The answer to this question is not as obvious as it may seem. Just because values are not mentioned in the principles of the Opinion it cannot automatically be assumed that they are promoted and not clearly highlighted. An example of a clear statement of an economic perspective including the value of *economic growth* can be found in the Opinion: "**From an economic perspective**, proving safeguards to users may encourage continued use of digital transactions" (RTD, 2017, p. 26). Another example explicitly including *economic growth, economic competitiveness*, and *security* can be found here: "Investing in core competences in cybersecurity **will strengthen Europe's cyber capability and its role as a trading partner**" (RTD, 2017, p. 28). Yet, economic values can also be found in a way that assumes them to be self-evident and natural: "Education and building a culture among professionals that focuses on resilience of systems is the essential approach to increase cybersecurity, while regulation that may be required, **should not stifle innovation or create barriers to new entrants**." (RTD, 2017, p. 28). Here the values of *economic competitiveness*, *economic growth*, and *innovation* appear as goals that are axiomatical to be pursued and thus supported by the scientific advisors writing this Opinion. A similar observation could be made in this quote: "However, the majority of leading businesses are from America or Asia, and so **growing of the European cybersecurity sector is crucial**" (RTD, 2017, p. 28). Why

would a growing European cybersecurity sector be crucial if not *economic competitiveness* and *growth* are promoted values? When describing the value code *innovation* earlier in this thesis a quote was employed that states the need for people to participate in the digital market to not "deprive current and future generations of innovative economic and social opportunities" (RTD, 2017, p. 29). Economic innovations are here generally seen as something positive that is necessary for future generations to strive for. It might be the case that the HLG did not maliciously promote these economic values to impose their ideas on policymakers but that these economic values are so obviously inherent to capitalist societies and their political leaders, that the HLG overlooked to flag these values as something unrelated to scientific facts. Even though it is to assume that the European Commission – that is the addressee of the Scientific Opinion – does pursue these economic values, too, it is still problematic in terms of Carrier's fact-value distinction. The internalization of these capitalist, economic values reminds of Marx's (1867/2019) description of a society circling the accumulation of capital in "Capital", to the point that it dominates all areas of politics and life in general. This is a possible explanation for why the HLG has failed to explicitly state the economic values as separate from scientific facts. From the other value families, at least some value codes are presupposed through the principles section. Therefore, the other values remain undiscussed in this section.

5.3 Policy packages: Analysis of Carrier's third criterion

For Carrier's third criterion "*Develop several consistent policy packages that allow room for choice"* the analysis included identifying policy recommendations in the Scientific Opinion and determining whether they are explicitly connected to non-epistemic premises. The elaborations of the High Level Group resulted in ten recommendations structured in four thematic groups. I am going to exemplary explain one policy recommendation and its value connection per thematic group. All recommendations and their corresponding values can be found in *Table 3*. The first group of recommendations considers policy suggestions regarding technical advancements which are the implementation of *cryptographic standards*, the adoption of a *systems engineering approach*, and the *reduction of technical vulnerabilities*. The recommendation about *cryptographic standards* highlights the importance of good, state-of-the-art encryption methods and the dangers that come along with manipulating cryptography:

> "Ensure that **cryptographic standards** in the EU reach and remain at state-of-the-art levels. **To maintain the trust of users/citizens** as well as **protecting their privacy and providing security**, neither back doors nor other ways of weakening encryption should be introduced." (RTD, 2017, p. 41, own emphases)

The HLG emphasizes that to ensure *trustworthiness*, *privacy*, and *security* high cryptographic standards are necessary and should not be weakened for any purpose (earlier in the Scientific Opinion there is a discussion about weakening cryptographic standards to track criminals online and gather information about criminal activities, RTD, 2017, p. 31). The connection between the recommendation and the non-epistemic values that would be pursued with it becomes apparent in the part quoted.

The next group of recommendations has a citizen-centered focus on cybersecurity. These suggestions to the European policymakers entail *attribute-based digital identity management, citizen education,* and *informed choice*. The least self-explanatory of these recommendations is *attribute-based digital identity management*. Basically, it means that users decide which attributes of their identity they want to reveal in which context and that personal data is not shifted from one context to another without explicit knowledge or consent of the user. The HLG recommends: "**To respect privacy**, promote the development and **context-tailored use of attribute-based digital identity management**" (RTD, 2017, p. 43). Here the main connection and use of this suggestion is made obvious, namely the protection of the users' *privacy*.

The professional recommendation deal with cybersecurity as a profession and what comes along with it. The two ideas brought forward at this point are *strengthening the EU cybersecurity industry* and *training of cybersecurity experts*. Concerning the EU cybersecurity industry, the HLG suggests:

> "Support the development of an EU cybersecurity industry ("made in Europe"), including data transfer and network technologies, protection of meta data, and "cloud"-based data storage and processing, **to enhance the security of digital systems and guarantee the fundamental rights of EU citizens, while also increasing job creation and European competitiveness in the global market**." (RTD, 2017, p. 45)

The non-epistemic values of *security, European values, economic growth,* and *economic competitiveness* that are connected to this suggestion are clearly described as a non-epistemic goal of the strengthening of the EU cybersecurity industry.
The last group refers to connecting recommendations between cybersecurity actors which consists of *evidence and information sharing,* and *the creation of an international cybersecurity governance framework*. The connection between the non-epistemic values is not as explicitly formulated as in the previous examples but it still becomes apparent:

> "There is a tension between the need for collecting and, most importantly, the sharing of evidence on cyber-incidents **in order to improve cybersecurity**, and national security concerns, which limit such sharing. While recognising this tension, the EU should foster such Europe-wide evidence collection and sharing, **including cooperation between public and private sectors**."

Even though the style of expressing the values at hand is different from the other recommendations, the values of *contributing to the public good* over national security concerns and the *enhancement of international cooperation* are still clearly expressed in this part of the suggestion.

The Scientific Opinion brings forward several policy recommendations that are clearly connected to non-epistemic goals. Therefore, the recommendations can be qualified as policy packages. What is questionable now is whether these policy packages really pose alternatives or whether the HLG brought forward just one big policy package. What speaks for the assumption that it is just one big policy package is that the different recommendations are not contrary to each other or provide for an "either… or" decision, but that they add up to each other and are meant to be equally implemented. On the other hand, the Commission is still able to choose and prioritize which values and areas are more important to her and which recommendation she wants to implement first or rather if she wants to leave out certain areas. Contradicting policy recommendations would also be confusing in terms of the use of scientific evidence since the HLG's task is to bundle and explain scientific discussions and only speak out recommendations if a consensus among experts could be identified. More about these discussions and the lack of concrete evidence for the effectiveness of certain policy measures will follow in the analysis of criterion four. Subsequently, it can be said that in the Scientific Opinion four thematically consistent policy packages are brought forward.

Table 3: policy packages - policy recommendations in connection to non-epistemic values

Policy recommendation code	Non-epistemic value connection
Technical recommendations:	
Cryptographic standards	Data protection, privacy, security, trustworthiness
Systems engineering approach	Privacy, security
Reduce technical vulnerabilities	Criminality and law enforcement, economic incentives, sustainability/comprehensiveness
Citizen-centered recommendations:	
Attribute-based digital identity management	Data protection, informed choice, privacy
Citizen education	Citizen participation, responsibility
Informed choice	Data protection, democratic governance, informed choice, privacy, transparency
Professional recommendations:	
Strengthen EU cybersecurity industry	Economic competitiveness, economic growth, enhance international cooperation, European values, security
Expert training	Security, sustainability/comprehensiveness
Connecting recommendations:	
Evidence/ information sharing	Contribution to public good, economic competitiveness, enhance international cooperation, trustworthiness
International cybersecurity governance framework	Economic incentives, enhance international cooperation, European values, privacy

5.4 Alternative evidence sources: Analysis of Carrier's fourth criterion

Lastly, the fourth criterion "*Do not support the maxim that there is no alternative"* demands a broader analysis. In addition to the policy recommendations brought forward in the Scientific Opinion, suggestions and discussions from relevant whitepapers and academic literature on the topic of cybersecurity in the EU are analyzed and compared.

The Scientific Opinion and the whitepapers

To start with, the Scientific Opinion refers to two whitepapers. One was published by the Association for Computing Machinery titled "Advancing Cybersecurity Research and Education in Europe" (ACM, 2016). The ACM paper is written in a similar style as the Opinion and advocates for twelve "Guiding Principles for Public Policies to Advance Cybersecurity Research and Education" (ACM, 2016, p. 4). These suggestions include for example international cooperation, greater incorporation and consideration of security and privacy in processes and approaches concerning the digital world, and increased education and public engagement about and in cybersecurity issues. One suggestion that is mentioned in the ACM whitepaper but not in the Scientific Opinion is the introduction of legal protections for privacy and security researchers. However, this "guiding principle" is not elaborated on further in the following sections of the whitepaper. Other than that, no differences of significance between the two documents could be found. Issues of security and privacy by design (ACM, 2016, p. 13; RTD, 2017, p. 33) and the necessity for proper verification of hard- and software (ACM, 2016, p. 12; RTD, 2017, p. 33) are for example discussed by both sets of authors. The other whitepaper was published by the European Research Consortium for Informatics and Mathematics (ERCIM, 2014). A

noticeable difference between this document and the Scientific Opinion is, that the ERCIM whitepaper is much more technical and entails more technical details and language. Therefore, more concrete ways to reach better cybersecurity are discussed in the whitepaper, e.g., while the Scientific Opinion only refers to state-of-the-art cryptography, in the ERCIM whitepaper concrete cryptography trends and possibilities are discussed (ERCIM, 2014, pp. 31–33). However, this is not problematic in terms of the inclusion of alternative sources of evidence in the Opinion. Since the Commission is the addressee, deep technical insights and discussions are not required as the Commissioners only need to be informed about general trends and what to pay attention to in policymaking and not the detailed technical realization of the trends and the priorities they choose. The ERCIM whitepaper provides more diverse discussions about solutions and a more comprehensive view of cybersecurity challenges. While the technical details are beyond the scope of the Scientific Opinion, general discussions with direct political applicability should be reflected in it. In the whitepaper, there is an elaboration on the possibility of "security-as-a-service" which cannot be found in the Opinion. The idea is that parts of information security can be outsourced to external service providers which have greater experience. This can be "especially relevant to organizations with limited information security resources and expertise (e.g., small and medium enterprises)" (ERCIM, 2014, p. 23). It is not possible to outsource information security completely as e.g. for the analysis of some incidents or attacks internal knowledge is necessary "[b]ut they can get at least those areas as a service where they have considerable shortcomings. With more and more sophisticated technologies deployed in the cloud, Security-as-a-Service is expected to become a valuable market" (ERCIM, 2014, p. 23). Other than that, no serious issues were omitted entirely. The analysis of the ERCIM whitepaper leaves behind the observation that the Scientific Opinion could have been generally more detailed.

The Scientific Opinion and wider scientific literature

The second type of alternative evidence sources is broader scientific literature on the topic of cybersecurity in the EU. To begin with, Bendiek, Bossong, and Schulze (2017) react with their paper to the EU's updated cybersecurity strategy in 2017 which lead the way to the Cybersecurity Act in 2019. The paper provides a critical view of the strategy and gives suggestions on what needs to be figured out more clearly until the actual Cybersecurity Act is adopted. The authors call for coherent EU action including legal measures and point to the institutional and financial difficulties that need to be overcome for proper cybersecurity since the EU lacks competencies in the area (Bendiek et al., 2017, pp. 2–3). Especially in expert training, which the authors recognize as an important means to improve Europe's cybersecurity, this could be a problem: "However, the EU has almost no formal competences in education. This structural deficit cannot be compensated by further proposals for a European "blueprint" on crisis-response mechanisms or reinforced cybersecurity exercises alone" (Bendiek et al., 2017, p. 3). The Scientific Opinion does not inform much about the feasibility of their suggestions but only proposes what they found to be a scientific consensus on the topic with relevance to policymaking. This, however, is not problematic since the HLG's task is to provide scientific evidence and not to discuss the political and institutional feasibility, which is other consultants' area of expertise, while this assessment of practicability is of course still a very relevant one. Bendiek et al. also discuss many aspects that are taken up in the Opinion. For example, the development of open-source software, meaning that the source code of software programs is openly accessible and traceable. They mention that open-source can be a way to greater cyber resilience (Bendiek et al., 2017, p. 2). The HLG goes into the topic in a section called "Observations" right before the recommendations where they discuss findings that lack concrete scientific evidence. While open-source can increase transparency and security other experts prefer "proprietary software and systems in the interest of business development" (RTD, 2017, p. 40). The HLG could not find a clear consensus to recommend open-source but they list it as a possibility to for example "enable trust in digital transactions" (RTD, 2017, p. 40).

Krumay, Bernroider, and Walser (2018) provide an analysis of the US National Institute of Standards and Technology (NIST) framework on which the European cybersecurity framework was based and check for uncovered parts in the NIST framework in a broad literature study. An interesting insight that is missing in the Scientific Opinion is the coverage of the impact of natural disasters, especially in the context of critical infrastructure. Natural disasters and climate change can have an impact on systems and "[f]ire, voltage and flood protection of buildings and premises" is necessary to secure for example servers (Krumay et al., 2018, p. 379). In the area of critical infrastructure, this is of special relevance but also for businesses and governmental activities.

Carrapico and Barrinha (2017) analyze whether the EU is a coherent cybersecurity actor and highlight that while the EU strives for coherency it is also important that they comply with the principle of democratic governance and respect fundamental rights: "it is fundamental that we understand that a coherent actor must also be coherent with the values it defends" (Carrapico & Barrinha, 2017, p. 1268). This is in line with the Opinion in which the scientific advisors set the EU Charter of Fundamental Rights as a principle of their cybersecurity recommendations (RTD, 2017, p. 19).

Equally like the HLG, Pupillo (2018) argues that cybersecurity should become a "collective responsibility and cyber awareness and computer hygiene should become an integral part of digital literacy programmes" (2018, p. 2). Pupillo fears collective-action problems if cybersecurity education programs, awareness-raising campaigns, and proper policies fail to be implemented. This is in line with HLG's recommendations (RTD, 2017, 43,45).

The CEPS report on the EU's cyber defense capabilities is more focused, as the title might suggest, on cyber defense than on cybersecurity in a broader sense (Pupillo et al., 2018). The authors' main call is the creation of an EU Cyber Defense Agency. This agency's mandate would go beyond the scope of ENISA's mandate (European Union Agency for Network and Information Security) as it should have shared executive competencies with the member states to be able "to develop and utilise strategic and operational capabilities at the EU level" (Pupillo et al., 2018, p. iv). This centralized agency could carry out tasks more efficiently as expertise could be gathered and the agency would serve as a center for all cyber defense issues, including monitoring of attacks, implementation of strategies, communication, and policy suggestions (Pupillo et al., 2018, pp. 64–65). The possibility of the creation of a new agency is not discussed in the Scientific Opinion.

5.5 Evaluation of the criteria and hypotheses' assessment

After the analysis of all four of Carrier's (2022) criteria, an assessment of their fulfillment can be made. The first criterion was about the presence or absence of non-epistemic values in the Scientific Opinion. In the analysis, several non-epistemic values could be identified which are summarized in *Table 2*. Therefore, **the first of Carrier's criteria is fulfilled**.

In the second criterion, a proper distinction between scientific facts and the beforementioned values was the object of the analysis. It was shown that, while quite many value choices become apparent and a proper fact-value distinction was made in many cases, the HLG sometimes gravitates to slip into what Pielke (2007) calls "stealth issue advocacy", especially in the case of economic values, which tend to be implicitly promoted. **The second criterion is therefore not met**.

In the analysis of the third criterion, it was looked for different consistent policy packages that combine policy recommendations with non-epistemic premises. Four policy packages could be identified in the Scientific Opinion that showcase a clear connection between the recommendation and the social goals that would be pursued with it. This results in the assessment that **the third criterion is met**.

Other sources of evidence were analyzed, answering the fourth criterion, to determine whether the Scientific Opinion presents the state-of-the-art alternatives and discussions of the scientific community. Looking at the two whitepapers no substantial differences in the kind of recommendations

could be found, while the ERCIM whitepaper did present a more comprehensive view than the Opinion. The analysis of broader critical literature showed that there are issues of feasibility and institutional coherence to bear in mind for the Commission which however go beyond the mandate of the HLG. Meaningful hints on the preservation of fundamental rights were incorporated in the Opinion same as other remarks of the papers analyzed. Only the discussion of the creation of a completely new agency for cyber defense (Pupillo et al., 2018) was omitted in the Opinion. Taking these insights into account it can be concluded that not all but the most important suggestions of alternative evidence sources are taken into account, ergo **the fourth criterion is met**.

The analysis of Carrier's (2022) criteria for good scientific policy advice made it obvious that **the advice given by the HLG met three out of four criteria**. Only the second criterion was classified as "not met". Going back to the established hypotheses this means that H1 and H3 can be rejected. The evidence found in the analysis suggests that H2 can be accepted which means that the advice given by the High Level Group regarding cybersecurity was reasonably adequate as it met three out of four criteria.

6 Conclusion

This bachelor thesis analyzed the Scientific Opinion on cybersecurity provided by the EU High Level Group of Chief Scientific Advisors to ultimately answer the question "**Was the scientific advice provided "good" scientific advice for the European policymakers in the sense of Carrier's framework?".** The framework provided by Carrier (2022) in combination with the contributions of other EBP scholars facilitated the determination of what good scientific policy advice looks like. The analysis of these criteria, which included a detailed qualitative content analysis of the Scientific Opinion and alternative evidence sources like whitepapers and critical literature, showed, that the Scientific Opinion meets three out of four analyzed criteria which results in the assessment that **the advice was neither good nor bad but reasonably adequate.** The European Commission was acceptably informed for the adoption of the Cybersecurity Act in 2019.

The most striking finding of this thesis was the role of economic values in the Scientific Opinion. These kinds of non-epistemic values were not explicitly presupposed by the HLG, like for example in the case of the values of citizens' rights, but could sometimes be found explicitly and other times even implicitly mixed up with scientific discussions. While it is to assume that the Commission does pursue these economic values, too, it is still a problem in terms of the fact-value distinction. A certain subscription to economic values can also be found in the discussion on open-source software. The HLG gives considerable weight to experts preferring proprietary systems that, unlike open-source, fit with an economic system headed towards marketizing digital security products (and hence with the non-epistemic values of economic competitiveness and growth), and do not give out a clear recommendation for the use of these systems. It appears that economic values are so intrinsically inherent to capitalist societies and their policymakers that the HLG overlooked distinguishing these values from their scientific elaborations. This can not only explain why the HLG might has failed to explicitly state the economic values as separate values but also why I did not consider these values to possibly appear in the Scientific Opinion in my coding scheme. Retrospectively, it is not that surprising that these values occur in the Opinion, but my own partial internalization of these values can be an explanation for why I did not actively consider them until I encountered them in the document. This result highlights the effectiveness of carefully done qualitative content analysis. Through thorough coding of the document, the economic values became obvious although I did not explicitly search for them. It can be said that the method of qualitative content analysis was thus an adequate research design for answering the research question. Even though the research design has shown its strengths in the analysis of non-epistemic values in the document, of course, there are also limitations and opportunities for improvement

for future research. Especially in the analysis of the fourth criterion more quantitative and systematic techniques could be helpful to provide a more comprehensive analysis of the broader literature and include more papers more detailly. A systematic literature review can for example be suitable to gain deeper insights into the cybersecurity research literature. However, this would have exceeded the scope of this thesis. Another suggestion for future research in this field is to work in interdisciplinary teams. For political scientists alone it may be difficult to grasp technical details and assess whether proposed technical measures are suitable or to understand the informatic details in papers on cybersecurity. Collaborating with scholars from informatics and computer science can expand the horizon and expertise on the topic of cybersecurity and enable a more profound analysis. Future work could also address how the Commission has incorporated the Scientific Opinion in the Cybersecurity Act.

This thesis makes an important contribution to evidence-based policy research on cybersecurity and the understanding of the work and role of scientific advisors in policymaking. It can also be taken as a point of learning for scientific advisors in general, on which aspects to pay attention to in giving scientific advice. Most important is to carefully distinguish between non-epistemic goals and scientific facts. Especially in times of rising scientific skepticism as seen in the examples of climate change and the Covid-19 pandemic where some people tend to think science is a matter of opinion and not of evidence, it is important to keep the line between the two clear and not give doubters a valid basis to criticize the influence of scientific evidence on policymaking and to prevent "research" that did not follow the scientific principles of researching to influence politicians. As we watch democratic quality suffer even in the EU looking at Hungary and Poland good evidence-based policymaking can be an opportunity to respect democratic principles and base policymaking on scientific evidence at the same time.

References

Association for Computing Machinery (2016). *Advancing Cybersecurity Research and Education in Europe: Major Drivers of Growth in the Digital Landscape*. Cybersecurity Policy White Paper. Retrieved from http://www.acm.org.ezproxy2.utwente.nl/binaries/content/assets/public-policy/2016_euacm_cybersecurity_white_paper.pdf

Bendiek, A., Bossong, R., & Schulze, M. (2017). *The EU's revised cybersecurity strategy: half-hearted progress on far-reaching challenges* (SWP Comment No. 47). Berlin.

Carrapico, H., & Barrinha, A. (2017). The EU as a Coherent (Cyber)Security Actor? *JCMS: Journal of Common Market Studies*, *55*(6), 1254–1272. https://doi.org/10.1111/jcms.12575

Carrier, M. (2022). What Does Good Science-Based Advice to Politics Look Like? *Journal for General Philosophy of Science*, *53*(1), 5–21. https://doi.org/10.1007/s10838-021-09574-2

Douglas, H. (2000). Inductive risk and values. *Philosophy of Science*. (67559-579).

ENISA (n.d.). Standards and Certification. Retrieved from https://www.enisa.europa.eu/topics/standards

European Commission (n.d.). Group of Chief Scientific Advisors. Retrieved from https://ec-europa-eu.ezproxy2.utwente.nl/info/research-and-innovation/strategy/support-policy-making/scientific-support-eu-policies/group-chief-scientific-advisors_en

European Commission (2022, February 22). Cybersecurity Policies. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies#ecl-inpage-kmq7cvh2

European Commission, Directorate General for Research and Innovation (2016). *Science Advisory Mechanism: Ensuring sound independent scientific advice for EU policies, matching the demands of the European Commission for scientific evidence and advice, with the best available science*. Publications Office. https://doi.org/10.2777/49251

European Commission, Directorate General for Research and Innovation (2017). *Cybersecurity in the European digital single market*. Retrieved from Publications Office website: https://data-europa-eu.ezproxy2.utwente.nl/doi/10.2777/978703 https://doi.org/10.2777/466885

European Commission, Directorate-General for Research and Innovation (2021). *How the Group of Chief Scientific Advisors works*. Luxembourg: Publications Office of the European Union. Retrieved from Publications Office website: https://data-europa-eu.ezproxy2.utwente.nl/doi/10.2777/490362 https://doi.org/10.2777/490362

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (2019).

European Research Consortium for Informatics and Mathematics (2014). *ERCIM White paper on Cyber-security and privacy research*. Retrieved from https://www.ercim.eu/images/stories/pub/white-paper-STM.pdf

Gonzáles Fuster, G., & Jasmontaite, L. (2020). Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. In M. Christen, B. Gordijn, & M. Loi (Eds.), *The Ethics of Cybersecurity* (pp. 97–115). Cham, Switzerland: Springer Nature.

Hawkins, B., & Parkhurst, J. (2016). The 'good governance' of evidence in health policy. *Evidence & Policy: A Journal of Research, Debate and Practice*, *12*(4), 575–592. https://doi.org/10.1332/174426415X14430058455412

Hix, S., & Høyland, B. (2011). *The political system of the European Union* (3rd ed.). Basingstoke: Palgrave.

Jasanoff, S. (1990). *The fifth branch: Science advisers as policymakers*. Cambridge: Harvard University Press.

Julien, H. (2008). Content Analysis. In L. M. Given (Ed.), *The Sage Encyclopedia of Qualitative Research Methods* (pp. 120–121). London: Sage.

Krumay, B., Bernroider, E. W., & Walser, R. (2018). Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework. In N. Gruschka (Ed.), *Lecture notes in computer science: Vol. 11252. Secure IT systems: 23rd Nordic conference, NordSec 2018, Oslo, Norway, November 28-30, 2018: proceedings* (pp. 369–384). Cham, Switzerland: Springer.

Marx, K. (2019). *Das Kapital. Kritik der politischen Ökonomie*. Hamburg: Felix Meiner Verlag (Original work published 1867).

Parkhurst, J. (2017). *The politics of evidence: from evidence-based policy to the good governance of evidence*. Abingdon, Oxon, UK: Routledge.

Pielke, R. A. (2007). *The honest broker: Making sense of science in policy and politics*. Cambridge: Cambridge University Press. Retrieved from https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=194300

Pupillo, L. (2018). *EU Cybersecurity and the Paradox of Progress*. Brussels. Retrieved from Centre for European Policy Studies (CEPS) website: https://www.ceps.eu/ceps-publications/eu-cybersecurity-and-paradox-progress/

Pupillo, L., Griffith, M. K., Blockmans, S., & Renda, A. (2018). *Strengthening the EU's Cyber Defence Capabilities: Report of a CEPS Task Force*. Brussels.

Rudner, R. (1953). The Scientist Qua Scientist Makes Value Judgments. *Philosophy of Science*. (20), 1–6.

Saldana, J. (2016). *The Coding Manual for Qualitative Researchers* (3rd ed.). London: Sage. Retrieved from https://www.sfu.ca/~palys/Saldana-CodingManualForQualResearch-IntroToCodes&Coding.pdf

Appendix

List of analyzed documents in alphabetical order:

1. Association for Computing Machinery (2016). *Advancing Cybersecurity Research and Education in Europe: Major Drivers of Growth in the Digital Landscape*. Cybersecurity Policy White Paper. Retrieved from http://www.acm.org.ezproxy2.utwente.nl/binaries/content/assets/public-policy/2016_euacm_cybersecurity_white_paper.pdf

2. Bendiek, A., Bossong, R., & Schulze, M. (2017). *The EU's revised cybersecurity strategy: half-hearted progress on far-reaching challenges* (SWP Comment No. 47). Berlin.

3. Carrapico, H., & Barrinha, A. (2017). The EU as a Coherent (Cyber)Security Actor? *JCMS: Journal of Common Market Studies*, *55*(6), 1254–1272. https://doi.org/10.1111/jcms.12575

4. Carrier, M. (2022). What Does Good Science-Based Advice to Politics Look Like? *Journal for General Philosophy of Science*, *53*(1), 5–21. https://doi.org/10.1007/s10838-021-09574-2

5. European Commission, Directorate General for Research and Innovation (2017). *Cybersecurity in the European digital single market*. Retrieved from Publications Office website: https://data-europa-eu.ezproxy2.utwente.nl/doi/10.2777/978703 https://doi.org/10.2777/466885

6. European Research Consortium for Informatics and Mathematics (2014). *ERCIM White paper on Cyber-security and privacy research*. Retrieved from https://www.ercim.eu/images/stories/pub/white-paper-STM.pdf

7. Gonzáles Fuster, G., & Jasmontaite, L. (2020). Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. In M. Christen, B. Gordijn, & M. Loi (Eds.), *The Ethics of Cybersecurity* (pp. 97–115). Cham, Switzerland: Springer Nature.

8. Krumay, B., Bernroider, E. W., & Walser, R. (2018). Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework. In N. Gruschka (Ed.), *Lecture notes in computer science: Vol. 11252. Secure IT systems: 23rd Nordic conference, NordSec 2018, Oslo, Norway, November 28-30, 2018: proceedings* (pp. 369–384). Cham, Switzerland: Springer.

9. Pupillo, L. (2018). *EU Cybersecurity and the Paradox of Progress*. Brussels. Retrieved from Centre for European Policy Studies (CEPS) website: https://www.ceps.eu/ceps-publications/eu-cybersecurity-and-paradox-progress/

10. Pupillo, L., Griffith, M. K., Blockmans, S., & Renda, A. (2018). *Strengthening the EU's Cyber Defence Capabilities: Report of a CEPS Task Force*. Brussels.