Evaluatie van de opbouw en meetbaarheid van de Nederlandse Cybersecurity Agenda

Evaluation of the structure and measurability of the Dutch National Cyber Security Agenda

Management summary

Management summary

Background

Security in the digital domain is a top priority for the Government, and so the Dutch Cyber Security Agenda (NCSA) was written in 2018 by various ministries in collaboration with public and private parties and the scientific community.[1] With the NCSA, the Government has set the course for its approach to cyber security in the coming years. There is therefore a great need to gain insight into the implementation and effect of the NCSA. The present study is one of the steps being taken to achieve this and concerns a plan evaluation of the policy measures. The research serves, among other things, as a preparation for a possible process and effect evaluation. The research was carried out by Dialogic, commissioned by the WODC.

In this management summary, we first discuss the objectives and research questions, then the research approach. We then go on to discuss the results of the study. The first part concerns the structure of the NCSA. Insight is given into the various aspects of the measures and their previously expected contribution to the realisation of the NCSA objective. In addition, a critical reflection on the construction of the NCSA has been carried out and described. The second part of this summary revolves around the measurability test. For each measure, we examined to what extent measuring the goal attainment is promising or not. Next, this management summary provides a critical reflection on the purpose of the NCSA. We conclude with a number of recommendations.

Objective and research questions

This research is the plan evaluation discussed in the previous section. In the first part of the research, the *policy theory* behind the policy measures is mapped out. Insight is given into the various aspects of these measures and their ex-ante expected contribution to the realisation of the NCSA's goal. In particular, it concerns the rationale, contribution, goals, policy instruments and involved organisations for each measure. The second part of the research is a *measurability test*. Per measure, we investigated to what extent measuring the goal attainment is promising or not.

The research questions of this study are as follows:

Structure NCSA

1. What were the objectives of the Dutch National Cyber Security Agenda (NCSA)?
2. What are the policy measures covered by the NCSA?
3. What can be said about each policy measure - in a concise manner - regarding:
   a) The reasoning behind (the choice for) the measure?
   b) The ex-ante expected contribution of the measure to the achievement of the strategy goals?
   c) The goals of the measure?
   d) The preconceived way in which the goals are to be achieved?
   e) The policy instruments covered by the measure?
   f) The organisations involved in the measure?

---

[1] Rijksoverheid (2018). *Dutch Cyber Security Agenda (NCSA)* [www.ncsc.nl].

Measurability NCSA

4. For which policy measures is measuring the goal attainment 'promising' or not? What aspects make it more difficult to measure the goal attainment?
5. Based on the answers to the research questions above, which policy measures are possibly suitable to be included in the possible follow-up research? For what reasons might they be suitable? And (as far as possible), why are the other measures not suitable to be included in the possible follow-up study?

Research approach

In line with the above, the research approach is divided into two aspects: an examination of the *policy theory* and the structure of the NCSA, and an examination of the *measurability* of the impact of the chosen policy measures.

Reconstruction of the policy theory

Central to this plan evaluation is the reconstruction of the policy theory. We have to find out what the set of assumptions is on which the policy is based. A good way to analyse this is to set up a goal tree.[2] Basically, this means naming the (1) resources that are used to carry out certain (2) activities. This leads to a certain (3) concrete output. This output leads - possibly in combination with other outputs - to (4) outcomes.

Within the framework of this study, the policy theory is translated into the following schematic representation, see Figure 1. The bottom line shows the reasoning behind the choice of the measure. In other words: what are the arguments for choosing this particular measure? This ties in with research question 3a. Above this we find the layer with activities that are developed for a specific measure. Typically, these are organisations (question 3f) that use policy instruments (question 3e) to achieve goals in a particular way (question 3d). Each measure has a clear intended output; a measure wants to achieve something. This is question 3c. Under each objective there are a number of measures, question 2. Next, it is mapped out which measures contribute to specific objectives, question 3b. This is where the question of effectivity comes in. On the green layer we see the objectives 1...m. This is where the term goal attainment comes in. This will be discussed under measurability. On the layer above the objectives, we see the red layer with ambitions 1. We view these as the intended outcomes of the objectives. The top layer is the overarching objective, the intended impact.

---

[2] Rijksoverheid. *Toolboxbeleidsevaluaties* [www.toolboxbeleidsevaluaties.nl]
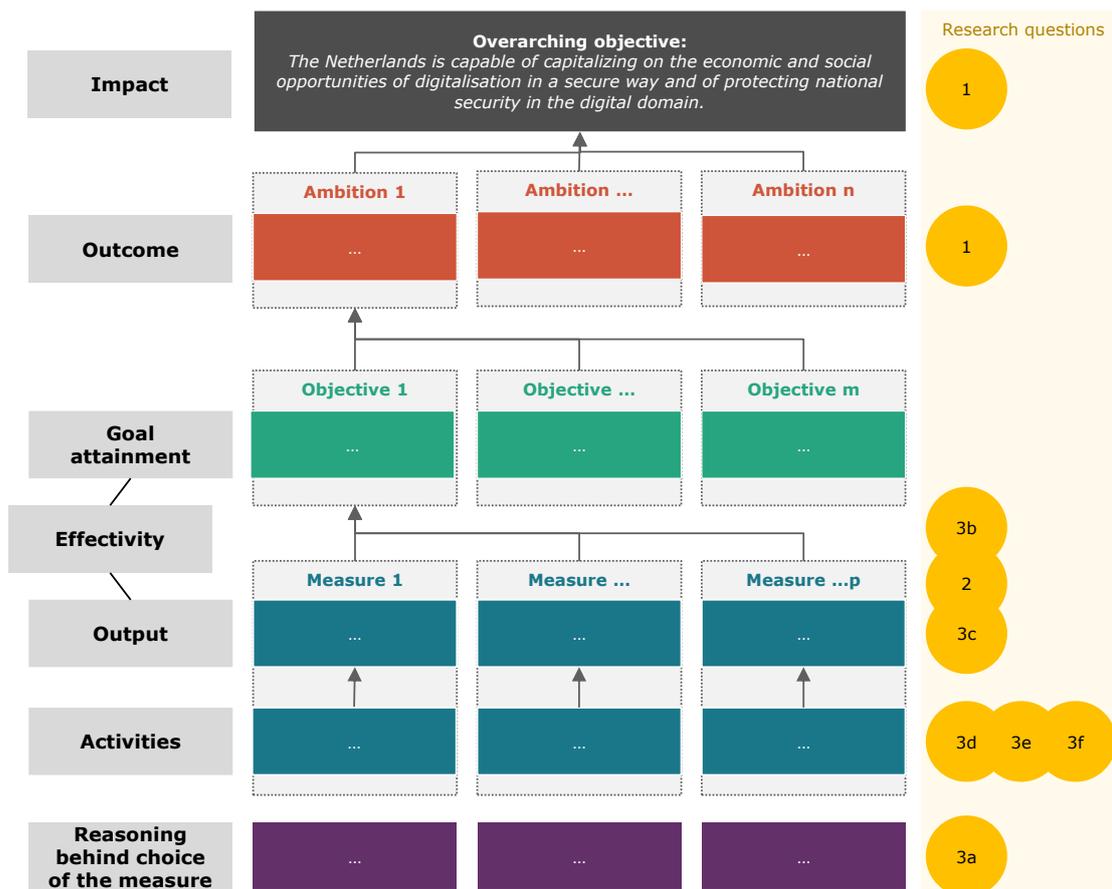
Figure 1. Schematic representation of the policy theory and the link to the research questions

A substantial part of this research revolves around reconstructing the policy theory of the NCSA as a whole, using the above methodology. This enables us to critically examine the logic of this theory. Central to this analysis are the expected causal relationships, which are indicated in Figure 1 by the black arrows. Logically, there are several aspects on which the policy theory can be lacking: [3]

   A. Measures may be mentioned that do not have an objective.
   B. Objectives may be mentioned that have no measures.
   C. Measures can be linked to an objective while *not* contributing to it.
   D. There may be targets for which the totality of measures contributes too little to the achievement of the target.

When using sources to reconstruct the policy theory, we adopt the approach that written sources are the primary source. Both the NCSA itself and parliamentary letters referring to it proved to be excellent sources. Interviews were used to properly interpret these sources and identify new literature. In many cases, the interviews helped us to read between the lines and understand how to interpret a particular passage in the text. If, based on the literature, there is ambiguity or a gap in the policy theory, we identified it. If a respondent made a logical remark about this, we did include it in the explanatory text, but we considered it as a *possible* explanation and not as a fact.

---

[3] For the sake of readability, we only use the terms objectives and measures here. We could also have chosen ambitions and objectives. Measures and instruments would also have been possible.

In addition to the critical reflection on the structure of the measures and objectives, this study also carried out a critical reflection on a higher level of abstraction. The focus was on the overall objective and the ambitions. At the level of the overarching objective, the primary question is what the NCSA's added value has been: *what has the NCSA added to the situation regarding cyber security (policy) in the Netherlands?* At the ambition level, this mainly concerns coherence and the relationship with the overarching objective. The main sources of data for this were the interviews. Literature was also used.

Assessing measurability

In assessing the measurability of the measures, we ask questions at four levels, again following Figure 1 and the aforementioned literature.

1. Is it measurable whether the <u>activities</u> have been carried out?
2. Is it measurable whether the <u>output</u> is realised?
3. Is it measurable whether the objective has been achieved? (<u>goal attainment</u>)
4. Is it measurable whether the output has led to the achievement of the objective? (<u>effectivity</u>).

The subject that is measured

Measuring is a central aspect of modern science.[4] An important criterion for being able to measure is having a **reference point**. After all, without a reference point it is not possible to determine whether and how much something has improved, deteriorated or remained the same. Next, two aspects are relevant to measurement:

- The first question is whether there is an **objective (or factual)** standard (the same for everyone) or a **subjective** standard (differs between individuals).
- Secondly, there is the question of whether **one dimension** or **several dimensions** are being measured.[5]

Measuring in practice

In addition to the above theoretical consideration of measurability, there is a third, much more practical aspect of measurability: is it actually feasible in practice to obtain the data that we can test against the reference point? This issue revolves, among other things, around the side effects of measuring. Below, we present three practical limitations, but we do not exclude the possibility that there are more aspects.

- **Costs**: Can you measure cost-effectively? Are the costs of measuring in proportion to the objective?
- **Values**: Doesn't measuring come at the expense of other values? An example is the privacy of citizens.
- **Realistic**: Is there an instrument available that can carry out the measurement properly?

In the context of this study, we take the above aspects together under the heading of *practical feasibility*.

---

[4] Stanford Encyclopedia of Philosophy, (2020). *Measurement in Science* [plato.stanford.edu].

[5] Lumen Learning (2021). *Chapter 6 Measurement of Constructs* [courses.lumenlearning.com].

Data and information collection

To reconstruct the policy theory and to test the measurability, different methods were used to collect data and information. We started with **document research** and **in-depth interviews** to describe the policy theory and to examine the measurability of the measures. In the last phase of the research, an integral analysis was used to bring together all the information gathered and to answer the research questions. These insights were tested in a **validation session** with stakeholders.

Results - Structure of the NCSA

Research question 1. What were the goals of the NCSA?

The NCSA has a clear layered character, as can be seen in Figure 1. There is a clear overarching objective, under which there are seven ambitions that are shown in Figure 2. Under the ambitions there are 24 objectives. In chapter 2, these are all named.
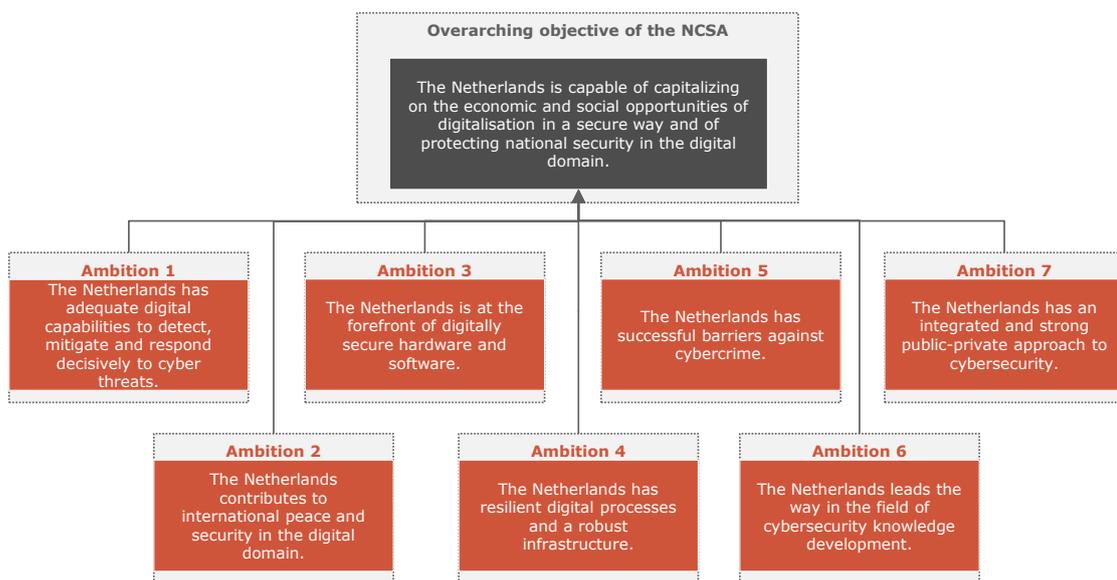

Figure 2. The overarching goal of the NCSA and the seven ambitions

Research question 2. Which policies are covered by the NCSA?

In total, 42 measures are covered by the NCSA. An overview of these can be found in the answers to the measurability questions, research questions 4 & 5.

Research question 3. What can be said for each policy measure - in a concise manner - about: (a) the reasoning, (b) the ex-ante expected contribution to the realisation of the strategy goals (c) the goals (d) the preconceived way in which the goals are to be realised (e) the policy instruments covered and (f) the organisations involved?

The above questions are in line with the vision of a plan evaluation of the NCSA presented in Innovalor's report *Verkenning brede evaluatie NCSA*.[6] It is impossible to present this concisely. It concerns 252 (42 measures and 6 aspects) answers which are mostly qualitative

---

[6] Innovalor (2020). *Verkenning brede evaluatie NCSA* [repository.wodc.nl].

and have nuances. Chapters 3 to 9 of this report systematically answer these questions for all 42 measures. Below, however, we present the red line of the critical reflection on the structure of the NCSA, of which these questions are a part. We do this at the level of the agenda as a whole and at the level of the various ambitions.

Critical reflection on the structure of the NCSA

In addition to the very specific answers to the first three research questions, an analysis was carried out in which the structure of the NCSA was critically evaluated. Here, it is possible to draw conclusions at a higher level of abstraction. Based on this, we come to five conclusions, which we will elaborate on below.

1. From a broad perspective, the NCSA has a logical structure.

There is a clear overarching objective, which is broken down into several ambitions, which are further broken down into objectives and measures, which have activities and a rationale. In our perspective, the right number of levels has been chosen. If one layer were to be removed (for example, objectives or ambitions), the chain of activities to impact would become unclear. Adding one layer adds little and mainly creates complexity. On the basis of the documentation, this pyramid can be reconstructed easily. However, the link between measures and objectives was not made explicit in the NCSA. If this had been done, 'floating' measures and objectives could probably have been avoided: in some cases, a measure does not seem to contribute to the objectives in the ambition, or there is an objective to which no measure in the ambition seems to contribute. In addition, in a few cases we came across illogical relationships or measures, but this is relatively small-scale and has a limited impact on the overall structure.

2. The ambitions are well aligned with the overarching goal, but are neither similar nor mutually exclusive.

Ambitions 1 and 7 can be seen as preconditions for the rest of the approach. Ambitions 2 to 6 have been given shape within it and have more specific policy effects. We could see the ambitions as a method to give each department its own ambition. This picture also emerges from the interviews with policymakers. The extent to which each ambition is linked to a single department does, however, differ. It is also clear that there is overlap between ambitions. A good example is ambitions 3 (secure hardware and software), 4 (resilient processes and robust infrastructure) and 5 (barriers against cybercrime). The overlap and relationships between the ambitions are evident. From a methodological perspective, we would have preferred a structure of ambitions that is MECE[7]. Perhaps the complex reality of cyber security (policy) does not make this entirely feasible, but it could be strived for.

3. Overall the structure of the ambitions is logical, but there are substantial differences between the ambitions

The differences lie mainly in (1) the number of measures per ambition and (2) the degree to which the structure is logical. We will discuss this for each ambition below.

Ambition 1 has a logical structure of measures and objectives that should bring the digital strength of the Netherlands up to standard. These include, for example, the detection of attacks and the response to them, as well as the effective sharing of information. We see

---

[7] 'MECE' stands for Mutually Exclusive and Collectively Exhaustive. With this grouping principle, a group (in this case, the overarching goal) is divided into subgroups (in this case, ambitions) that do not overlap and together cover the entire group (overarching goal). (Minto, B. *The Pyramid Principle Logic in Writing and Thinking*, 2008: Pearson Education Limited.)

that some aspects and measures are separated on paper while in practice the processes are strongly interwoven. Aside from that, we identify hardly any weaknesses in the policy theory behind this ambition.

Ambition 2 relates to international peace and security in the digital domain. This is to be achieved through international cooperation and the strengthening of our own and others' cyber capacity. Although there are measures among them that are very extensive and open to multiple interpretations, every measure has a structure and rationale. Both the ambition itself and most of the objectives and some measures are formulated in terms of 'contributing to' or 'promoting'. This is easily explained in this case, as there is an international playing field in which the Netherlands is not in control of everything. An important point of criticism is that within and between departments there is not always agreement on (the interpretation of) some objectives.[8] This applies in particular to capacity building in the global cyber security chain and the pursuit of an open, free and secure internet. Interdepartmental agreement on objectives is pre-eminently something that the NCSA should contribute to, so this is an opportunity that unfortunately has not been taken.

Ambition 3 revolves around the promotion of safe hardware and software. The structure of the policy theory of the ambition is in itself logical. Everywhere, it is clear why measures are being taken and the relationship between measures and objectives is, with a few exceptions, clear. There are, however, a lot of weak relationships, because many measures go no further than doing research or holding discussions. We realise, of course, that these are often useful and even necessary steps, but the gap to the objectives and to the ambition itself remains very large. The measures within this ambition also often remain somewhat non-committal, think of gaining knowledge, but also of identifying possible next steps or 'proposing' to include an obligation.

In ambition 4, resilient digital processes and a robust infrastructure are the key points. Because ICT is becoming increasingly interwoven in Dutch society, companies and governments are becoming more data-driven through smart applications. This takes place in chains and they depend on other organisations for data or execution. If data exchange with other organisations is not safe and reliable, the business process can be disrupted. If this happens in chains of vital providers, it leads to far-reaching failures, damage to physical safety and social disruption. The structure of the policy theory that falls under ambition 4 is, on the whole, logical. There is a structure in which logical objectives are formulated on the basis of an ambition. This in turn leads to logical measures that respond to specific challenges. Our main point of criticism is that, similar to ambition 3, there are relatively many weak relationships across the board and we question the extent to which they contribute to the corresponding objectives. It is explicitly not a question of illogical connections, but in many cases we estimate that the actual effects will be relatively small. There is a large gap between "*research into supplementary measures*", "*examine how support can be provided*", "*explore with private parties*", "*put on agenda in Europe*" on the one hand and "*prevent far-reaching failure, damage to physical safety and social disruption*" on the other.

Ambition 5 revolves around successful barriers against cybercrime. It works in three ways: strengthening investigative capabilities, increasing digital skills and stimulating safe hardware and software. What is immediately striking is that this ambition, like ambition 6, has only three measures. This is considerably less than the other ambitions. Two of the three measures focus on subjects that are already covered in ambitions 3 and 6. This is easy to

---

[8] This is based mostly on the evaluation of the international cyber security policy conducted by the Directorate of International Research and Policy Evaluation (IOB) of the Ministry of Foreign Affairs. The evaluation will probably be published shortly after this research, see [iob-evaluatie.nl].

explain, as there is a great deal of overlap between erecting barriers against cybercrime and, for example, wanting to lead the way in promoting secure hardware and software. In addition, this ambition was added to the NCSA at a late stage in the creation process. The relationship between the ambitions remains somewhat unclear, however, because the overlap between the ambitions is only addressed by including the phrase "see also the objectives and measures for ambition..." in the measures. The integral approach to cybercrime is also important for this ambition, which was sent to the House at the same time as the NCSA and to which reference is made in a separate box in the NCSA. [9]The integral approach consists of four tracks that partly overlap with the NCSA: 1. investments are made in prevention (measures 5.2 and 5.3); 2. detection is reinforced, criminal activities are disrupted and offenders are tackled (measure 5.1); 3. victim support is geared to cybercrime; 4. scientific knowledge of cybercrime is increased. The integrated approach indirectly works on the measures of ambition 5 and makes it clear that more is happening in this area than the limited number of measures would suggest.

In ambition 6, knowledge development is the central issue. This relates to knowledge development at various levels. From fundamental and applied (scientific) cyber security research to the development of (basic) knowledge by citizens and companies. High-quality cyber security knowledge development in the broadest sense of the word must be maintained and deepened. The policy theory under ambition 6 is somewhat fragmented. It is clear that the measures and objectives focused on cyber security research have been worked out in detail and serve as the core of this ambition. The logic is correct, the activities are concrete, the substantiation is solid and the link with the objectives to which the measure relates is clear. This also has an effect on the measurability of the measure. A well-developed theory also makes it easier to measure the results. The objective concerning the resilience of citizens and companies, achieved by focusing on the subject at school and through awareness campaigns, is further removed from the core of the ambition (wanting to be a leader in cyber security knowledge development). This creates the illusion that the measures have little coherence and are mainly compiled because they are about knowledge of cyber security in the broadest sense of the word. The policy theory behind the measures on curriculum revision in primary and secondary education and on the development of digital skills of citizens and employees has therefore been minimally elaborated in the NCSA. As a result, the measurability is also a lot less.

Ambition 7 can be seen as a precondition for the rest of the approach drawn up in the NCSA. We work integrally in public-private form on the goals of the NCSA. By formulating a separate ambition, the work form has become subject and goal in itself. In that sense, ambition 7 is somewhat strange and this is reflected in the policy theory. Relationships are not always strong or logical, parts are missing in the logic and the level of measures (seen from the policy theory) is different. The first two objectives (government's role as manager and all parties fulfilling their responsibilities), for example, have been formulated broadly, so that they serve as a kind of umbrella for the first four measures. As a result, goal attainment and effectivity can hardly be measured for these measures. The last measure and objective (on information security in digital government) deal with a different subject, are formulated much more specifically and are more measurable.

4. The impact-outcome-objective-output -activity chain often has a weak link.
For the overarching goal to be realised, it is important that there is a solid chain. See Figure 1 for a representation of this chain. However, relatively often we see that somewhere in this chain there is a relationship that is far too weak. Sometimes the measure contributes only

---

[9] Tweede Kamer (2019). *26643-614* [zoek.officielebekendmakingen.nl]

to a very limited extent to the goal, and sometimes the activities are not formulated as the actual action, but as a derivative of it (review, explore, put on agenda). This can lead to a situation where all the measures are successfully implemented, but the objectives are not achieved. It seems that there is a schism between the (1) overarching objective, ambitions and objectives on the one hand and (2) the output and activities on the other. The first set has a clear coherence and a focus on the longer term. The measures are much more loosely connected and in some cases can be realised quickly. We could say that the first part mainly has characteristics of a strategy and the second part resembles an agenda.

We could also see the gap as the gap between what our ambitions as a society are and what resources we want to make available. If we want to eliminate this gap, we will have to lower our ambitions, raise our resources, or both. Just before completing this report, the Cyber Security Council published its advisory report *'Integrale aanpak cyberweerbaarheid'.*[10] They make it clear that in order to achieve improved cyber resilience in Dutch society, the coming cabinet period will require more than €800 million in additional resources. In other words: the resources must be increased if we want to realise these ambitions.

5. There are several omissions at the level of measures.

To reach a certain objective, a measure is proposed and it should be clear *why* this measure is chosen. If this is not done, the logic of why this measure fits the objective is missing. A logical step in the reasoning is missing. It should also be clearly stated which activities will be undertaken. If this is missing, the measure is not concrete enough. So the questions "*how?*" and "*why?*" are not always answered when it comes to measures.

Results - Measurability of the NCSA

The next two research questions concern the measurability of the NCSA:

Research question 4. For which policy measures is measuring the goal attainment 'promising' or not? What aspects make it more difficult to measure the goal attainment?

Research question 5. Based on the answers to the research questions above, which policy measures are possibly suitable to be included in the possible follow-up research? For what reasons might they be suitable? And (as far as possible), why are the other measures not suitable to be included in the possible follow-up study?

In view of the interrelated nature of the questions, they shall be answered jointly.

Analysis of the extent to which measuring is promising

In chapters 3 to 9, an analysis has been made per measure of the extent to which the activities, output, target range and effectiveness are measurable. The following table gives an overview.

---

[10] Cybersecurityraad (2021). *Intergrale aanpak Cyberweerbaarheid. Een integrale aanpak om de open, vrije en welvarende Nederlandse samenleving structureel cyberweerbaar te maken en (digitale) kansen te verzilveren.* [www.cybersecurityraad.nl]

Table 1. Overview of measurability per level per measure

Measure	Activities	Output	Goal attainment	Effectivity
1.1: Strengthening the response capacity of public and private parties	Fairly good	Moderate	Bad	Bad
1.2: Vital organisations ensure their own adequate response capacity or make arrangements for this with a trusted third party (certification system)	Fairly good	Good	Bad	Bad
1.3: Updating of the National ICT Crisis Plan and drafting of an integrated ICT crisis exercise policy	Good	Bad	Bad	Bad
1.4: Structurally strengthening the understanding, detection and disruption of threats and digital attacks	Good	Fairly good	Bad	Bad
1.5: The national situational picture is strengthened	Good	Fairly good	Bad	Bad
1.6: The nationwide system of cyber security partnerships is taking shape	Good	Fairly good	Fairly good	Fairly good
1.7: Establishment and further development of cybersecurity partnerships for governments, the business community and civil society organisations	Fairly good	Good	Fairly good	Moderate
1.8: Knowledge of laws aimed at protecting national security	Fairly good	Good	Fairly good	Fairly good
2.1: Uphold and promote international law and work to enlarge the international coalition	Moderate	Moderate	Moderate	Bad
2.2: Develop a broad strategic framework and a set of tools for responding to cyber attacks and for diplomatic response respectively.	Good	Good	Bad	Bad
2.3: Developing offensive cyber capabilities in the armed forces	Good	Bad	Bad	Bad
2.4: Making a strong contribution to a free, open and secure internet and to promoting the protection of human rights online	Fairly good	Fairly good	Moderate	Bad
2.5: Strengthening the global cyber security chain	Moderate	Moderate	Good	Good
3.1. Standards and certification make an important contribution to the digital security of H&S	N/A	N/A	N/A	N/A
3.2 Establishment of the CSA and (mandatory) European certifications	Fairly good	Fairly good	Fairly good	Moderate
3.3: Wider adoption of international standards, partnerships and frameworks	Fairly good	Good	Fairly good	Bad
3.4. A monitor with information on the digital safety of digital products	Good	Good	Moderate	Moderate
3.5. Internet providers will contribute to the fight against unsafe IoT devices & cross-sector test platform	Good	Fairly good	Good	Fairly good
3.6. Research aimed at developing and commercialising innovative solutions for safe H&S	Good	Good	N/A	N/A
3.7: Obligation for security updates included and possible next steps	Good	Good	Fairly good	Moderate
3.8: Minimum requirements for devices via the RED	Good	Good	Fairly good	Moderate
3.9: Knowledge of necessary and desirable additional measures in procurement within the State	Good	Good	Fairly good	Moderate
3.10: Deployment of regulators	Good	Fairly good	Fairly good	Fairly good
3.11: Consumers and SMEs are aware of the digital security risks of IoT devices, and of their options for action	Good	Moderate	Fairly good	Moderate
4.1: Substantially increase the number of vital providers that are subject to care and reporting obligations	Good	Good	Fairly good	Fairly good
4.2: Methodology for identifying dependencies of vital providers	Good	Good	Fairly good	Bad
4.3: Limiting the impact of disruption to the services of foreign providers	Good	Good	Fairly good	Bad
4.4: Support communities that develop and maintain free software	Fairly good	Fairly good	Fairly good	Moderate

Measure	Activi-ties	Output	Goal attain-ment	Effec-tivity
4.5: Suppliers apply modern internet protocols and standards	Good	Good	Fairly good	Bad
4.6: Cybersecurity requirements in procurement	N/A	Fairly good	Moder-ate	Moder-ate
4.7: Awareness of the parties from whom secure services can be obtained	Good	Fairly good	Fairly good	Fairly good
5.1 Strengthening police and judicial investigation of digital attacks	Fairly good	Good	Bad	Bad
5.2 Develop proposals to make citizens and businesses more digitally literate.	Good	Bad	Good	Good
5.3 Use of secure hardware and software is encouraged to prevent cybercrime	Fairly good	Bad	Bad	Bad
6.1: Structural investment in fundamental and applied cyber security research	Good	Good	Fairly good	Moder-ate
6.2: Digital skills as points of attention in the integral curriculum review in primary education and secondary education	Good	Fairly good	Moder-ate	Bad
6.3: Encouraging business and civil society organisations to further develop the digital skills of citizens and employees	Fairly good	Bad	Moder-ate	Bad
7.1 The NCTV is responsible for managing the integrated approach	N/A	Good	Moder-ate	Bad
7.2 Cybersecurity alliance connecting public and private parties	Good	Fair Good	Bad	Moder-ate
7.3 Progress of the cyber security approach will be monitored, recalibrated where necessary and evaluated.	N/A	Good	Moder-ate	Moder-ate
7.4 Establishment of a nationwide system of cyber security cooperative arrangements	Moder-ate	Good	Bad	Bad
7.5 Coherent package of measures for information security and cybersecurity in public administration	N/A	Good	Good	Moder-ate

Aspects that negatively affect measurability

During the research, we came across several aspects that negatively influence the measurability of measures. We will discuss these in more detail below.

1. Absence of a deadline

The SMART principle is often used to formulate objectives in a good way. Goals must be Specific, Measurable, Achievable, Realistic and Time-bound.[11] Within the NCSA, with a few exceptions, no measures are time-bound. This means that it becomes almost impossible to determine that a goal has not been achieved. If it was not achieved today, it could be achieved tomorrow.[12] Innovalor's research also shows that the fact that objectives and measures are not formulated in a SMART way creates an additional challenge with regard to measurability.[13]

2. Lack of clear standards

Having a standard is a central aspect of measurement. Only then can the question be answered whether the standard is being met. However, we see that many measures have a

---

[11] Doran, G.T. (1981). *There's a S.M.A.R.T. way to write management's goals and objectives.* Management Review. 70 (11): 35–36.

[12] Although it is somewhat outside the realm of measurability, we also note that the aspect of *specificity* is too limited. It should be clear which party is responsible for taking the action. However, this is lacking in the vast majority of measures.

[13] Innovalor (2020). *Verkenning brede evaluatie NCSA* [repository.wodc.nl]

subjective and multifaceted character. As a result, it cannot actually be determined whether a measure has been successfully implemented or not. We acknowledge that the nature of the issue does not allow for clear standards in all cases. However, even for those measures where it is possible to use concrete standards, this is rarely done.

3. Practical feasibility

In addition to the above theoretical consideration of measurability, there is a third, much more practical aspect of measurability: is it actually feasible in practice to obtain the data that we can test against the reference point? In determining the measurability of the NCSA measures, we have explicitly included this aspect. There are often major methodological challenges in demonstrating causal relationships in a policy context.[14] Often there is a complex context with many interacting relationships and it is difficult to isolate one dimension. For example, we have encountered several variations of the problem that it is impossible to measure how many attacks go undetected.

4. Embedding in the NCSA structure

In the above table, the score "*n/a"* has been included in some places. We do this if the measure is not included in the structure of the NCSA in a valuable way. For example, measure 3.1 is not a measure, but rather an observation.

Measures for follow-up research

Across the board, we see that activities are often relatively easy to measure. It often concerns concrete actions that need to be undertaken. When measuring the output of a measure, we see considerable differences between measures, but here too, there is often a relatively high degree of measurability. The measurability there is mainly reduced because it is practically difficult (expensive, time-consuming) to measure. Nevertheless, for all ambitions it is possible to carry out a process evaluation. In some cases, however, certain aspects are difficult to measure.

If we look at the goal attainment, we see considerable differences between the different measures and ambitions. The measures under ambitions 3 and 4 score well, while the other ambitions always have several measures that are difficult to measure. Because objectives are often formulated in a more abstract way than measures, their measurability is often more complex. In many cases, there is simply no standard to measure. The measurability of the goal attainment strongly depends on the interpretation or operationalisation of soft formulations such as 'The Netherlands will work on'. The fact that measures are taken may be sufficient for the conclusion that such an objective has been achieved, regardless of the content or effect of the measures, or the effort put into them. This reasoning, however, would lead to the conclusion that almost any objective is achieved automatically, regardless of whether anything is actually achieved. The measurability of effectivity is the lowest. This requires not only good measurability of output and goal attainment, but also of the alleged causal relationship between these two concepts. The latter is often severely limited by the complex environment with many interacting effects. In addition, a *counterfactual*[15] is also lacking in many cases. Only a part of the measures can be investigated with an effect evaluation. The measures under ambition 3 and 4 lend themselves best to further research by means of an effect evaluation, but here too, the effect cannot be properly investigated for

---

[14] A good overview of methods can be found at [toolbox-policy-evaluations.com].

[15] A counterfactual is the situation in which the measure was/was not taken. By comparing this with the situation with the measure, a statement can be made about the effect of the measure.

many measures. Ambition 7 faces major challenges in terms of measurability, making an effect evaluation impossible. From ambition 6, only the first measure seems to be good to investigate with an effect evaluation.

The measurability of the NCSA in a broader perspective

In the previous sections, the measurability of the NCSA was related to the measures and related objectives. As this is one of the central questions of this research, it is the primary focus. However, we could also look at the measurability of the NCSA from a broader perspective. How measurable is the overarching objective ("*The Netherlands is capable of capitalizing on the economic and social opportunities of digitalisation in a secure way and of protecting national security in the digital domain.*")? And how measurable are the seven ambitions?

1. The Netherlands has <u>adequate</u> digital capabilities to detect, mitigate and respond decisively to cyber threats.
2. The Netherlands <u>contributes </u>to international peace and security in the digital domain.
3. The Netherlands i<u>s at the forefront of</u> digitally secure hardware and software<u>.</u>
4. The Netherlands has <u>resilient </u>digital processes and a <u>robust </u>infrastructure
5. The Netherlands has <u>successful</u> barriers against cybercrime.
6. The Netherlands <u>leads the way</u> in the field of cyber security knowledge development
7. The Netherlands has an <u>integrated and strong, public-private approach </u>to cyber security.

The seven ambitions above each have a number of words underlined. These are criteria that need to be assessed in order to determine whether the ambition has been achieved. For the first ambition, the key question is therefore: *when does the Netherlands have adequate digital capabilities?*[16] For all ambitions except the second, it is evident that there is a subjective norm that also encompasses various dimensions.[17] Because all these ambitions involve broad concepts (digital capabilities, international peace and security, etc.), this raises the question of attribution. It is difficult to determine to what extent the NCSA has contributed to the goals. It is therefore difficult to determine whether the ambitions have been achieved and what the role of NCSA was in this.

For the overarching objective, roughly the same applies. In which cases is it *secure*? When are *opportunities capitalised on*? What exactly do we mean by *national security*? We endorse the conclusion drawn by Innovalor on this subject: *"Central [...] is the concept of 'digital resilience'. This is a complex concept that cannot be captured in an unequivocal definition and changes over time, partly because threats and therefore also the approach to them are constantly changing. Due to the lack of a further operationalisation of the concept of digital resilience in the NCSA, it is not only difficult to determine its measurability but also its completeness.*[18]

---

[16] In line with Karl Popper's ideas on falsifiability, it might be better to formulate this question in negative terms as: *in what exact cases does the Netherlands clearly <u>not have</u> adequate digital capabilities*? (Popper, K.R. (1968). *The logic of scientific discovery,* New York: Harper & Row).

[17] If we look at ambition 2 word for word, there is an objective standard. If the Netherlands has contributed even minimally to the target, then the ambition has been achieved. If we interpret this ambition as the *Netherlands contributes <u>sufficiently</u> to…* then we are dealing with a subjective, multiple standard.

[18] Innovalor (2020). *Verkenning brede evaluatie NCSA* [repository.wodc.nl]

Reflection on the purpose of the NCSA

The above paragraphs have answered the research questions. However, this research has identified two realities when it comes to the purpose of the NCSA. The first perspective revolves around policy theory and forms the core of this report. Here, we use the classical, rational-analytical perspective of a policy theory with objectives, effects, effectivity, etc. The NCSA aims to achieve the following goal through a variety of measures: *The Netherlands is able to securely cash in on the economic and social opportunities of digitisation and to protect national security in the digital domain*. In this paradigm, we reason strongly bottom-up. Another perspective that we can adopt is much more top-down and revolves around the added value of the NCSA as a whole. In other words: *What has the NCSA added to the situation with regard to cybersecurity (policy) in the Netherlands?* Or vice versa: What would the Netherlands have looked like if we had not had an NCSA? This is also a question that we discussed with various interviewees and in the validation sessions. Three central aspects emerged from this that we will explain in more detail below.

However, before we go into that, we would like to point out that we should always be careful about reformulating the goals of policies after the fact. The overarching objective is and remains the goal of the NCSA. The aspects mentioned below are (perhaps intended) side effects, but can never be the focus of a policy evaluation. Nevertheless, it can be valuable to explore this perspective as well.

Mutual coordination

From the interviews and validation sessions, it is clear that the main added value of the NCSA lies in coordination within the public sector. The whole process of drawing up the NCSA has led to a greater understanding among the parties involved of what issues are important to other parties. Had the NCSA not been in place, departments would probably have coordinated their policies less well, resulting in gaps, (more) duplication or even contradiction of policy. The NCSA has (to some extent) contributed to a clearer delineation of which departments are responsible for which activities and how various other agendas (on sub-topics, sectors or threats) relate to each other. This is not to say that coordination is now sufficient, but many parties do indicate that there has been an improvement. However, a small number of interviewees also indicate that the NCSA is too 'compartmentalised' to lead to major improvements in this respect. The directory for International Research and Policy Evaluation of the Ministry of Foreign Affairs also indicates that it was mostly this last signal that was received during the evaluation of the international cyber security policy.

Here, a perspective is used whereby the goal of the NCSA is to improve cyber security *policy* in the Netherlands. This is much narrower than the purpose of the NCSA, which is to improve cyber security in the Netherlands in general. The NCSA also refers to this to a certain extent: *"The joint direction is laid out and various measures are considered collectively. This enhances the impact of public and private actions."* For many respondents, however, this aspect plays a fairly prominent role. In line with the above, we could also see the NCSA as an outcome of the Dutch 'polder model'. All stakeholders deliberate until a consensus document is produced. From this perspective, it is easy to explain why ambitions are quite similar to the policy areas of specific departments. It also explains why this NCSA is so broad. The strength of this model is that interests are well balanced and all parties are included. A disadvantage of this is that there is a risk of making limited explicit and pronounced choices for a certain direction. In several interviews and also in the validation session with experts in the field, this came up as a weakness: because so many parties were able to contribute what they themselves considered important, the agenda is very broad, and because hardly

any priorities are indicated within the agenda, the reader is quickly left with the question of what we as a country really consider important and what we are really going to focus on.

Common reference point

Various interviewees who reason from the perspective of cyber security policy in the broad sense, both policy officers and interviewees from other backgrounds, indicate that the NCSA has ensured that a common reference point in relation to cyber security (policy) has been created. This also emerged strongly in the validation sessions. The document is seen as a *conversation starter* and an *agenda-setting document.*

Because cybersecurity is a highly dynamic domain, it is complex to create a single agenda that also has a good shelf life. The NCSA also indicates this: *"Of course, this agenda is not set in stone. Over the coming years, it will be important to keep a finger on the pulse to closely follow technological and social developments to see where new digital vulnerabilities and threats may occur".* The fact that the NCSA nevertheless sets down concrete ambitions, objectives and measures on paper means that there is a point of reference that can be discussed. Aspects of the NCSA have become a standard and it can be discussed per aspect whether more, less or a different policy should be pursued. From the parliamentary letters discussing the progress of the NCSA,[19] it is clear that certain objectives receive much more attention over time, while others become relatively less relevant.[20] With the knowledge of today, we can state that the NCSA at the time paid relatively too little attention to certain aspects (and too much to others), but this can only be *because* a certain standard was issued at the time.

Additionality

A relevant question is, of course, to *what extent measures would have been implemented anyway without an NCSA*. There is broad consensus that a significant proportion of the measures would also have been implemented without an NCSA. Many of the measures identified in the NCSA were already part of ongoing processes. In this case, the NCSA is old wine in new bottles. On the other hand, it is also indicated that the NCSA may have given these measures a different form, implementation and available resources.

Recommendations

Based on the above, we come to the following recommendations.

1. In order to further evaluate the NCSA, it is possible to do a *process evaluation* of all ambitions. This analysis can provide valuable input for the design of possible future agendas. Mutual coordination within the public sector on this topic should play a prominent role in this evaluation.

---

[19] Ministerie van Economische Zaken en Klimaat (2020). *Voortgang Roadmap Digitaal Veilige Hard- en Software* [www.rijksoverheid.nl]; Ministerie van Economische Zaken en Klimaat, (2020). *Resultaten verkenningen en vervolgaanpak cybersecurity kennisontwikkeling en innovatie.*

[20] For example, the national system of cyber security partnerships has been developed further over the years, while the measures formulated (1.6 and 1.7) did not go very far, see section 3.7 of the main report. An example of a measure that was ultimately not implemented is the intersectoral test platform of measure 3.5, see section 5.6 of the main report.

2. It is possible to carry out a high-quality *effect evaluation* for only a part of the measures. Nevertheless, we expect that these evaluations can offer many insights into the effectivity of this policy in the broad sense. Side effects should also be taken into account.

3. When drawing up *future cybersecurity agendas,* it is advisable, from the perspective of evaluability, to elaborate on a number of aspects:

- Be more explicit about underlying goals or intended side effects of the agenda.
- There should be much more focus on the measurability of the agenda. This applies to all levels: from the overarching objective to the measures. More specifically, standards should be established around the reformulated ambitions of the agenda.
- Make the link between measures and objectives clearer.
- Prevent illogical constructions in policy theory.