CSR Cyber Security Raad

Visiting address
Turfmarkt 147
2511 DP The Hague

Postal address
PO Box 20011
2500 EA The Hague

I www.cybersecurityraad.nl
T +31 (0)70 751 5333 (secretariat)
E info@cybersecurityraad.nl

Research and Documentation Centre (WODC)
Attn Prof. G.J.L.M. Lensvelt-Mulders
PO Box 20301
2500 EH The Hague

Date
12 March 2021

Subject
CSR recommendation concerning focus of and approach to the evaluation of the NCSA

Dear Ms Lensvelt-Mulders,

Enclosed you will find a recommendation from the Cyber Security Council (hereinafter referred to as the CSR) regarding the focus of and approach to the evaluation of the National Cyber Security Agenda (NCSA). This recommendation is in response to the request from the Minister of Justice and Security that the CSR received on 4 March 2020, asking the CSR to issue a recommendation regarding a broad evaluation of the effectiveness of the approach set out in the NCSA as well as the necessary investments in cybersecurity in this context, to be made during the term of the new government. At the request of the Minister of Justice and Security and others, the CSR has agreed to issue a recommendation with regard to the focus of and approach to this evaluation. The CSR has been informed that your organisation will carry out or commission this evaluation at the behest of the National Coordinator for Security and Counterterrorism and is therefore addressing this recommendation to you.

Rationale

Together with a wide range of public, semi-public and private organisations, the Dutch government established the NCSA in 2018. Annual reports on progress made in the implementation of the agenda are submitted to the House of Representatives. It is important that these reports identify the effects of the NCSA as well. The House was informed that the NCSA would undergo broad evaluation in 2021,[1] principally in order to establish whether, and to what extent, the agenda contributes to digital resilience in and of the Netherlands.

It is not easy to ascertain the state of digital resilience of and in the Netherlands, nor the manner in which (and/or to what extent) the NCSA has contributed to this state. There are a number of reasons for this. First of all, the impact of security interventions is always difficult to quantify because the goal of such interventions is to prevent incidents from occurring. Quantifying incidents that have not taken place is rather tricky. Secondly, even if it were possible to quantify such incidents, the question arises as to whether the incidents did not occur because interventions prevented them, because of other causes or simply as a matter of chance. Thirdly, finding a proper metric (benchmark) and measuring instrument for quantifying digital resilience is a complex undertaking. By what metric should an increase in digital resilience be measured? In addition, the NCSA distinguishes three target groups: citizens, businesses and private sectors of vital importance. This leads to questions regarding the differences and comparability of the measurements and measuring instruments used by different groups (and gives rise to the question of why the government has not explicitly been included as a separate target group here – more on this below). All things considered, it must be concluded that achieving absolute quantification in this evaluation is not a reasonable aim.

[1] https://www.tweedekamer.nl/downloads/document?id=473adfeb-4a4d-4120-841b-8b263c29fb21&title=Nederlandse%20Cybersecurity%20Agenda%20%28NCSA%29.pdf

One last issue is that no baseline was established with regard to digital resilience before the agenda was implemented. This makes it challenging to compare the situation surrounding digital resilience in the Netherlands in 2021 with the situation as it was in 2018. So long as we cannot establish the starting position from which measures were initiated, there is no point in measuring the results. In fact, such uncertainty renders it impossible to **monitor a shift in the facts** (initiatives, implementation of recommendations). Whereas quantification with regard to an increase in digital resilience is difficult (for the reasons outlined above), it should however be possible to monitor such shifts, assuming we have an overview of the 'lay of the land' at a specific point in time. To that end, in the focus document corresponding to this recommended method, you will note that **the CSR's recommends that the evaluation be used in two ways:**

1. Through reporting on the current **state of affairs** in connection with the measures identified in the NCSA, linked to the seven themes, it will be **evaluated** which matters set out in the agenda have received sufficient attention, as well as which matters may have been insufficiently addressed.
2. At the same time, through reporting on the state of affairs in 2021, it is still possible to establish a **baseline**, which can – in a number of years' time – be used as a qualitative benchmark to determine which shifts have taken place.

In this light, the CSR advises you not to commission a quantitative measurement but rather to choose a different approach, one that is based on extensive, in-depth consultation with experts in accordance with the **Nominal Group technique.** This will make it possible to gather a large volume of relevant, in-depth *and* factual information in a short period of time. Moreover, the recommended technique can provide the **traceability** (over time) that is so vitally necessary, by ensuring a data set that enables us to perceive the shifts taking place over the coming years. In this document, the CSR will issue a recommendation concerning the **evaluation method** to be applied.

The CSR wishes to emphasise that this is a recommendation only. Your organisation is free to adopt a different methodology. In light of our independent position, the CSR will also withdraw from the evaluation of the NCSA (and corresponding process) after offering this advice. When the results of the evaluation are made public, the CSR will take note of these results and issue a recommendation to the House of Representatives.

Recommendation on how to approach the evaluation

The concept of digital resilience is expansive and difficult to quantify. Digital resilience is subject to countless definitions and interpretations. As a result, any evaluation of the concept must necessarily begin by defining and demarcating its scope. The NCSA focuses on three distinct target groups: citizens, businesses and private sectors of vital importance. The CSR notes that the **government** is not explicitly listed as a target group in the agenda and recommends including the government in this evaluation as a separate target group in order to demonstrate when, and in what manner, the implemented measures are applicable to the government as well. The notion of digital resilience should therefore be operationalised for these four target groups. In addition, the evaluation should show whether the NCSA has contributed to greater digital resilience and, if so, to what extent the measures from the agenda have played a role in this. The evaluation should therefore focus on three aspects:

1. **defining** the notion of 'digital resilience' and **demarcating its scope**;
2. **operationalisation** of this definition in relation to the four target groups of the NCSA: citizens, businesses, the government and private sectors of vital importance; and
3. establishing the **impact** (and extent of the impact) of **measures and interventions** from the NCSA on digital resilience in and of the Netherlands.

In order to satisfy these three aims, the CSR recommends that three instruments be used:
(1) a **literature review**, (2) a **quick scan** of policy evaluations in the area of cybersecurity in the Netherlands and abroad, and (3) a **Nominal Group technique**. The following table sets out which methods are appropriate for which purposes.

	Definition and demarcation	NCSA target groups	Impact of measures
1. Literature review	X	X	
2. Quick scan of policy evaluations	X	X	X
3. Nominal Group technique	X	X	X

Further reasoning and elaboration will be provided below to support the recommended multi-stage solution.

1. Literature review

The best tool for effectively defining and demarcating the scope of 'digital resilience' is a systematic literature review in combination with data from the quick scan of policy evaluations (see below). The literature review could comprise an exploration of the current state of the art, including definitions and interpretations of digital resilience. It could also be used to examine how digital resilience is understood in relation to the four target groups in the NCSA: citizens, businesses, government and private sectors of vital importance. Ideally, the literature review should focus on a combination of scientific articles, grey literature and relevant policy documents.

Recommended method(s): desk research, for example, based on snowball sampling.[2] It would be preferable if thematic[3] and conceptual analysis[4] were applied in processing the results.

2. Quick scan of evaluations in the area of cybersecurity policy

The NCSA is not the first cybersecurity agenda to be evaluated, neither in the Netherlands nor abroad. Because this evaluation must be completed by 2021, it would be useful to conduct a quick scan of other, similar evaluations in the Netherlands and elsewhere. This might include evaluations of cybersecurity strategies and/or agendas as well as evaluations of cybersecurity policy from specific government bodies, such as the ongoing evaluation of cybersecurity policy at the Dutch Ministry of Foreign Affairs. This will make it possible to learn lessons about:

(1) the approach used in the evaluation;
(2) conceptualisation and demarcation of the evaluation;
(3) the methods chosen;
(4) insight into various target groups of cybersecurity strategies, agendas and policy;
(5) the analysis of the impact of the instrument being evaluated.

Especially where the methodology of the latter includes a chosen approach similar to the one suggested below (the Expert Consensus technique), this kind of quick scan can help to save time and offer other benefits.

Recommended method(s): quick scan.[5]

[2] For example, see https://journals.sagepub.com/doi/abs/10.1177/004912418101000205
[3] For example, see https://psycnet.apa.org/record/2011-23864-004
[4] For example, see https://link.springer.com/article/10.1007/s10502-005-2594-8
[5] For example, see https://www.sciencedirect.com/science/article/pii/S1462901116304385

3. Nominal Group technique

When evaluating strategies, policy or national agendas, one of the most important ways to gather information is to conduct interviews with stakeholders in the field. In an effective evaluation, these stakeholders will come from different target groups. They can be expert representatives from the government, from the business community, from think tanks and from the scientific community – and, if possible, also from interest groups or other parties that represent citizens. After all, together, these stakeholders have combined oversight of the field, the challenges present within it and the actual or potential impact of interventions. Moreover, they have insight into aspects realised in the past: which interventions have been implemented in recent years for the purposes of strengthening digital resilience in the Netherlands? That information is crucial in order to create a comprehensive overview of the 'lay of the land' for the Netherlands in this area.

There are also a number of disadvantages to conducting interviews with stakeholders. One is the time-intensive nature of interviews, whether with a group or an individual. Another disadvantage is that interviews lead to a multitude of subjective opinions and ideas, which cannot then be easily converted into objective or quantifiable data.

In response to this problem, a number of new techniques for stakeholder interviews have been developed in recent decades. The CSR recommends using the '**Nominal Group technique**'.[6] [7] When experts take part in a study in which the Nominal Group technique is applied, they conduct discussions with one another – in several rounds and according to a fixed structure – concerning a problem or set of questions presented to them, or they may use the rounds to supply requested information (facts). In the first round, participants write down their own ideas about a given subject individually and without consulting one another. They then take turns presenting ideas from their lists, one at a time, until all ideas have been discussed. All ideas are recorded and clustered. In the subsequent round, the ideas are then discussed in a highly structured fashion. Participants will evaluate each idea individually and on paper. In the following round, the 'group response' is shared and discussed. This serves to slowly narrow the bandwidth of the ideas and allow conclusions to converge. This yields valid, objective and 'soft' quantifiable results, also known as an expert consensus.

Recommended method(s): Expert Consensus technique[8] or Modified Delphi Method.[9]

In conclusion

In view of the second request from the Minister of Justice and Security, the CSR hopes that the evaluation of the NCSA will be successfully concluded and made available to it in January 2021. This will enable the CSR to incorporate the results in its recommendations for the next term of government.

I look forward to your response.

On behalf of the Cyber Security Council,

Hans de Jong
Co-chair

[6] For example, see https://researchonline.jcu.edu.au/22604/4/JCU_22604_Harvey_and_Holmes_2012_accepted.pdf
[7] For an example of a description of the technique used, see https://ajph.aphapublications.org/doi/pdf/10.2105/AJPH.74.9.979
[8] See footnote 5
[9] For example, see https://ascelibrary.org/doi/abs/10.1061/(ASCE)0887-3801(1995)9:4(244)