Exploration for a broad evaluation of the NCSA

Assessment of the possibilities for an evaluation of the completeness, realisation and impact of the Dutch Cyber Security Agenda on the cyber resilience of the Netherlands

Independent summary to the final report

DATE	8-5-2020
VERSION	1.0 – final version
PROJECT REFERENCE	Ministerie van Justitie en Veiligheid - Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) - Verkenning brede evaluatie NCSA
WODC PROJECT NUMBER	3095
ACCESS RIGHTS	Public
EXECUTIVE ORGANISATION	InnoValor
AUTHOR(S)	Dr. Bob Hulsebosch, Dr. Henny de Vos, Koen de Jong, MSc.

The Dutch National Cyber Security Agenda (NCSA)[1] was established in 2018 as a successor of the National Cyber Security Strategies I and II. The NCSA comprises the Dutch governmental strategy for increasing the cyber resilience of Dutch society. It contains seven ambitions with underlaying objectives and measures that allow for realisation. At the launch of the agenda, an evaluation was promised. However, it was not determined how such an evaluation should take place. This report explores the possibilities for the NSCA evaluation.

NCSA Evaluation Goals

The central question for the NCSA evaluation is to what extent the NCSA has made the Netherlands more cyber resilient. The answer to this question can, for various reasons, not be given very easily. The domain of cyber resilience is complex and consists of multiple dimensions. There are social, economic and international political interests. There are different target groups that need to be addressed, e.g. citizens, organisations, vital sectors, each having its own characteristics. In other words, cyber resilience and its implementation through cyber security measures depend on the considered context. Moreover, the cyber security domain is very dynamic, as it involves the ongoing appearance of new threats and risks in an increasingly digitally developed Dutch society. Although the NCSA recognizes these aspects, it lacks clarification of the concept of cyber resilience.

Providing a clear, unambiguous definition of cyber resilience is not trivial, due to complexity and scope. In order to determine the impact of the NCSA on Dutch cyber resilience, a further elaboration of this concept is necessary. This also enables checking how the NSCA sufficiently covers all facets of digital resilience. The NCSA, however, does not clearly state the impact it wants to achieve, how such an impact should be assessed and who should be responsible for the evaluation. The absence of a baseline measurement does not help in this respect. To improve on the effectiveness of the NCSA we can state that it is desirable to evaluate the NCSA in the broadest sense and from different perspectives, typically the following three:

- Plan evaluation focused on coverage of the NCSA: does the NCSA cover all aspects of cyber resilience or are there blind spots that hinder cyber resilience? This evaluation can be a starting point to build on the coverage of a next NSCA.
- Process evaluation concerning realization of measures proposed: how was the execution of the NCSA organized? Which parties were involved? How is this realization evaluated?
- Effect evaluation: What was the impact of the measures on the digital resilience of the Netherlands? This is the most important evaluation and also the hardest one given the design of the current NCSA.

These evaluations have the following goals:

- Demonstrate to what extent the Netherlands has implemented the required activities to increase cyber resilience in an integrated and structured manner, taking into account the Dutch characteristics. Provide insight into missing essential objectives and measures including its reasons (plan evaluation)
- Determine whether the Netherlands is implementing the agenda correctly (process evaluation) and whether its activities are positively contributing to improving cyber resilience (effect evaluation).
- Inspire and learn for the next NCSA. The evaluation focuses primarily on increasing knowledge and understanding of the success of cyber security policy, with the aim of benefiting from this in new policy interventions / the next agenda. An agenda that can focus on achieving more maturity and achieving more completeness and dedication.

Evaluation Framework

We developed a framework to evaluate the current and future NCSAs in an unambiguous, effective and systematic manner. It operationalizes the concept of cyber resilience by combining core elements for the different target groups of the NCSA (citizens, companies, government and vital sectors). These elements are

[1] NCSA, 2018, see https://english.ncsc.nl/topics/national-cybersecurity-agenda/documents/publications/2019/juni/01/national-cyber-security-agenda

either organizational (strategic, tactical, operational), process (identify, protect, detect, respond)[2] or operational (behaviour, governance, technical)[3] nature. The framework is visualized in the figure below.

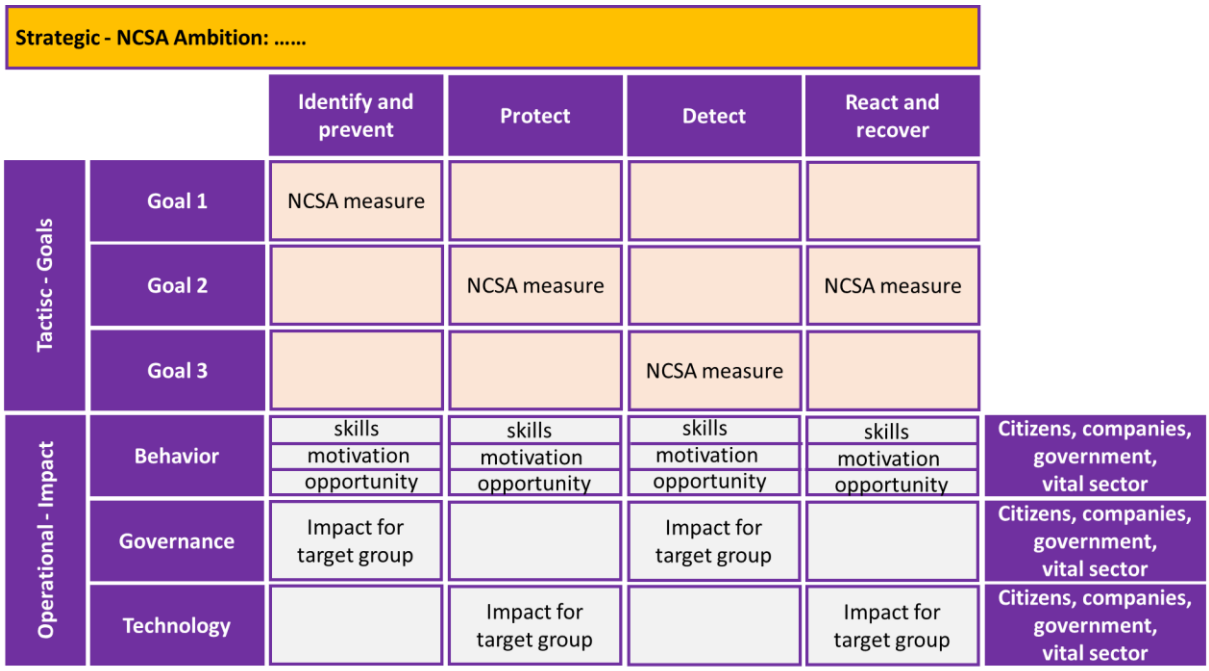

Figure 1: Framework for NSCA evaluation. This framework comprises the main elements of cyber resilience. It can be used to determine the impact of the NCSA on target groups for each ambition.

The bottom layers of the framework relate to the impacts or effects of the measures for the specific target groups and provide structure to the effect evaluation. This can be done, for example, by identifying whether citizens, companies, the government and vital sectors have the required skills, motivation and opportunities to improve their cyber resilience. As indicated earlier, this is the most important evaluation variant, as it shows whether the government is fulfilling its protective task in the digital domain.

Use of the Evaluation Framework

The framework can be effectively applied for the three evaluations[4].

The **plan evaluation** can easily be done by plotting all elements of the NCSA onto the framework. In this way a systematic insight is gained into the coverage of the NCSA concerning cyber resilience. It reveals any elements that are not addressed by the NCSA. In such cases it should be decided whether it was a conscious or unconscious choice to omit such elements in the agenda. Any "blind spots" that are disadvantageous to cyber resilience can be filled in in a future version of the NCSA, taking the different target groups into account. Further elaboration could be done by a critical reflection of the underlying arguments and logic of the agenda items. It should be critically examined whether the assumptions that have been made to motivate the strategy, the tactics followed, and the measures taken are (still) sound and correct.

The basis of the **process evaluation** are the spending plans for the government instruments which are the additional investments for cyber security following the Dutch 2017 Coalition Agreement and which largely form

[2] Derived from the NIST cybersecuirty framework, see https://www.nist.gov/cyberframework
[3] Derived from the ISACA business model for cyber security, see http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx
[4] For more information on evaluation research: "Evaluatie van justitiële (beleids)interventies", 2010 (WODC), see https://www.wodc.nl/binaries/memorandum2010-2-volledige-tekst-nieuw_tcm28-78177.pdf
and "Evaluatiebeleid en richtlijnen voor evaluatie", 2009 (BZK), see https://www.rijksoverheid.nl/documenten/brochures/2009/10/01/evaluatiebeleid-en-richtlijnen-voor-evaluaties

the core of the NCSA's implementation. Based on a document analysis of spending plans, ambitions and status reports, the results of the NCSA realization can be assessed and compared with the original NCSA ambitions. In addition to document analysis, interviews with the implementing organizations involved about the realization of the plans provide further details. The pitfall here is that the evaluation has a subjective character as organisations evaluate their own activities. Therefore, an external view of (parts of) the process is also necessary, for example by involving domain experts, supervisors or customers of the results in the evaluation. The result of this evaluation is a weighted overview of which parts of NCSA have been carried out and how.

The implementation of the **effect evaluation** is challenging due to the design of the current NCSA, but especially desirable for financial accountability and from an inspiring and learning point of view. As far as the lessons are concerned, the main focus should be on gaining experience on *how* to evaluate measures and objectives for digital resilience and to create a specific attitude for doing this. In addition, the outcomes provide a good baseline measurement to use when evaluating a future agenda or strategy. It is not feasible to evaluate the NCSA in all its aspects because the subject of digital resilience is too broad to tackle. It is therefore important to prioritize and harvest the easy to evaluate elements of the NCSA (the "low-hanging fruit"). We propose the following strategy along the dimensions of the framework:

1. Include a minimum of one goal of the NCSA within the process phases: identify, protect, detect and react.
2. Include a minimum of one goal for each target group.
3. Include a minimum of one goal for the operational characteristics: behaviour, governance and technology.

The prioritization of focus areas for the evaluation will have to be determined by the evaluating party in consultation with the client. An important aspect that should be taken into account are availability of data and (other) evaluation sources. For example, Statistics Netherlands or a supervisor with a knowledge on the status of cyber resilience for specific target groups. If such sources are not available or of insufficient quality, the evaluating party must collect the data itself, for example by conducting surveys, interviews, expert sessions, observations, social media analyses, logging and monitoring data-analyses, or counting. As a rule, such data collection is an intensive and lengthy process. Other factors to take into account when prioritizing are evaluating the measures with clear targets - the low-hanging fruit for evaluation - or that are considered of utmost importance for cyber resilience.

The following evaluation approach can then be used for each objective[5]:

- Inputs: the (financial) means that have been spent on the goal, like laws, funds/efforts for (stimulating) research and knowledge building, supporting means, participations in discussions, coordination activities.
- Activities: activities between inputs and outputs.
- Outputs: the results of the activities, e.g. year reports, cyber security baselines, alert systems, scientific publications, self-service awareness education and cooperations.
- Impact: the effect of the outputs on NCSA's ambitions and Dutch cyber resilience in general.

In the absence of a baseline measurement or indicators of success, a lower limit or desired target should be defined upfront, for example from expert consultation. The results of the evaluation can then be compared with such a norm. An alternative is to apply benchmarking, for example by comparing The Netherlands with ambitions and objectives in other countries or confront Dutch measures with those of other countries. However, information that allows for benchmarking is scarce.

Additional Recommendations

We conclude with a set of guidelines that are strongly recommended from an evaluation perspective for the evaluation of current and future NCSAs:

- Apply the evaluation framework to operationalize and structure cyber resilience for future NCSAs in order to achieve a uniform, integrated and systematic approach for increasing cyber resilience;

[5] An evaluation Framework for National Cyber Security Strategies, ENISA, November 2014, see https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies

- Make future NCSAs easier to evaluate on effect by taking into account the following aspects:
    - Define expected effects of measures and how measures contribute to the realization of goals and ambitions;
    - Prepare a more risk-driven approach to define cyber resilience and for setting priorities. Take qualities and characteristics of The Netherlands into account;
    - Consider a further breakdown of the target groups. For example, a more detailed classification of companies (a high-tech multinational has a completely different resilience profile than a small entrepreneur) and sectors (managing cybersecurity risks in different sectors often requires a sector-specific approach);
- Cyber resilience is extremely complex and has many interests and stakeholders. Therefore, assign evaluation to a highly qualified and reputable party, whose core business consists of conducting evaluations and has excellent knowledge of the cyber security domain;
- Organize the evaluation so that the emphasis is on learning from the current NCSA for the future (as compared to punish for things that did not work out);
- Use the results of the evaluation for a subsequent NCSA. In this way, the maturity of Dutch cyber resilience can be traced;
- Align with ENISA's approach to enable benchmarking the Dutch agenda, since experts indicate that this adds value. ENISA defines fifteen strategic goals for cyber resilience[6] that are comparable to the ambitions of the NCSA. Take this into account when drawing up a next agenda.
- Get inspiration for future strategies from the national strategies of other countries like the United Kingdom[7], Estonia[8] and Denmark[9]. The strategies of those countries are fed with evaluation results of previous strategies, take into account characteristics of their own society and the risks that arise from them, better safeguard measures with ongoing activities, set concrete indicators for success, indicate who is responsible for them, and how to evaluate them.

[6] See https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool

[7] The UK Cyber Security Strategy 2011-2016, Annual Report, April 2016, see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf.

[8] Cybersecurity Strategy - Republic of Estonia, 2019 – 2022, see https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

[9] Danish Cyber and Information Security Strategy 2018-2021, see https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategy-for-cyber-and-information-security