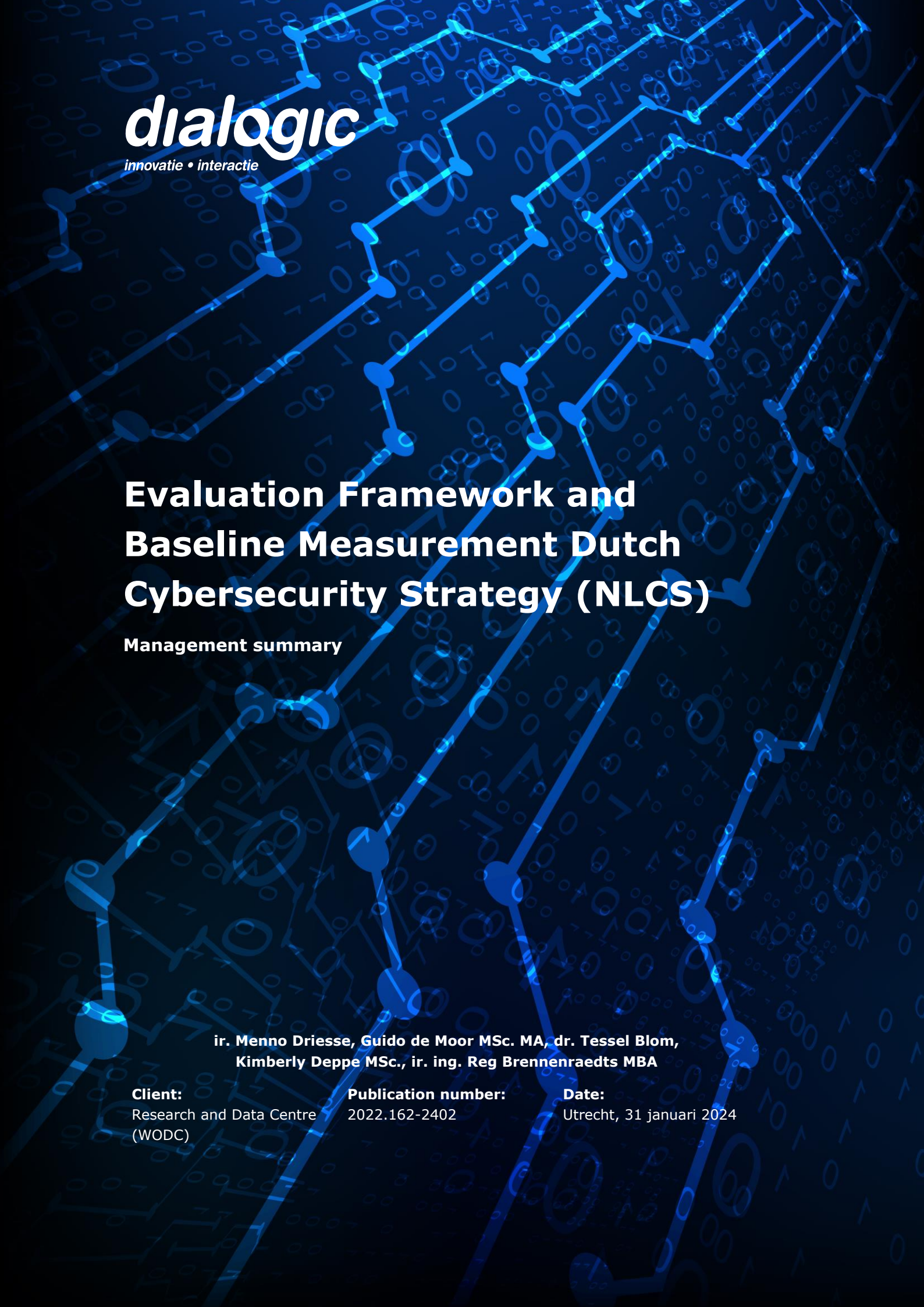

dialogic
innovatie • interactie

Evaluation Framework and Baseline Measurement Dutch Cybersecurity Strategy (NLCS)

Management summary

ir. Menno Driesse, Guido de Moor MSc. MA, dr. Tessel Blom, Kimberly Deppe MSc., ir. ing. Reg Brennenraedts MBA

Client:
Research and Data Centre (WODC)

Publication number:
2022.162-2402

Date:
Utrecht, 31 januari 2024

The authors of this report would like to thank the advisory committee for their critical reflections on the content. The committee consisted of: Prof. Dr. Ir. Jan van den Berg (TU Delft; Chairman), Dr. Mark de Bruijne (TU Delft), Mr. Dr. Pieter Wolters (Radboud University), Policy Officer Department of Cybersecurity (NCTV, involved until May 2023, name known to the advisory committee), Policy Officer Department of Cybersecurity (NCTV, involved from May 2023, name known to the advisory committee), and Dr. Leontien van der Knaap (WODC).

Cite as: Dialogic, Driesse, M., De Moor, G., et al. (2023). *Evaluatiekader en Nulmeting Nederlandse Cybersecuritystrategie - managementsamenvatting*. WODC, Den Haag.

Management summary

Background

Following the Dutch Cyber Security Agenda (NSCA), the Dutch cabinet aims to increase the digital resilience of the Netherlands, strengthen the cybersecurity system, and address digital threats. To this end, the **Dutch Cybersecurity Strategy** (NLCS) has been formulated. In this strategy, the responsibility for safety and digital resilience shifts from end users more towards the government and sectors. Additionally, the strategy aims to be less non-committal than its predecessor. The NLCS specifies a clear long-term goal, with priorities, allocated budgets, and well-reasoned choices.

Compared to the NCSA, the NLCS has been modified in several ways from an evaluation perspective. For instance, significant efforts have been made in establishing a monitoring structure by collectively considering the logic of policy deployment beforehand. However, a **formal determination of the starting situation** (a baseline measurement) is often still missing. Moreover, it happens that the **formulated activities** are not (well) suited for an effectiveness evaluation. Finally, due to more than 100 action lines, it is **complicated to identify the focus and prioritization** within the strategy. This also makes it difficult to determine the internal coherence between the activities and objectives of the strategy.

The NLCS and the Action Plan

The structure and context of the NLCS are, especially for outsiders, complex and extensive. To give an impression of the coherence, we provide a brief introduction to the strategy, the underlying action plan, the involved actors, and the budget.

- **The Dutch Cybersecurity Strategy (NLCS)** is intended as a future-oriented, sustainable vision of the Dutch government on how to strengthen digital security in the Netherlands. To realize this vision, the NLCS includes twelve concrete objectives grouped under four central pillars of the strategy. These pillars and the corresponding objectives from the NLCS have been visualized by us in Figure 2.

- **The Action Plan Dutch Cybersecurity Strategy 2022-2028** (hereinafter: action plan) describes all policy actions that will be executed within the framework of the NLCS. The action plan is an adaptive policy document that can be adjusted during the NLCS's duration based on changes in interests, threats, resilience, or other political-administrative needs. The initial version includes a total of **136 activities**. The activities in the action plan are clustered into 35 sub-goals or themes. The action plan is updated annually, allowing for adaptation to developments and trends.

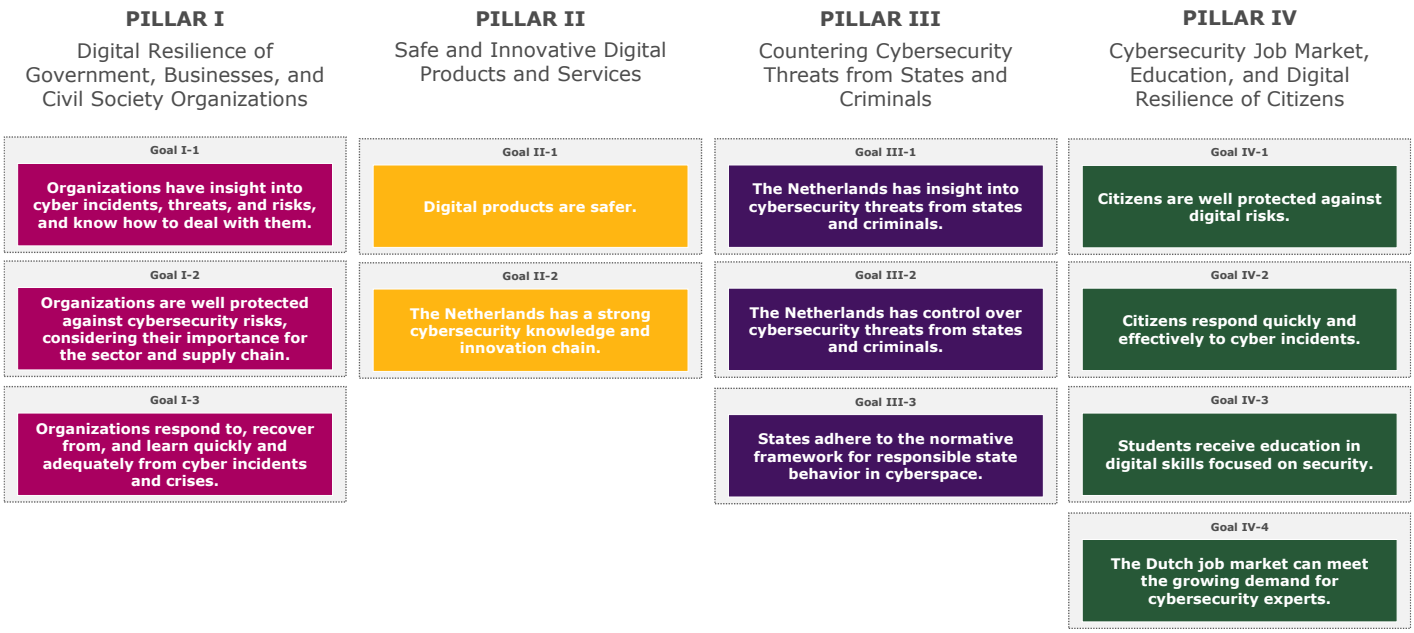

Figure 1. Pillars and Goals in the NLCS (source: Dialogic based on the NLCS)

The budget for implementing the action plan through 2028 totals **€568 million**. Of the **involved departments**, the Ministry of Justice and Security (hereinafter referred to as JenV) receives the largest portion of the funds, namely 32% (€183 million). The majority of these resources are allocated to the National Cyber Security Centre (NCSC) (€168.8 million), which is under the responsibility of JenV. The Ministry of the Interior (hereinafter referred to as BZK) allocates 29% (€166.2 million) of the assigned resources. Over 58 percent of this (€97.6 million) is reserved for the deployment of the AIVD.

Research Objective, Design, and Methodology

With the lessons learned from the evaluation of the NSCA and previous observations regarding the challenges in monitoring the NLCS, Dialogic was asked to conduct a baseline measurement of the NLCS activities and to establish a monitoring framework for the strategy. We use a research design with five steps. These will be carried out for each pillar of the NLCS:

1. **Identifying key points**. At the level of the pillars, we describe the essential activities to gain insight into the chosen priorities within the NLCS.
2. **Reconstructing the policy logic** of the Action Plan Dutch Cybersecurity Strategy 2022-2028. We do this by taking the policy rationale of the action plan as a starting point and examining whether the causal relationships between the formulated activities in the action plan and objectives in the NLCS are logical and plausible. We do not conduct additional empirical research (an effectiveness evaluation) on the causality of each activity ourselves.
3. **Assessing the measurability of an activity's implementation**. In other words, to what extent can an objective statement be made about the progress of the activity over time in the future? We do this based on four categories, namely: (1) **easily measurable**, (2) **complex but measurable**, (3) **poorly measurable**, and (4) **confidential**.
4. Determining the current status of an activity through a **baseline measurement**. Without a baseline measurement, it is impossible to measure the difference (Δ) between the situation before and after the implementation of the Action Plan, and thus to make a statement about the effect of the activities.

5. Setting up a **monitoring structure** for the NLCS. In this study, we make a proposal at both the activity and goal level on how a follow-up measurement (effect measurement) can be carried out in the future.

To achieve the intended assessment of the core activities, policy logic, measurability, baseline measurement, and monitoring suggestions, we have employed a collection of research methods:

- **Desk study**: Firstly, based on the Action Plan, we established a database containing all announced policy activities. This database formed the basis for our analysis of measurability, inventory of involved departments and implementing organizations, and the baseline measurement itself. In addition to a thorough analysis of the action plan, we studied various additional source materials during the research period, such as previous evaluations, agendas, strategies, progress reports, and letters to Parliament (see footnotes in this report). The inventory of generic measuring instruments (Chapter 7) is based on a study of relevant sources (snow-ball sampling) where existing knowledge is summarized. This knowledge is supplemented and enriched by conversations with activity owners, where necessary.

- **Interviews**: During the research, we conducted multiple rounds of discussions with the involved case managers and participated in meetings of the Directors' Meeting on Cybersecurity (DOCS) and the Interdepartmental Meeting on Cybersecurity (IOCS). These talks and sessions were an important input for the reconstruction of the policy logic, identifying the key points, the baseline measurement, and the assessment of measurability.

- **Validation session**: In the concluding phase of the research, case managers holders validated the baseline measurement. In this way, a fact-check for inaccuracies in the baseline measurement (appendix 2) was conducted for each activity.

Research Results (per pillar)

In Chapters 3, 4, 5, and 6, we provide a detailed overview of the research results for each of the four pillars. This includes detailed consideration of the context of the activities and the associated policy logic, leading to an interpretation of the core activities, the concrete baseline measurement, and the associated suggestion(s) for monitoring progress. The table below shows our research results at a high level, providing an overview of the results for each of the five research steps per pillar.

In interpreting the results, we emphasize that the (demonstrated by the baseline measurement) adequate execution of (measurable) activities does *not* automatically lead to the conclusion that the objectives of the NLCS are also being achieved. The policy context of cybersecurity is too complex for that, as a range of external factors (geopolitics, technical innovations, human aspects) impact the objectives of the strategy.

	Pillar 1	Pillar 2	Pillar 3	Pillar 4
Core activities	• The revision of the national cybersecurity system • Implementation of the NIB2 Directive / revision of the Wbni • The further development of (national) incident, continuity, and recovery plans	• Introduction of the Cyber Resilience Act (CRA) • Strengthening government procurement policies • Strengthening the Dutch innovation ecosystem in the cybersecurity sector	• Increasing visibility of cyber threats (from state actors) • Interventions on cybercrime • Investing in cybersecurity at the diplomatic level	• Awareness campaigns • Integrating digital skills into the education curriculum • Reskilling and upskilling programs
Policy Logic	The policy resources logically and plausibly add up to the objective of making the government, businesses, and civil society organizations more digitally resilient. However, we note that the involvement of, in particular, the broader SME sector and civil society organizations requires additional attention.	The policy resources logically and plausibly add up to the goal of leading to safer digital products and services. However, we note that the additionality of the NLCS for policy activities that were already underway before the strategy is difficult to objectively assess. We also observe that less attention is given to scaling up innovations in the strengthening of the cybersecurity and innovation chain.	The policy resources logically and plausibly contribute to increasing the visibility of threats. Potential challenges we see lie in the area of international and diplomatic efforts and the balance between defensive/offensive actions and the corresponding threats. Additionally, the additivity of the NLCS in enhancing control over cybercrime is unclear to us.	The policy resources logically and plausibly add up to enhancing the digital resilience of citizens. However, we identify a challenge in increasing cybersecurity expertise in the labor market, as these shortages essentially receive the same priority as other shortages. This makes the additivity of the NLCS in this area unclear.
Baseline	The policy activities in this pillar largely consist of a collection of activities where existing organizations, laws, and procedures are being developed further, often being in the first phase of this development.	In the area of legislation and regulation, a large part of the activities depends on progress at the European level. This is currently delaying the execution of these activities.	Conducting a baseline measurement for activities within Pillar 3 is not possible everywhere, as the efforts of the AIVD (General Intelligence and Security Service) and MIVD (Military Intelligence and Security Service) are largely confidential and thus limited in measurability.	The revision of the curriculum concerning digital skills was already underway prior to the strategy. The focus for awareness activities is particularly during the 'cybersecurity month' in October each year.
Measurability	Out of a total of 67 activities, we determine that 37 activities are easily measurable, 24 are complex but measurable, 2 are poorly measurable, and 4 are confidential.	Out of a total of 28 activities, we determine that 15 activities are easily measurable, 9 are complex but measurable, 3 are poorly measurable, and 1 is confidential.	Out of a total of 23 activities, we determine that 6 activities are easily measurable, 9 are complex but measurable, 3 are poorly measurable, and 5 are confidential.	Out of a total of 18 activities, we determine that 15 activities are easily measurable and 3 are complex but measurable.
Monitoring	We determine that for monitoring the progress of Pillar 1, the end of 2024 is an important benchmark. Since most policy activities are aimed at the (further) development of organizations, laws, and plans, it is relatively easy to measure based on output.	For monitoring the progress of activities under Pillar 2, attention should be given to the establishment of legislation at the European level. Subsequently, the progress of the activities in the Dutch context can be determined based on several specific indicators.	The monitoring of confidential activities will take place via regular accountability channels. For diplomatic efforts, we suggest that monitoring is best achieved by looking strictly at the (numerical) output.	In monitoring progress within this pillar, existing measurement tools, such as the research conducted by the Public Service and Communication Department (Dienst Publiek en Communicatie - DPC) for government campaigns, can be used. However, new instruments may also be required.

Conclusions

Core Activities

The NLCS originally comprises five focal points. *We conclude that the core activities from the four pillars align well with these focal points*. The distribution of resources across departments also reflects the importance attached to an activity. We have observed the following for each focal point:

- **Better insight into threats** – Substantial efforts (resources and actions) are dedicated to this component, *aiming to increasingly position the central government as a hub in the information provision around cybersecurity*. The action plan envisions a significant role for the NCSC and the intelligence and security services. For the latter however, there is a limitation that information about their deployment, activities, and results is confidential. Therefore, we cannot make statements about the deployment, policy logic, and outcomes of these activities within this research.

- **More cybersecurity specialists** - *We note that for achieving this objective from the NLCS, relatively few additional resources are allocated within the action plan.* This is apparent, among other things, from the fact that the Ministry of Education, Culture and Science (OCW) is responsible for a large part of Pillar 4, but has only 3% of the total budget at its disposal. The ministry's activities are mainly a continuation of existing policy efforts. This raises the question of what the additional contribution in the action plan to this objective is.

- **Government and sectors taking responsibility** – Achieving this requires a redistribution of responsibilities, including more intensive public-private cooperation and new legislation for digital products and services. We see that the NLCS focuses on this, but *it is difficult for us to determine how much funding is available for this focal point*. The objective is elaborated through various activities and departments. The current substantiation (resources and involved parties) in the action plan is insufficient for gaining a clear insight.

- **Better supervision and necessary laws and regulations** – Departments are attempting to implement the objectives in the NLCS quickly and efficiently by setting up parallel legislative trajectories. However, the departments are heavily dependent on the progress of decision-making and legislative procedures in the EU for the realization of this focal point. Additionally, the action plan lacks focus on (the challenges of) supervision. This is expected to change by 2025.

- **Clear information via a national cyber authority** – The establishment of a central, national cyber authority is an important part of Pillar 1. Its completion will not take place until 2027. Plans for integration are already being developed. For providing clear information to organizations, such as on basic measures or common threats, the DTC (part of the Ministry of Economic Affairs and Climate Policy, EZK) is the central actor. *The focus of the activities lies on centralization, as well as on the sustainability and accessibility of information.*

Policy Logic

At the level of the pillars, we analyzed whether the policy activities, if executed well, logically add up to the objectives formulated in the strategy. *We conclude that this is the case for the majority of the action plan.* This is partly due to the fact that policymakers paid explicit attention to the policy logic when drafting the action plan. This represents a clear improvement over the NCSA. *The main points of attention per pillar are*:

- Within **Pillar 1**, we see that improving the digital resilience of organizations requires additional focus on the involvement of the broader SME sector and social organizations. We notice that relatively few concrete policy activities have been formulated for these two target groups.

- Regarding **Pillar 2**, we conclude that in the strengthening of the cybersecurity and innovation chain through the development of high-quality knowledge, relatively little attention is paid to the scaling of innovations into products.

- For **Pillar 3**, we identify two challenges. In the activities related to international and diplomatic engagement, it remains to be seen whether, and to what extent, other countries and international organizations are actually willing to contribute. Moreover, we cannot determine the quality of Dutch offensive and defensive organizations. Therefore, we cannot assess whether the three response options (diplomatic, offensive, defensive) are sufficient to counter threats and repel attacks.

- For **Pillar 4**, we identify potential challenges regarding the coherence between activities and the realization of more cybersecurity expertise in the labor market. The shortage of cybersecurity personnel essentially receives the same priority as other personnel shortages in policy areas such as healthcare or technical professions. Since no extra efforts appear to be made in the action plan, the added value of the NLCS in this area is unclear.

Baseline Measurement

The baseline measurement forms a crucial deliverable of this research. The results are included in the appendix of this report. We identify three different types of activities with specific characteristics:

- The first category involves existing or **ongoing activities**. Examples include sector plans in scientific education or the Human Capital Agenda ICT. For these activities, it has been established when they started and what the progress is.

- The second category consists of **newly established activities** that are now in the implementation phase. An example is the realization of one national cybersecurity authority through the integration of the NCSC, DTC, and CSIRT-DSP. We have determined the progress of these activities since the end of 2022 until the third quarter of 2023.

- The third category includes activities that are **newly established but cannot yet be fully implemented due to dependencies on other ongoing actions**. An example is activities that will be concretized once the legal frameworks at the European level are established. This can include the further development of cooperation between RDI and ACM based on the Radio Equipment Directive. For this category, we have mapped out (1) when the activities are expected to start and (2) what these starts depend on.

Measurability

We can conclude that the measurability of the NLCS has significantly improved compared to its predecessors. This is mainly due to the formulation of the activities, the naming of owners and stakeholders, and the structure of the strategy (with activities, sub-goals, goals, and pillars). As a result, the coherence of the activities is clearer than before.

- *More than half of the activities (n = 73) are assessed by us as easily measurable.* These are activities where, at the next measurement moment, it can be unequivocally (often binary) determined whether the activity has been completed or executed. These are activities that typically require departmental output, such as developing a roadmap for cooperation with the business sector or carrying out a reconnaissance.

- *Activities classified as 'complex, but measurable' comprise a large part of the total set (n = 45).* These are activities such as the integration of CSIRT-DSP and DTC into the NCSC. It must first be determined how to ascertain when the activity is completed (such as integrating into one physical location, joint staff, and/or shared website).

- *A number of activities are assessed as poorly measurable (n=8)*. The most common reason for this assessment is an unclear description of the activity, such as the Dutch government's 'active contribution' in the international field. It would be valuable to further develop such an action into more concrete actions and outcomes.

- *The last category includes activities whose measurability we cannot assess (n=10)* because they are carried out by I&V services and are thus confidential.

We want to emphasize (again) that the extent to which policy efforts will actually lead to results and impact depends on factors such as the quality of execution and external factors influencing the policy context. Measurability is therefore not a simple guarantee of successful execution and results.

Monitoring

In establishing monitoring, we must distinguish between monitoring **progress** (output) and monitoring **effect** (outcomes and impact).

*For **monitoring progress**, it makes sense to do the same type of measurement as we do in this research*. An overview or our detailed results can be found in Appendix 2. In many cases, existing monitors or accountability channels (such as annual reports, parliamentary letters) can be used. A mid-term evaluation of the strategy is planned for 2025. *By then, a number of crucial parts of the action plan should be completed according to the schedule*. Besides a progress measurement, indicators for effect measurement can also be established at the mid-term evaluation. It is also advisable for monitoring progress to analyze how the distribution in terms of measurability is over the core activities. This is an analysis we have not performed. If it turns out that a significant part of the core activities is poorly measurable or confidential, this could be a reason to push for better defined and measurable actions and performances.

For monitoring policy effects, various generic measuring instruments are available, such as the National Security Assessment (Nationale Veiligheidsbeeld), Cybersecurity Assessment Netherlands (Cybersecuritybeeld Nederland), etc. However, Pillar 2 is only partially covered by these instruments. It is important to note that no statements can be made about causality. In other words, as already mentioned, it cannot be determined to what extent the

activities do or do not contribute to the policy effects. In the research, we do provide insight into the evaluation methods that can help open this 'black box' between policy performances and effects and analyze the direction and magnitude of the relationships.

Recommendations

We conclude with several recommendations regarding the implementation and monitoring of the strategy and action plan, followed by a brief reflection on our research approach.

Progress and Monitoring of the NLCS and Action Plan

Our research concludes that the activity owners have made a vigorous start with the implementation of the action plan. There are differences between departments, for example, caused by the degree of urgency and available resources, but overall, it is not evident that any activities have stalled since the start of the NLCS.

The focus of implementation lies on performing activities that are prerequisite for subsequent actions. This is most applicable to activities aimed at developing legal frameworks, such as the amendment of the Wbni and the legislative proposal to promote digital resilience in companies. If these legal frameworks are not established, the execution of related activities, such as arranging supervision, is delayed. Our recommendation is to specifically monitor the progress of these activities to ensure the realization of the action plan as a whole.

We have **three concrete recommendations** regarding the challenges identified in our research:

1. *The issue of increasing cybersecurity expertise in the labor market is linked to the overall labor market shortage in other professions*. For cybersecurity, competition with other IT professions is particularly relevant. This makes it a political issue: where should the country prioritize in terms of labor market policy? We can't make this choice, but it is very current. Once more concrete choices are made, policymakers can use various ongoing labor market studies to specifically maintain or increase the supply of cybersecurity expertise.

2. *The second challenge is the oversight of the implementation and effectiveness of activities conducted by the intelligence and security services*. These confidential activities are an essential part of the NLCS and also account for a substantial portion of the resources. We, as external researchers, cannot comment on this part of the action plan. *However, it is crucial for the implementation, progress, and adjustment of the action plan that there is internal oversight and control of these activities within the national government to discuss their relative effectiveness*. We cannot assess whether this is currently the case, but we note that the services are connected to the DOCS meeting to share relevant information with stakeholders. This responsibility lies with the relevant policymakers, and we urge them to continue to monitor and adjust as needed.

3. The last challenge is related to the above and concerns the existing accountability lines of the involved implementing organizations. From an efficiency and capacity constraint standpoint, we understand that it is challenging to deviate from the fixed pattern for the NLCS alone. *However, it is essential that there is a central information provision from which the progress of the strategy can be read*. The annual progress reports provide this, and the monitoring suggestions from Appendix 2 can be used to carry out the reporting request.

For **monitoring**, we establish that at the mid-term evaluation in 2025, several key activities are expected to be completed according to the plan. In addition to measuring progress, indicators for effect measurement can also be established at the mid-term evaluation. The extent to which the available generic measuring instruments are sufficient to monitor policy effects can also be determined.

Measuring the contribution of the strategy to improving cyber resilience is complex, as it is a sum of various internal and external factors. Digital resilience must always be considered in relation to digital threats. Since the sources of digital threats (viruses, ransomware attacks, phishing) are constantly changing, effect measurements of a strategy to increase digital resilience should also be adjusted to the source of the digital threat. Therefore, it is important to look at **goal achievement** ("are the goals being met, regardless of the policy's contribution?") in addition to understanding and substantiating the direct contribution of the policy to the objectives ("are the goals being met due to the policy's contribution?").

Reflection on Our Research Approach

Our research approach provides valuable tools for the implementation and monitoring of similar interdepartmental policy agendas and strategies. Both the research steering committee and the NCTV have indicated that the process has yielded **valuable lessons in terms of outcomes and process**.

The chosen approach of mapping out the core activities, policy logic, baseline measurement, measurability, and monitoring suggestions in advance using a five-step approach helps to make sharper choices in policy and implementation. The multitude of objectives, actions, and involved parties in the case of the NLCS means that it's easy to lose sight of the bigger picture. The **integral assessment** between the different action lines has been challenging, partly due to limited insight into causal relationships and the additionality of the NLCS (since some actions were already underway). This is further complicated by the confidentiality of some actions, as well as the tension between central steering and existing reporting and accountability lines. With a view to the **effectiveness of implementation and (public) accountability**, this poses a potential risk in addressing complex societal issues such as cybersecurity.

This research fits into the growing awareness among policy staff to think early about the objectives, logic, and measurability of performances when developing policy. It may not be beneficial for all policy efforts and programs to set up as intensive a measurement, monitoring, and evaluation trajectory as with the NLCS. However, even drawing a simple overview of the intended efforts, actions, performances, objectives, and effects can help in making **better policy choices** and structuring accountability. The philosophy from this study and the available tools, such as those from the Toolbox for Policy Evaluations (Toolbox Beleidsevaluaties), can be a valuable source of inspiration in this regard.

Dialogic innovatie & interactie
Hooghiemstraplein 33
3514 AX Utrecht
030-215 05 80
www.dialogic.nl