Visiting address
Turfmarkt 147
2511 DP The Hague

Postal address
Postbus 20011
2500 EA The Hague

I www.cybersecurityraad.nl
T 070 751 5333 (secretariat)
E info@cybersecurityraad.nl

Ministry of Justice and Security
Attn. Ms D. Yeşilgöz-Zegerius
Postbus 20301
2500 EH The Hague

Date
15 May 2023

Subject
CSR Advisory letter on Governance of the Cyber Security Council

Your Excellency,

On 1 July 2011, the Cyber Security Council (hereinafter the Council) was established by the Minister of Security and Justice, becoming a national and independent advisory body to the government composed of high-ranking representatives of public and private organisations and the scientific community (the so-called *triple helix*). The Council is committed at the strategic level to strengthening cyber security in the Netherlands and increasing cyber resilience, and as per its constituent act, the Council provides advice on the implementation and refinement of the Dutch Cyber Security Strategy (NLCS).

Over the past decade, the Council's activities and advice have taken on a broader scope and have thus become increasingly strategic in nature. As confirmed by the report of consulting firm Berenschot, which recently conducted the periodic Council review, this broad, independent advice is considered highly relevant by stakeholders, now that the reality in which we find ourselves appears to be becoming ever-more complex[1]. The Council therefore believes the continuation of its strategic advice on policy to be of paramount importance, which also implies that a significant part of the Council's activities will fall within the scope of the Advisory Bodies Framework Act. Crucially, the Council does not yet meet the necessary prerequisites outlined in this act.

As cyber security is a relatively new topic for both the government and private parties, the value of triple-helix dialogue on all strategic cyber security matters is universally recognised, as is also attested by the aforementioned review report.

Advice on Council governance

At several meetings in recent months, the Council has discussed possible options for amending Council governance based on shared principles that do justice to the Council's core values.

It is recommended that the current Council be discontinued and two bodies be set up instead:

- *The **'Cyber Security Advisory Board'** (hereinafter the Advisory Board), subject to the Framework Act, for strategic advice to the government on a variety of cyber security topics, themes and trends for the purpose of developing new policy. This also includes advice on legislation.*

[1] Report of the Second Cyber Security Council Review, Berenschot, February 2023

- *The **'Cyber Security Committee'** (hereinafter the Committee) which does not fall within the scope of the Framework Act, serving as a consultative body. In this Committee, high-level representatives of public, private and scientific parties will consult and coordinate on a wide range of cyber security topics (similar to the current Council) on an equal footing.*

Notes to this advice

The following is a brief explanation of the intended composition and remit of the two bodies, including their interaction, as well as a series of recommendations on the current Secretary's Office and the transition phase to the new governance structure.

Composition

Advisory Board. In line with the Framework Act, the Council recommends that the Advisory Board have authoritative members with ample cyber security and/or managerial expertise, experience and insight. Moreover, they should have an affinity with the major societal issues accompanying digitalisation. For advice issued by the Advisory Board to crystallise into new cyber security policy, it is essential that the members represent different fields of expertise, in addition to an independent chair.

Committee. The Council considers it essential that the committee be firmly anchored in the cyber security ecosystem in order to take up a prominent position therein, echoing the same triple-helix structure of the current Council, with similar members. At the same time, it is crucial that grassroots representation remains strong among private parties. To ensure continuity, it is proposed that current members of the Council initially go on to serve on the Committee. If necessary, the Committee could be supplemented with some missing departments or other government organisations (beyond the safety and security apparatus), as well as new private sectors. The aforementioned review report by consulting firm Berenschot provides guidelines for this process.

The effectiveness and impact of the Committee hinge on having members at the highest possible level, which is why the Council proposes that the Committee's bylaws stipulate that public sector members must be Directors-General (or similar officials) to guarantee sufficiently high-level representation. The Council recommends that this also be addressed in periodic reviews.

Remit

Because the Advisory Board will address new strategic policy topics, it will operate independently of the Committee in formulating, shaping and issuing its advice - in line with the Framework Act. However, the Committee will be able to make proposals to the Advisory Board on (potential) advisory topics. In addition, one of the Committee's core tasks will be to widely communicate views and recommendations on existing cyber security policies to public and private parties, with the aim of creating impact at the strategic level and improving the refinement and implementation of the Dutch Cybersecurity Strategy 2022-2028, as per the constituent act of the current Council[2].

While it is true that the two bodies have different objectives and operate in different frameworks, they should work alongside and with each other as effectively and efficiently as possible. The Committee could, for example, serve as a sounding board for the Advisory Board. This can be made possible by various forms of consultation and deliberation, such as an having the Advisory Board take a seat on the Committee in a purely non-contributing

[2] Examples could include proposals on information exchange to promote the digital resilience of organisations (see Pillar I of the NLCS) or proposals on reducing the shortage of cyber security personnel (see Pillar IV).

capacity. The interaction between the two new bodies will be considered in the follow-up to this proposal, and specific provisions on this interaction will be included in the bodies' bylaws.

Secretary's Office

The positioning and embedding of the Council's current Secretary's Office should be adapted to the new governance. For the sake of efficiency, the Council suggests having the current office facilitate both bodies and housing it centrally within the Ministry of Justice and Security's Administrative Department.

Transition phase

During the transition phase to the new governance structure, a legislative process for the Advisory Board will be undertaken by the Ministry of Justice and Security, in close consultation and coordination with the Ministry of the Interior and Kingdom Relations. In addition, a constituent act will have to be drafted for the Committee, while bylaws will have to be drawn up for both bodies. These documents will elaborate on the aforementioned issues of composition, remit and interaction. This phase should preferably be kept as short as possible.

The Council intends to continue to pursue its current CSR Multi-Annual Strategy 2022-2025[3] during the transition phase. The guiding principle remains that any advisory reports should - in accordance with the Council's constituent act - mainly concern the implementation and refinement of the NLCS. This is the case for the vast majority of the CSR Multi-Annual Strategy 2022-2025.

On behalf of the Cyber Security Council,

Theo Henrar
Acting co-chair CSR

Pieter-Jaap Aalbersberg
Co-chair CSR

[3] CSR Multi-Annual Strategy 2022-2025, June 2022