CSR Cyber Security Council

WORK PROGRAMME 2020-2021

Since its establishment in 2011, the Cyber Security Council – through its recommendations – has contributed to improving and strengthening the digital resilience of the Netherlands in order to realise an open, safe and prosperous society. The direction set out in the CSR Multiannual Strategy for 2018-2021 is clear and in the past two years, via the corresponding work programme, the council has maintained this focus on strengthening the digital resilience of Dutch society by providing recommendations and drafting guidelines. The new CSR Work Programme 2020-2021 continues to build on these initial results.

Based on the CSR Multiannual Strategy 2018-2021 and the results of the CSR Work Programme 2018-2019, the agenda for the coming period has now been set. Over the past two years, the council has once again dedicated itself to strengthening the digital resilience of the Netherlands. Digital resilience must become a natural part of our digital society. In practice, the pressure on our digital resilience appears to be growing. Cybercrime is increasing and the Cyber Security Assessment Netherlands 2019 indicates that social and economic disruption are imminent due to constant cyber threats. This perception is confirmed by reports of The Netherlands Scientific Council for government policy (WRR) and the Netherlands Court of Audit: we have not always structured basic matters as effectively as we think and greater supervision with regard to coordination, centralised standards, preparedness and adequate powers are needed.

It is the council's view that it is vital not to underestimate the gravity of the situation. Much is at stake and this notion should pervade every fibre of our society. Technological developments are increasing the levels of dependence, interconnection and the complexity of the issues (ethical and otherwise) we face. We depend heavily on foreign parties such as suppliers, manufacturers and service providers. The current approach is too fragmented and the pace must be accelerated. If we are to optimise our digital resilience, we must opt for an integral approach that extends to education and innovation as well. The speed at which we enhance our digital resilience and combat cybercrime must keep pace with technological developments. It is the council's goal to see the supervision of cooperation, long-term programming and sufficient funding of our digital resilience effectively established during the term of the next government. Agenda priorities for the next two years have been set based on this objective.

The council will furthermore keep a keen eye on current developments. The cyber landscape is in a constant state of flux. This never-ending rat race requires us to be vigilant and prepared for all possible scenarios at all times. This is no less true for the council itself. Since our agenda is determined by current events, this work programme, like the CSR Multiannual Strategy 2018-2021, will be a living document that the council will supplement and adapt as required in order to reflect current trends.

In 2020, the council will also issue a recommendation for tackling the major cybersecurity-related problems affecting Industrial Automation & Control Systems (IACS) and another recommendation regarding the deployment of new and existing technologies for the purposes of cybersecurity. Both recommendations are part of the CSR Work Programme 2018-2019. Where these and previous recommendations are concerned, the council will continue to monitor their impact and, when necessary, take steps to achieve the desired effect in the interest, for example, of cybersecurity in the education and business sectors[1] and the creation of an effective nationwide network of information exchanges[2]. The council will also remain involved in the launch and progress of the pilot on making data breach reports more widely available for research purposes[3].

SPECIFIC TOPICS

IIn the next two years, the council intends to address four specific topics. These topics link back to the strategic themes found in the CSR Multiannual Strategy 2018-2021: supervision and guidance, the growing dependence on digital and other technologies, and investment in cybersecurity. The council will also give substance to the request of the Minister of Justice and Security. He has asked the council to provide recommendations on the following:[4]

1. A broad evaluation of the effectiveness of the approach set out in the National Cybersecurity Agenda (NCSA)[5].
2. Necessary investments in cybersecurity in this context, to be made during the term of the new government[6].

The following are the topics in respect of which the council will develop products and recommendations over the 2020-2021 period:

1. Recommendation concerning focus of and approach to a broad evaluation of the National Cybersecurity Agenda (NCSA)
2. Recommendation for the comprehensive approach to digital resilience
3. Cybersecurity priorities
4. Digital autonomy and digital resilience

All topics will serve to strengthen the digital resilience of the Netherlands and guide the agenda set by the council. Depending on the topic, further exploration will take place through subcommittees.

1. Recommendation concerning focus of and approach to a broad evaluation of the National Cybersecurity Agenda (NCSA)

In 2018, the government established the NCSA under the responsibility of the National Coordinator for Security and Counterterrorism (NCTV) in cooperation with various parties. The NCSA can be viewed as an update to the 2013 National Cybersecurity Strategy 2, 'From awareness to competency'. The council made various contributions to the creation of the NCSA, including the publication of the Verhagen advisory report, 'The economic and social need for more cybersecurity: Keeping "dry feet" in the digital era'[7].

Commissioned by the National Coordinator for Security and Counterterrorism the Dutch Research and Documentation Centre (WODC) will complete a broad evaluation of the National Cyber Security Agenda (NCSA). Following the request of the Minister of Justice and Security the council will provide the WODC a recommendation concerning the focus of and approach to a broad evaluation of the NCSA and also inform the Minister of Justice and Security. The council looks forward to the results of the broad evaluation of the NCSA in a timely manner. These results will be used to provide the Minister of Justice and Security a response to the broad evaluation of the NCSA.

2. Recommendation for the comprehensive approach to digital resilience

Despite the many steps taken at both the national and EU level to increase digital resilience, cybersecurity has yet to become a self-evident component of our digital society. Cohesion, the ability to act decisively, speed and the preservation of our knowledge position continue to require our attention. We need a vision for a comprehensive approach to digital resilience to ensure effective digital defences, now and in the future. Such a comprehensive approach to digital resilience of our society must take into account the risk of digital social disruption in conjunction with the increase in cybercrime and the growing dependencies in our digital society. As such, detecting, prosecuting and thwarting digital criminality are important components of a broad approach to increasing cybersecurity in the Netherlands. One important piece of

advice from the aforementioned Verhagen report concerns the necessity for supervision and guidance with regard to cybersecurity. Verhagen recommends appointing a commissioner for cybersecurity. Apart from the limited coordinating role played by the Minister of Justice and Security, this recommendation was not adopted. Certain aspects, such as innovation and education, are beyond the scope of the Minister's authority. The council will therefore provide a recommendation for the comprehensive approach to digital resilience focusing ensuring effective coordination and a programmatic long-term approach, including the associated financial resources. In so doing, the council will be able to respond to the request made by the minister of Justice and Security to provide a recommendation on the necessary investments in cybersecurity to be made during the term of the new government. This recommendation focuses in particular on the next reign (2021 – 2025). The council will also publish a declaration of urgency with the urgent call to all political parties to ensure that cybersecurity issues feature prominently in their election programmes. A subcommittee comprehensive approach to digital resilience to guide this process will be established.

3. Cybersecurity priorities

The council's vision that the speed of our joint efforts to enhance digital resilience is insufficient. The strengthening of digital resilience and the prevention of cybercrime must more effectively keep pace with technological developments. The government cannot achieve this alone: doing so will require efforts from all of us, those in the public and private sectors and those in the scientific community. In response to the rapidly changing nature of technology and the digital threat, the council will publish the cyber-related priorities for the Netherlands in 2020-2021 and adjust these each year to ensure the priorities remain aligned to the current situation. In this way, the council wants to instil focus with regard to the digital resilience of society and accelerate the pace of efforts in this area. Subcommittee(s) will be established to guide this process.

4. Digital autonomy and digital resilience

The ever increasing digitalisation of our society and the use of digital means can, in addition to benefits, entail (digital) dependencies. Every day our dependency on digital products and services of large foreign suppliers is growing strong which causes an increasing pressure on our digital autonomy. Foreign states can influence the degree of (in)security of our products and services supporting vital processes in Dutch society. As this dependence continues to grow, so does the importance of cybersecurity. After all, our national and economic security are in part dependent on this. Conscious and realistic choices must be made in the field of digital autonomy to take full advantage of the benefits the digitalisation offers.

Therefore the council is commissioning research into the various cyber-related aspects of digital autonomy. The goal is to advise the government (and through the government, the business community) with regard to forecasts, consequences and perspectives for action aimed at safeguarding our national autonomy with regard to digital resilience. In addition to the positioning of the Netherlands, the research will focus on the European aspects of this topic as well. The council will establish a subcommittee on Digital Autonomy to guide this process.

1 CSR Recommendation 2015, No. 1, 'Recommendation on Cybersecurity in the education and business sectors'

2 CSR Recommendation 2017, No. 2, 'Towards a nationwide network of information exchanges, advice on information sharing in the field of cybersecurity and cybercrime'

3 CSR Recommendation 2020, No. 1, 'Recommendation on making data breach reports more widely available for research purposes'

4 Letter of request NCTV, recommendation regarding NCSA evaluation and investment by the new government, dated 4 March 2020

5 Letter accompanying the National Cybersecurity Agenda (NCSA), Parliamentary paper 26643-536

6 General Consultation Report on Cybersecurity, 30 October 2019, Parliamentary paper 26643-650

7 'The economic and social need for more cybersecurity: Keeping "dry feet" in the digital era', Herna Verhagen, 2016

RESULTS

Recommendation concerning focus of and approach to a broad evaluation of the National Cybersecurity Agenda (NCSA)

The council will:

- advise the Dutch Research and Documentation Centre (WODC) on its focus and approach for the investigation regarding the broad evaluation of the NCSA.
- provide a response on the broad evaluation of the NCSA.

Recommendation for the comprehensive approach to digital resilience

The council will:

- provide a recommendation for the comprehensive approach to digital resilience focusing ensuring effective coordination and a programmatic long-term approach, including the associated financial resources.
- offer a declaration of urgency to to political parties with the urgent call to ensure that cybersecurity issues feature prominently in their election programmes.

Cybersecurity priorities

The council will:

- publish the cyber-related priorities for the Netherlands and adjust these each year to ensure the priorities remain aligned to the current situation. In this way, the council wants to instil focus with regard to the digital resilience of society and accelerate the pace of efforts in this area.

Digital autonomy and digital resilience

The council will:

- based on research, issue a recommendation for safeguarding the national autonomy with regard to digital resilience.

CSR Cyber Security Council