CSR Cyber Secur ty Council

2018-2019 WORK PROGRAMME

In the CSR Multi-annual strategy, the council has clearly set out the areas it will focus on over the next four years. The objective of the council is to publish an average of three recommendations each year. The council has a wide range of methods at its disposal ('standard' recommendations, guidelines, discussions and meetings), which it employs in a considered manner. In addition to this, the individual members will engage public and other organisations in discussions at boardroom level and the council will enhance the impact of its recommendations by launching a range of activities, such as the National Cybersecurity Summer School (NCS3).

The CSR Multiannual Strategy 2018-2021 will be used to set the 2018-2019 agenda. The topics derive from the strategic themes as specified in the multiannual strategy. These are:

1. Supervision and guidance
2. Growing dependence on digital and other technologies
3. Enforcement and monitoring
4. New technologies

Specific topics

Led by the strategic themes, the council will concentrate on five specific topics over the next two years. The topics link back to the strategic themes of supervision and guidance, growing dependence on digital and other technologies and new technologies. All topics will serve to strengthen cybersecurity in the Netherlands and guide the agenda set by the council. Depending on the topic, further exploration will take place through subcommittees.

The following are the topics in respect of which the council will develop a range of products and recommendations over the 2018-2019 period:

1. National Cyber Security Agenda (NCSA)
2. New technologies
3. Data breach reporting obligation
4. Industrial Automation & Control Systems (IACS)
5. Evaluation of the Verhagen report: 'The economic and social need for more cybersecurity, Keeping "dry feet" in the digital era'

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. Since our agenda is determined by current events, our work programme, much like our multiannual strategy, will be a living document that we will supplement and adapt as required in order to reflect current trends.

1. National Cyber Security Agenda (NCSA)

In its coalition agreement 'Confidence in the Future' the government has set out its intention to establish an ambitious cybersecurity agenda, the objectives of which include standards for Internet-of-Things devices, software liability provisions, strengthening of the National Cyber Security Centre (CCSC), fostering cybersecurity research and improvement of public information campaigns. The National Coordinator for Counterterrorism and Security (NCTV) will, in collaboration with various actors, be responsible for incorporating these objectives in the National Cyber Security Agenda (NCSA). The NCSA can be regarded as an updated version of the most recent Cyber Security Strategy II, dating from 2013. The NCSA must help to ensure that the Netherlands can continue to function as a secure, open and prosperous society and that our country remains a frontrunner in the area of digitalisation. The NCSA will be published in the spring of 2018. The CSR will assist in the development of the agenda by fulfilling an advisory role. The council will work to amalgamate the various agendas – including National Cyber Security Strategy 2.0 - From awareness to capability (Ministry of Justice and Security), Digital Agenda - Innovation, trust, acceleration (Ministry for Economic Affairs and Climate Policy), International Cyber Strategy - Building digital bridges (Ministry of Foreign Affairs) and Defence Cyber Strategy (Ministry of Defence) – and establish an integrated vision supporting the NCSA.

2. New technologies

The coming years will see a surge in the deployment of new technologies and data streams, including robotics, biometrics, the Internet of Things, artificial intelligence, quantum computing and big data. The opportunities for deploying new technologies and data streams can make a positive contribution to the digital resilience of the Netherlands and the ability to capitalise on opportunities for a secure digital economy. To this end, the council will commission scientific research into the possible deployment of new technologies in connection with cybersecurity. The council will use this study to prepare a recommendation on how new technologies can be used to increase the level of cybersecurity.

3. Data breach reporting obligation

The data breach reporting obligation has been in force since 1 January 2016. This reporting obligation requires organisations (both business and government agencies) to report any serious data breaches directly to the Dutch Data Protection Authority (AP). Under specific circumstances they are also obliged to notify the data breach to data subjects (the individuals whose personal details are involved in the leak). Although the details of individual reported data breaches are confidential in

the Netherlands, the AP is still able to provide general information on the number of reports within individual sectors.
The General Data Protection Regulation (GDPR) will take effect on 25 May 2018. This privacy law will apply throughout the European Union (EU) and will replace the Dutch Data Protection Act (Wbp). Amongst other things, the GDPR will strengthen and extend privacy rights, impose additional responsibilities on organisations and ensure all European data protection authorities have the same powers, including the power to impose penalties up to 20 million euros.
The council wishes to commission research into the impact of public reporting of data breaches within the frameworks and possibilities provided under the data breach reporting obligation and the GDPR. The public disclosure of data breaches could have a positive impact on cybersecurity. One possible outcome is that information could become available on the policy effects of specific measures. However, the public disclosure of reports could also compromise the basic right to privacy.

4. Industrial Automation & Control Systems (IACS)

More and more physical objects are being connected to the digital infrastructure. The main focus here is on ICT. Little priority is given to Industrial Automation & Control Systems (IACS), although it is predominantly these systems that are used to support the Dutch infrastructure. This means IACS have a crucial role to play when it comes to protecting our critical infrastructures. Industrial control systems, such as ICS or SCADA, have a life that extends well beyond that of IT equipment. IT equipment typically has a write-off period of between three and five years, whereas IACS equipment is commonly in use for a period of fifteen to twenty years. The key consideration in the development of IACS is not cybersecurity but functionality. Targeted disruption of critical sectors could take the form of sabotage or the exploitation of vulnerabilities in IACS and could lead to economic losses and social disruption.
The council wishes to commission research into the key cybersecurity challenges in relation to IACS and issue a recommendation on how these challenges might be tackled.

5. Evaluation of the Verhagen report

At the request of the CSR, Ms Herna Verhagen LLM, CEO of PostNL, carried out an independent review of the state of cybersecurity in the Netherlands. The advisory report titled ‘The economic and social need for more cybersecurity, Keeping "dry feet" in the digital era' was presented to Prime Minister Mark Rutte and VNO-NCW chairman Hans de Boer on 6 October 2016. The recommendations in the report relate to the role of the government, the role of the private sector, the collaboration between them as well as digital skills.
The council wishes to determine the extent to which the recommendations of Ms Verhagen were followed up and move the recommendations in the report forward in order to enhance their impact.

RESULTS

National Cyber Security Agenda (NCSA)

The council will:

- draw up a recommendation for setting the course of the NCSA based on an integrated vision.

New technologies

The council will:

- draw up a research-based recommendation on how new technologies can be used to benefit cybersecurity.

Obligation to report data breaches

The council will:

- draw up a research-based recommendation on whether data breaches should be reported publicly in the Netherlands.

Industrial Automation & Control Systems (IACS)

The council will:

- draw up research-based recommendations on tackling the main cybersecurity issues of IACS.

Evaluation of the Verhagen report

The council will:

- evaluate the main impacts of the Verhagen report.

CSR Cyber Security Council