CSR Cyber Security Raad

DECLARATION OF URGENCY

7 August 2023

Additional efforts to advance cyber resilience needed to foster digital security and seize economic opportunities

Unrelenting threats, incidents and vulnerabilities put pressure on our country

The Netherlands benefits greatly from its highly digitalised society, but the rapid advancement of technological developments such as (generative) Artificial Intelligence (AI) and quantum technology has also sparked critical cyber resilience issues. In addition to the vast opportunities these technologies bring to our economy, widespread digitalisation can also create vulnerabilities and unwanted dependencies if insufficient attention is paid to cyber security. Relationships within the digital domain are becoming increasingly complex and the consequences for our freedom, security and economic revenue model can be momentous, as recent ransomware attacks on leading companies and institutions have shown. The security of industrial systems is also coming under increasing pressure, and more and more attention must be paid to combating the whole gamut of cybercrime Geopolitical developments are also further compromising our digital security and autonomy, which is why the Cyber Security Council (hereinafter the Council) would exhort the incoming government to step up its commitment to cyber security and increase investments. In doing so, it should focus on driving cooperation, reinforcing our digital autonomy and maintaining our knowledge position, and strengthening education.

The above is confirmed by the 2023 Cyber Security Assessment of The Netherlands (CSBN). The European war between Russia and Ukraine has demonstrated once more how state actors employ cyber-attacks to achieve their geopolitical goals, with the digital threats to Dutch government organisations, companies and knowledge institutes also continuing unabated. Another risk, though one of a different nature, is that state actors are trying to collect data from companies and citizens on a large scale, which they can use for their own benefit. The CSBN warns that cybercrime is an attractive revenue model, wreaking havoc on citizens, organisations and government agencies, and malicious actors have fully embraced novel technological developments such as generative AI in the process.

In 2021, to support the cabinet formation process, the Council issued an advisory report on a 'Comprehensive approach to cyber resilience', providing insight into how the Netherlands can get its cyber resilience up to par.

The aggregate outlay needed for the recommended measures amounted to €833 million over a four-year period, consisting of almost €600 million in structural funding and about €200 million for 2024 alone. Only part of the Council's advice was adopted in the previous coalition agreement, and the budget committed to increasing cyber resilience was significantly lower than recommended, with less than half of the investments proposed by the Council materialising on a structural basis.

Under the previous government, the Netherlands and Europe became increasingly aware that cyber security is a key prerequisite for secure digitalisation and that cyber security policy should be based on public values such as privacy, security and digital autonomy. Both nationally and at European level, promising initiatives have been taken to tighten requirements, strengthen oversight of (government) organisations, improve the exchange of information and make products and services safer. Cyber resilience requires our constant, unwavering attention: not only are there still vulnerabilities that need to be fixed, but malicious actors are also persistently devising new ways to penetrate systems. Bringing and keeping our cyber resilience up to par is no mean feat and will require both additional attention and the investments previously proposed by the Council. Implementation of European laws and regulations in particular should be a priority, which will affect various levels of the national and regional government, as well as organisations big and small. Moreover, it will prove essential to equip implementing bodies in the cyber domain with appropriate, robust legal frameworks.

The Council believes that the following issues in particular merit additional attention and investment:

1. Diligently driving collaboration

The above shows that the cyber resilience of the Netherlands is still at risk in key areas. This is a risk we simply cannot afford to take. In order to pave the way for secure continued digitalisation, ***collaboration must be driven across domains***, with cyber security, digital autonomy and combating cybercrime serving both as key components and necessary preconditions. This starts with a national strategy, countering departmental compartmentalisation and the realisation that cyber resilience is an executive matter: the highest-ranking political-administrative actors should bear responsibility. The Dutch Cyber Security Strategy (NLCS) was published in autumn 2022 alongside the Digital Economy Strategy and Working Agenda for Value-Driven Digitisation. The Council contributed to the NLCS and broadly endorses the objectives and actions it contains.

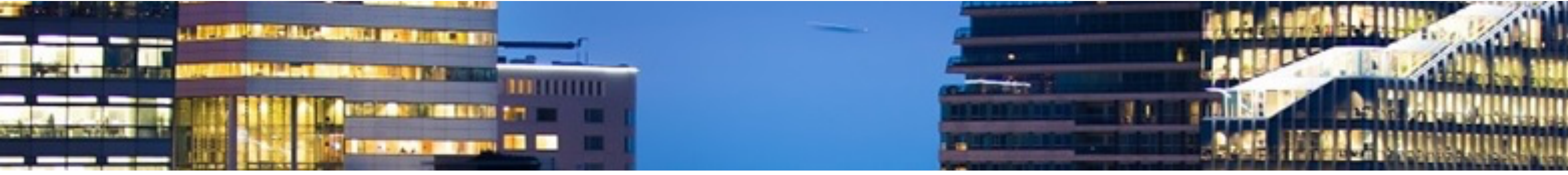
The new government should commit to driving the joint implementation of the strategy, while maintaining focus and responding to novel developments through public-private partnerships. Joint implementation is also highly relevant for provinces, municipalities and water boards, whose policies are also based on national strategy-making. At the operational level, the tendency to work with value chains means that organisations are highly dependent on one another and that many systems are intertwined. Careful attention should be paid to our IT infrastructure and industrial systems, such as those used in the energy sector and in flood defences, bridges and locks.

2. Strengthening digital autonomy

Given the increase in overall dependency, including our reliance on large tech companies, decisions on safeguarding our digital autonomy must be entrusted to the ***highest political and administrative levels***. Reinforcing the national cloud policy is a prime example, and while this will require European cooperation, the Netherlands can play a leading role based on a comprehensive vision of digitalisation that will also give a much-needed boost to our cyber resilience. Achieving digital autonomy will also require targeted innovation by the government and industry alike.

3. Safeguarding the country's knowledge position and strengthening education

Finally, measures to increase our cyber resilience rely on sufficient cyber security knowledge across the full breadth of society, including a healthy and well-equipped research and innovation ecosystem, ***along with additional public-private investment opportunities***. The shortage of suitably qualified cyber security specialists is becoming an increasingly pressing issue and influx into relevant degree programmes is lagging behind. It is also important to boost the cyber awareness of the general population, which starts with paying more attention ***digital literacy*** (including digital safety awareness) in primary and secondary education, given the ongoing technologisation of this domain and in anticipation of a comprehensive review of the curriculum.



With a view to the urgency of the cyber resilience issue, the Council calls on you to include in your manifesto the necessary plans as outlined above. The structural budget of around €200 million per year (from 2024 onwards), as previously recommended by the Council, will be necessary over the next four years for the various ministries to enable safe & secure digitalisation with public-private scientific cooperation. This is the only way to prevent unnecessary incidents and keep our society digitally secure.

Naturally, we are more than willing to go into more detail where necessary.

The members of the Cyber Security Council,

Private sector

Mr Th.J. (Theo) Henrar LLM
(acting co-chair)
Chair of FME (business association for the technology industry), CSR member on behalf of FME

Ms C. (Claudia) de Andrade-de Wit MA
CIO, Digital & IT director for the Port of Rotterdam, CSR member on behalf of CIO Platform

Mr J. (Joost) de Bruin MA
CEO of Ordina Netherlands,
CSR member on behalf of NLdigital

Ms S.C. (Sylvia) van Es LLM
President of Philips Netherlands,
CSR member on behalf of VNO-NCW

Mr J. (Joost) Farwerck LLM
CEO and Chair of the Executive Board of KPN,
CSR member on behalf of critical infrastructure

Ms T. (Tineke) Netelenbos
Chair of the ECP Platform for the Information Society, CSR member on behalf of ECP, the Platform for the Information Society

Mr S.J.A. (Steven) van Rijswijk
CEO of ING and board member of the Dutch Banking Association, CSR member on behalf of the financial sector

Public sector

Mr P.J. (Pieter-Jaap) Aalbersberg EMPM
(co-chair)
National Coordinator for Security and Counterterrorism (NCTV)

Mr E.S.M. (Erik) Akerboom MPM
Director-General of the General Intelligence and Security Service (AIVD)

Vice-admiral B.G.F.M. (Boudewijn) Boots
Acting Chief of the Netherlands Defence Staff at the Ministry of Defence

Mr M.P. (Michiel) Boots LLM
Director-General for Economy and Digitalisation at the Ministry of Economic Affairs and Climate Policy

Ms E. (Eva) Heijblom MSc
Director-General for Public Administration at the Ministry of the Interior and Kingdom Relations

Mr H.P. (Henk) van Essen LLM
National Police Chief

Mr A.R.E. (Guus) Schram LLM
Procurator General and deputy chair of the Board of Procurators General

Scientific sector

Prof. B. (Bibi) van den Berg
Professor of Cyber Security Governance affiliated with the Institute of Security and Global Affairs at Leiden University

Prof. E.M.L. (Lokke) Moerel LLM
Senior Of Counsel at Morrison & Foerster LLP, professor at Tilburg University