Visiting address
Turfmarkt 147
2511 DP The Hague

Postal address
PO Box 20011
2500 EA The Hague

I www.cybersecurityraad.nl
T +31 (0)70 751 5333 (secretariat)
E info@cybersecurityraad.nl

Ministry of the Interior and Kingdom Relations
Attn: Ms A.C. van Huffelen
PO Box 20011
2500 EA The Hague

Date
25 July 2024

Subject
Informative letter from the Cyber Security Council on strengthening education and developing knowledge

Your Excellency,

During your visit last 15 June to the Cyber Security Council ('the Council'), we discussed various topics, including the shortage of cyber security specialists and the need to retain and enhance cyber security knowledge in the Netherlands. You asked the Council for clarification on this pressing topic. The Council explores the various causes of the shortage in this letter, including the mismatch between supply and demand, emerging developments in the field, the increasing scarcity of lecturers, a lack of direction and challenges with knowledge migration.

The Council stresses the need for coordinated action to address key obstacles, such as remodelling training courses and countering the current brain drain. In this letter, it appeals to all directly involved ministries, educational institutions and the business sector to assist in this regard. Given the seriousness and scale of the problem, central government leadership is also needed.

Background

The Netherlands has a high level of digitalisation. While this contributes significantly to our economic business model, it also entails certain inherent risks. The Netherlands has relatively extensive infrastructure, for example in the transport sector, which is digitally vulnerable. It also has critical hydraulic engineering works and the Amsterdam Internet Exchange (AMS-IX), one of the largest internet hubs in the world. Keeping these environments running properly and securely requires much high-level expertise.

Tightness across the entire labour market puts increasing pressure on the available cyber security expertise. New developments in artificial intelligence (AI), internet security and quantum technology, coupled with rising cybercrime and threats from state actors, continue to drive the need for various types of cyber security professionals. According to Cybercrime Magazine, the global shortage will reach 3.5 million by 2025[1]. Meanwhile, the risks of potential cyber attacks are unprecedented: the cost of cybercrime could reach $10.5 trillion worldwide by 2025[2].

Shortage of specialists

[1] Cybersecurity Jobs Report: 3.5 Million Unfilled Positions In 2025 (cybersecurityventures.com)
[2] Cybercrime To Cost The World $10.5 Trillion Annually By 2025 (cybersecurityventures.com)

The Council addressed the growing shortage of cyber security professionals as far back as 2015, specifically calling for more coherence in cyber security initiatives in education and the business sector[3]. Studies and reports from other leading institutes have also been warning of the shortage for several years[4]. Since then, the demand for cyber security specialists has exploded, while the development of Dutch cyber security education lags significantly behind.

The Council sees a growing cyber-skills gap, which is now starting to pose a security risk in its own right. Although the absolute number of cyber security specialists in the Netherlands has increased in recent years, it remains the same as a percentage of the total workforce. According to international cyber security organisation ISC2's Cyber Workforce Study[5], the workforce gap for cyber security in the Netherlands for 2022 is estimated at 21.5%. This gap makes the Netherlands score poorly compared to countries such as France, Spain, the UK and the US.

As in many other sectors in the Netherlands, the shortage of cyber security specialists is a major concern. Both government agencies and businesses are feeling the strain, as the country has significant ambitions for secure digitalisation. As a result, an important precondition for implementing the various government strategies in this area, including the National Cyber Security Strategy (NLCS) and your 'Value-Driven Digitalisation' Work Agenda, cannot be properly met.

Causes of the shortage

Several phases of research have been completed in the Netherlands in recent years on (i) what types of cyber security specialists companies need (roles), (ii) which competences and skills are associated with these roles, and (iii) what specific shortages exist. The National Cyber Security Strategy (NLCS) therefore pays due attention to the cyber security labour market under Pillar IV.

The Talent for Technology Platform is currently conducting a comprehensive additional study on behalf of the Ministry of Economic Affairs and Climate Policy. This ought to provide a more complete picture of the current scale of the shortage, the different types of expertise required, and the evolving offering of cyber security education in both the public and commercial sectors. These insights can help to continue developing education. The results of the study are expected in the first quarter of 2024. In anticipation of this, the Council notes that the following causes of the shortage still exist:

1. **Mismatch of supply and demand**
   This cause remains problematic. Cyber security has recently evolved from a technical subject to a multidisciplinary and even interdisciplinary field, requiring many different skills and competences. The differing profiles of specialists[6] also illustrate this, with senior staff in particular needing to fulfil a variety of profiles. This cross-disciplinary knowledge and expertise is often not available in a single training institution. Meanwhile, the fast-growing offering of commercial parties appears extremely diverse, fragmented and of unclear quality.

[3] CSR Advisory Document 'Cybersecurity in onderwijs en bedrijfsleven' (Cyber security in education and business) – Cyber Security Council, November 2015 and CSR Advisory Document 'Integrale aanpak cyberweerbaarheid' (Integrated approach to cyber resilience) – Cyber Security Council – April 2021
[4] 'Arbeidsmarkt voor Cyber Security Professionals' (Labour Market for Cyber Security Professionals), study commissioned by the Ministry of Security and Justice's Research and Documentation Centre (WODC), Platform Opleiding, Onderwijs en Organisatie B.V. (PLATO), Leiden University, December 2014
[5] See page 8 of Cyber Workforce Study, 2022, Cybersecurity Workforce Study (isc2.org)
[6] For an overview, see the European Cybersecurity Skills Framework – User Manual
European Cybersecurity Skills Framework (ECSF) - User Manual — ENISA (europa.eu)

2. **Developments in the field of expertise**

Important practical knowledge about cyber security, such as risk management, information sharing, incident response and new legislation, is being developed primarily in the private and public organisations themselves. This knowledge is not readily available at training institutes. As the exchange of new experiences and practical knowledge among the business sector, regulators and universities is not yet well established, the quality of the educational offering lags behind. This applies both to training new cyber security talent across the education spectrum (from intermediate and higher vocational education to universities), and to upskilling workers already working in the cyber security field or retraining workers from other sectors.

3. **Shortage of lecturers**

There are not enough qualified trainers available to develop cyber security education and train talent. More specifically, there are too few professors who can devote sufficient time to teaching and development, and the number of senior lecturers is hardly increasing. Businesses now often train new graduate employees themselves and retrain experienced staff where necessary. While the private sector is willing to assist training institutions with their expertise, as previously advised by the Council[3], this also does not result in the required volumes.

4. **Current lack of direction**

Various human capital agendas, plans of attack and a national growth fund proposal have now been launched, often in public-private partnerships. These initiatives mainly address the shortage of ICT and other technical workers and focus, for example, on stimulating interest in science subjects in secondary schools. But they are not specifically designed to meet the growing demand for cyber security specialists or are not sufficiently scalable to a national level. Moreover, the envisaged success of initiatives for the tech/ICT sector may suppress the potential for more cyber security workers. Lastly, the Ministry of Education, Culture and Science (OC&W) also does not specifically oversee the development of cyber security education, but focuses on general measures for STEM education, combined with creating more digital literacy.

5. **Knowledge migration challenges**

Knowledge immigration to the Netherlands or outsourcing of organisational units abroad is often mentioned as a solution to shortages in technical/ICT professions. But movements such as these pose additional risks in terms of autonomy and knowledge security. The Advisory Council for Science, Technology and Innovation (AWTI) also warned against this earlier this year in an advisory report[7].

Although knowledge migration is still urgently needed, it is unlikely to provide a definitive solution to the shortage of cyber security specialists. The Council sees three main reasons for this:

- Dutch talent is already repeatedly poached by neighbouring countries, partly because of the global shortage.

[7] 'Kennis in conflict, veiligheid en vrijheid in balans' (Knowledge in conflict, security and freedom in the balance), Advisory Council for Science, Technology and Innovation (AWTI), November 2022

- Limited career prospects, heavy workloads and poor funding in the research environment[8] make it difficult to attract top researchers from abroad to Dutch research universities and universities of applied sciences.
- Foreign students, researchers and other cyber security specialists who come to the Netherlands often have no direct ties to the country, and it is likely that they will also seek employment elsewhere after a while.

Note: There is talk of partly reintroducing Dutch as a primary language at universities. This will compound the challenges for cyber security education, which is international in scope and largely English-speaking. Many of the existing lecturers and researchers already have a foreign background and there will be no Dutch replacements for them.

Potential solutions

The cyber security skills shortage will persist for the foreseeable future and cannot be solved by a single intervention. Several Council members (public, private and scientific sectors) are discussing this with various stakeholders to highlight the urgency and discuss possible solutions. The Council sees the following options:

1. **Pressing ahead with research findings and existing education initiatives**
   The results of the various studies must lead to targeted action and investment. Only then will future educational development be able to gather momentum in the form and on the scale needed to better match supply and demand (cause 1). The multidisciplinary nature of cyber security, both in training new talent and in retraining and upskilling, must be front and centre in this regard. Existing bottom-up initiatives for high-quality cyber security education and training need to be made scalable. Examples include:

   - Successfully launching dual university of applied sciences degree programmes, combining cyber security education and work placements.
   - Designing new cyber security courses at universities. These courses, taught by senior cyber security practitioners from both government and the business sector, focus on upskilling staff already working in the field.
   - Providing cyber security education to students by having companies partner with universities to develop specific courses.

2. **Remodelling courses**
   Educational institutions must better align the content of their courses with developments in the field (cause 2). The current form of educational development is generally unsuited to this, and this also cannot be expected of general course designers. Specific expertise is required to develop this training in partnership with companies and governments (including regulators). The aim is to develop training modules, test them in pilots and roll them out. Management or supervisory boards of the relevant institutions should also encourage such transformation.

   Learning loops to develop new best practices could be considered to respond quickly to changes in the field. Another option is to set up dedicated cyber security labs, bringing together representatives from

[8] These factors also hamper other forms of knowledge migration. For example, there is very little interest among sector workers to return to research universities and universities of applied sciences later in their careers, although this could reduce other causes such as limited interaction with companies.

education, business and the public sector, including regulators. Several regional centres funded by the public and private sectors are already being developed for this purpose.

3. **Dedicated appointment of lecturers**
   The Council recommends appointing dedicated lecturers and professors at institutes of intermediate and higher vocational education and universities who, in addition to cyber security research, wish to make a name for themselves by developing successful cyber security courses. Together, they will be tasked with developing and delivering comprehensive cyber security education, drawing on their own areas of expertise and research, with an accompanying financial incentive.

   This should create close interdepartmental and interinstitutional cooperation. These lecturers would be judged by their employers primarily on their personal contribution to interinstitutional and other educational development. Again, it is essential to seek private cooperation, for example through sectoral associations, in order to recruit additional lecturers (cause 3). These lecturers can also play an important role in the cyber security labs mentioned in point 2.

4. **Coordinated implementation of the actions**
   The shortages are now too great for any one party, sector or region to solve alone. Besides more money, coordinated direction of existing initiatives and targeted actions to strengthen cyber security training programmes (cause 4) are needed. In line with the NLCS objectives in this area, the ministries directly involved need to work from their position of ownership with educational institutions and the business sector to overcome the current situation.

5. **Countering the brain drain**
   It is essential to keep existing lecturers on university and intermediate and higher vocational education courses engaged and interested, while conducting high-quality cyber security research and establishing the right links with the business sector. Apart from making employment conditions more attractive, this also requires improving the image of education and research[9]. This is the only way to improve the business climate for lecturers and researchers and to prevent a continued exodus abroad (or into our own business sector) (cause 5).

   Such additional measures are also needed to continue promoting knowledge migration: there is a pressing need to encourage foreign lecturers, researchers and students who have come to the Netherlands to stay. A key precondition for achieving this, and for preventing the current influx from diminishing further, is to maintain English as the language of instruction at universities.

This letter will also be sent to the Minister of Education, Culture and Science, with copies to the Ministers of Justice and Security, and Economic Affairs and Climate Policy.

Yours faithfully,
On behalf of the Cyber Security Council,

[9] A related image issue is that many companies see limited added value in having PhD candidates in-house, making entry into research and teaching even less attractive for recent graduates.

Pieter-Jaap Aalbersberg
CSR co-chair

Theo Henrar
Acting CSR co-chair