
NCSEA
National Cyber Security Education Agenda
dcypher

Preface

When it was founded, dcypher (the Dutch Cybersecurity Platform for Higher Education and Research) was given a specific assignment in the sphere of higher education. There are major challenges involved in providing a suitable, high-quality education in the field of cyber security. In an effort to get a better handle on this, dcypher has developed a range of activities over the past four years. One such activity was a working breakfast on cyber security educational programmes. This event, which was held on June 30, 2017, was staged jointly by dcypher and the Ministry of Justice and Security. It was prompted by the educational system's lack of focus on cyber security, as highlighted in a 2016 report entitled '*De economische en maatschappelijke noodzaak van meer cybersecurity - Nederland digitaal droge voeten*' (The economic and social necessity of increased cyber security - keeping the Netherlands' digital opponents at bay)[1].

Herna Verhagen (CEO of PostNL and author of this advisory report) was one of those who took part in that event. In an article for dcypher's 2018 Magazine,[2] she was asked to comment on the topics discussed during that working breakfast:
"I was struck by the sheer number of campaigns that are already underway in the areas of cyber security educational programmes and awareness. However, the landscape is certainly very fragmented: many of the players involved are unaware of each other's existence and of their respective initiatives. A joint plan could greatly augment these players' efforts. I favour the notion of the education authorities drawing up and implementing a joint education agenda. ***dcypher can play a part in this by encouraging and galvanizing collaboration and by forging links between individual initiatives****."*

That call has not gone unheard. dcypher has had countless conversations and has taken numerous initiatives. It has also forged links between various initiatives related to its assignment in the sphere of education, some of which have yet to be launched while others are already up and running. Together, these form a series of interventions, which are at the very heart of this National Cyber Security Education Agenda. Where possible, these interventions are linked together by means of logical interfaces.

Wouldn't it be great if, in five years' time, we were able to claim that: 'The Netherlands recognized the challenge and fulfilled the associated aspirations'.

Table of Contents

Reading Guide

This document can be broadly divided into three parts:

1. The first part starts by specifying the reasons for publishing this agenda, followed by background details and a description of the context. It will show what dcypher has learned, in the course of its work, about cyber security agenda-setting in higher education. This part defines the agenda's scope and target group. With the aid of an infographic, the Netherlands' quantitative and qualitative shortage of people with cyber security skills and an understanding of this field is then 'placed on the agenda'. In addition to cyber security experts, this concerns other professions that involve some aspects of cyber security. The current mismatch between supply (by higher education institutions) and demand (from the labour market) can only be resolved by formal collaboration between the educational, public, and private sectors. In this way, the first part acts as a prelude to what is to follow.
2. The second part consists of a list of interventions in cyber security educational programmes (including higher education programmes). This provides a summary of current events in various 'triple helix' collaborations. It also sets the scene for what needs to be done in the upcoming years by the educational, private, and public sectors if we are to achieve temporary and – ultimately – fixed, structural improvements. The interventions are classified into six main themes. Four of these themes ('enhance professionalism', 'teach', 'collaborate', and 'expand scope') relate to higher education, and are at the very heart of this agenda. The other two themes, 'make preparations' and 'trigger interest', largely relate to primary and secondary education, and to senior secondary vocational education and training. These include interventions that should be seen as preconditions for enrolment in (or progression to) higher education.

   N.B. The list of interventions is a 'dynamic' summary, which can evolve over time and as lessons are learned. It is not intended to be a roadmap. Furthermore, it is recommended that the prioritization and implementation of this entire range of interventions should be carefully managed.
3. Details of the full extent of dcypher's assignment in the sphere of higher education are set out in an annex. This includes a summary of dcypher's activities in the area of higher education, spanning the period from 2016 to 2020. In these three parts, dcypher describes how it has acquitted itself with regard to the assignment in the sphere of higher education that it was given in 2016. This document concludes with a list of the abbreviations used and a reference list.

The challenge

With the increasing digitization of society, there is a growing need for people with knowledge and expertise in the field of digital security. Our dependence on IT requires everyone to possess a basic knowledge of this topic, and to be digitally resilient. In addition, people's education in this field must start at an early age. There is a need for training in cyber security at all levels and in all fields of study.[3]

A matter of urgency

Developments in the area of digitization are coming thick and fast. Indeed, this field has become part and parcel of the very fabric of our society. We are training (or retraining) people to competently and efficiently address the security aspects of this development. In many areas (technology, social sciences, and humanities), however, this effort is falling far short of what is required, both in terms of numbers (quantitative) and in terms of knowledge levels (qualitative). This has led to a labour-market mismatch between the demand for cyber security expertise and the available supply. This is not limited to technical areas alone. It's impact is also being felt in organizational, administrative, legal, economic, and ethical terms. Indeed, this situation was the very reason for publishing this agenda.

Not a day goes by without someone being adversely impacted by poorly functioning, insecure technology or by the insecure use of technology. This can have a wide range of impacts (economic, social, community-based, technical, legal, and political). Professional criminals and state actors pose a growing threat in the cyber domain. Indeed, their attacks are becoming ever more sophisticated and complex. As long ago as 2012, it was estimated that the damage caused to Dutch society by cybercrime amounted to at least 10 billion euros per annum. At the time, this involved activities such as industrial espionage, fraud, extortion, and phishing.[4] However, the situation in 2020 has become much more complex and urgent.


prijslijst
Team Hangout Hogeschool
CTC
Coca-Cola
Nutella
Ferrero
Ferrero Rocher
Duc d'O
Penotti
Lipton
Coca-Cola

dcypher and cyber security agenda-setting in higher education

In addition to its research role, dcypher (the Dutch Cybersecurity Platform for Higher Education and Research) was given a specific assignment in the sphere of higher education. This is reflected by the name of this platform. In its 2016 long-term policy plan, dcypher formulated its vision as follows: *With regard to cyber security, the Netherlands positions itself as a country that achieves scientific excellence in this area, that offers top-quality education in the field (including in higher education), that uses knowledge (including academic knowledge) and expertise deriving from research activities to benefit the innovative capacity of the public and private sectors, and that produces top-quality highly skilled professionals for these very sectors.*

The dcypher platform has been tasked with setting the agenda for – and facilitating – research and training in the area of cyber security (at the scientific and applied levels). dcypher also coordinates efforts to forge links within the knowledge and innovation chain. When it published the NCSRA-III[5] in 2018, dcypher was building on a tradition of bottom-up agenda-setting for Dutch cyber security research that dates back to 2007. When it comes to cyber security agenda-setting in higher education, however, there is no such tradition on which to build. Accordingly, this education agenda can be regarded as an achievement that **fulfils the task of setting the agenda for cyber security in higher education**. However, higher education does not exist in isolation. Accordingly, a conscious effort has been made to forge a link with its foundations, i.e. primary education, secondary education, and senior secondary vocational education and training.

In addition to an NCSRA, there is also an NCSEA

It is important to emphasize the interdependence of research and education in the field of cyber security. The fruits of research conducted within the framework of the NCSRA are disseminated through various media. Knowledge dissemination initially occurs within the very knowledge institutions in which that new knowledge was developed. This knowledge seeps through into educational curriculums, such as those of university Master's degree programmes. This process involves an intra-university multiplier. It is often the case that the knowledge obtained in a single PhD project is ultimately disseminated among hundreds of Master's students.

The interweaving of education and research is a strength, but it is now coming under pressure.
One of the strengths of the Dutch higher education system is the relationship between teaching and research (Finance, 2014; Royal Netherlands Academy of Arts and Sciences (KNAW), 2019).
This helps students in the Netherlands to develop an inquisitive attitude. It also teaches them to think creatively and encourages them to explore new avenues.
Research also delivers substantive improvements to teaching activities, as recent insights and innovations become integrated into curriculums.
> Strategische agenda hoger onderwijs en onderzoek (Strategic agenda for higher education and research), Ministry of Education, Culture and Science, December 2019[6]

Following consultations with those working in the field and with dcypher's Advisory Board, we arrived at an agenda that essentially consists of a **series of interventions** that bring new and existing initiatives together and forge links between them. Interventions in this context are defined as a planned **change activity**, or a whole series of such activities. The goal of these activities is to mitigate the qualitative and quantitative shortage of cyber (or cyber security) competences (i.e. knowledge and skills in the field of digital security).

As with the **research agenda**, we have decided to adopt a national approach and positioning for the **higher education agenda**. One feature of the latter agenda is that it intersects with top sectors (including economic sectors) and various Dutch National Research Agenda (NWA) routes. This agenda can also be regarded as a partial implementation of the top-sector-related Human Capital Agendas (HCAs). After all, every one of the top sectors involves cyber security, to some extent.
In their 2020 - 2023 Human Capital Roadmap,[7] the top sectors indicate a desire to strengthen their cooperative activities with one another and with other partners in the field of Human Capital[I].

The dcypher higher education agenda has been dubbed **NCSEA**, which stands for the **National Cyber Security Education Agenda**. This name bears a striking similarity to another dcypher agenda, the NCSRA, and that is certainly no coincidence. However, this agenda's objective and approach are quite different. The NCSEA focuses on the labour-market mismatch between the demand for graduates who are familiar with cyber security and the available supply, in both quantitative and qualitative terms. On the demand side, we are not confining ourselves to the cyber security profession alone (the experts). We are also exploring any fields in which a familiarity with cyber security is becoming increasingly important. On the supply side, the focus is very much on the graduates emerging from institutions of higher education.

I. The term 'Human Capital' refers to the competences, knowledge, social skills, and personality traits that enable people to create value.

Scope and target group

As previously stated, the focus of this agenda is the higher education system (universities of applied sciences or traditional universities) in the Netherlands. The goal is to produce cyber security professionals in both the numbers and quality required, while also making those in allied fields more conversant with cyber security.
Efforts to resolve the mismatch on the labour market include 'Lifelong learning',[II] which, as a result, also appears on this agenda. Workers are becoming increasingly aware that, in a rapidly changing world, they need to supplement their Master's degree with refresher training after a number of years. This is certainly applicable to the field of cyber security in particular. Numerous commercially available short courses and certificates have, of course, been developed to meet this demand. However, there is also a rising trend for working people to sign up for all types of postgraduate programmes (ranging from modular and online offerings to complete part-time courses) at universities of applied sciences or traditional universities. There is also a growing demand and aspiration for 'Lifelong learning' in the boardrooms of Dutch higher education institutions.
One important consideration concerns the opportunities for progression from an institution for senior secondary vocational education and training to a university of applied sciences.
The ability to hit the further education targets is conditional on making the primary and secondary education systems more conversant with cyber security, as part of a package of digital skills (or basic skills).

The goal of the interventions described later in this agenda is to create a balance between the labour market's need for sufficient numbers of qualified personnel with cyber security competences and the numbers of graduates emerging from institutions of higher education.

Those who (potentially at least) will be required to implement these interventions make up this agenda's primary target group.
Policymakers can also be seen as part of the target group. Many interventions are aimed at cooperation between institutions of higher education, companies, government bodies, and professional organizations (within educational institutions, companies, and government bodies). Together, these make up the triple helix.

'Educational institutions have a responsibility to provide educational programmes that match the demands of the labour market. Accordingly, it makes no sense for them to impose intake restrictions on the numbers of students being admitted to programmes in fields where there are severe shortages on the labour market. However, the institutions do not bear sole responsibility for this situation. Employers can also do their bit to help make jobs in the sector more attractive to potential employees.'

> Strategische agenda hoger onderwijs en onderzoek (Strategic agenda for higher education and research), Ministry of Education, Culture and Science, December 2019

II This is sometimes referred to as: 'Lifelong development'.

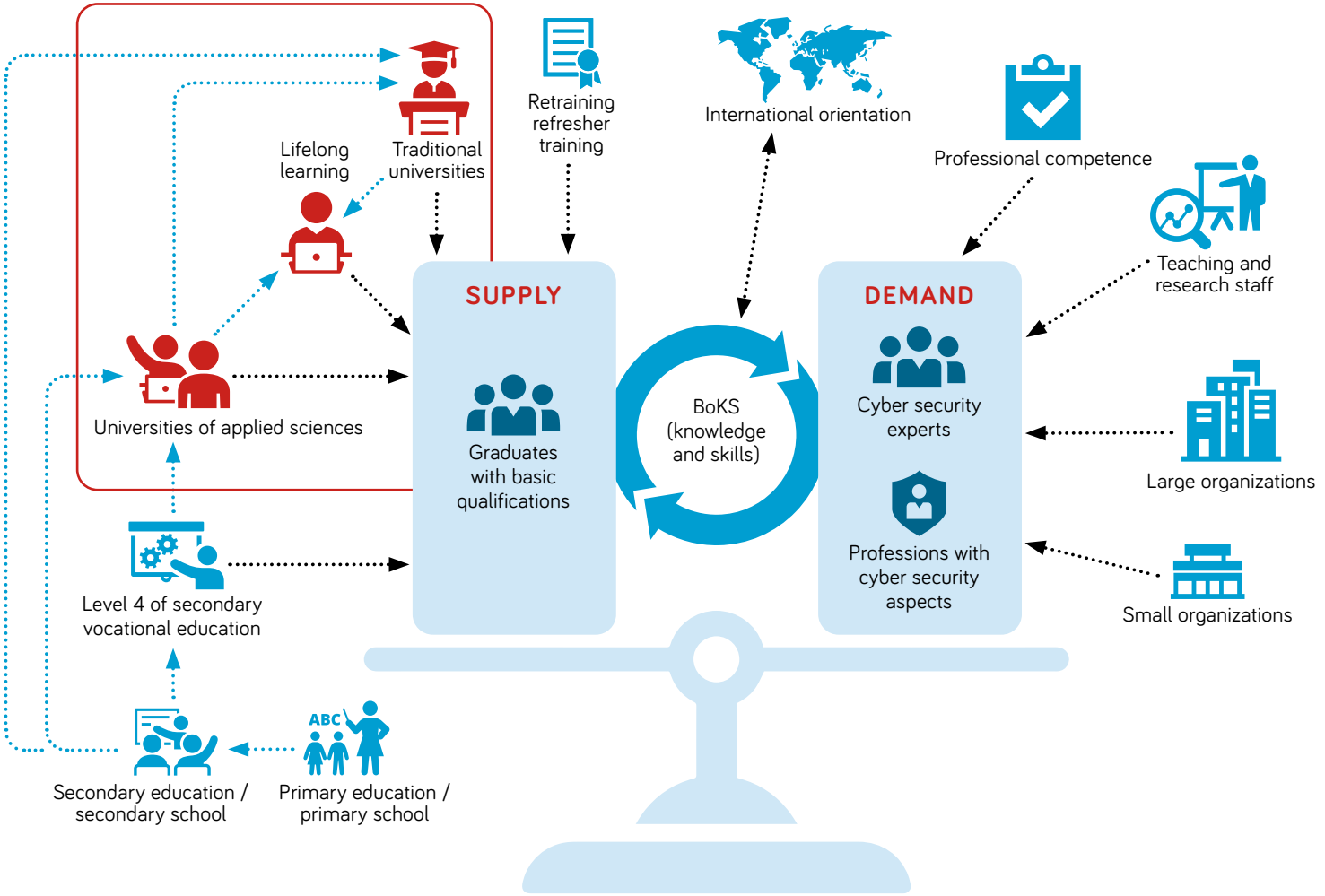
Balance between the labour market and the educational system

To compare the labour market's demand for cyber security professionals with the supply or numbers of graduates emerging from the country's educational system, dcypher first completed a survey of cyber security programmes at Dutch institutions of higher education. It has now posted the results of this survey on its website.[8]

A survey among stakeholders in the educational, public, and private sectors, concerning the need (or needs) of the labour market has confirmed that there is an increasing shortage (both in qualitative and quantitative terms) of knowledge and expertise in the field of cyber security.[9] Aside from specialist cyber security expertise, this issue also involves basic skills and cyber security knowledge related to other fields. As a result, organizations are insufficiently conversant with the field of cyber security, which makes them less resilient to current digital threats. Thus it is becoming increasingly important for the workforce to develop a more professional approach to cyber security. Individual professions or fields must have enough people with the requisite level of knowledge and skill in the field of cyber security. When tackling the mismatch (in quantitative and qualitative terms) between the supply and demand of cyber security competencies (knowledge and skills), a model is used to balance these two factors. This model (depicted as an infographic in Figure 1) provides an overview of the entire arena.

The various interventions (which exhibit varying degrees of coherence, at least potentially) help to achieve an ideal balance between supply and demand.

Figure 1. The quantitative and qualitative balance between study programmes and labour-market demand, in terms of cyber security knowledge and skills



Explanation of the infographic:

1. The current level of market demand for cyber security knowledge and skills (professional competence) is dictated by the labour market (public and private organizations, both small and large, including educational and knowledge institutions with the associated need for teaching and research staff).
2. The Dutch government sees the basic qualification (on the supply side) as the minimum level of education that people require if they are to have any real chance of obtaining lasting skilled work in the Netherlands.
3. In a qualitative sense, the match between study programmes and the demands of the market is largely a matter of knowledge and skills. These are the basic qualifications that match the specified professional competence requirements. In professional practice, these qualifications are further refined into specific knowledge and skills, tailored to individual jobs. Example: From September 2020 onwards, the curriculum for the senior secondary vocational education and training 'IT management' programme (level 4), which has been approved by the Ministry of Education, Culture and Science, will meet the basic qualifications for the post of IT Security Specialist.[10] In quantitative terms, this is all about obtaining sufficient numbers of graduates.
4. Pupils in primary and secondary schools are taught how to operate securely, responsibly, and independently in the digital domain (21st century skills).[11]
5. The part of the figure that is outlined in red concerns higher education (universities of applied sciences and traditional universities, as well as pathways for the graduates of these institutions, see below).
6. Institutions of higher education (universities of applied sciences and traditional universities) produce sufficient numbers of graduates with the necessary basic qualifications for professional competence.[12] The curriculum includes sufficient scope for meeting the labour market's specific needs for knowledge and skills (as the institution sees fit), at regional level, and for the development of academic competences (which are part and parcel of a rapidly developing research field).
7. Retraining workers and providing refresher training programmes influences the quality and quantity of lateral-entry staff.
8. Retraining and refresher training programmes at the level of higher education are referred to as 'Lifelong learning', continuous professional education, and pathways for the graduates of universities of applied sciences and traditional universities. For instance, professionals taking a post-Master's programme in cyber security often end up in the cyber security sector, even though they had previously worked in other sectors. At present, the numbers involved are quite small. However, they are expected to increase over the upcoming years. Compare this to the 'lateral-entry staff' who switched from all kinds of other professions to IT in the 1990s and in the first decade of the new millennium.

National government policy

Dutch government policy anticipated the current mismatch.[13] Details of the support for implementing this policy are specified in the 2020-2023 Knowledge and Innovation Agenda for Key Technologies[14] and the Mission-driven top sector and innovation policy[15]. The policy addresses the qualitative and quantitative mismatch. The NCSEA:

a. was developed in connection with, or as further refinement of, intentions (or policy intentions) arising from the NCSA and the strategies of the Ministries of Education, Culture and Science; Defence; and Economic Affairs and Climate Policy;
b. is in keeping with Dutch aspirations in the field of cyber security;
c. endorses the importance of 'Lifelong Learning'. The role of higher education in this regard will become increasingly important in the upcoming years. This is certainly true of the field of cyber security, where people's knowledge and capacities quickly become obsolete, while new challenges, new technologies, new methodologies and theories are continually emerging;
d. takes developments outside the country into account, as national borders are of little or no significance in the cyber world.

International

Increasing digitization, cyber security incidents, legislation, and the development of IT have triggered a growing worldwide demand for cyber security professionals. However, the extent, scale, and nature of the shortages cannot be determined with any accuracy.[16] With regard to the debate concerning the role of the education system in preparing students for the labour market, there is a need for consensus regarding the knowledge and skills (BoKS = Body of Knowledge and Skills) required and about who is to take on which roles in developing such knowledge and skills. Employers, too, have a part to play here. Governments in other countries have mainly invested in higher education, research, and encouraging organizations to enable their staff to pursue personal development. Australia, France, the UK, and the US have also developed certification schemes for national cyber security training programmes.[17]

We need to expand cooperation (within Europe too) and to join forces. This will enable us to contribute effectively to the regional community and economy, and to earn a place among global leaders in education and research.
Universities of applied sciences should be given the opportunity to strengthen their applied research.

> **Strategische agenda hoger onderwijs en onderzoek (Strategic agenda for higher education and research), Ministry of Education, Culture and Science, December 2019**

ECSO's European Human Resources Network for Cyber Task Force creates awareness among decision makers (private companies, regional/local administrations, national/EU administrations) about the need to develop education and training measures which will address the demand in the cyber security field. The target is to increase public and private spending in the relevant field, to enhance the potential of the educational programmes and training courses that recruiters are seeking, both in the private and public sectors. Our focus is the professionalization of cyber security professionals.

> **EHR4CYBER Task Force [18]**

Implementation of this agenda, subject to careful management

This agenda is action-oriented. Interventions have been defined that, when coherently implemented, will deliver improvements. Some interventions also have an impact when implemented individually. These interventions vary in terms of their size, duration, and complexity. The interventions involve the educational sector, government bodies, and companies. An action-oriented approach was adopted because:

a. the urgency of the problem is quite evident, as is the need to improve the situation;
b. a practical approach is needed, due to the constantly evolving nature of the threat assessment and to the need to keep pace with new knowledge;
c. little added value can be expected from new analyses (into the extent, scale, and nature of the shortages, for example), which can also delay and obstruct tangible and decisive action.

The nature of the interventions set out in this agenda may vary. There are interventions that:

- have an owner and are already in progress;
- have yet to be assigned an owner;
- will deliver results in the near future;
- require a long period of preparation and only deliver results in the longer-term future;
- can be launched in the near future, but which can also lead to structural improvements;
- are highly visible and can serve as an example, as well as being a driver for subsequent actions or interventions;
- demand commitment from the educational sector, with due regard for personal responsibility, scientific freedom, and the degree of autonomy.

Each intervention requires an owner/individual with ultimate responsibility, who must have a project goal and a project plan.
Individual interventions can have different owners (operations managers). One or more actors implement interventions, which can each involve one or more parties. Sooner or later, all interventions will help to improve the qualitative and quantitative balance between supply and demand.
The owners are expected to monitor their interventions, together with the actors. This involves periodically interpreting their intervention's effectiveness and results, and adjusting and/or recalibrating the goals and actions, as required. The idea behind getting actors to actively monitor the interventions and to adjust them where necessary is to motivate them to remain involved in the change process.

It is recommended that the implementation of every single implementation be subject to central, independent **management**. This will help to promote cohesion and collaboration, while preventing fragmentation. Management is also needed to determine whether the extent, scale, and nature of the shortages are trending towards the set goals. This involves monitoring the results (and interim results) of the interventions. It must also be clear how the ideal balance between cyber security supply and demand can be safeguarded, and which tools are needed to do the job. The institutionalization of this management role should be part of the 'master plan', as described below.

It will take several years to gather all of the knowledge generated by the implementation of this series of interventions. Part of this involves training talented young people. Accordingly, it will take about five years to implement (adjust and modify) this NCSEA.

List of interventions in cyber security programmes (including higher education programmes)

Individually or collectively (and coherently), the following interventions will help to create a situation in which institutions of higher education produce adequate numbers of graduates with the required skills and expertise in cyber security. These planned and targeted activities are undertaken by one or more actors, to achieve the set goal. The second column in the figure shown below lists current initiatives. The next two columns give details of new, short-term and long-term initiatives. Individual interventions – or clusters of interventions – can have different owners or operations managers. Gathering the interventions together at a single location, in a clear (and structured) way, serves to highlight their mutual cohesion and to facilitate coordination.

The description of each intervention includes a title and a goal, as well as details of the associated activities and of the intervention's added value or desired outcome. There are also brief explanatory notes, giving details of the intervention's status, and/or one or more examples.
Mention is also made of the organizations (actors) involved.

Figure 2. Thematic grouping, cohesion, and positioning of the interventions over time

Main theme	Already underway	Short term	Long term
1 **Make preparations** (primary & secondary education = PE / SE)	CS in PE / SE curriculum; CS in NLT profile	CS lessons taught by experts	CS in teacher training courses
2 **Trigger interest** (quantity)	CS summer school (or schools)	Explanatory details about professions	Strong image; Diversity
3 **Enhance professionalism** (CS experts)	Summary of programmes; Professorial platform	Lifelong learning; Curriculum guide	Certified programmes; Certified experts
4 **Lecturers** (CS programmes)	Partnerships in education	Matchmaking platform	Qualified CS lecturers
5 **Collaborate** (supply/demand)	Challenge the Cyber / ECSC		National; International
6 **Expand scope** (other fields)		CS BoKS per field	CS professional competence requirements

The interventions are classified into six main themes:

1. **Make preparations:** People have to start young if they are to develop the ability to operate digital infrastructure securely. Pupils in primary and secondary schools should be taught about digital security and privacy by teachers with an understanding of cyber security. As a short-term measure, cyber security experts could be involved in teaching classes and in developing lessons.
2. **Trigger interest:** When students have to decide on a course of study, a cyber security programme must be a realistic option. A positive image of the field, together with a clear idea of what it involves and of the associated career options, will attract more students. In the short term, efforts can be made to spark the interest of advanced students (from other fields) in cyber security.
3. **Enhance professionalism:** Employers, educational institutions, students, and experts all stand to benefit from a set of independently compiled professional competence requirements that are both uniform and transparent. Drawing on clear professional profiles[III] and on an internationally aligned Body of Knowledge and Skills (BoKS), educational institutions can design a suitable curriculum. This will deliver graduates who possess up-to-date knowledge and skills and who are competent experts in their chosen fields.
4. **Teach:** There is a need for additional qualified teachers with cyber security skills and an understanding of this field. As a short-term measure, cyber security experts could take on a knowledge-transfer role within the educational system. Over the longer term, we will need to train more qualified teachers.
5. **Collaborate:** Educational institutions and the labour market work hand-in-hand to manage supply and demand. This involves periodically monitoring the requirements, in terms of quality and quantity, and actively responding to them.
6. **Expand scope:** 'Expanding the scope' refers to professions that are not specifically related to cyber security. Each profession sets requirements with regard to the level of cyber security expertise required, which must be in keeping with the demands of professional practice.

Four themes, 'enhance professionalism', 'teach', 'collaborate', and 'expand scope', relate to higher education. The other two, 'make preparations' and 'trigger interest', mainly relate to primary and secondary education, and to senior secondary vocational education and training. These two themes should be seen as preconditions for enrolment in (and progression to) higher education. The 'summer school' intervention is an exception to this rule. Here, the aim is to induce higher education students to pursue a follow-up programme in cyber security.

III At this point, in the interests of clarity, we should clarify the difference between the terms 'professional profile' and 'job description'. A professional profile is effectively a formal description of a profession. It describes the mission, duties and responsibilities of practitioners in the relevant profession. In addition, it specifies the competences (knowledge and skills) that these practitioners are required to possess. A job description gives details of each employee's roles and responsibilities, and of the knowledge and skills they are required to possess. While the professional profile is not itself a job description, it can be included in a job description for specification purposes. On the other hand, it is also possible to compile a job description from several professional profiles, or even from a portion of a single professional profile.

Make preparations

Digital security - the basics

If security and privacy in the digital world are incorporated into primary and secondary education curriculums, young people will quickly become familiar with cyber security. Indeed, cyber security already features in secondary education, as a course of study. Thus there is a need for additional qualified teachers with cyber security skills and an understanding of this field in both primary and secondary schools. As a short-term measure, cyber security experts could take on a knowledge-transfer role within the educational system. For instance, they could develop teaching materials for use by primary and secondary school teachers. Over the longer term, new teacher training courses will have to be developed and current training courses adapted.

1.1. Cyber security in primary and secondary school curriculums	
Aim	It is already quite commonplace for children to start using digital tools at an early age. Each age group will be familiarized with the aspects of security and privacy in the digital world.
Activities	The theme of 'security and privacy in the digital world' will be incorporated into the digital literacy curriculums of upper and lower year groups in primary and secondary schools. The teaching materials involved will be developed and updated as necessary.
Added value	When the topics of digital security and privacy are taught as part of the curriculum, they will become a matter of course for young people. Cyber security skills and an understanding of this field are gradually gaining ground within society.
Explanation	1. In recent years, there has been a wide-ranging, national debate concerning a comprehensive review of the curriculums used in primary, secondary, and special education. See SLO[19]; 2. In 2019, curriculum.nu's nine development teams submitted their proposals to the Minister for Primary and Secondary Education and Media. Before the summer of 2020, the minister sent a letter to the House of Representatives concerning frameworks for the follow-up process's practical assignments. Experiments are already under way at schools. See also: curriculum.nu[20]

1.2. Cyber security as a component of the NLT elective subject in the upper year groups of senior general secondary education and pre-university education

Aim	Pupils in the upper year groups of senior general secondary education and pre-university education who have opted for the NLT (Nature, Life and Technology) profile will learn about cyber security as part of the Digital Technologies learning pathway.
Activities	Developing and teaching the Digital Technologies learning pathway, in the context of the NLT course, with cyber security as the overarching theme.
Added value	Explanatory details about individual professions are a central feature of many NLT modules. This involves transferring knowledge to a large group of pupils, while at the same time sparking their interest in the field of cyber security.
Explanation	1. NLT's examination programme is designed to establish frameworks. This avoids years spent waiting for the curriculum to be revised, or for examination programme committees to update the curriculum. The Talent for Technology Platform and the NLT Association[21] have set up a project to this end; 2. See CyBoK.org, Bringing Cyber To School: Integrating Cyber Security Into Secondary School Education.[22]

1.3. Cyber security experts teach pupils in primary and secondary schools about cyber security

Aim	Pupils in primary and secondary schools will learn about aspects of digital security and privacy that are appropriate to their age group.
Activities	1. Cyber security experts are trained in teaching skills and in how to master the teaching material that has been developed (based on curriculum.nu's learning goals for security and privacy in the digital world); 2. Cyber security experts work with primary and secondary school teachers to develop teaching materials that these teachers can use themselves. 3. Hack in the Class gives workshops at schools all over the country. These workshops are run by volunteers who feel that it is important for the younger generation to be trained in digital resilience.[23]
Added value	Children and young people develop cyber security skills and an understanding of this field that are appropriate to their age group. Such knowledge and skills are gradually gaining ground within society.
Explanation	A working group from the Platform for Information Security[24] (a professional association) has already made a great deal of progress in this area, and is currently pooling existing initiatives.

1.4. Training qualified primary and secondary school teachers in cyber security

Aim	Qualified primary and secondary school teachers will learn the necessary cyber security skills and will acquire an understanding of this field.
Activities	Cyber security will be included in the curriculums of standard teacher training courses and of upskilling programmes for qualified teachers.
Added value	With regard to teachers who have an understanding of security and privacy in the digital world, the topic will also be formally included in discussions with parents/guardians.
Explanation	The Centre of Expertise Cyber Security (CoECS) at The Hague University of Applied Sciences[25] is trialling the introduction of age-appropriate tools into the Primary School Teacher Training College (PABO) curriculum.

Trigger interest

2

Boost image and raise awareness

We need to develop a clear profile for this versatile field, which is still relatively young, and to highlight the associated career options. This will boost the numbers of student registrations. The young, talented people following these programmes will have a clear reason for selecting their course of study, as well as a clear picture of their future in the labour market.

2.1. Boosting interest in cyber security among advanced students	
Aim	To reach out to advanced students (i.e. those in the final year of their Bachelor's degree programme, or those nearing the end of their Master's degree programme) who have no prior, in-depth knowledge of cyber security, and spark their interest in the multidisciplinary nature of the field.
Activities	Holding summer schools, where students with an interest in cyber security but no in-depth knowledge of the subject can quickly become acquainted with both the technical and non-technical aspects of this field.
Added value	The participating students are presented with a broad overview of all cyber-security-related topics, in an effort to entice them to pursue careers in cyber security in the Netherlands. Accordingly, this is just one of the measures being implemented to mitigate shortages in the Dutch labour market.
Explanation	1. The annual National Cyber Security Summer School for advanced students in the Netherlands (NCS3; the brainchild of the Cyber Security Council) was staged by dcypher from 2016 to 2019; 2. Europol, NATO, Leiden University, EY, Dutch Innovation Factory, and The Hague Security Delta have jointly staged the annual International Cyber Security Summer School (ICSSS) for students and PhD candidates (from the Netherlands and elsewhere) since 2015.

2.2. Cyber security experts explain the nature of their job to school leavers	
Aim	To promote interest in cyber security programmes by explaining details of the field, its status, professional standards, and career options, etc. to upper year groups in senior general secondary education, pre-university education, and level 4 of secondary vocational education.
Activities	1. Developing teaching materials for upper year groups in senior general secondary education and pre-university education 2. Cyber security experts who are also trained instructors teach classes in secondary education and secondary vocational education. They cover a range of cyber security topics, as well as the content and impact of this work, and the available professional and training opportunities.
Added value	More potential students will be able to make a more informed choice when selecting their course of study. They will also be more highly motivated, thus there will be fewer dropouts.
Explanation	A working group from the Platform for Information Security (a professional association) has already made considerable progress in this area, and is currently pooling existing initiatives.

2.3. Boosting the image of the profession (and of the subject area)	
Aim	To create a clear profile of the field and to provide a good overview of the associated career paths and career options, as a way of motivating potential talent to enter the field of cyber security.
Activities	Defining professional associations, in conjunction with existing programmes aimed at inspiring entrants, professional image, career options, and the steps (or developmental steps) to be taken.
Added value	Promotes the influx of potential talent into cyber security programmes and sparks people's interest in cyber-security-related professions (in education and science, as well as in the public and private sectors).
Explanation	See also: 1. the Platform for Information Security's professional profiles (based on the EU e-CF standard EN-16234);[26] 2. Programme I – Partnership (collaboration between Central Government and the Higher Education sector);[27] 3. Economic Board Zuid Holland.[28]

2.4. Promote diversity in cyber security	
Aim	To ensure that the field of cyber security offers equal opportunities for talented individuals from many different backgrounds (age, gender, ethnicity, and culture), and that it has a reputation for diversity.
Activities	1. Current initiatives aimed at promoting diversity (in the Netherlands and elsewhere) are listed; 2. Diversity is a component of other interventions (such as 'Challenge the Cyber').
Added value	Latent potential is being tapped.
Explanation	VHTO (the Dutch national expert organization on girls/women and science/technology)[29] has staged effective interventions to encourage girls to develop their digital skills and to explore a future in Tech/IT, both at school and elsewhere. 'Girls Day' is a striking example of this.

3

Qualified talent for the cyber security labour market

It is not immediately clear what type of profile a capable information security officer or cyber security expert should have. This makes it difficult for educational institutions to design a suitable curriculum. When choosing a course of study, many students find it difficult to picture exactly what it is they want. Employers find it difficult to formulate realistic expectations for those who are just starting out in the profession. A widely supported and accepted Body of Knowledge and Skills (BoKS) can be a great help in this regard. Given the international nature of the field, it is essential for those involved to coordinate their efforts in this area. Any professionals who meet the requirements, in terms of education, experience, and professional ethics, must be able to achieve a level of professional competence that carries national (or international) accreditation.

3.1. Summary of cyber security programmes in the Netherlands	
Aim	To deliver a publicly accessible, updated summary of cyber security programmes in the Netherlands, which provides details of their content and composition.
Activities	1. The owner (or owners) of the data is identified and made accountable; 2. The summary compiled by dcypher in 2018 is updated annually, and expanded if necessary.
Added value	Talented individuals with potential are able to make more informed choices with regard to their course of study. In addition, employers can be more focused with regard to recruitment and selection, and there is a basis for exchanging details about the design of curriculums.
Explanation	Since 2018, dcypher has maintained and regularly updated the details of accredited educational programmes for Associate degrees, Bachelor's degrees, and Master's degrees at universities of applied sciences and traditional universities. This information is posted on dcypher's website.[30]

3.2. Using new knowledge from research (and applied research) in higher education	
Aim	To exchange good practices in applied research, cooperate in the allocation of research capacity, join forces in research proposals for applied cyber security research, and encourage staff to collaborate with university-based researchers. Using new knowledge in education.
Activities	At universities of applied sciences, professors of cyber security from all relevant fields sit on a professorial council/platform. Cyber security lecturer-researchers at traditional universities join forces to create a similar council.
Added value	Professorial research groups develop new knowledge as they pursue demand-driven research. Professors, researchers, lecturer-researchers, and PhDs explore current issues and developments in society and in professional practice. This ensures that educational programmes (Bachelor's and Master's) to stay up to date and relevant.
Explanation	dcypher has brought professors of cyber security from various universities of applied sciences and a range of different fields together to form a cyber security professorial cluster (in collaboration with the National Taskforce for Applied Research SIA (NRPO) and the national Practical ICT Research platform (PRIO)[31]).

3.3. Lifelong learning	
Aim	To offer additional knowledge and skills to professionals who are already working in the security (or cyber security) domain, and to retrain highly educated individuals (even those without a specifically IT background) for cyber-security-related jobs.
Activities	1. Develop programmes for training highly educated people with work experience, with or without a specifically IT/ cyber security background, for cyber-security-related jobs. (It should also be possible to offer IT staff refresher training programmes, where necessary. After all, it cannot be assumed that every computer science student is automatically an expert in security technology); 2. Further training of graduates from level 4 of secondary vocational education, by means of a cyber security sandwich course.
Added value	By facilitating 'Lifelong learning', educational institutions help to mitigate the mismatch on the labour market.
Explanation	Some examples of this are: 1. The Executive Master's programme in Cyber Security at Leiden University, the Delft University of Technology, and The Hague University of Applied Sciences;[32] 2. The Professional Master's programme in Cyber Security Engineering at The Hague University of Applied Sciences;[33] 3. Make IT Work[34] at the Amsterdam University of Applied Sciences and NHL Stenden University of Applied Sciences (in Leeuwarden) for highly educated individuals without a specifically IT background; and 4. Cloud IT Academy,[35] which offers paid jobs in 'cloud security' to secondary vocational education graduates in IT or Network Management. It also allows them to follow a sandwich course in Cyber Security & Cloud at HU University of Applied Sciences Utrecht.

3.4. Defining a cyber security curriculum guide	
Aim	To create a guide that sets out the main themes of a cyber security curriculum, and make it available to educational institutions (following the example set by the Canadian Centre for Cyber Security). This also makes it easier to coordinate curriculums (at institutions of secondary vocational education, universities of applied sciences, and traditional universities).
Activities	1. With the help of professional advisory committees, the main themes of the study programme are defined at national level (including ongoing learning pathways); 2. New and relevant insights from the domains of everyday practice and research are added, by means of periodic updates.
Added value	1. Provides a catalogue of the elements needed to construct a curriculum; 2. Serves as a national benchmark against which higher education institutions can assess their own programmes, classes, and curriculums; 3. In the longer term, this can deliver national training profiles, specifically designed to offer scope for differentiation (in line with regional developments); 4. Students progress more rapidly from level 4 of secondary vocational education to universities of applied sciences, and from universities of applied sciences to traditional universities.
Explanation	1. See: Joint Task Force on Cybersecurity Education, a manual for the design of cyber security curriculums;[36] 2. See the Canadian Government's Cyber Security Curriculum Guide.[37]

3.5. Certification of cyber security programmes	
Aim	To make it clear, both to students and employers, that study programmes instil students with specific competences (knowledge and skills) that meet the needs of the labour market.
Activities	1. The social partners agree on the required Body of Knowledge and Skills (BoKS); 2. Accredited educational programmes that meet the standards, that are certified, and that are recorded and updated in a register; 3. The periodic certification of cyber security programmes that meet the standards set out in the BoKS, in terms of knowledge and skills.
Added value	1. Establishment of the basic qualifications at institutions of secondary vocational education, universities of applied sciences, and traditional universities; 2. For employers, there is transparency about which programmes meet the criteria; 3. Students choose the right course of study.
Explanation	Bachelor's and Master's programmes in cyber security are certified by NCSC-UK and by GCHQ.[38]

3.6. Certification of cyber security experts	
Aim	To ensure that qualified experts who meet the educational requirements and the socially agreed professional competence requirements are acknowledged as such by the national and international labour markets.
Activities	The implementation of certification, based on a Body of Knowledge & Skills (BoKS), professional profiles and continuous professional development, including relevant knowledge derived from scientific and applied research.
Added value	1. There are clear, transparent, and uniform professional competence standards that are internationally comparable; 2. An expert's professional competence is readily demonstrable, and meets current requirements.
Explanation	1. Since 2014, the Platform for Information Security (a professional association) has published professional profiles that are widely accepted and that are based on international standards (EN-16234, ISO-27000);[39] 2. In the context of a public-private partnership, QIS has developed a certification system based on ISO/IEC 17024, the international standard for the certification of persons.

4

Qualified teachers

There is a need for additional qualified teachers with cyber security skills and an understanding of this field. In the short term, a coordinated operation can be established to enable cyber security experts to be made available for knowledge transfer in the educational system (including higher education). Over the longer term, additional qualified cyber security teachers will need to be trained.

4.1. Partnerships in education	
Aim	In terms of content, educational programmes will dovetail perfectly with professional practice in small and large organizations, as well as with the fields of education and research.
Activities	1. Cyber security experts from the business community and government bodies collaborate with the educational sector to develop and implement alternative teaching approaches, designed to incentivize the transfer and application of knowledge and skills; 2. The PRIO professorial platform augments the exchange of innovative practical applications.
Added value	Organizations play an active part in mitigating the shortage of teachers, while graduates enter the labour market with up-to-date knowledge and skills.
Explanation	For details, see examples such as the various types of cooperation between the business community and Fontys University of Applied Sciences (Partners in Education), The Hague University of Applied Sciences (Dutch Innovation Factory), and HU University of Applied Sciences Utrecht (Cloud IT Academy).[40]

4.2. Matchmaking platform for lecturers at universities of applied sciences and traditional universities	
Aim	To ensure that the educational programmes at universities of applied sciences and traditional universities have sufficient cyber security lecturers.
Activities	A platform is being established to match the educational sector's demand for teachers/lecturers with the supply of instructors (or visiting lecturers) from the business community/government bodies.
Added value	Greater numbers of students will be trained, by more motivated teachers. There will no longer be any intake restrictions due to teacher shortages.
Explanation	The Cyber Security Council has initiated discussions on this issue with the Ministry of Education, Culture and Science.[41]

4.3. Training qualified cyber security lecturers by providing expert knowledge	
Aim	To ensure that institutions of secondary vocational education, universities of applied sciences, and traditional universities have sufficient qualified lecturers to transfer the necessary (up-to-date) knowledge and skills to students.
Activities	1. The specific didactic and subject-related requirements for future cyber security lecturers at universities of applied sciences and traditional universities will be defined; 2. Based on this, a curriculum will be developed, together with the necessary teaching resources; 3. Upskilling programmes for qualified lecturers will be developed.
Added value	More than enough lecturers possess the knowledge and skills needed to present stimulating classes and to guide their students' development. This will enable educational programmes to deliver motivated and well-equipped entrants to the labour market.
Explanation	1. CyBoK (the Cyber Security Body of Knowledge[42]) is an open collection of university teaching materials to which universities throughout the world can contribute; 2. MOOCs (Massive Open Online Courses) such as those provided by the Delft University of Technology ('Cyber Security Economics') and the University of Twente ('Internet Security – Attack & Defence') make it possible to transfer knowledge to larger groups of students.

Collaborate

Educational institutions collaborate with the labour market

Consultations between educational institutions and the labour market (employers' umbrella organizations) create clarity (or greater clarity) about what is needed (qualitatively and quantitatively), in terms of properly prepared new entrants.

5.1. 'Challenge the Cyber' and participation in the ECSC competition between European states	
Aim	1. To access new cyber security talent, including young people (14-25 age group); 2. To inspire young people to pursue careers in cyber security; 3. To enhance the coordination of cyber security educational programmes between institutions of secondary vocational education, universities of applied sciences, and traditional universities, in conjunction with EU member states.
Activities	1. Staging the annual 'Challenge the Cyber' (CtC) event – a 'Capture The Flag' competition for young Dutch people with a talent for cyber security (secondary schools, institutions of secondary vocational education, universities of applied sciences, and traditional universities); 2. Staging an annual cyber security boot camp, spanning a period of several days, to train the most talented individuals in CtC, and to select the Dutch ECSC team; 3. Taking part in the annual European Cyber Security Challenge (ECSC), with a 10-strong team of highly talented individuals; 4. Staging activities for alumni, and engaging in networking.
Added value	This will promote the influx of talented young people into the field. In addition, efforts to coordinate with the European curriculum and to involve the educational sector and the business community in 'Challenge the Cyber' will help to mitigate the mismatch between supply and demand.
Explanation	'Challenge the Cyber' was first held in 2019. That pilot event, which was jointly staged by the National Cyber Security Centre of the Netherlands and dcypher, was repeated in 2020. This involved closer collaboration with students, lecturers, and cyber security experts from government bodies and the business community.

5.2. Cyber security – the balance between study programmes and labour market demand	
Aim	To achieve a quantitative and qualitative balance between the labour-market demand for cyber security experts and what the educational sector is able to supply.
Activities	1. At regional level, the supply and demand for cyber security experts will be coordinated within regional partnerships between the business community and educational institutions; 2. At national level, there will be a formal dialogue between umbrella organizations in the educational sector and social partners, to ensure that this balance can be maintained over the long term.
Added value	A flexible approach in which the existing, critical mismatch is resolved at regional level. At the same time, the resolution of any future issues will involve the use of a management role to balance supply and demand.
Explanation	1. This intervention will be prepared by an overseer; 2. The need/demand is related to the interests of society (both economic and in terms of social digital security). In many cases, this comes down to professional competence requirements defined by the umbrella organizations of various professions.

5.3. Coordinating with international developments	
Aim	To create education-related forums in which the Netherlands can contribute to the security of digital societies throughout the world.
Activities	1. There will be exchanges of knowledge about developments in the field of education and about the BoKS to be used; 2. Efforts will be made to coordinate with international programmes in the fields of cyber security research, knowledge and expertise, qualification, and certification.
Added value	Cyber security takes no account of national borders and continental divides. An understanding of – and coordination on – the content and level of education serves to promote the exchange of professionals and to enhance the security of the international digital society.
Explanation	1. EU programmes such as CEN/e-CF, Cybersecurity4Europe, ECSO, ENISA; 2. Cyber security skills on the UK labour market, based on CyBoK;[43] 3. NIST/ National Initiative for Cybersecurity Education - NICE;[44] 4. ANSSI France.[45]

Expand scope

Cyber security in other professions

Each profession sets its own requirements for cyber security, which are in line with the professional competence requirements of its own particular field. In the course of their studies, students acquire the requisite cyber security knowledge and skills for the field in question. Each profession keeps its own particular cyber security requirements up to date.

6.1. Identifying the cyber security knowledge and skills required in specific professions	
Aim	To ensure that the cyber security knowledge and skills required by individual professions are identified and brought up to date.
Activities	1. The cyber security knowledge and skills required by specific fields or individual professions will be identified and brought up to date; 2. The cyber security knowledge and skills required for a given profession or field will be included in the relevant educational curriculums.
Added value	New entrants to the labour market will possess the cyber-security-related knowledge and skills needed for their own particular field.
Explanation	1. Fontys ICT offers a cyber security minor for students from other fields of study; 2. Commencing in the 2021-2022 academic year, Leiden University will offer a cyber security minor for all LDE (Leiden University, Delft University of Technology, and Erasmus University Rotterdam) students studying technical and social science subjects; 3. The cyber security expert field is based on professional profiles and the accompanying BoKS.

6.2. Cyber security is an integral part of each individual profession's requirements for continuous development and professional competence	
Aim	To ensure that Dutch professionals' cyber security knowledge and skills are in line with the expectations, requirements and/or agreements regarding professional practice.
Activities	The professional competence requirements of trade associations, professional associations, and sector associations will specify the required level of education for cyber security. These associations will also ensure that cyber security is included in educational curriculums.
Added value	The working population of the Netherlands will become increasingly skilled in the field of digital security.
Explanation	The cyber security expert field is based on the professional competence requirements specified the QIS certification scheme (a public-private project, see PvIB.nl and references[11] and[12]).

Annex: Summary of dcypher's higher education activities

List of cyber security activities in higher education

For many years, the cyber security sector was very unsure about how effectively educational activities matched labour market demand, in terms of quality and quantity. In 2018, dcypher listed the range of cyber security programmes offered by higher education institutions. Here, the educational institutions in question specified the study load involved in their curriculum's cyber security topics. The full list is available at: https://www.dcypher.nl/onderwijs. Here you can download a detailed and updated profile of each educational programme. This helps students, educational institutions, and employers to understand what types of programmes are involved. The main findings are:

a. a total of twenty cyber security programmes are currently being offered by eighteen different educational institutions;
b. these consist of **fifteen** full-time programmes (ten Bachelor's, five Master's) and **five** part-time programmes (two Bachelor's, three Master's);
c. thirteen programmes focus on technology;
d. one programme focuses mainly on the way in which cyber security is organized, while another focuses on people/behaviour. Five programmes offer a mix of subjects.

A total of 394 students graduated from their cyber security programmes in 2018, 307 of whom had a technical profile. Most educational institutions experienced difficulty in finding the right lecturers, in sufficient numbers.

Cyber security professorial cluster

For many years, various traditional universities (universities of technology) have cooperated on educational programming in the area of cyber security. To create similar links between the programmes offered by universities of applied sciences, dcypher committed itself to creating a cyber security professorial council. As a result, cyber security professors from various universities of applied sciences and from a range of disciplines have formed a cyber security professorial cluster, in conjunction with the PRIO platform (Applied IT Research). Its goal is cooperation (in educational programming, curriculum development), the exchange of good practices and of lessons learned, and to get people to join forces in the field of applied cyber security research. In addition to introducing innovations from research, cyber security professors can formally incorporate newly acquired knowledge (including applied knowledge) into cybersecurity programmes. In addition to developments from everyday practice, this helps to keep educational programmes up to date and innovative.

Round Table meetings for cyber security programme staff (consultations with the profession)

Various Round Table meetings and educational sessions took place in the course of several symposia held by dcypher in the period from 2015 to 2017. The participants explored various topics and approaches in connection with a higher education agenda for cyber security.
A report entitled '*Digitaal Droge Voeten*' (Keeping digital opponents at bay), which addressed the issue of cyber security in education, prompted dcypher and the Ministry of Justice and Security to hold a Round Table meeting on June 30, 2017. They concluded that a focus on trust and security is needed if digitization is to achieve its full economic potential. Due to the highly fragmented nature of the cyber security landscape, many players are unaware of each other's initiatives. A jointly formulated plan would greatly augment these players' efforts. When institutions jointly draft an education agenda, this tends to promote collaboration while also forging links between different initiatives.

National Cyber Security Summer School

dcypher has been hosting the annual National Cyber Security Summer School (NCS3) since 2016.
The NCS3 is the brainchild of the Cyber Security Council (CSR). The goal is to introduce students to both the technical and non-technical aspects of

cyber security. The summer school is intended for advanced students, in any discipline, who may lack a detailed knowledge of cyber security but who are nevertheless sufficiently curious about the subject to shift the focus of their studies in that direction. Spanning a period of five consecutive days, the summer school gives students a basic understanding of this very broad field. Cyber security is 'demystified', and they are encouraged to further explore those aspects of cyber security that are related to their own individual fields. The NCS3's design features a 'triple helix' approach, involving knowledge institutions, companies, and government organizations. The NCS3 shines a light on the activities of the various sectors, and on their respective interests in this area. In 2019, dcypher evaluated the first four summer schools and submitted the resulting assessment report to the CSR.

Challenge the Cyber

'Challenge the Cyber' is a 'Capture The Flag' competition for 14 to 25-year-olds with a talent for cyber security. It offers them an opportunity to qualify for the European Cyber Security Challenge. Staging 'Challenge the Cyber' (CtC) involves a collaborative effort by students, educational institutions (secondary schools, institutions of secondary vocational education, universities of applied sciences, and traditional universities), government bodies, and private parties. The event is coordinated by dcypher and NCSC. In addition, talented individuals are trained in technical skills, soft skills, and ethical conduct, by means of a development programme based on the ECSC curriculum drawn up by the European Union Agency for Cybersecurity (ENISA). This approach facilitates the development of national and international communities of cyber security experts.[46]

Abbreviations used

ANSSI	Agence nationale de la sécurité des systèmes d'information
BoKS	Body of Knowledge and Skills
CoECS	Centre of Expertise Cyber Security
CSR	Cyber Security Council
CtC	Challenge the Cyber (dcypher/NCSC)
CyBoK	Cyber Security Body of Knowledge
dcypher	Dutch Cybersecurity Platform for Higher Education and Research
DIF	Dutch Innovation Factory
e-CF	e-Competence Framework
ECSC	European Cyber Security Challenge
ECSO	European Cyber Security Organisation
ENISA	European Union Agency for Cybersecurity
EHR4CYBER	European Human Resources Network for Cyber
GCHQ	Government Communications Headquarters (UK)
HCA	Human Capital Agenda
HSD	The Hague Security Delta
ICSSS	International Cyber Security Summer School
LDE	Leiden, Delft, Erasmus
MOOCs	Massive Open Online Courses
NCSA	National Cyber Security Agenda (J&V)
NCS3	National Cyber Security Summer School (dcypher/CSR)
NCSRA	National Cyber Security Research Agenda (dcypher)
NCSEA	National Cyber Security Education Agenda (dcypher)
NCSC	National Cyber Security Centre
NCTV	National Coordinator for Terrorism and Security
NLT	Nature, life and technology
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NRPO SIA	National Taskforce for Applied Research SIA
PO	Primary education / primary school
PRIO	Practical ICT Research platform
PvIB	Platform for Information Security
QIS	Qualification scheme for Information Security professionals
SLO	Netherlands institute for curriculum development
SOC	Security Operations Center
VO	Secondary education / secondary school

References

1 '*De economische en maatschappelijke noodzaak van meer cybersecurity - Nederland digitaal droge voeten*' (The economic and social necessity of increased cyber security - keeping the Netherlands' digital opponents at bay), 2016

2 '*Roep om Gezamenlijke Onderwijsagenda*' (A call for a Joint Education Agenda), dcypher 2018 Magazine https://www.dcypher.nl/sites/default/files/uploads/magazines/dcypher-magazine-nr2-nl/mobile/index.html#p=6

3 *Naar een open, veilig en welvarend digitaal Nederland* (Towards an open, secure and prosperous digital Netherlands) - CSR advisory report 2018, no.1, Cyber Security Council, 2018

4 https://www.computeridee.nl/nieuws/tno-cybercriminaliteit-kost-nederland-10-miljard/

5 National Cyber Security Research Agenda - NCSRA III, dcypher, June 2018

6 *Strategische agenda hoger onderwijs en onderzoek* (Strategic agenda for higher education and research), Ministry of Education, Culture and Science, December 2019

7
- Collectively rolling up our sleeves and getting started – the top sectors' 2020 - 2023 Human Capital Roadmap, November 2019
- Human Capital Agenda Security 2019-2022, The Hague Security Delta, 2019

8 Details of dcypher's summary of cyber security programmes in the Netherlands can be found at https://www.dcypher.nl/cybersecurity-opleidingen.

9
- *De arbeidsmarkt voor cybersecurity professionals en ICT'ers, Notitie Centraal Planbureau* (The labour market for cyber security professionals and IT professionals, CPB Netherlands Bureau for Economic Policy Analysis memorandum), 2018
- *Arbeidsmarktonderzoek ICT met topsectoren, Naar een digitaal vaardiger beroepsbevolking* (IT labour market survey among the top sectors, Towards a more digitally skilled workforce), Berenschot, 2019
- *Onderzoek arbeidsmarkt ICT met topsectoren* (IT labour market survey among the top sectors), CA-ICT, 2019
- *Samen aan de slag - Roadmap Human Capital 2020 - 2023 van de topsectoren* (Collectively rolling up our sleeves and getting started – the top sectors' 2020 - 2023 Human Capital Roadmap), November 2019

10
- Optional senior secondary vocational education and training module: Security in systems and networks 1 (K0400), Sectoral committee for IT and the creative industries, 2015
- Optional senior secondary vocational education and training module: Security in systems and networks 2 (K0444), Sectoral committee for IT and the creative industries, 2015
- Optional senior secondary vocational education and training module: Secure programming (K0501), Sectoral committee for IT and the creative industries, 2016
- Professional Profiles in Information Security, security 2.0, A basis for a uniform qualification, Platform for Information Security, 2017

11 21st century skills: see https://slo.nl/thema/meer/21e eeuwsevaardigheden/

12
- European e-Competence Framework, A common European Framework for ICT Professionals in all industry sectors, CEN Workshop Agreement (CWA) 16234-1, European Committee for Standardization (CEN)
- European ICT Professional Role Profiles, CWA part 4: Case Studies, CEN

13
- The Dutch Cyber Security Agenda (NCSA), The Netherlands digitally secure, Ministry of Justice and Security, 2018
- Dutch Digitization Strategy, Ministry of Economic Affairs and Climate, June 2018
- The Ministry of Defence's Cyber Strategy, Investing in digital capability for the Netherlands, Ministry of Defence, 2018

14 2020-2023 Knowledge and Innovation Agenda for Key Technologies, TKI HTSM (Top Consortium for Knowledge and Innovation/High Tech Systems and Materials) Foundation, 2019, https://www.hollandhightech.nl/sites/www.hollandhightech.nl/files/inline-files/20191015%20KIA-ST.pdf

15 The Ministry of Economic Affairs and Climate's Mission-driven top sector and innovation policy, April 2019

16
- Mind the Gap: The Cyber Security Skills Shortage and Public Policy Interventions, by Tommaso De Zan, Centre for Technology and Global Affairs, University of Oxford, 2019
- Australia, Estonia, France, Japan, South Korea, the Netherlands, Norway, Singapore, Sweden, Switzerland, the United Kingdom (UK), and the United States (US) *(countries that feature in the International Telecommunication Union's (ITU) top 20 countries in terms of the IT Development Index and the Global Cybersecurity Index)*

17 Cyber security skills development in the EU, ENISA, December 2019

18 https://www.ecs-org.eu/working-groups/wg5-education-awareness-training-cyber-ranges,

19 Curriculum in motion, 2017 - 2020 Strategic Agenda of the SLO (Netherlands institute for curriculum development)

20 Proposals for the content of future educational programmes, https://www.curriculum.nu/

21 https://betavak-nlt.nl/nl/p/vereniging-nlt/vereniging-nlt/

22 CyBoK.org, Bringing Cyber To School: Integrating Cyber Security Into Secondary School Education

23 The Hack in the Class Foundation, https://hackintheclass.nl/

24 Platform for Information Security, https://www.pvib.nl/

25 The Hague University of Applied Sciences' Centre of Expertise Cyber Security (CoECS), see https://www.dehaagsehogeschool.nl/onderzoek/kenniscentra/details/centre-of-expertise-cyber-security

26 EU e-CF standard EN-16234

27 Programme I – Partnership (collaboration between Central Government and the Higher Education sector) https://www.ubrijk.nl/i-partnerschap

28 Economic Board Zuid Holland, https://www.economicboardzuidholland.nl/projecten-hca/

29 VHTO (the Dutch national expert organization on girls/women and science/technology), https://www.vhto.nl/

30 List of accredited cyber security programmes in the Netherlands, Platform for Information Security's *Informatiebeveiliging* (Information Security) Magazine, edition 3, 2019

31 https://www.platformprio.nl/

32 https://www.csacademy.nl/educatie/masteropleidingen/executive-masteropleiding-cyber-security

33 https://www.dehaagsehogeschool.nl/opleidingen/masters/master-cyber-security-engineering

34 https://www.it-omscholing.nl/nl/

35 https://jobinthecloud.nl/

36 2017 Cyber security Curriculums. ACM_IEEE-CS. Curriculum Guidelines, December 2017

37 Cyber Security Curriculum Guide, A role-based guide for Training and Education providers, Government of Canada, 2019

38 https://www.ncsc.gov.uk/information/ncsc-certified-degrees

39 European ICT professional role profiles, part 4: CASE STUDIES, CEN ICT Skills Workshop, 2018

40
- https://www.piefontysict.nl/nl/
- https://www.dutchinnovationfactory.nl/
- https://jobinthecloud.nl/

41
- CSR Advisory letter on the cancellation of intake restrictions, Cyber Security Council, July 26, 2018
- CSR Minutes on mitigating teacher shortages, Cyber Security Council, 30 August 2018

42 CyBoK, Cyber Security Body of Knowledge, https://www.cybok.org,

43 Cyber security skills in the UK labour market 2020, Ipsos MORI, Department for Digital, Culture, Media & Sport (DCMS), 2020

44 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

45 https://www.ssi.gouv.fr/uploads/2015/05/anssi_annual_report_2018_en.pdf

46 Learning by hacking, the Platform for Information Security's *Informatiebeveiliging* (Information Security) Magazine, edition 1, 2020

Colophon

This is a dcypher publication. dcypher is a Dutch public-private agenda-setting platform for cyber security research and higher education.

Editorial team
Fred van Noord
Melanie Lemmen
Jan Piet Barthel

Production
Juul Brouwers

Design
Haagsblauw

Photography
Sjoerd van der Hucht
Shutterstock

This agenda was drawn up in consultation with stakeholders in higher education, government bodies, and businesses, and in consultation with members of dcypher's Advisory Board.

dcypher

dcypher's work is funded by the Ministries of Education, Culture and Science; Justice and Security; Economic Affairs and Climate; and Defence; and by the Dutch Research Council (NWO).

Rijksoverheid

NWO

31 March 2020, translated 18 September 2020


dcypher