

Human Capital Agenda Security

2019-2022



Human Capital Agenda Security

2019-2022

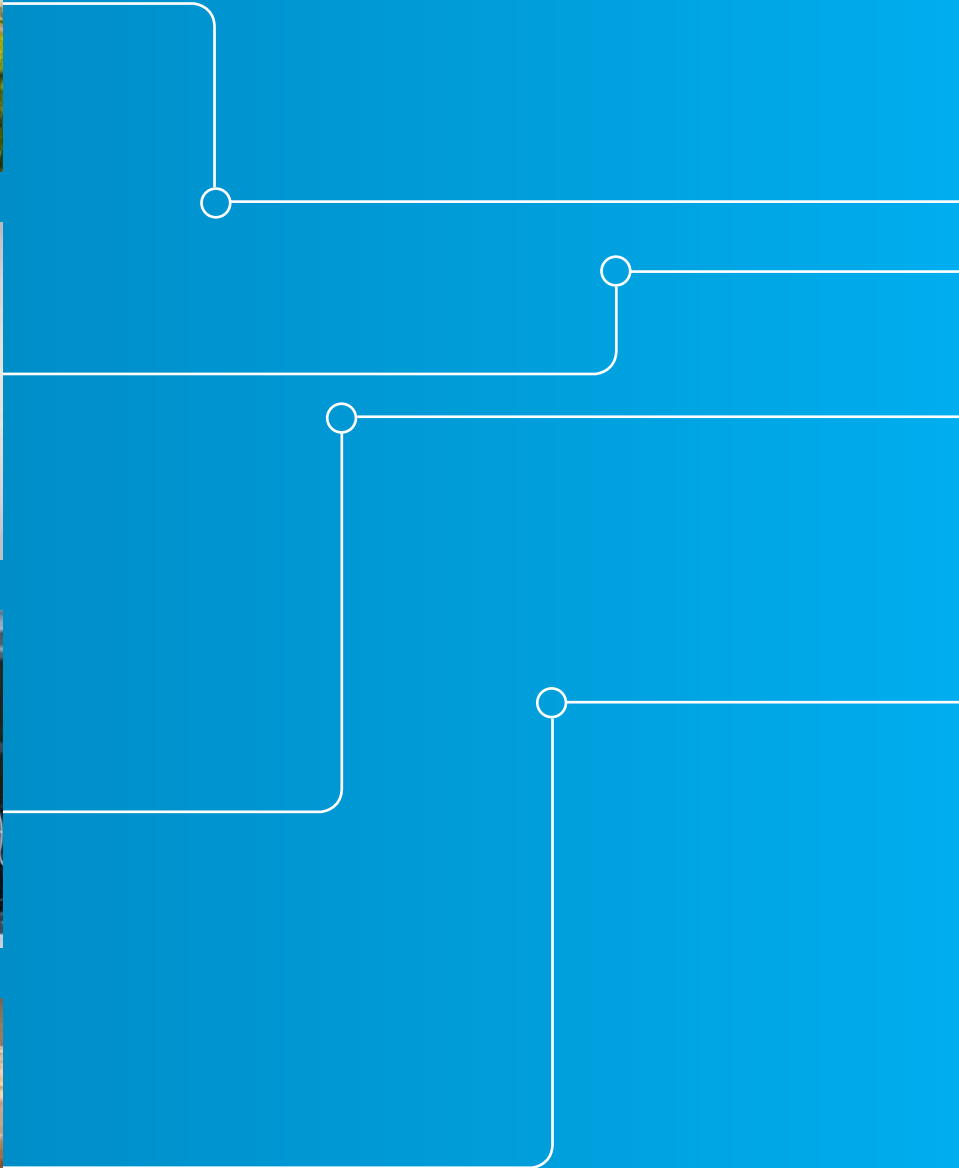


Table of Contents

| | |
|---------------------------|----------|
| Management summary | 4 |
|---------------------------|----------|

| | |
|-------------------------|----------|
| 1 – Introduction | 7 |
|-------------------------|----------|

| | |
|------------------------------|-----------|
| 2 – Results 2016-2018 | 11 |
|------------------------------|-----------|

| | |
|------------------------|----|
| 2.1 HCA Cyber Security | 11 |
|------------------------|----|

| | |
|----------------------------------|----|
| 2.2 Highlights results 2016-2018 | 11 |
|----------------------------------|----|

| | |
|--|-----------|
| 3 – Security labour market in the Netherlands | 15 |
|--|-----------|

| | |
|--------------------------------|----|
| 3.1 Definition and demarcation | 15 |
|--------------------------------|----|

| | |
|-------------------|----|
| 3.2 Labour market | 16 |
|-------------------|----|

| | |
|---------------------|----|
| 3.3 Security trends | 17 |
|---------------------|----|

| | |
|--------------------------|----|
| 3.4 Education & training | 18 |
|--------------------------|----|

| | |
|-------------------------------|----|
| 3.5 Attract and retain talent | 19 |
|-------------------------------|----|

| | |
|------------------|----|
| 3.6 Requirements | 21 |
|------------------|----|

| | |
|------------------------|-----------|
| 4 – Action plan | 23 |
|------------------------|-----------|

| | |
|----------------------------------|----|
| 4.1 Approach of the HCA Security | 23 |
|----------------------------------|----|

| | |
|--|----|
| 4.2 Track 1: Connect education and employers | 24 |
|--|----|

| | |
|--|----|
| 4.2.1 Action line 1.1: Specific educational offerings and more educators | 24 |
|--|----|

| | |
|---|----|
| 4.2.2 Action line 1.2: Better connection between education system and employers | 25 |
|---|----|

| | |
|---|----|
| 4.3 Track 2: Attracting and developing talent | 25 |
|---|----|

| | |
|---|----|
| 4.3.1 Action line 2.1: Enlarging bottom-up influx | 25 |
|---|----|

| | |
|---|----|
| 4.3.2 Action line 2.2: Enhancing competences existing personnel | 26 |
|---|----|

| | |
|--|----|
| 4.3.3 Action line 2.3: Stimulating lateral entry | 27 |
|--|----|

| | |
|---|----|
| 4.3.4 Action line 2.4: Enlarging talent pool by external influx | 28 |
|---|----|

| | |
|--------------------------------------|----|
| 4.4 Realisation and intended results | 28 |
|--------------------------------------|----|

| | |
|-------------------|-----------|
| Appendices | 30 |
|-------------------|-----------|

| | |
|--------------------------------------|----|
| Appendix 1 – Consulted organisations | 31 |
|--------------------------------------|----|

Management summary

Several studies and the daily news exemplify the importance of security and the distinct role the Netherlands has in security areas such as Cyber Security, Privacy & Ethics and Forensics. These societal challenges are growth areas for Dutch businesses. There are challenges and opportunities created by cross-over technologies such as Internet of Things (IoT), Artificial Intelligence (A.I.) and Quantum and also by other developments such as the shift from risk aversion to resilience, growing attention in the boardroom for cyberrisks, and new rules, regulations and laws. For these reasons, and the shared needs from our partners, we developed the Human Capital Agenda Security. Access to talent is a crucial prerequisite for the creation of innovative security solutions and the growth of the security sector and therefore one of the pillars of The Hague Security Delta.

This Agenda serves the Dutch security clusters' overarching goal: A Safe & Secure Society and More Economic Growth. This Agenda builds on the successful previous agenda by keeping 80% of the former focus, and to differentiate for 20% in the following way:

- Broadening the scope to security;
- The area of application is the Netherlands;
- Duration of 4 years.

The role of HSD Office is one of liaison, facilitator, organiser, communicator, driver or initiator. We can take the initiative to set up studies and courses or articulate and bring about a demand for talent. HSD Office does however not participate in execution (only if there is no-one else to take the role, such as creating this agenda and the www.securitytalent.nl platform). We do not educate groups of students or act as an employer in this field.

Building on the positive experience of the approach we took with the previous agenda, we will continue working on two tracks with underlying action lines and actions.

1. Connect education and employers (primarily focussed on organisations)

- 1.1 Specific educational offerings and more educators.
 - Additional courses and studies are developed by HSD-partners and others.
 - Partners of HSD are connected to education providers to help overcome the shortage in educators
- 1.2 Better connection between education system and employers.
 - Educators table MBO-HBO cybersecurity to organize continued learning paths
 - Train to attain hard to find talent, support for Human Resources professionals and line managers

2. Attracting and developing talent (primarily focussed on talents)

- 2.1 Enlarging bottom-up influx.
 - Attract and educate a broad group in cybersecurity with the P@CT programme
 - Develop cybersecurity consultants for SME's at vocational level with Cyberwerf
 - Create career navigator to show the perspectives between job profiles
- 2.2 Enhancing competences existing personnel.
 - Securitytalent.nl for transparency in demand for talent and supply of education
 - Share job profiles for professional development or career move
 - Limiting the need for SOC-personnel through A.I.
 - Security awareness, Cyber Security and Cyber Crime for specific groups
- 2.3 Stimulating lateral entry.
 - Security a la Carte to shape and help realise the future workforce with training
 - Unleashing broader potential by supporting retraining initiatives
- 2.4 Enlarging talent pool by external influx.
 - Attract international talents through educational programmes

The action lines and underlying actions as outlined above will be subject to further detailing, operationalization or adaptation. It is therefore a 'rolling agenda'. Through the HSD Office yearly plan, we will communicate further details, planning and new activities. The HSD Office delivers 2 FTE to activate partners, initiate or organize concrete projects and communicate results.

They realise and maintain the supporting infrastructure www.securitytalent.nl. Important asset in most of the actions is the intensive and structural cooperation between education, companies and government. The HSD-network is a strong base for this.

Some of the running programmes connected to the action lines mentioned above are:

| Programme | Goal | HSD Office role | Intended outcome |
|-----------------------------------|--|---|--|
| Security á la Carte | (Re)training, development of professionals, strengthen career pathways, broad focus on security | Organise, facilitate, communicate | 200 people educated |
| Cyberwerf | Development of cybersecurity consultants for SME's, new job profile, outflux at Vocational Level and task differentiation | Initiate, connect partners, communicate | 100 Vocational-level cybersecurity consultants |
| P@CT | Develop cybersecurity skills, create educational pathways and train the trainer | Advisor, connect partners, communicate | 20 educators trained, 350 students cyberaware and 165 cybersecurity specialists |
| Educators table | Better transfer through education levels, more and better educators, attractive education | Organise, facilitate | 10 (Hybrid) educators, 200k€ investment or savings in security education |
| Jobs of the future | Monitoring of needs and trends, function profiles for security | Initiate, execute, advisor, communicate | Annual trend analysis, 30 HR-professionals educated in security function trends |
| Securitytalent.nl platform | Transparency in employers needs and educational offerings, connection with partners for all security functions, promotion of the field. | Initiate, execute, communicate | 1.500 vacancies shared, 2.500 visits p/month, 100% growth in redirection to partners |
| (Inter)national talent | Attract talent through education: Summer Schools, International Security Master, Professional Master Cybersecurity, Entrepreneurial Skills Programme, Collaboration with Indonesia | Programme dependent: initiate, advisor, connect partners, communicate, facilitate | 80 Master-students to NL, 400 people trained for Security |



1 – Introduction

Several studies and the daily news exemplify the importance of security and the distinct role the Netherlands has in security areas such as Cyber Security, Privacy & Ethics and Forensics. These societal challenges are growth areas for Dutch businesses. There are challenges and opportunities created by cross-over technologies such as Internet of Things (IoT), Artificial Intelligence (A.I.) and Quantum and also by other developments such as the shift from risk aversion to resilience, growing attention in the boardroom, and new rules, regulations and laws (such as the General Data Protection Regulation) that change the take on security and required talents. For these reasons, and the shared need from our partners, we developed the Human Capital Agenda Security. Our underlying vision is that:

“The Netherlands has a leading international position in the field of innovative security such as cybersecurity, fully utilizes the opportunities of digitization and is resilient to advanced physical and digital threats. There is a sufficient number of qualified personnel who make this leading position, innovation and exchange of knowledge possible. The security community is attractive to work in and talent “flows” between organizations for optimum knowledge exchange. The security sector offers talent a sustainable career perspective and the quantity and quality of talents meets the demands. The sector is inclusive and diverse to meet all challenges, now and in the future. Working in the security sector is synonymous with challenge, content-driven, flexible, lifelong learning, relevance, societal engagement, entrepreneurship and initiative.”

Access to talent is a crucial prerequisite for the creation of innovative security solutions and the growth of the security sector and therefore one of the pillars of The Hague Security Delta. A rising number of security courses, studies and security related vacancies demonstrate that the innovative security domain is a fast-growing and interesting field and that there is a need for sufficient qualified personnel. In 2016, HSD Office published the ‘Human Capital Actieagenda Cyber Security 2016-2018’ to tackle the discrepancies on the Cyber Security labour market.

The chosen approach has proven fruitful and HSD Office’s role is supported by many as proven by the results shared in Chapter 2. The focus of the previous agenda was on Cyber Security in the province of Zuid-Holland. This remains a valid problem and region based on the shortages we see, but to be more efficient and serve more partners we need to expand. Several results have been achieved but the demand grows quicker than expected and some of the goals are more difficult to realise (e.g. the ‘wicked problem of shortage in educators’) or actions are still in progress due to slow change in formal education’s curriculum, rigid function structures from employers, duration of educational programmes or because the change in perception of the security domain does not translate in direct availability of talent.

This Human Capital Agenda for Security serves the Dutch security clusters' overarching goal: A Safe & Secure Society and More Economic Growth. The longer-term ambition is to reduce the number of hard to fill job openings (those that are open for more than 45 days). This Agenda builds on the successful previous agenda by keeping 80% of the former focus, and is different in the following way for 20%:

- *Broadening the scope to security.* The dynamics in the innovative security domain make it impossible to predict its shortages in the coming years with great accuracy. We do know that our scope will remain security, but whether shortages will remain most profound in technical cybersecurity or if it will move to cross-overs with forensics, Artificial Intelligence, quantum encryption or privacy remains to be seen. At the same time, we noticed in the execution of last years' HCA Cyber Security that some necessary actions are not confined to Cyber Security. Therefore, a broader scope suits our goals better and forces us to keep making explicit market-oriented choices. So, our efforts will be on cyber security for 80% and 20% on the broader security domain.
- *The area of application is the Netherlands.* There is a need and added value in taking interregional and national initiatives next to local or regional ones. The shortages are a national problem and efficiencies can be realized through cooperation between regions or nationally. Also, scaling up solutions makes them more viable and cost effective. Previous years have shown for instance modules in Forensic IT from the Leiden University of Applied Sciences are at the base of modules at the NHL Stenden University of Applied Sciences. Also, the national obligation for vocational level IT-education to address Cybersecurity in their curriculum will grow the use of these modules at the ROC Mondriaan and the talent in the province of Zuid-Holland region. This last region is home to many security employers that will benefit from this agenda and cybersecurity is one of the key economic sectors of the region¹.

- *Duration of 4 years.* We noticed that some actions take several years to result in effect. It takes 3 years before a new Master education (such as the recently started Professional Master Cybersecurity and the Master in International Security Management that starts in 2020) results in availability of talent or to get subjects in the educational curriculum, but these are necessary steps to grow the attractiveness of the domain as a whole. We increase the duration from 2.5 to 4 years.

Our vision and ambition regarding talent is bold. The Security Cluster has many active partners who help execute the HCA. Even more partners and others support the realisation of this vision. The present agenda relies on using their expertise, execution power and ambitions. It is connected with national, regional and local policies set out by Nationaal Cyber Security Centrum (NCSC) and dcypher, ECP's Human Capital Agenda for ICT, Economic Board Zuid-Holland (EBZ) Human Capital, MetropoolRegio Den Haag Roadmap Next Economy (MRDH RNE): Next Education and Economic Board Den Haag (EBDH).

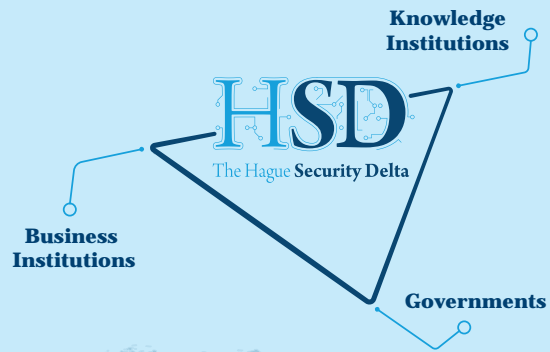
The role of HSD Office is one of liaison, facilitator, organiser, communicator, driver or initiator. We can take the initiative to set up studies and courses or articulate and bring about a demand for talent. HSD Office does not participate in execution (only if there is no-one else to take the role, such as creating this agenda and the www.securitytalent.nl platform). We do not educate groups of students or act as an employer in this field.

1 Human Capital Agenda Economic Board Zuid-Holland. EBZ, 2019.

About HSD

The Dutch security cluster 'The Hague Security Delta' (HSD) is a network of businesses, governments and knowledge institutions that work together on innovative security solutions and knowledge development. In this network, security issues are discussed and knowledge is shared on cyber security, national and urban security, protection of critical infrastructures, and forensics. The HSD partners have a common goal: a more secure world, more business activity and more jobs. The core of the security cluster is the HSD Campus, the national innovation centre for security in The Hague.

Security is a societal issue with many challenges in today's complex world. Knowledge sharing and collaboration are crucial for the realisation of the necessary and viable innovations in the field of security. Now and in the future.





2 – Results 2016-2018

2.1 HCA Cyber Security

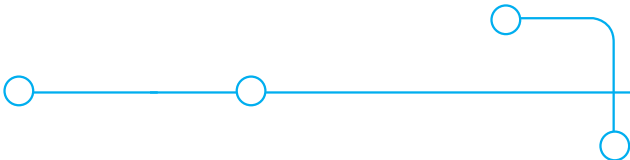
The goal of the Human Capital Actionagenda Cyber Security (HCA) 2016-2018, executed by HSD partners and others, and supported by HSD Office, was to tackle discrepancies in the cyber security education and labour market by improving the qualitative and quantitative match between 'demand' and 'supply' of cyber security personnel. There is a need for talent to realise safety and security, and economic growth of the sector. The contributing organisations have done so by executing two programme tracks. Track 1 focussed on improving the connection between education and employers (organisations oriented) by enlarging the supply of educational offerings and number of educators; and strengthening the connection between education and the needs of employers. Track 2 focussed on attracting and developing talent (talents oriented), through enlarging bottom-up influx; enhancing competences of existing personnel; stimulating lateral entry and an additional action line on growing the talent pool by external influx.

Our approach has been to grow the transparency and attractiveness of the labour market and education, for instance by articulating the specific talent needs, show role models and education & training offers on the www.securitytalent.nl platform. We took initiative and supported actions to enlarge lateral entry through retraining and sharing an inventory of job profiles. By attracting students to choose for cybersecurity related studies and specialisations and support the work on task differentiation we helped enlarge the talent pool. We also worked on the external influx, attracting specific talents from other countries as an additional action line. Organisations expand their business to the Netherlands which makes it even harder to match the Dutch talent need. By bringing together and sharing the training possibilities from partners we stimulate the enhancement of competences of existing personnel.

2.2 Highlights results 2016-2018

Several successes have been achieved, some of them as output of the HSD Office, most of them in correlation with support from HSD Office and the HSD HCA Cyber Security (see figure 1). In the period of 2016-2018 three International Cyber Security Summer Schools have been organized that educated over 170 students and young professionals. The 2018 edition resulted in at least 5 filled jobs that we know of. The Cyber Security Academy has educated three cohorts of over 50 Masters in Cybersecurity in total. The P@CT-programme created new successful educational modules, trained 15 educators, enhanced the number of guest lectures, strengthen the link between secondary education and vocational level training and cybersecurity will become a mandatory part of vocational level IT education from 2019 onward.

Through the HSD Office executed www.securitytalent.nl website 900 vacancies, 700 studies and courses, 40 job profiles and 20 role models have been shared which lead to an average of 1.800 visits per month. Several HSD-initiated studies contributed to the transparency of market demand and -development and thereby supported policymaking in this field. The shortage of cybersecurity talents has been addressed at a national level through a letter signed by several partners and follow-up dialogue with the Ministry of Education. Organised events and meetups powered by HSD Office resulted in the matchmaking of over a 100 (young) professionals per year with employers.

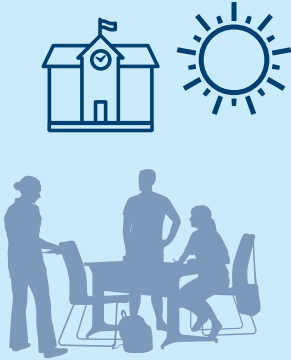


Results Human Capital Actionagenda Cyber Security 2016-2018

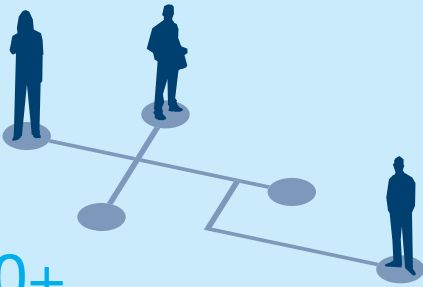


3X
Summerschool

170+
Students



250+
Matches with employers



3X
MSc Cyber
Programme

37
Professionals



6 New courses

700+ Students



16
Teachers
trained



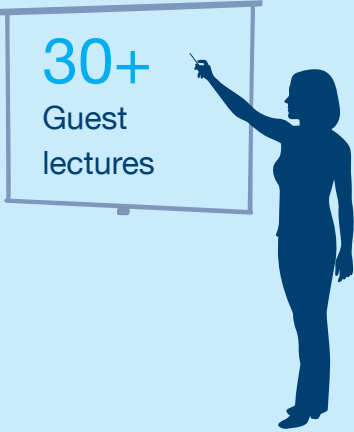
4 Labour/education
market reports



Security in MBO
IT-Curriculum



30+
Guest
lectures



Securitytalent.nl:

900+ Vacancies
700+ Studies
40+ Job profiles
1.800 Visits/month



Involved organisations

Networks, Stakeholders, Educators, Employers



Networks and stakeholders that were involved included:

ECP, dcypher, Ministry of Education, Culture and Science, Platform voor InformatieBeveiliging (PvIB), InnovationQuarter, Municipality of The Hague, Municipality of Zoetermeer, MRDH, Economic Board The Hague, Economic Board Zuid-Holland, Platform BetaTechniek/Techniekpact, VHTO, Platform Hybride Docent and the European Commission. Education and training institutions involved were: ROC Mondriaan, ROC Friese Poort, ROC of Amsterdam, The Hague University of Applied Sciences, Technical University Delft, Leiden University, University of Applied Sciences Leiden, University of Applied Sciences Amsterdam, NHL Stenden University of Applied Sciences, Security Academy, Cyber Security

Academy, Fortress, SECO-institute, SANS, ISACA, Studietoelichting voor Bedrijf en Overheid (SBO), Cisco and ITvitae amongst others. Employers that took an active role included: Siemens, KPN, Fox-IT, Dutch Police, Ministry of Defence, NATO Communications and Information Agency (NCIA), Europol, Thales, Rabobank, Deloitte, EY, CGI, Public Prosecutors Office, Hackershub, Compumatica, Strict, Certified Secure, Palo Alto, Cybersprint ... and over 40 of the most active partners on the www.securitytalent.nl platform. This organization of contributing partners is an important second-order result of the HCA Cyber Security.

Figure 1 Highlighted results and contributing partners HCA Cyber Security 2016-2018



3 – Security labour market in the Netherlands

3.1 Definition and demarcation

One of the first questions to be answered is: What belongs to the security domain? We define security rather broadly. It comprises the traditional forms of security expressed in occupations like armed forces, police officers and security guards. But it also includes more general security occupations like lawyers and judges and the corresponding educational programmes; occupations and programmes which contribute to ‘security’ at a more institutional level. A large number of ICT-occupations are related to security as well. More and more elements of these occupations and educational programmes are dedicated to security to guarantee the integrity of ICT-systems and protect against cybercrime and fraud, hence the focus of the previous agenda on cybersecurity.

Some functions are ‘mainly security related’ others are only partially dedicated to security related tasks. In developing talent and acquiring security professionals, different sectors fish in the same pond. Our focus is the safety & security sector, but where demands overlap, we embrace cooperation and joint efforts.

Therefore, we broaden our view with this agenda to different economic sectors where there is a growing or changing security need. Professor Jan van den Berg² made figure 2 to describe the scope of cybersecurity; the useful differentiation between the technical, socio-technical and governance layer in different application domains works for safety & security in a broader sense as well. This agenda covers all three layers, the focus will be different per action. We notice that physical and digital security are traditionally separate domains and education lines, but they are growing towards each other in practice.

With ‘Human Capital’ we mean the competences, knowledge, social skills and personality traits that enables people to create value. This agenda has a national scope to enhance human capital for innovative security. The level of education and training is from medium until higher level, both formal education and training. Primary and secondary education is out of scope, unless in connects strongly with our primary objectives and our role is small. HSD Office will, when relevant and opportune, connect with national and regional initiatives and encourage upscaling and conjunction.

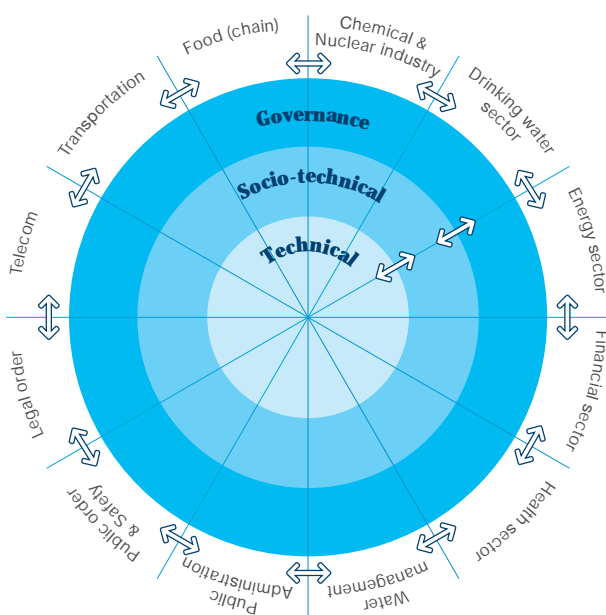


Figure 2 **Conceptualisation of Cyberspace in three layers (rings) and sub-domains (pie points)**

² Developing the Next Generation Safety & Security Courses and Programs. Jan van den Berg, 2018. Delft University of Technology, Leiden University & Cyber Security Academy The Hague.

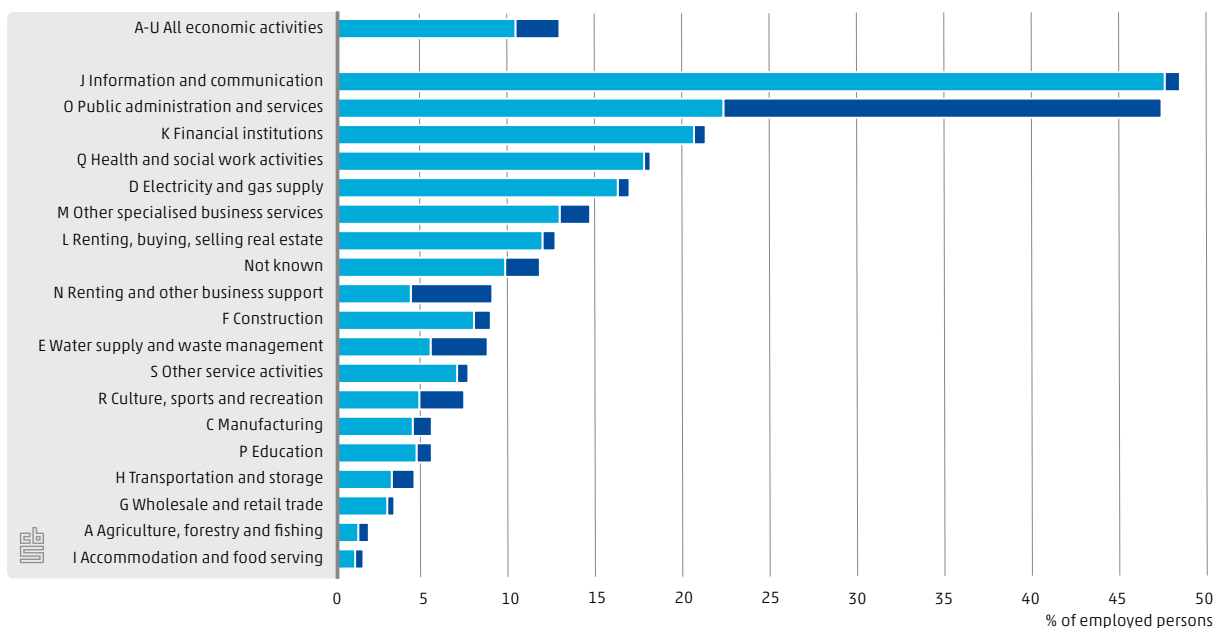
3.2 Labour market

In 2016, 12,8% of the Dutch workforce (1.078.000 people) was employed in a security related occupation³. Compared to other occupations, people with security related jobs more often have a full-time and permanent contract, are somewhat older and more often highly educated. The share of employed persons, those that are traditionally reckoned as security-workers such as firefighters, police officers and military personnel, showed a slight decrease of 0.2% between 2013-2016 (133.000 people in 2016). Non-traditional security personnel (including lawyers, judges, cyber security specialists, fraud examiners and social workers that i.e. deal with domestic violence, mentally disordered people and radicalisation) show a small increase of 0.2% between 2013-2016 (945.000 people in 2016, so this increase is over 1.850 people). This is in line with the analysis made for the HCA Cyber Security in 2016.

Almost half of security and security-related professionals are active in two big sectors (as defined by the Central Bureau of Statistics): Health & Social Work Activities (22%) and Public Administration & Services (also 22%). Relatively, the number of employed persons in a security related occupation is largest in the Information & Communication sector (which has a big impact on all sectors and includes cyber security) and Public Administration & Services (which includes police forces

and military personnel), see Figure 3. In March 2019, an analysis on the Dutch 'vacatures.nl' website (which held over 145.000 job openings at the time) showed about 28.000 contained safety & security related words (19% of the job openings contained: veiligheid, safety, security, cyber, recht, juridisch, protection, privacy, politie or defensie). Of these 28.000, 14% was open for more than 60 days what we interpret as 'hard to fill'. This is similar to all vacancies at time of measurement. For subsets found with keywords 'security', 'cyber', 'police' and 'defence' this percentage was worse, between 16 and 23% is hard to fill. For 'legal' and 'protection' jobs it is better with 12 and 7% open for more than 60 days.

From the data that stems from the HSD-website www.securitytalent.nl, vacancies related to job profiles in cybersecurity (such as CISO, ICT security specialist and ethical hacker) account for more than 75% of the job openings from HSD-partners in the period September 2016 until March 2019. HSD-partners show a strong concentration of cybersecurity openings, a sample from 'vacatures.nl' in March 2019 showed less than 10% IT-openings included the term 'security'. In the last 2.5 years, 74% of all vacancies on www.securitytalent.nl were for people with an engineering background, 23% with a security background and small numbers for social work, legal and organisation & government.



B Mining and quarrying, T Activities of households and U Extraterritorial organisations are not shown separately because of a too small number of cases.

Figure 3 **Employed persons in a security related occupation by branch of industry in 2016 (CBS/HSD, 2018)**

3 Education and labour market in the security domain. CBS/HSD, 2018.

A more detailed textual analysis of job opening descriptions in the security domain, conducted on behalf of HSD Office in 2018⁴, has found that a significant amount includes confusing and sometimes unrealistic requirements. This may discourage candidates to apply for these jobs. The analysis, based on vacancies collected through publicly accessible recruitment websites, found 91 unique job titles amongst 127 job openings. The top 5 most in demand security professionals from this analysis are (based on content of the job description, not job titles): Consultant Information Security, Security Guard, Information security officer, Cybersecurity specialist/engineer and Environment, Health and Safety (EHS) officer. Other analysis for instance by UWV⁵ shows a high demand for IT Security Specialists, Software Developers, Data Scientists, Security Installation Engineers and Technology/IT Educators.

To further detail the need for specific competences (to recruit and develop personnel) or rethink workforce development strategies (to cope with structural shortages in the labour market), more detailed analysis of specific fields of security work are performed. A method to do so is described by TNO⁶ commissioned by Dutch National Cyber Security Centre. It is exemplified for the staffing of Security Operation Centres and Computer Security Incident Response Teams. Detailed competence needs analysis combined with 'skills passports' of individuals that use a matching competence definition makes jobmatching, reskilling and labour market analysis more efficient in the future.

The demand for talent is not unique for the Netherlands. There is a worldwide shortage in cybersecurity talent for instance⁷. The availability of well-trained talent is a prerequisite for employers to set up their business in a land or region. Employers in the Netherlands also recruit foreign talent to fulfil specific demands, amongst other through the 2018 edition of the International Cyber Security Summer School, 5 young international professionals were recruited. For them as well as new

4 Wanted Security Professionals. An Analysis of Job Advertisements. HSD, 2018.

5 Moeilijk vervulbare vacatures. Landelijk overzicht van beroepen. UWV, 2018. Kansberoepen. Update najaar 2018. UWV, 2018

6 Improving Human Capital for SOCS and CSIRTS: A Collective Need for Individual Competencies. TNO, 2018.

7 Human Capital Action Agenda Cyber Security 2016-2018. HSD, 2016.



local talent the domain needs to be attractive, transparent and offer a career perspective. We see a trend of employers who start their own academy to optimize the fit between employee and employer. The biggest resource for improvement and growth are the employees that are already working in security related jobs or in jobs that will become obsolete in the near future. Training and re-training has a big impact on attaining new skills but needs a strong connection between employers and educators to fulfil employers demand.

3.3 Security trends

Security trends that may affect the Human Capital needs are diverse and subject to change. Horizonscanning is a good tool to look a bit further. Bigger reported trends⁸ include: international threats & collaborations, terrorism, separation of social groups, influencing through news and social media, diversity of cyberthreats, uncontrollable automatic systems, dependency on technology, chain dependencies and safety incidents by climatic change. In general, we see a big impact of technology on operations and threats in the security domain. This is reflected by the need for security talent with an engineering background we observed, but also the opportunity for non-technical staff to train themselves, life-long learning in the security domain (enhance competences) and all people to become more technology-aware. At the same time the topics that were traditionally more technical in nature get a broader scope including business and personal behaviour.

8 Horizonscan Nationale Veiligheid 2018. Analistennetwerk Nationale Veiligheid, 2018. ISF Threat Horizon Report 2020. Information Security Forum, 2019.



Societal and business developments such as the rise of Business Continuity- and Crisis Management, the shift from risk aversion to resilience and the enforcement of the General Data Protection Regulation (GDPR, or AVG in Dutch) impacted the take on security and required talents. All these developments give room for some specific training or education on topics such as: international security management, cybersecurity, risk management and human behaviour training (spotting, cyberawareness).

There are several technologies that will impact security and corresponding jobs as well (and some that still do such as big data, drones, IoT). Examples are Artificial Intelligence (A.I.), Quantum and Blockchain. Per example: one of the factors that might contribute to solving the shortage of cybersecurity personnel is the development of A.I. for Security Operations Centres and automated threat analysis. Steps are being made in this domain by for example studying existing frameworks regarding the competencies of SOC and CSIRTS personnel and identifying how they can be used in practice⁹. Research by ISC2¹⁰ identified that by 2022 there will be a global shortage of approximately 1.8 million cybersecurity professionals. Part of this can be solved by automating labour intensive tasks and augmenting workers with A.I.. According to Esther van Luit¹¹, 22.1% of security tasks could be fully outsourced and 37.1% of the tasks could be partially outsourced to artificial intelligence. This will however increase the need for hard to find A.I.-related talent and new job crafting in the cybersecurity domain. The technology itself poses new risks as well¹², says a study by Deloitte. A strong majority of respondents agree that AI leads to either moderate or substantial changes in job roles and skills both already (72%), and in three years (8%).

3.4 Education & training

In 2016, 60% of all employed persons in a security related occupation had a security related education. This is an increase of 6% compared to 2013. Nearly 40% of all security occupations are in engineering. In the 2016/'17 school year, 118,000 students were enrolled in a security related programme (9,8% of vocational and tertiary education). Higher education and engineering security studies showed a growth in student numbers. Of the graduates in security-related education programmes in 2013/'14, 81% found a paid job within 3 months after graduation¹³. Commercial trainers and certifiers (ISC2, ISACA, SECO-institute, Security Academy, SBO, Fox-IT, Strict, NCOI, Cisco) all report growth in followed training. Combined, private but also public partners provide hundreds of courses, conferences, incompany training and certifications and educate thousands of professionals each year. Over half of the Dutch workforce between 25 and 65 years followed a work-related non-formal education in 2016¹⁴, making them one of the most active learners in Europe. An overview of security related education- and training items from HSD-partners can be found on www.securitytalent.nl.

Security professionals generally require similar character traits in both cybersecurity and other safety & security jobs. Good communication skills, being able to work in a team as well as independently, and the ability to cope with stress are examples of traits that they all need. In cybersecurity the ability to take initiative is highly valued and not often mentioned within the other safety & security jobs. In this domain there is a demand for a neat and professional appearance, which is rarely mentioned in cybersecurity jobs. Safety & security job vacancies generally do not state many specific technical skills. The most frequently asked are knowledge of MS-office and affinity with computers. A few employers require knowledge of First Aid, ISO 14000, VCA certification requirements and management systems for EHS (KAM in Dutch) or ISO 9001. On the other hand, the total list of competences mentioned in cybersecurity job vacancies counts no less than 85 different areas of technical knowledge. A large amount of the technical competences is related to working with products from different vendors.

9 Improving Human Capital for SOCS and CSIRTS: A Collective Need for Individual Competencies. TNO, 2018.

10 2017 Global Information Security Workforce Study. ISC2, 2017.

11 Can a Robot Do My Job? A Study on the Potential of Artificial Intelligence to Take on Cybersecurity Tasks. Esther van Luit (Deloitte/CSA), 2018.

12 State of AI in the Enterprise, 2nd Edition. Deloitte, 2018.

13 Wanted Security Professionals. An Analysis of Job Advertisements. HSD, 2018.

14 Adult Education Survey. CBS, 2018.



To grow lateral entry towards the security domain, successful reskilling programme formats and traineeships can be used. Examples are the training of data protection officers by NCOI, creating different IT professionals through the Make IT Work programme and training people with some distance from the labour market in becoming penetration testers (ITvitae/Northwave),

3.5 Attract and retain talent

The variety of educations, occupations and job vacancies mentioned earlier makes security an attractive career domain with opportunities for a diverse group of people. At the same time, the plethora of possibilities makes it difficult to navigate between professions, courses and career paths. Within new fields such as cybersecurity, career paths are unclear as well as the articulation of the employers' demand through their job openings. The complexity of these descriptions may discourage candidates from other relevant professions to apply for a role in cybersecurity. Roles in traditional safety & security are more structured. But although there are overlaps between these jobs and cybersecurity jobs, the pathways between them are not indicated separating the talent pool.

Regarding the required education, there is a big difference between cybersecurity jobs and other safety & security

jobs. Jobs in cybersecurity require, in 78% of the cases, a higher education degree (HBO and WO in Dutch). In contrast, 76% of the safety & security jobs require a vocational level education in security or environmental management or do not state any requirements at all. Amongst the cybersecurity jobs, employers tend to state that the candidate should have either a degree from a university of applied sciences (HBO) or university level education (WO) background. This is remarkable, as higher vocational education institutes and universities provide different types of education. It suggests that employers do not acknowledge this difference in their job descriptions. Further confusion arises when employers use the terms Bachelor or Master. Employers do not specifically ask for any of these, instead they just state: 'Bachelor or Master' while there is at least one year of additional education between them.

Within cybersecurity, 56% of the employers ask for professional certificates (the research found 46 unique desired certificates). This is where employers demonstrate insufficient knowledge of the professional development and career paths of cybersecurity professionals. In fact, this group asks for 'one or more of the following lists of certificates:...'. This is then followed by a list, showing certificates that support different career paths.



Figure 4 **Inventory and clustering of Safety & Security occupations ranked by European Qualifications Framework, EQF 1-8 (HSD, 2018)**

As a first step to contributing to a common framework for Safety & Security professions, we have mapped a large number of professions (see figure 4 for an impression) and their associated descriptions and qualifications¹⁵. Professions that are close to each other in terms of skills and knowledge, or those that often cooperate in practice, are placed close to one another on the radar. The innovative nature of the Safety & Security domain implies that new professions and courses will evolve, and some will disappear.

The overview in figure 4 is instrumental for the further elaboration of professional profiles and to connect courses to professions and career paths. By identifying projectable career steps, professionals as well as students gain insight into how their career can evolve from their current position. It also shows how they

can switch to a different profession that at first sight may seem very different, but requires similar skills or knowledge, making the transition feasible with the right training or education. This contributes to the resilience and flexibility of the labour market.

To get more students and career-switchers (lateral entry) to choose the right development path towards an 'in demand' security function, generic factors that are important for the selection process are¹⁶: information about education and career, influencers like parents and educators, intrinsic motivators (development possibilities, interests and capacities) and external factors (well-paying job, chance of diploma). There is still a big group that quits their education in the first year and also vocational level students that are unable to finish higher education

15 Beroepenradar Safety & Security. HSD, 2018.

16 <http://www.hboaanluitingsmonitor.nl/factoren-van-invoeldd-op-het-keuzeproces/>

after a successful first year. Clarifying the scope and requirements of education (better choices), exemplifying the career possibilities (better motivation) and creating additional exit points such as commercial certificates and associate degrees (better exit profile) can all help attract and retain talent for security education and training. For the recruitment and retainment of this group, research by Young Capital ¹⁷ shows that next to salary, the purpose of the job, growth- and development opportunities are most important. These requirements are closely related to trends for all human capital, such as the need for meaning in a job, combining a diversity of jobs in functions, diverse teams and lifelong learning (Deloitte, 2019).

Safety & Security tasks are often part of other functions and the scope of security functions shifts, probably because of the growing impact of technology. This is a generic trend¹⁸, well recognised in the security domain. People in security-related functions have a higher level of education in general. They are above average of age, which calls for attracting young talent and monitoring the age structure. Well educated personnel and a higher influx of young talents are the future for the security domain.

3.6 Requirements

Based on the CBS-study in 2018, discrepancies between education and the 'needs' of the labour market in the security domain cannot be concluded. If people specialise in a required area for a security related occupation, experienced gaps may be filled. Of course, we know that this is not realistic: not all students in IT will chose to be in cybersecurity for instance and not all lawyers specialise in privacy regulations. Based on the previous paragraphs, there are several topics that need to be addressed:

The shortage of cybersecurity educators is mentioned as a 'wicked problem' in the introduction. *A lack of educators* can lead to a lack of students, which in turn lead to the first. Growing the talent pool in cybersecurity can lead to more educators in the long run, but they are needed now and not all experts are good educators. Commitment of employers and enthusiasm of experts in the field needs to be supported and additional effort has to come from schools to build long term relations with employers and support the onboarding of external personnel. Some school systems (for example vocational schools) require formal education training of instructors which takes two

years, this forms a barrier. Technology and IT educators are still in high demand (see 3.2), the growing commercial training sector second this as well (see 3.4). There is a *need for specific educational offerings* based on future looking trends. The number of cybersecurity related training and education is still growing, the big market demand for specialists supports this. International threats and growing attention for human behaviour also require training (see 3.3).

The security field is educated above average (3.2), vacancies in the area of cybersecurity, police and defence are hard to fill. Job postings are often ill defined or have complex requirements (3.4, 3.5) which makes it harder to get a good response. *A better connection between the education system and employers* can help getting more 'in demand' functions filled. Otherwise even more employers start their own academy. With shifting needs this may result in expensive training and education (3.3).

The security sector is growing (3.2), specifically the non-traditional roles with an engineering background. *To enlarge the bottom-up influx*, the jobs and their requirements need to clear including pathways between them. Young professionals need to be attracted to keep the growth (3.5). A big sector like safety & security means that there is a lot of learning potential among the workers. *Enhancing competences of existing personnel* is one of the main challenges (3.2). Not once but life-long because of the impact of rapidly progressing technology on professionals. To deal with limited availability of talent for specific functions, technology can also be used to relieve people from standardized tasks (3.3).

To grow the talent pool for functions that need it, such as CISOs, ICT security specialists and ethical hackers, *stimulating lateral entry* by offering re-training can be quicker than waiting for young talents to grow in these roles (3.2, 3.4). A final resource to cope with local shortages is to *enlarge the talent pool by external influx*. This way you can quickly enlarge the pool with talents from a specific background. Of course, this does bring other challenges such as housing and cultural fit.

¹⁷ Recruitment Guide 2019-2020. Young Capital, 2019.

¹⁸ Leading the social enterprise: Reinvent with a human focus. Deloitte Global Human Capital Trends, 2019.



4 – Action plan

4.1 Approach of the HCA Security

Building on the positive experience of the approach we took with the previous agenda; we will continue working on two tracks with underlying action lines and actions.

Track 1: Connect education and employers (primarily focussed on organisations)

- Action line 1.1. Specific educational offerings and more educators.
- Action line 1.2. Better connection between education system and employers.

Track 2 Attracting and developing talent (primarily focussed on talents)

- Action line 2.1. Enlarging bottom-up influx.
- Action line 2.2. Enhancing competences existing personnel.
- Action line 2.3. Stimulating lateral entry.
- Action line 2.4. Enlarging talent pool by external influx.

The frame of mind that we operate from is shown in the figure 5. Action lines are realised through one or more actions or activities. Examples of these actions are given in this chapter, based on those that stem from the previous agenda and are still active, progress and effect, dialogue with partners and opportunity-based we add new actions or stop those mentioned. By combining and

connecting initiatives by others or in other fields we can realise more results. As chapter 1 describes, the HSD Office role is seldom in execution (only if there is no-one else to take the role, such as with the www.securitytalent.nl platform), but works as a liaison, facilitator, organiser, communicator and sometimes sets the agenda, drives or initiates actions.

To support the mentioned tracks we will keep researching, monitoring and charting developments in the security domain and society, education and labour market. Enhancing the transparency in talent needs and educational offerings also serves both employers and talents (and policy makers as well). By analysing trends in historical data in combination with a scenario-based approach we can shorten the time between identifying a bottleneck and solution. The last three years we were focused on defining and filling functions, this period more attention should be spent on moving between functions and supporting career paths (including life-long learning). We can grow the talent pool through focused influx from profiles outside the innovative security domain and work together with other sectors where security-related functions are in demand. By this growing of scale our actions can get a bigger mass and get realized quicker or more efficiently. So, actions mentioned below may serve more than one line of action.

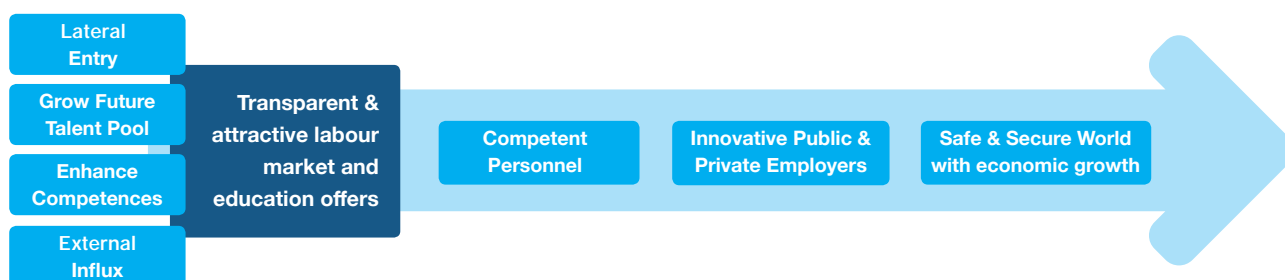


Figure 5 Talent for a safe & secure world

4.2 Track 1: Connect education and employers

4.2.1 Action line 1.1: Specific educational offerings and more educators

In specific fields such as the technical part of cybersecurity there is a shortage in educators and those that are active in this field are challenged to keep their knowledge up to date. The lack of educators forms a 'wicked problem': no educators no professionals, no professionals no future educators. The vacancies for educators are shared through the connections of HSD and partners can share their job openings on www.securitytalent.nl to reach another and broader audience. On some levels, locations and topics there is a shortage in education- and training offers for security related functions. Educational institutes and training organisations, but also employers, act on this themselves. Some initiatives are supported by HSD Office to break through initial barriers or to get them accelerate. Actions are:

- Additional courses and studies are developed by HSD-partners and others, based on current demand and security trends such as those mentioned in paragraph 3.3. Amongst other the secondary master from the Cyber Security Academy (Professional Master Cyber

Security), the P@CT-programme led by ROC Mondriaan (modules and awareness training developed and implemented on cybersecurity and safe programming, educators trained by The Hague University of Applied Sciences and Security Academy), an Associate Degree Cybersecurity by the University of Applied Sciences Amsterdam starts in 2019 and a Master in International Security is planned to start in 2020 by a consortium led by the Rotterdam School of Management with HSD Office in an advisory role. For the implementation of Cyber Security at Vocational Level IT-education that becomes mandatory in 2020, HSD Office will direct education providers to relevant partners on demand.

- Partners of HSD are connected to education providers to help overcome the shortage in educators; events are organised or supported by HSD Office to connect security professionals with education providers (matchmaking with Platform voor InformatieBeveiliging PvIB) and partners help realise train-the-trainer sessions. If generic barriers are encountered specific action can be taken, for instance by supporting 'The Hybrid Educator' that enables professionals to work both at an education provider and in the security field.





4.2.2 Action line 1.2: Better connection between education system and employers

To make security related education relevant and attractive there need to be strong ties to the field of application. This is typically done by organising work field committees that are consulted every now and then and through students that do their internship or thesis outside the school walls. These experiences do not scale well on average. Stronger ties exist when external specialists give lectures or are involved in setting up the curriculum. Also, site visits by educators and students or internships for educators can have a big impact. In fields that change quickly, like the cybersecurity and forensic field, both the curriculum and the educators need to be able to adopt these changes. At the same time employers find it hard to make their needs explicit, either because it is not their expertise or because they suffer from the same unpredictable changes in their field of work. Supporting activities are:

- Educators table MBO-HBO cybersecurity to organize continued learning paths (because of the general trend in security that there is a growing need in higher educated personnel, connection between vocational and higher education is important). The table will also be instrumental in addressing the attraction of educators (see action line 1.1) and attractiveness

of education. This should lead to 10 new (hybrid) educators and 200k€ in investments or savings in security education in the coming years.

- Train to attain hard to find talent. Sharing insights in security market developments and the job market will help Human Resources professionals and line managers to articulate their needs and rethink their requirements. For this, labour market developments are researched and shared (Jobs of the future of security) and knowledge or training sessions are supported by HSD Office. Employers could improve their vacancy description and help lessen the Human Capital problem by consistently using an agreed framework for career paths. The framework should include a cross-reference to the Dutch educational system and to professional certificates. Development of a toolkit for retaining talent, next to tools for acquiring them, is explored.

4.3 Track 2: Attracting and developing talent

4.3.1 Action line 2.1: Enlarging bottom-up influx

Based on the image of the professions, the transparency and attractiveness of education and the labour market and with unclear development perspective, not enough

students choose for this career. Although our focus is on tertiary and professional education for security, initiatives that focus on primary and secondary education either to promote the security field or develop necessary competences for instance in cybersecurity can be connected to relevant experts and knowledge for instance to develop educational material (initiative with ECP, CSR, City of The Hague). To grow the talent pool stemming from regular education, the following actions are necessary:

- Attract and educate a broad group in cybersecurity. Within the P@CT programme cybersecurity skills are developed, educational pathways are created and a train the trainer programme is enrolled. This will result in 20 trained educators, 350 students with a non-IT background will be made cyberaware and 165 cybersecurity specialists are added to the talent pool by 2020. By creating and sharing testimonials we support enhancing the image of the sector. This can also be used by national or regional programmes, such as Techniekpact¹⁹ VHTO, Platform BètaTechniek, ECP/ Dutch Digital Delta, Wetenschapsknooppunten²⁰ and HAI-Tech to attract young adults for technical studies. During matchmaking events, hundreds of future professionals are attracted, trained and connected to employers and educators (for instance during the Cyber Security Event, Cyber Security Week and site visits).
- Cyberwerf. Develop cybersecurity consultants for SME's at vocational level and learn how to work together with cybersecurity companies, Higher Education professionals and train your consulting skills. This new job profile will grow the talent pool and support task differentiation. Ambition is to train 100 of these cybersecurity consultants during this agenda.
- Create career navigator. This will show the career perspectives between job profiles in the security field and the way you can make steps between them through education and experience. It will also show employers looking for people with specific profiles. The content of this navigator stems from the Security a la Carte programme mentioned under action line 2.3 amongst others and requires keeping the job profiles up to date. Next to making the security domain more transparent and attractive, lateral entry is also supported by this action.

4.3.2 Action line 2.2: Enhancing competences existing personnel

Partly due to the increasing technology and digitization, security is a dynamic field that is developing rapidly and constantly changing. This requires professionals to keep their knowledge and skills up to date. In short, security professionals must be life-long learners. To this end, it is necessary to a) know which competences are required by employers (job profiles) and b) to make (contract) education and training easily accessible for employers and employees. Trends in for instance technology (A.I., Blockchain, Quantum) and application domains (Smart cities, subversive crime) are monitored through HSD programmes that can result in changing competence needs. The following activities are carried out for enhancing competences:

- The Securitytalent.nl platform offers transparency in demand for talent and supply of training and education for security functions. By promoting this more we will be sharing over 350 jobs & internships per year, 2.500 visits per month and a 20% growth in redirection to partners. Educational offerings and training are related to job profiles and opportunities.
- Share actual job profiles with clear demands regarding knowledge and competences. This will help employees to find the right next step in their professional development or career move.
- A new Artificial Intelligence chair is developed at the TU Delft that might help limiting the need for SOC-personnel through the use of task automation for instance in incident handling or threat analysis. TNO is also working on this topic. HSD Office supports this through development of a programme (not part of this HCA).
- Existing personnel needs to be trained in security awareness and given support to act on or prevent risks. For specialists in Cyber Security and Cyber Crime for the Public Prosecutors Office, HSD Office supports by matching needs to partners to develop a training programme. CSA already trains diplomats from the Ministry of Foreign Affairs in cybersecurity, this can be extended to the aforementioned Public Prosecutors Office and others. TNO, Interpol and the SECO-Institute develop Dark Web Trainings for security professionals. Modular and part-time

19 <http://www.techniekpact.nl/>

20 Wetenschap & Technologie in het basisonderwijs, <http://www.wetenschapsknooppunten.nl/>



education by schools' support life-long learning and can lead to a higher level of graduation, experiments²¹ are conducted.

4.3.3 Action line 2.3: Stimulating lateral entry

In the current market there is a shortage of IT- and cybersecurity talent. We need to find 'hidden treasures' to grow the security pool. For instance, talents with an IT background not working in the security sector might be developed through training and certification to become an Information Analyst, Information Security Officer or Cybersecurity specialist. Therefore, we need to identify these individuals or special groups that can be retrained within a year and start working as pentester for instance. We will do this by:

- Security a la Carte helps shaping and realising the future workforce for the security domain together with employers. Next step is defining and testing the routes for (re)training and upskilling, identifying

and developing educational offers to realise growth, and supporting students, professionals and employers in taking their next step. There are currently 6 educational partners supporting this programme that should result in 200 people re-educated and supported in their transition to a security related job. By scanning for soon-to-be obsolete functions or diminishing demand, both within the security domain and in other domains, hidden treasures are uncovered and can be directed to educational programmes or initiatives.

- Unleashing broader potential. Initiatives for retraining such as Make-IT-Work and IT-Vitae can be supported by HSD Office by sharing knowledge and network. In addition, the possibility, relevance and feasibility of a Summer School Re-school Cybersecurity for mid-career professionals is investigated. Active contributions to media, events and HSD-office resources supports attracting other talents.

²¹ Experimenten om deeltijdonderwijs flexibeler te maken 2016-2022, <https://www.rijksoverheid.nl/onderwerpen/hoger-onderwijs/experimenten-om-deeltijdonderwijs-flexibeler-te-maken>

4.3.4 Action line 2.4: Enlarging talent pool by external influx

To enlarge the talent pool, we started working on attracting specific talents from other countries as an additional action line. Companies and international organisations expand their business to the Netherlands which makes it even harder to match the talent need.

- Attract international talents amongst other through internationally oriented Summer Schools initiated by HSD Office, communicate Dutch talent need in English by HSD Office and set up collaboration with other countries such as Indonesia to train and intern at employers in the Netherlands (HSD Office communicates). Also create visibility of the Dutch security sector in expat-communities. Through educational offerings like Summer Schools (with several partners including NCIA, Europol and EIT Digital), International Security Master by Rotterdam School of Management, Professional Master Cybersecurity by the CSA, Entrepreneurial Skills Programme with 4TU and a cooperation with Indonesian government and universities, partners will be able to train 400 students in cybersecurity and get 80 Master-students to the Netherlands.

4.4 Realisation and intended results

This Human Capital Agenda for Security is the framework of activities for the coming years regarding access to talent for HSD Office. The action lines and underlying actions are outlined but will be subject to further detailing, operationalization or adaptation. It is therefore a 'rolling agenda'. Through the HSD Office yearly plan, 2019 edition is already published, we will communicate further details, planning and new activities. The HSD Office dedicates 2 FTE to activate partners, initiate or organize concrete projects and communicate results. They realise and maintain the supporting infrastructure www.securitytalent.nl. Important asset in most of the actions is the intensive and structural cooperation between education, companies and government. The HSD-network is a strong base for this.

Some of the already running programmes connected to the action lines mentioned above are summed up in table 1. The goals per programme and their intended result are also mentioned to exemplify the type of actions taken and intended outcomes by 2022.

| Programme | Goal | HSD Office role | Intended outcome |
|-----------------------------------|--|---|--|
| Security á la Carte | (Re)training, development of professionals, strengthen career pathways, broad focus on security | Organise, facilitate, communicate | 200 people educated |
| Cyberwerf | Development of cybersecurity consultants for SME's, new job profile, outflux at Vocational Level and task differentiation | Initiate, connect partners, communicate | 100 Vocational-level cybersecurity consultants |
| P@CT | Develop cybersecurity skills, create educational pathways and train the trainer | Advisor, connect partners, communicate | 20 educators trained, 350 students cyberaware and 165 cybersecurity specialists |
| Educators table | Better transfer through education levels, more and better educators, attractive education | Organise, facilitate | 10 (Hybrid) educators, 200k€ investment or savings in security education |
| Jobs of the future | Monitoring of needs and trends, function profiles for security | Initiate, execute, advisor, communicate | Annual trend analysis, 30 HR-professionals educated in security function trends |
| Securitytalent.nl platform | Transparency in employers needs and educational offerings, connection with partners for all security functions, promotion of the field. | Initiate, execute, communicate | 1.500 vacancies shared, 2.500 visits p/month, 100% growth in redirection to partners |
| (Inter)national talent | Attract talent through education: Summer Schools, International Security Master, Professional Master Cybersecurity, Entrepreneurial Skills Programme, Collaboration with Indonesia | Programme dependent: initiate, advisor, connect partners, communicate, facilitate | 80 Master-students to NL, 400 people trained for Security |

Table 1 Active HSD Human Capital programmes

For some of the described activities there is already project funding, subsidies, revenue streams and/or committed partnership available or foreseen (such as P@CT, Cyberwerf, Security a la Carte, Summer School and Master programmes), others are funded by the limited resources of the HSD-Office together with 'in kind' execution power of partners. Out of pocket costs are foreseen to create material and perform research, maintain and further develop www.securitytalent.nl and the costs associated with the logistics of meetings and events. The advancement and focus area of certain actions depend on the acquisition of funds and support by partners.

The role of HSD Office is one of liaison, facilitator, organiser, communicator, driver or initiator. HSD Office participates in execution only if there is no-one else to take the role, such as creating this agenda and the www.securitytalent.nl platform. We welcome partnerships that contribute to common goals mentioned in this agenda.

Appendices



Appendix 1 – **Consulted organisations**

HSD has worked and talked with many organisations that thereby delivered valuable input for the content of the Human Capital Agenda Security. In particular the work and inputs of the following organisations have supported the drafting of this document (in alphabetical order):

- Amsterdam University of Applied Sciences/Make IT Work
- CGI
- Cisco
- City of The Hague
- City of Zoetermeer
- Cyber Security Academy
- Cyber Security Council
- Dcypher
- Deloitte
- Economic Board Den Haag
- Economic Board Zuid-Holland
- ECP/Dutch Digital Delta
- EIT Digital
- Expertisecentrum Hybride Docent
- EY
- HSD Advisory Board
- INIT-Group Foundation
- International Community Platform
- ITvitae
- KIVI Engineering Society
- Leiden University
- Leiden University of Applied Sciences
- Metropool Regio Den Haag
- NCOI/Computrain
- NCSC-NL
- NHL Stenden University of Applied Sciences
- Platform for Information Security (PvIB)
- Province Zuid-Holland
- Public Prosecutors Office
- ROC Mondriaan
- ROC van Amsterdam
- RSM/Erasmus University
- Saxion University of Applied Sciences
- SBO/Euroforum
- Security Academy
- Security Field Lab
- Statistics Netherlands (CBS)
- The Hague University of Applied Sciences
- TNO
- TU Delft
- Van Aetsveld
- and all active HSD-partners on securitytalent.nl

Human Capital Agenda Security 2019-2022 @2019,
The Hague Security Delta

A publication from

The Hague Security Delta (HSD)
Wilhelmina van Pruijsenweg 104
2595 AN Den Haag
T + 31 (0)70 204 5180
Info@thehaguesecuritydelta.com
www.thehaguesecuritydelta.com
🐦 @HSD_NL

Authors

Mark Ruijsendaal & Rik Schiffelers

Reviewer(s)

HSD Office Management Team

Design

Studio Maartje de Sonnaville by the design of
Studio Koelewijn Brügenwirth

Print

Drukkerij Edauw + Johannissen

This study was commissioned by the Hague Security Delta (HSD). HSD does not guarantee the accuracy of the data included in this study. Neither HSD nor any person acting on behalf of HSD may be held responsible for the use which may be made of the information contained therein.

Together we Secure the Future

www.thehaguesecuritydelta.com

